Grupos lineares livres e o Paradoxo de Hausdorff-Banach-Tarski

Susan Wouters

Março de 2006

"Grupos Lineares Livres e o Paradoxo de Hausdorff-Banach-Tarski"

Susan Wouters

Dissertação submetida ao corpo docente do Instituto de Matemática da Universidade Federal do Rio de Janeiro como parte dos requisitos necessários à obtenção do grau de Mestre em Ciências.

Área de concentração: Matemática Pura.

Aprovada por:

Adilson Gonçalves (UFRJ-presidente)

Guilherme Augusto De La Rocque Leal (UFRJ)

Manoel José Machado S. Lemos (UFPE)

Luciane Quoos Conte (UFRJ).

Rio de Janeiro

Abril de 2006

Resumo

O objetivo principal deste trabalho é provar o famoso paradoxo de Hausdorff-Banach-Tarski, cuja solução, dada por Hausdorff em 1914, se baseia na construção de um subgrupo livre F de $SO(3, \mathbb{R})$ gerado por duas especiais rotações no espaço real 3-dimensional.

Abstract

The main goal of this text is to prove the famous Hausdorff-Banach-Tarski paradox, which solution, given by Hausdorff in 1914, is based on the construction of a free subgroup F of $SO(3, \mathbb{R})$ generated by two special rotations in the real 3-dimensional space.

Agradecimentos

Ao meu orientador, professor Adilson Gonçalves, pela atenção, dedicação e principalmente sensibilidade que sempre teve para entender e atender aos meus questionamentos. Quero demonstrar aqui minha enorme satisfação em tê-lo como orientador.

Ao professor Guilherme Leal pelas sugestões, grande incentivo e disponibilidade em ajudar.

A todos os colegas, em especial aos colegas e amigos Andréa Luiza Martinho, André Pereira, André Valente, Leandro Tomaz de Araujo, Marcelo Tavares Ramos Luiz e Régis Castijos que tornaram esses dois anos mais fáceis e agradáveis; obrigada pelas conversas, paciência, companheirismo e verdadeira amizade.

Ao meu amigo e companheiro, Tiago Gobbi, pelo apoio e carinho dedicados nesses últimos meses.

À minha maravilhosa família que sempre esteve, mesmo de longe, me apoiando com palavras e demonstrações de carinho; em especial à minha mãe e à minha irmã Marta que se fizeram muito presentes em todos os momentos.

Ao CNPq pela bolsa de estudo recebida, tornando possível o desenvolvimento deste trabalho.

Enfim, gostaria de agradecer a todas as pessoas que direta ou indiretamente

contribuíram na elaboração dessa dissertação e foram de fundamental importância durante todo o mestrado.

Sumário

Introdução:

A teoria que aborda, de forma mais sistemática, os subgrupos dos grupos $GL(n, K)$ sobre um corpo K, os chamados grupos lineares, aparece na segunda metade do Sec. XIX, com C. Jordan estudando grupos lineares solúveis (1870) e Felix Klein, com seu famoso"Erlangen Programme"(1872). Nessa dissertação, essencialmente, vamos estudar métodos de construção e importantes exemplos de grupos lineares livres(não-abelianos), inicialmente motivados pelo famoso paradoxo de Hausdoff-Banach-Tarski, cuja solução, dada por Hausdorff em 1914, se baseia em uma construção de um subgrupo livre F de $SO(3, \mathbb{R})$ gerado por duas especiais rotações no espaço real 3-dimensional. A demonstração envolve o axioma da escolha, na escolha de uma transversal, na ação livre de F sobre a esfera bidimensional no espaço real 3-dimensional.

Teorema(Hausdorff, 1914): "Não existe uma medida finitamente aditiva, definida em todos os subconjuntos da esfera bidimensional do espaço 3-dimensional real, que seja invariante pelo grupo de rotações $SO(3, \mathbb{R})$".

Um interessante critério geométrico, de Felix Klein(conhecido como Lema do Ping-Pong), e alguns critérios similares são utilizados na construção de subgrupos lineares livres de $GL(n, \mathbb{C})$, que serão livres, em determinadas regiões do plano $\mathbb{C}$, dependendo do módulo de um parâmetro complexo. O tema é muito abrangente e tem sido estudado por importantes matemáticos. Um dos resultados mais destacados foi dado em resposta a uma conjectura de Bass e Serre, no contexto de grupos lineares livres.

Teorema(J. Tits, 1972): "Um grupo linear , em característica zero, que não contém um subgrupo solúvel de índice finito, contém um subgrupo livre".

No capítulo 1 apresentamos resultados preliminares que serão utilizados nos capítulos seguintes, incluindo os seguintes tópicos: Medidas Finitamente Aditivas, Ação de Grupos, Grupos Topológicos e Transformações de Möbius.

No capítulo 2 abordamos ações topológicas, relacionando os conceitos de grupos discretos e grupos descontínuos. Nesse capítulo provamos a equivalência desses conceitos para subgrupos do grupo $\mathcal{M}$ de Möbius agindo no espaço hiperbólico 3-dimensional.

No capítulo 3 apresentamos a construção de grupos livres e produtos livres, destacando na Proposição 3.11, o critério de F. Klein, para a construção de produtos livres e grupos livres. Incluímos nesse capítulo exemplos de grupos livres de matrizes 2x2; subgrupos livres discretos do subgrupo modular; os grupos livres de Schottky; a discussão, a menos de um parâmetro complexo, se alguns grupos de matrizes 2x2, complexas, em dois geradores, são ou não livres e no exemplo 3.19, o Grupo de Hausdorff livre, gerado por duas rotações no espaço real 3-dimensional, finalizando com o teorema 3.21, onde demonstramos o famoso Paradoxo de Hausdorff-Banach-Tarski, que foi a motivação inicial para a elaboração dessa dissertação de Mestrado.

Gostaria ainda de mencionar que alguns trabalhos recentes em Anéis de Grupos linhas de destaque em Álgebra no IMUFRJ e no IMEUSP, abordam o estudo de subgrupos livres no grupo de unidades desses anéis.

Capítulo 1

Preliminares

1.1 Medidas Finitamente Aditivas

Definição 1.1. *Seja* X *um conjunto qualquer,* $S \subset P(X)$. S *é um* ***semi-anel****(de* X*) se:*

(i) $S \neq \emptyset$,

(ii) $A, B \in S \Rightarrow A \cap B \in S$,

(iii) $A, B \in S \Rightarrow A \setminus B$ *pode ser escrito como:*

$$A \setminus B = \sum_{i=1}^{n} C_i, \quad C_i \in S,$$

onde $\setminus$ *denota a diferença de conjuntos e* $\sum$ *designa a união de conjuntos disjuntos.*

Observação 1.2. *A definição acima implica que* $\emptyset \in S$*.De fato,*

$$S \neq \emptyset \Rightarrow \exists\, A \in S \Rightarrow \text{ existem } C_i \in S \text{ tais que } A \setminus A = \emptyset = \sum_{i=1}^{n} C_i,$$

o que implica que todos os C_i*'s são vazios.Como* $C_i \in S$*, então* $\emptyset \in S$*.*

Exemplo 1.3. *: $X = \mathbb{R}$, $S \subset P(\mathbb{R})$; $S = \{I \subset \mathbb{R} : I$ intervalo limitado $\}$.*

S constitui um semi-anel.

Observação 1.4. *A Definição 1.1 é equivalente a:*

Definição 1.5. *$S \subset P(X)$ é um **semi-anel** de um conjunto não-vazio X se:*
(i') $\emptyset \in S$,
(ii') $A, B \in S \Rightarrow A \cap B \in S$,
(iii') $B_0, B \in S,\ B_0 \subset B \Rightarrow$ existem $C_i \in S$ tais que $B \setminus B_0$ pode ser escrito como:

$$B \setminus B_o = \sum_{i=1}^{n} C_i, \quad C_i \in S.$$

De fato, para vermos que são equivalentes,basta observarmos que se $A, B \in S$, então $A \setminus B = \{x \in A \text{ e } x \notin B\} = A \setminus (A \cap B)$. Como $A \cap B \in S$ e $A \cap B \subset A$, temos por (iii') que existem $C_i \in S$ tais que:

$$A \setminus B = A \setminus (A \cap B) = \sum_{i=1}^{n} C_i.$$

Proposição 1.6. *(Produto cartesiano de semi-aneis): Se X', X'' são conjuntos quaisquer e S' e S'' semi-aneis de X' e X'' respectivamente, então:*

$$\hat{S} = \{A' \times A''; A' \in S', A'' \in S''\} \text{ é um semi-anel de } \hat{X} = X' \times X''$$

Demonstração. (i) $\emptyset \times \emptyset = \emptyset \Rightarrow \emptyset \in \hat{S}$,
(ii) Sejam $A' \times A'' \in \hat{S}$ e $B' \times B'' \in \hat{S}$, com $A', B' \in S'$ e $A'', B'' \in S''$. $(A' \times A'') \cap (B' \times B'') = (A' \cap B') \times (A'' \cap B'')$. Como $(A' \cap B') \in S'$ e $(A'' \cap B'') \in S''$, temos $(A' \times A'') \cap (B' \times B'') \in \hat{S}$,
(iii)Se $A'_0 \times A''_0, A' \times A'' \in \hat{S}$, com $A'_0 \times A''_0 \subset A' \times A''$, então existem $C_i \in \hat{S}$ tais que $A' \times A'' \setminus A'_0 \times A''_0 = \sum_{i=1}^{n},\ C_i \in \hat{S}$. Como S' e S'' são semi-anéis,

temos: $A' \setminus A'_0 = \sum_{i=1}^{n} A'_i$, $A'_i \in S'$, $\forall 1 \leq i \leq n$ e $A'' \setminus A''_0 = \sum_{j=1}^{m} A''_j$, $A''_j \in S''$, $\forall 1 \leq j \leq m$. Daí,

$A' \times A'' \setminus A'_0 \times A''_0 = \sum_{(i,j)\neq(o,o)} A'_i \times A''_j$, basta notar que $A'_0 \subset A'$ e $A''_0 \subset A''$.

Logo,

$A' = A'_0 + \sum_{i=1}^{n} A'_i = \sum_{i=0}^{n} A'_i$

$A'' = A''_0 + \sum_{j=1}^{m} A''_j = \sum_{j=0}^{m} A''_i$

Portanto, $A' \times A'' = \sum_{i=0}^{n} \sum_{j=0}^{m} (A'_i \times A''_j) = \sum_{i,j} A'_i \times A''_j$. $\square$

Definição 1.7. *(Anel de X) : Uma coleção U de subconjuntos de um conjunto X é um* ***anel de conjuntos*** *se:*

(i) $\emptyset \in U$

(ii) Se $A_1, A_2 \in U \Rightarrow A_1 \cup A_2,\ A_1 \cap A_2^c,\ A_1 \cap A_2 \in U$

Note que se U é anel, então U é semi-anel.

Definição 1.8. *Chamamos de* ***medida*** *a qualquer função $\mu : S \to \mathbb{R}$ (ou na reta estendida $\mathbb{R} \cup \{\infty\}$) de um semi-anel S tal que:*

(i) $\mu(\emptyset) = 0$ *e*

(ii) μ seja finitamente aditiva, isto é, sempre que tenhamos $S_j \in S, 1 \leq j \leq n$ disjuntos tais que $\sum_{j=1}^{n} S_j$ também pertença a S, então:

$$\mu\left(\sum_{j=1}^{n} S_j\right) = \sum_{j=1}^{n} \mu(S_j)$$

A medida μ é dita **σ-aditiva** se n acima puder ser ∞ e , se tivermos $\mu : S \to [0, \infty]$, μ é dita **medida positiva**.

Lema 1.9. *Seja U um anel e $\mu : U \to [0, \infty)$ uma medida (positiva, finitamente aditiva). Então:*
(i) $A \subset B \Rightarrow \mu(A) \leq \mu(B)$, $\forall\ A,\ B \in U$
(ii) $\mu\left(U_{i=1}^{n} A_i\right) \leq \sum_{i=1}^{n} \mu(A_i)$, $\forall A_1, ..., A_n \in U$.

Demonstração. (i) Como $A \subset B$, temos $B = A + (B \setminus A) \Rightarrow \mu(B) = \mu(A) + \mu(B \setminus A) \Rightarrow \mu(B) \geq \mu(A)$(pois, μ é medida positiva).
(ii) Para $n = 1$ é trivial. Para $n = 2$, temos:
$A_1 \cup A_2 = A_1 + (A_2 \setminus A_1) \Rightarrow \mu(A_1 \cup A_2) = \mu(A_1) + \mu(A_2 \setminus A_1) \leq \mu(A_1) + \mu(A_2)$(pelo item (i)).
Procedemos por indução:
Suponha válido para n. Para $n + 1$, temos:
$\mu(A_1 \cup ... \cup A_n \cup A_{n+1}) \leq$ (devido ao caso $n = 2$)
$\mu(A_1 \cup ... \cup A_n) + \mu(A_{n+1}) \leq \sum_{i=1}^{n} \mu(A_i) + \mu(A_{n+1}) = \sum_{i=1}^{n+1} \mu(A_i)$.

$\square$

Proposição 1.10. *Seja S um semi-anel e $U(S)=$ **U** a coleção das uniões finitas disjuntas de elementos de S. Então:*
(i) **U** *é anel,*
(ii) Toda medida μ em S se estende de maneira única para uma medida $\overline{\mu}$ em **U**, *definida por:*

$$\overline{\mu}\left(\sum_{j=1}^{m} S_j\right) = \sum_{j=1}^{m} \mu(S_j),\ \textit{se}\ S_j \in S\ \textit{e}\ m < \infty$$

(iii) Se uma medida μ em S é σ-aditiva, sua extenção $\overline{\mu}$ a **U** *também é σ-aditiva.*

Proposição 1.11. *Sejam S um semi-anel e $\mu : S \to [0, \infty)$ uma medida(σ-aditiva). Seja $A_n \in S$, $\forall n \in \mathbb{N}$ e seja $A \in S$.*
(a) Se $A_n \subset A_{n+1}$, $\forall n \geq 1$, $n \in \mathbb{N}$ e $A = \bigcup_{n=1}^{\infty} A_n$, então:

$$\mu(A_n) \nearrow \mu(A), \text{ o que significa que } \mu(A_1) \leq \mu(A_2) \leq ... \text{ e } \mu(A_n) \to \mu(A),$$

quando $n \to \infty$.
(b) Se $A_n \supset A_{n+1}$, $\forall n \geq 1, n \in \mathbb{N}$ e $A = \bigcap_{n=1}^{\infty} A_n$, então:

$$\mu(A_n) \searrow \mu(A), \text{ o que significa que } : \mu(A_1) \geq \mu(A_2) \geq ... \text{ e } \mu(A_n) \to \mu(A),$$

quando $n \to \infty$.

Extensão de medidas :

Como estamos trabalhando com medidas σ-aditivas, é natural estendermos medidas definidas em coleções que, quando muito, eram fechadas para uniões, interseções e diferenças para coleções (em geral) maiores, fechadas para união, interseção enumeráveis infinitas de seus elementos; além de passagem ao complemento.

Definição 1.12. *Seja X um conjunto e $A \subset P(X)$, $A \neq \emptyset$.*
*(a) A é uma **álgebra** $\Leftrightarrow$ A é um anel e $X \in A$ ($\Leftrightarrow$ A é fechada para uniões finitas,interseções finitas e passagem ao complemento),*
*(b) A é σ-**álgebra** se as uniões e interseções acima puderem ser enumeráveis.*

Observação 1.13. *A interseção de σ-álgebras de (partes de) X é uma σ-álgebra(o mesmo se aplica a interseção de anéis de X, que é anel de X e de álgebras de X, que é álgebra de X). Qualquer que seja o conjunto X, $P(X)$ é uma σ-álgebra de partes de X; portanto, o conjunto das σ-álgebras de X é diferente do vazio.*

Definição 1.14. *Os elementos de uma σ-álgebra A são chamados de* ***conjuntos* $\mathbf{A}$*-mensuráveis*** *ou simplesmente* ***mensuráveis****,quando a σ-álgebra A estiver subentendida no contexto.*

Definição 1.15. *Dado $T \subset P(X)$, a σ-**álgebra** $\mathbf{A}$ **gerada por** $\mathbf{T}$ é simplesmente a interseção de todas as σ-álgebras de X contendo T.*

Definição 1.16. *Um* ***espaço de medida*** *é um terno (X,A,μ), onde X é um conjunto, A é σ-álgebra de partes de X e μ é uma medida σ-aditiva, positiva definida em A.*

Definição 1.17. *Um* ***espaço de medida*** *(X,A,μ) é* ***completo*** *se $A \in A$, $B \subset A$, $\mu(A)$=o implicar que $B \in A$.*

Neste caso, $\mu(B)=0$, já que $0 \leq \mu(B) \leq \mu(A)=0$.

1.2 Ação de Grupos

Definição 1.18. *Seja Ω um conjunto qualquer não-vazio. Uma* ***permutação*** *de Ω é uma aplicação bijetora de Ω em Ω.*

Por exemplo, uma reflexão na esfera é uma permutação de $\hat{\mathbb{R}}^n = \mathbb{R}^n \cup \{\infty\}$

Definição 1.19. *Dizemos que o grupo* $\mathbf{G}$ ***age sobre o conjunto*** $\mathbf{\Omega} \neq \emptyset$ *se para todo $g \in G$, temos definida uma permutação $\sigma_g : \Omega \to \Omega$ de G, tal que:*
(i) $\sigma_e = Id_\Omega : \Omega \to \Omega$, onde e=identidade de G;
(ii) Se $g, h \in G$, $\sigma_g : \Omega \to \Omega$ e $\sigma_h : \Omega \to \Omega$ são permutações de g e h, respectivamente, então $\sigma_{gh} = \sigma_g \sigma_h$

Notação: $\sigma_g : \Omega \to \Omega$, $\sigma_g(\alpha) = \alpha^g$.

Definição 1.20. *Sejam Ω um conjunto não-vazio e $\alpha \in \Omega$. Se G é qualquer grupo de permutação de Ω, então o* ***estabilizador*** *(em G) de α é o subgrupo de G definido por:*

$$G_\alpha = \{g \in G : \alpha^g = \alpha\}.$$

Definição 1.21. *A* ***órbita****(ou G-órbita) de α é o subconjunto de Ω definido por:*

$$\alpha^G = \{\alpha^g \in \Omega : g \in G\}.$$

Observe que existe uma correspondência bijetiva natural entre o conjunto das classes G/G_α e a órbita α^G. Se g e h estão em G, então $\alpha^h = \alpha^g \Leftrightarrow hG_\alpha = gG_\alpha$ e isto mostra que a aplicação $hG_\alpha \to \alpha^h$ está bem definida e é bijetora. Isto claramente aplica G/G_α em α^G e esta é a correspondência requerida.

1.3 Grupos topológicos

Definição 1.22. *Uma topologia é uma família τ de conjuntos os quais satisfazem as duas condições: a interseção de quaisquer dois membros de τ é um membro de τ e a união de membros de cada subfamília de τ é um membro de τ. O conjunto $X = \bigcup\{U : U \in \tau\}$ é necessariamente um membro de τ porquê τ é uma subfamília dela mesma, e todo membro de τ é um subconjunto de X. O conjunto X é chamado o espaço da topologia τ e τ é a topologia de X. O par (X, τ) é um* ***espaço topológico****.*

Chamamos de **espaço topológico discreto** ao espaço no qual todo subconjunto é aberto.

Definição 1.23. *Um* ***grupo topológico*** *é um conjunto G com duas estruturas:*

(i) G é um grupo,

(ii) G é um espaço topológico, tal que as duas estruturas são compatíveis, isto é, a aplicação multiplicação $(x, y) \to xy$ (de $G \times G$ em G) e a aplicação inversão $x \to x^{-1}$ (de G em G) são contínuas. Nesta definição, o conjunto $G \times G$ representa o produto topológico.

Dois grupos topológicos são isomorfos quando existe uma bijeção entre eles, a qual é um isomorfismo de grupos e homeomorfismo de grupo topológico: esta é a identificação natural de grupos topológicos.

Exemplos:

1) $\mathbb{R}$ considerado como um grupo aditivo com a topologia usual;

2) $\mathbb{R}^*$, o conjunto de todos os números reais não-nulos, considerado como um grupo com respeito a topologia usual;

3) O grupo linear geral $GL(n, \mathbb{R})$(o conjunto de todas as matrizes $n \times n$ não-singulares(det $\neq 0$) com coeficientes em $\mathbb{R}$) é um grupo com respeito a multiplicação e tem a topologia induzida pela inclusão em $\mathbb{R}^{n^2}$. Operações de multiplicação e inversão são dadas por n^2 funções racionais e $2n^2$ e n^2 variáveis reais, respectivamente, e são contínuas. Assim, $GL_n(\mathbb{R})$ é um grupo topológico.

4) $GL(n, \mathbb{C})$ é um grupo topológico de modo similar.

1.4 Transformações de Möbius e a extensão de Poincaré

Definição 1.24. *Um **quaternion** é uma matriz complexa da forma:*

$$q = \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$$

O conjunto dos quaternions é denotado por $\mathbb{H}$. Como a adição e a multiplicação dos quaternions é como para matrizes, temos:

(i) $(\mathbb{H}, +)$ é grupo abeliano;

(ii) $(\mathbb{H}^*, .)$ é grupo não-abeliano;

(iii) $\mathbb{H}$ é um espaço vetorial real de dimensão 4, com bases:

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Como a multiplicação de matrizes é distributiva, a multiplicação dos quaternions é determinada pelo produto dos quatro elementos: $\mathbf{1}, \mathbf{i}, \mathbf{j}$ e $\mathbf{k}$. De fato, estes elementos geram um grupo multiplicativo de ordem 8 e:

$$\mathbf{i^2} = \mathbf{j^2} = \mathbf{k^2} = \mathbf{-1}$$

$$\mathbf{ij} = \mathbf{k},\ \mathbf{jk} = \mathbf{i},\ \mathbf{ki} = \mathbf{j}$$

$$\mathbf{ji} = -\mathbf{k},\ \mathbf{kj} = -\mathbf{i}, \mathbf{ik} = -\mathbf{j}$$

Os quaternios contém uma cópia de $\mathbb{C}$ pela aplicação:

$$x + iy \to x\mathbf{1} + y\mathbf{i}$$

de $\mathbb{C}$ em $\mathbb{H}$. Escrevendo $x + yi = z$ e $u + iv = w$, temos:

$$q = (x\mathbf{1} + y\mathbf{i}) + (u\mathbf{j} + v\mathbf{k}) = (x\mathbf{1} + y\mathbf{i}) + (u\mathbf{1} + v\mathbf{i})\mathbf{j} \qquad (*)$$

É conveniente mudar a notação e reescrever $(*)$ na forma:

$$q = z + wj.$$

Definição 1.25. *Uma **tranformação de Möbius agindo em** $\hat{\mathbb{R}}^{\mathbf{3}}$ é uma composição finita de reflexões(em esferas ou planos).*

Claramente uma transformação de Möbius é um homeomorfismo de $\hat{\mathbb{R}}^n$ em $\hat{\mathbb{R}}^n$.

Definição 1.26. *O grupo das tranformações de Möbius agindo em* $\hat{\mathbb{R}}^n$ *é chamado o* ***grupo de Möbius geral*** *e é denotado por:* $\mathbf{GM}(\hat{\mathbb{R}}^{\mathbf{n}})$.

Definição 1.27. *O* ***grupo de Möbius*** $\mathbf{M}(\hat{\mathbb{R}}^{\mathbf{n}})$ *agindo em* $\hat{\mathbb{R}}^n$ *é o subgrupo de* $GM(\hat{\mathbb{R}}^n)$ *constituindo de todas as transformações de Möbius que preservam orientação em* $GM(\hat{\mathbb{R}}^n)$.

Se $x = se_{n+1}$ (ou seja, s é a $(n+1)$-ésima coordenada de x) e $y = te_{n+1}$, então temos definida uma métrica hiperbólica em H^{n+1} da seguinte forma:

$$\rho(x, y) =\mid log(s/t) \mid$$

e assim,

$$cosh\rho(x, y) = 1 + \frac{\mid x - y \mid^2}{2x_{n+1}y_{n+1}}. \tag{1.1}$$

De fato, $cosh\rho(x, y) = cosh|log(s/t)| = \frac{e^{|log(s/t)|}+e^{-|log(s/t)|}}{2}$; se $s/t \geq 1$, então $cosh \mid log(s/t) \mid= \frac{e^{log(s/t)}+e^{log(t/s)}}{2} = \frac{s/t+t/s}{2} = \frac{s^2+t^2}{2ts} = \frac{(s-t)^2+2st}{2ts} = 1 + \frac{|x-y|^2}{2ts} = 1 + \frac{|x-y|^2}{2x_{n+1}y_{n+1}}$. Se $s/t < 1$, obtemos a igualdade de modo similar.

A esfera hiperbólica :

$$\{x \in H^{n+1}/\rho(x, y) = r\}$$

com centro hiperbólico $(y_1, ..., y_{n+1})$ e raio hiperbólico r é precisamente a esfera euclidiana :

$$(x_1 - y_1)^2 + ... + (x_n - y_n)^2 + (x_{n+1} - y_{n+1}coshr)^2 = (y_{n+1}senhr)^2. \tag{1.2}$$

De fato, pela equação 1.1 temos: $\mid x-y \mid^2= 2x_{n+1}y_{n+1}cosh\rho(x, y)-2x_{n+1}y_{n+1} \Rightarrow (x_1-y_1)^2+...+(x_n-y_n)^2+(x_{n+1}-y_{n+1})^2 = 2x_{n+1}y_{n+1}cosh\rho(x, y)-2x_{n+1}y_{n+1}$. Logo,

$(x_1-y_1)^2+...+(x_n-y_n)^2+x_{n+1}^2-2x_{n+1}y_{n+1}+1y_{n+1}^2-2x_{n+1}y_{n+1}cosh\rho+$ $2x_{n+1}y_{n+1}$. Como $1=cosh^2\rho-senh^2\rho$, obtemos a igualdade desejada.

Identificaremos (x,y,t) em $\mathbb{R}^3$ com o quaternion:

$$x+yi+tj$$

O plano complexo estendido $\hat{\mathbb{C}}$ é $\mathbb{C}\cup\{\infty\}$ e este é identificado com $\hat{\mathbb{R}}^2$. Em termos dos quaternios,

$$H^3=\{z+tj : z\in\mathbb{C}, t>0\}$$

e a fronteira de H^3 em $\hat{\mathbb{R}}^3$ é $\mathbb{C}$.

As transformações de Möbius são frequentemente encontradas da forma:

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

onde a,b,c e d são números complexos com $ad-bc\neq 0$.
A classe $\mathcal{M}$ das aplicações da forma $(*)$ é um grupo com a composição usual de funções e pode-se mostrar que $\mathcal{M}=M(\hat{\mathbb{R}}^2)$.

A **extenção de Poincaré** de uma tranformação de Möbius da forma $g(z)=\frac{az+b}{cz+d}$, onde a,b,c e d são dados números complexos com $ad-bc\neq 0$ é dada por:

$$g(z+tj)=\frac{(az+b)\overline{(cz+d)}+a\bar{c}t^2+\mid ad-bc\mid tj}{\mid cz+d\mid^2+\mid c\mid^2 t^2}, \tag{1.3}$$

onde $z=x+iy$.

Representação por matrizes :

Qualquer matriz 2 x 2 A em $GL(2,\mathbb{C})$ induz uma aplicação g em $\mathcal{M}$ pela fórmula $A \to g_A$, onde:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, g_A(z) = \frac{az+b}{cz+d}.$$

Denotaremos a aplicação $A \to g_A$ por ϕ, a qual aplica $GL(2,\mathbb{C})$ em $\mathcal{M}$; diremos que A projeta ou representa g_A.
Seja N=Núcleo de ϕ; $A \in N \Leftrightarrow \frac{az+b}{cz+d} = z, \forall z \in \hat{\mathbb{C}}$.

Se $A \in N$, tomamos $z = 0, \infty$ e 1 e obtemos que:

$A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, g_A(z) = \frac{az+0}{0z+a} = z, \forall a \neq 0$. Portanto,

$$N = \text{Núcleo}(\phi) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \neq 0 \right\}.$$

Em particular, $\mathcal{M}$ é isomorfo a $GL(2,\mathbb{C})/N$: numa linguagem menos formal, g_A determina a matriz A a menos de um múltiplo não-zero.
Analisemos a restrição de ϕ para $SL(2,\mathbb{C})$. O Núcleo desta restrição é:

$$N' = N \cap SL(2,\mathbb{C}) = \{I, -I\}$$

e cada g em $\mathcal{M}$ é portanto a projeção de exatamente duas matrizes, digamos A e $-A$, em $SL(2,\mathbb{C})$. Deduzimos que $\mathcal{M}$ é isomorfo a $SL(2,\mathbb{C})/\{I, -I\}$.

As duas funções:

$$\frac{tr^2(A)}{det(A)}, \ \frac{\| A \|^2}{| det(A) |}, \ A \in GL(2, \mathbb{C}) \text{ com } \| A \| = (| a |^2 + | b |^2 + | c |^2 + | d |^2)^{1/2}$$

são invariantes sob a transformação $A \to \lambda A, \lambda \neq 0$, e assim elas induzem funções correspondentes em $\mathcal{M}$:

$$\text{traço}^2(g) = \frac{tr^2(A)}{det(A)} \text{ e } \| g \| = \frac{\| A \|}{| det(A) |^{1/2}},$$

onde A é qualquer matriz que projeta g.

Teorema 1.28. *Para cada g em $\mathcal{M}$, temos:*

$$\| g \|^2 = 2cosh\rho(j, g(j)).$$

Demonstração. Seja $g(z) = \frac{az+b}{cz+d}$, $ad - bc = 1$.
Então, por 1.3 (com $z = 0$ e $t = 1$), temos:

$$g(j) = \frac{(b\overline{d} + a\overline{c}) + j}{| c |^2 + | d |^2}.$$

Por 1.1, se $\xi_1 = z_1 + t_1 j$ e $\xi_2 = z_2 + t_2 j$, então:

$$cosh\rho(\xi_1, \xi_2) = \frac{| z_1 - z_2 |^2 + (t_1 - t_2)^2}{2t_1 t_2} + 1.$$

Agora, fazendo as substituições $z_1 = 0$, $t_1 = 1$ (e portanto, $\xi_1 = j$) e $\xi_2 = g(j)$, obtemos:

$$cosh\rho(j, g(j)) = \frac{|-z_2|^2 + (1-t_2)^2}{2t_2} + 1 =$$

$$\left[\frac{|b\overline{d}+a\overline{c}|^2}{(|c|^2+|d|^2)^2} + \left(1 - \frac{1}{(|c|^2+|d|^2)}\right)^2\right]\left(\frac{(|c|^2+|d|^2)^2}{2}\right) + 1 =$$

$$\left(\frac{|b\overline{d}+a\overline{c}|^2}{(|c|^2+|d|^2)^2} + \frac{(|c|^2+|d|^2-1)^2}{(|c|^2+|d|^2)^2}\right)\left(\frac{(|c|^2+|d|^2)^2}{2}\right) + 1 = \frac{|b\overline{d}+a\overline{c}|^2+(|c|^2+|d|^2-1)^2}{2(|c|^2+|d|^2)} + 1$$

Agora, usando a identidade:

$$| b\overline{d} + a\overline{c} |^2 + 1 = | b\overline{d} + a\overline{c} |^2 + | ad - bc |^2 = (| a |^2 + | b |^2)(| c |^2 + | d |^2 ,$$

temos:

$cosh\rho(j, g(j)) = \frac{(|a|^2+|b|^2)(|c|^2+|d|^2)-1+(|c|^2+|d|^2-1)^2+2(|c|^2+|d|^2)}{2(|c|^2+|d|^2)}.$

Portanto,

$2cosh\rho(j, g(j)) = | a |^2 + | b |^2 + | c |^2 + | d |^2 = || g ||^2,$

para $ad - bc = 1$.

$\square$

É conveniente introduzir certas transformações de Möbius normalizadas. Para cada k não zero em $\mathbb{C}$, definimos m_k por:

$$m_k(z) = kz \ \ (\text{ se } k \neq 1) \qquad (1)$$

e

$$m_1(z) = z + 1 \qquad (2)$$

Chamamos (1) e (2) de formas padrão.

Se $g(\neq I)$ é qualquer transformação de Möbius, então g tem exatamente dois pontos fixos α e β em $\mathbb{C}$ ou g tem um único ponto fixo em $\mathbb{C}$(neste caso escolhemos β algum outro ponto diferente de α).

Agora, seja h qualquer transformação de Möbius com:

$$h(\alpha) = \infty, h(\beta) = 0, h(g(\beta)) = 1 \text{ se } g(\beta) \neq \beta$$

e observe que:

$$hgh^{-1}(\infty) = \infty, \ \ hgh^{-1}(0) = \begin{cases} 0 & \text{se } g(\beta) = \beta \\ 1 & \text{se } g(\beta) \neq \beta \end{cases}$$

Portanto, se g fixa α e β, então hgh^{-1} fixa 0 e ∞ e assim,como $\mathcal{M}$ é isomorfo a $SL(2, \mathbb{C})/\{I, -I\}$, temos que para algum $k(k \neq 1)$, $hgh^{-1} = m_k$. Se g fixa somente α, então hgh^{-1} fixa somente ∞ e $hgh^{-1}(0) = 1$; assim, $hgh^{-1} = m_1$. Isto mostra que qualquer transformação de Möbius $(g \neq I)$ é conjugada a uma das formas padrão m_k.

Definição 1.29. *Seja $g(\neq I)$ qualquer transformação de Möbius. Dizemos que:*

*(i) g é **parabólica** se, e somente se, g possui um único ponto fixo em $\hat{\mathbb{C}}$(equivalentemente, g m_1);*

*(ii) g é **loxodrômica** se, e somente se, g possui exatamente dois pontos fixos em $\hat{\mathbb{R}}^3$(equivalentemente, g m_k para algum k satisfazendo $\mid k \mid \neq 1$);*

*(iii)g é **elíptica** se, e somente se, g possui infinitos pontos fixos em $\hat{\mathbb{C}}$(equivalentemente, g m_k para algum k satisfazendo $\mid k \mid = 1, k \neq 1$).*

Observe que se g é parabólico ou loxodrômico, então $o(g) = \infty$.

Capítulo 2

Grupos Discretos e Grupos Descontínuos

Definição 2.1. *Um grupo topológico G é dito **discreto** se a topologia em G é a topologia discreta(na qual todo subconjunto é aberto).*

Observação 2.2. *Se G é qualquer grupo topológico e H é um subgrupo de G, então H é um grupo topológico com respeito a topologia induzida. Note que, $\mathbb{Z}$, o grupo dos inteiros, é discreto como um subgrupo topológico de $\mathbb{R}$. Mas, $\mathbb{Q}$,o grupo dos racionais, não é discreto como um subgrupo topológico de $\mathbb{R}$.*

Vamos focar agora nossa atenção para subgrupos do grupo topológico $GL(2, \mathbb{C})$.

Definição 2.3. *Um subgrupo G de $GL(2, \mathbb{C})$ é **discreto** se, e somente se, o subespaço topológico em G é o topológico discreto.*

Segue que se G é discreto e se $X, A_1, A_2, ...$ estão em G com $A_n \to X$, então $A_n = X$ para todo n suficientemente grande.

Observação 2.4. *Não é necessário assumir que* $X \in G$*, mas somente que* $X \in GL(2, \mathbb{C})$*. De fato, neste caso pela continuidade,* $A_n(A_{n+1})^{-1} \rightarrow XX^{-1} = I$ *e assim, para quase todo* n*, nós temos* $A_n = A_{n+1}$ *e portanto* $A_n = X$*.*

Em termos de sequência, G é discreto se, e somente se, $A_n \rightarrow I$ e $A_n \in G$ implica que $A_n = I$ para quase todo n.

No caso de subgrupos de $SL(2, \mathbb{C})$ uma formulação alternativa de ação discreta pode ser dada diretamente em termos da norma:
Um subgrupo G de $SL(2, \mathbb{C})$ é discreto se, e somente se, para cada positivo k, o conjunto:

$$\{A \in G : \| A \| \leq k\} \qquad (\bullet)$$

é finito.
De fato, se este conjunto é finito para cada k, então G claramente não pode ter qualquer ponto limite(a função norma é contínua) e assim G é discreto.
Por outro lado, se este conjunto é infinito então existem distintos elementos A_n em G com $\| A \| \leq k, n = 1, 2, ...$ Se A_n tem coeficientes a_n, b_n, c_n e d_n então $\| a_n \| \leq k$ e assim a sequência a_n tem uma subsequência convergente. O mesmo é verdade para os outros coeficientes e usando o "processo da diagonal" nós vemos que existe uma subsequência na qual cada um dos coeficientes converge. Nesta subsequência, $A_n \rightarrow B$, para algum B e como det é contínuo, $B \in SL(2, \mathbb{C})$; assim, G não é discreto.
O critério $(\bullet)$ mostra que um subgrupo discreto de $SL(2, \mathbb{C})$ é enumerável.
De fato,

$$G = \bigcup_{n=1}^{\infty} G_n,$$

onde G_n é o conjunto finito de A em G com $\| A \| \leq n$. Qualquer subgrupo de um grupo discreto é obviamente discreto. Finalmente, se G é discreto então qualquer grupo conjugado BGB^{-1} também é discreto; pois, $X \to BXB^{-1}$ é um homeomorfismo de $GL(2,\mathbb{C})$ nele mesmo.

Exemplo 2.5. *: Seja $G = GL(2,\mathbb{C})$ agindo pelas transformações lineares fracionárias na esfera de Riemann $\mathbb{C} \cup \{\infty\}$. Então, o grupo*
$\Gamma_2(\mathbb{Z}) = \{\gamma \in SL(2,\mathbb{Z}) : \gamma \equiv 1(mod2)\} =$

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a \equiv 1(mod2), b \equiv 0(mod2), c \equiv 0(mod2), d \equiv 1(mod2) \right\}$$ *é discreto em G.*

De fato,

Suponha que exista uma sequência de distintas matrizes tais que:

$$\begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

ou seja, existem N_1, N_2, N_3 e N_4 tais que para todo n maior ou igual a N_1, N_2, N_3 e N_4, respectivamente, $a_n \to 1$, $b_n \to 0$, $c_n \to 0$, $d_n \to 1$. Seja $N = máx\, \{N_1, N_2, N_3, N_4\}$. Então, $\forall n \geq N$, $a_n, d_n = 1$ e $b_n, c_n = 0$, o que não é possível.

Definição 2.6. *Seja X qualquer espaço topológico e G um grupo de homeomorfismos de X em X. Dizemos que* **G** ***age descontinuamente em*** *X se para todo subconjunto compacto K de X,*

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

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

Exemplo 2.7. *Seja G agindo como no exemplo anterior em $\mathbb{C}\cup\{\infty\}$. Considere quatro círculos $C_1, ..., C_4$ em $\mathbb{C}$ com interiores não interceptados e escolha g_1 (respectivamente g_2) em G aplicando o exterior de C_1 (respectivamente C_2) no interior de C_3 (respectivamente C_4). Então, o grupo gerado por g_1 e g_2 é descontínuo em um subconjunto S não-vazio de $\mathbb{C}\cup\{\infty\}$.*
De fato, considere $C_1 = (0, 2), C_2 = (2, 2), C_3 = (4, 2), C_4 = (6, 2)$, S tal que a interseção de S com qualquer um dos quatro círculos seja vazia e g_1, g_2 da seguinte maneira:

$$\begin{aligned} g_1 : Ext(C_1) &\to Int(C_1) \to Int(C_3) \\ z \ &\to \left(\frac{1}{z}\right) \to \left(\frac{1}{z}\right) + 4 \end{aligned}$$

$$\begin{aligned} g_2 : Ext(C_2) &\to Int(C_2) \to Int(C_4) \\ w \ &\to \left(\frac{1}{w-2}\right) \to \left(\frac{1}{w-2}\right) + 4 \end{aligned}$$

Logo, para todo subconjunto compacto K de S temos:
$g_1(K) \cap K = \emptyset, g_1^2(K) = g_1 \circ g_1(Ext(C_1)) = g_1(Int(C_3)) \subset Int(C_3) \Rightarrow g_1^2(K) \cap K = \emptyset, ..., g_1^n(K) \cap K = \emptyset$ *e* $g_2(K) \cap K = \emptyset, g_2^2(K) = g_2 \circ g_2(Ext(C_2)) = g_2(Int(C_4)) \subset Int(C_4) \Rightarrow g_2^2(K) \cap K = \emptyset ..., g_2^n(K) \cap K = \emptyset$ *o que implica que, a menos da identidade, $f(K) \cap K = \emptyset, \forall f \in G$. Portanto, $G =< g_1, g_2 >$ é descontínuo em um subconjunto aberto não vazio de $\mathbb{C}\cup\{\infty\}$.*

Em nossas aplicações, X será sempre um subconjunto de $\hat{\mathbb{R}}^3$ com a topologia usual.

Proposição 2.8. *Suponha que G age descontinuamente em X, então as seguintes afirmações são verdadeiras:*
(i) Todo subgrupo de G age descontinuamente em X.

(ii) Se ϕ é um homeomorfismo de X em Y, então $\phi G \phi^{-1}$ age descontinuamente em Y.

(iii) Se Y é um subconjunto G-invariante de X, então G age descontinuamente em Y.

(iv) Se $x \in X$ e se $g_1, g_2, ...$ são elementos distintos de G, então a sequência $g_1(x), g_2(x), ...$ não pode convergir para qualquer y em X.

(v) Se $x \in X$, então o estabilizador G_x é finito.

(vi) G é enumerável.

Demonstração. (i) É trivial, pois $H \subset G$. (ii)Temos que G é subgrupo dos homeomorfismos de X em X. Considere funções $g : X \to X$ e $h : Y \to Y$ e seja $\phi(K) = \hat{K}$, onde K e $\hat{K}$ são subconjuntos compactos de X e Y, respectivamente. Para todo compacto $\hat{K} \subset Y$ e para toda função $h : Y \to Y (h = \phi G \phi^{-1})$ e $g = \phi^{-1} h \phi : X \to X$, temos: $\Rightarrow \phi^{-1} h \phi(K) \cap K = \emptyset \Rightarrow \phi^{-1} h(\hat{K}) \cap K = \emptyset \Rightarrow h(\hat{K}) \cap \phi(K) = \emptyset \Rightarrow h(\hat{K}) \cap \hat{K} = \emptyset$.

(iii) Temos $Y \subset X$, logo qualquer subconjunto compacto de Y é também compacto de X.

(iv) Suponha que a sequência $g_1(x), g_2(x), ...$ converge para algum y em X. Então, $K = \{y, x, g_1(x), g_2(x), ...\}$ é compacto. Como $g_n(K) \cap K \neq \emptyset (n = 1, 2, ...)$ e como os g_n são distintos, segue que G não age descontinuamente em X.

(v) Suponha que o estabilizador seja infinito e tome $K = \{x\}$. Logo, $g(K) = K \forall g \in G_x$ o que implica que $g(K) \cap K \neq \emptyset \forall g \in G_x$.

(vi) Vimos que existe uma correspondência bijetiva entre G/G_x e a órbita $G(x)$. Assim, por (v) G é enumerável se, e somente se, $G(x)$ é enumerável. Mas, qualquer conjunto não-enumerável em $\hat{\mathbb{R}}^3$ contém um ponto limite. Suponha então que existe uma órbita x^G não-enumerável em $\hat{\mathbb{R}}^3$. Logo, existe x_0 em X que é limite de uma sequência $\{g_n\}$, o que contradiz (iv). $\square$

Teorema 2.9. *Um subgrupo G de $\mathcal{M}$ é discreto se, e somente se, ele age descontinuamente em H^3.*

Demonstração. ($\Rightarrow$): Como G é a imagem homomorfa de um subgrupo discreto(e portanto enumerável) de $SL(2, \mathbb{C})$, temos que G é enumerável, digamos:

$$G = \{g_1, g_2, ...\}$$

Como G é discreto, $\| g_n \| \to +\infty$ e usando 1.28, nós vemos que, como $n \to +\infty$,

$$\rho(j, g_n(j)) \to +\infty \qquad (*)$$

É claro, por 1.2, que um subconjunto compacto K de H^3 está contido em alguma bola hiperbólica:

$$B = \{x \in \mathbb{R}^3 : \rho(x, j) < k\}.$$

Suponha, por absurdo, que G não age descontinuamente em H^3, ou seja, $g(K) \cap K \neq \emptyset \Rightarrow g(B) \cap B \neq \emptyset \Rightarrow \rho(j, g(j)) < 2k$. Mas, por $(*)$, isto só pode acontecer para um número finito de G em G.

($\Leftarrow$): Suponha que G age descontinuamente em H^3(ou qualquer subdomínio de $\hat{\mathbb{C}}$). Se G não é discreto, podemos achar distintas matrizes $A_1, A_2, ...$ em $SL(2, \mathbb{C})$ projetando $g_1, g_2, ...$ em G, com

$$A_n \to I \text{ quando } n \to \infty.$$

Usando 1.3, vemos que se $g = Id_{\hat{\mathbb{C}}}$, então a extensão de g : $\hat{g} = Id_{H^3}$, ou seja, $g_n(x) \to x$ quando $n \to \infty, \forall x \in \hat{\mathbb{R}^3}$. Contradição com o item (iv) da proposição 2.8.

$\square$

Agora, daremos atenção para o plano complexo estendido e estudaremos a relação entre ações discretas e descontínuas em subconjuntos de $\hat{\mathbb{C}}$. A prova do terorema 2.9 mostra que se G age descontinuamente em algum subconjunto aberto não-vazio de $\hat{\mathbb{C}}$, então G é discreto. Mas, a recíproca é falsa. Para darmos um simples exemplo disto, estabeleceremos um critério que exclui a possibilidade de uma ação descontínua.

Lema 2.10. *Seja G qualquer subgrupo de $\mathcal{M}$ e seja D um subconjunto aberto de $\hat{\mathbb{C}}$ que contém um ponto fixo v de algum elemento parabólico ou loxodrômico g de G. Então, G não age descontinuamente em D.*

Demonstração. Tome $G_v = \{g \in G : g(v) = v\}$. Observe que se $g \in G_v$, então $g^i \in G_v, \forall i = 1, 2, ...$Mas, se g é parabólico ou loxodrômico então $o(g) = \infty$. Logo, o estabilizador G_v é infinito. Contradição com o item (v) da proposição 2.8.

□

Exemplo 2.11. *Seja G o grupo de Picard, a saber, o grupo das transformações da forma:*

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

onde a, b, c e d são inteiros Gaussianos(da forma $m + in$, onde $m, n \in \mathbb{Z}$) e $ad - bc = 1$. Mostra-se que G é discreto de maneira similar ao exemplo 2.5. Pelo lema 2.10 é suficiente provar que os pontos fixos parabólicos de G são densos em $\hat{\mathbb{C}}$. Seja $w = (p + iq)/r$, onde p, q e r são inteiros; obviamente, o conjunto de tais w é denso em $\hat{\mathbb{C}}$. Agora, simplesmente observe que

$$h(z) = \frac{(1 - wr^2)z + r^2w^2}{-r^2z + (1 + wr^2)}$$

é um elemento parabólico de G que fixa w. De fato, claramente $h(w) = w$. Suponha agora que $h(z) = z$, com $z \neq w$. Logo, $-r^2(z^2 + w^2) + 2wr^2z = 0 \Rightarrow -z^2 - w^2 + 2wz = 0 \Rightarrow -(z - w)^2 = 0 \Rightarrow z - w = 0 \Rightarrow z = w$.

Capítulo 3

Grupos Livres

Definição 3.1. *Seja X um conjunto não-vazio, F um grupo contendo X e $\sigma : X \to F$ uma função. F é **livre** em X se para todo grupo G e para toda função $\alpha : X \to G$ existe um único homomorfismo $\beta : F \to G$ tal que $\alpha = \beta\sigma$.*

A equação $\alpha = \beta\sigma$ expressa a comutatividade do seguinte diagrama de conjuntos e funções:

$$\begin{tikzcd} & F \arrow[dr, dotted, "\beta"] & \\ X \arrow[ur, "\sigma"] \arrow[rr, "\alpha"'] & & G \end{tikzcd}$$

Observação 3.2. *A função $\sigma : X \to F$ é necessariamente injetiva. De fato, suponha $\sigma(x_1) = \sigma(x_2)$ e $x_1 \neq x_2$. Seja G um grupo com pelo menos dois elementos distintos g_1 e g_2 e escolha uma função $\alpha : X \to G$ tal que $\alpha(x_1) = g_1$ e $\alpha(x_2) = g_2$. Então, $\beta(\sigma(x_1)) = \beta(\sigma(x_2)) \Rightarrow \sigma(x_1) = \sigma(x_2)$ e $g_1 = g_2$.*

Claramente F é também livre em $I_m\sigma$, a aplicação inclusão $I_m\sigma \to F$ tomada no lugar de σ. Portanto, um grupo livre é sempre livre em um subconjunto; neste caso a comutatividade do diagrama diz que a restrição de β a X é α. Assim, β é a única extensão de α para F.

A definição não mostra que grupos livres realmente existem; para isso veremos o resultado abaixo:

Proposição 3.3. *Se X é um conjunto não-vazio, existe um grupo F e uma função $\sigma : X \to F$ tal que F é livre em X e $F =< I_m\sigma >$.*

Demonstração. Escolha um conjunto disjunto de X com a mesma cardinalidade e que denotaremos por:
$X^{-1} = \{x^{-1} : x \in X\}$, onde x^{-1} é meramente um símbolo.
Uma palavra em X é uma sequência finita de símbolos de $X \cup X^{-1}$, escrita por conveniência na forma :

$$w = x_1^{\xi_1}...x_r^{\xi_r},\ x_i \in X,\ \xi_i = \pm 1,\ r \geq 0.$$

No caso $r = 0$ a sequência é vazia e w é a palavra vazia, a qual será denotada por 1.
Duas palavras são consideradas iguais se, e somente se, elas tem os mesmos elementos em posições correspondentes.
O produto de duas palavras $w = x_1^{\xi_1}...x_r^{\xi_r}$ e $v = y_1^{\eta_1}...y_s^{\eta_s}$ é formado pela justaposição:

$$wv = x_1^{\xi_1}...x_r^{\xi_r}y_1^{\eta_1}...y_s^{\eta_s},$$

com a convenção que $w1 = w = 1w$.
A inversa de w é a palavra $w^{-1} = x_r^{-\xi_r}...x_1^{-\xi_1}$ e $1^{-1} = 1$.
Se S denota o conjunto de todas as palavras em X, definimos uma relação

de equivalência em S da seguinte maneira: $w \sim v$ se é possível passar de uma palavra para a outra por meio de uma sequência finita de operações dos seguintes tipos:

(a) **inserção** de um xx^{-1} ou um $x^{-1}x$, $(x \in X)$, como elementos consecutivos de uma palavra.

(b) **deleção** de algum xx^{-1} ou $x^{-1}x$.

Claramente esta relação é uma relação de equivalência.

A classe de equivalência que w pertence será denotada por $[w]$.

Defina F como sendo o conjunto de todas as classes de equivalência (nosso objetivo é construir F em um grupo). Se $w \sim w'$ e $v \sim v'$, é imediato que $wv \sim w'v'$, então é significativo definir o produto de $[w]$ e $[v]$ por: $[w][v] = [wv]$. Então, $[w][1] = [w] = [1][w]$ e $[w][w^{-1}] = [ww^{-1}] = [1]$. Além disso, o produto é associativo pois, $(wv)u = w(vu)$ é obviamente verdade; o que implica que, $([w][v])[u] = [(wv)u] = [w(vu)] = [w]([v][u])$. Portanto, F é um grupo com esta operação binária; o elemento identidade é $[1]$ e o inverso de $[w]$ é $[w^{-1}]$.

Agora, defina a função $\sigma : X \to F$ tal que $\sigma(x) = [x]$. Devemos provar que F é livre em X.

Suponha que $\alpha : X \to G$ é uma função de X para algum grupo G. Primeiro, tomemos uma função β' do conjunto de todas as palavras em X para G levando $x_1^{\xi_1}...x_r^{\xi_r}$ para $g_1^{\xi_1}...g_r^{\xi_r}$, onde $g_i = \alpha(x_i)$. Temos que $w \sim s$ implica que $\beta'(w) = \beta'(v)$ pois, no grupo G produtos como gg^{-1} ou $g^{-1}g$ são iguais a 1_G. Com isto é possível definir uma função $\beta : F \to G$ por: $\beta([w]) = \beta'(w)$. Então, $\beta([w][v]) = \beta([wv]) = \beta'(wv) = \beta'(w)\beta'(v)$ pela definição de β'. Por esta razão, $\beta([w][v]) = \beta([w])\beta([v])$ e β é um homomorfismo de F para G. E mais ainda, $\beta(\sigma(x)) = \beta([x]) = \beta'(x) = \alpha(x),\ x \in X$.

Finalmente, se $\gamma : F \to G$ é outro homomorfismo tal que $\alpha = \gamma\sigma$, então

$\gamma\sigma = \beta\sigma$ e γ e β coincidem em $I_m\sigma$. Mas, claramente $F =< I_m\sigma >$; assim,$\gamma = \beta$(pois elas coincidem nos geradores). $\square$

Definição 3.4. *Uma palavra w em X é chamada **reduzida** se ela não contém pares de símbolos consecutivos da forma xx^{-1} ou $x^{-1}x$, $(x \in X)$.*

Por convenção a palavra vazia é reduzida.

Proposição 3.5. *Se F_1 é livre em X_1 e F_2 é livre em X_2 e se $\mid X_1 \mid=\mid X_2 \mid$, então $F_1 \simeq F_2$.*

Demonstração. Sejam $\sigma_1 : X_1 \to F_1$ e $\sigma_2 : X_2 \to F_2$ as injeções dadas e seja $\alpha : X_1 \to X_2$ uma bijeção. Então, existem diagramas comutativos:

$$\begin{tikzcd} & F_1 \arrow[dr, dotted, "\beta_1"] & \\ X_1 \arrow[ur, "\sigma_1"] \arrow[rr, "\sigma_2\alpha"'] & & F_2 \end{tikzcd} \qquad \begin{tikzcd} & F_2 \arrow[dr, dotted, "\beta_2"] & \\ X_2 \arrow[ur, "\sigma_2"] \arrow[rr, "\sigma_1\alpha^{-1}"'] & & F_1 \end{tikzcd}$$

com β_1 e β_2 homomorfismos. Logo, $\beta_2\beta_1\sigma_1 = \beta_2\sigma_2\alpha = \sigma_1\alpha^{-1}\alpha = \sigma_1$ e o diagrama:

$$\begin{tikzcd} & F_1 \arrow[dr, dotted, "\beta_2\beta_1"] & \\ X_1 \arrow[ur, "\sigma_1"] \arrow[rr, "\sigma_1"'] & & F_1 \end{tikzcd}$$

comuta. Mas, a função identidade 1_{F_1} também fará o diagrama comutar. Logo, pela unicidade, $\beta_1\beta_2 = 1_{F_1}$.

Fazendo $\beta_1\beta_2\sigma_2 = \beta_1\sigma_1\alpha^{-1} = \sigma_2\alpha\alpha^{-1} = \sigma_2$, obtemos de maneira análoga que $\beta_1\beta_2 = 1_{F_2}$. Como $\beta : F_1 \to F_2$ é homomorfismo e bijeção, segue que $F_1 \simeq F_2$.

$\square$

Proposição 3.6. *Todo grupo G é um quociente de um grupo livre.*

Demonstração. Considere G como um conjunto, e seja F livre em G. Se $\alpha : G \to G$ é a aplicação identidade, então existe um homomorfismo $\beta : F \to G$ (extensão de α). Temos que β é sobrejetiva, pois α é sobrejetiva. Logo, temos $\beta : F \to G$ homomorfismo sobrejetor, o que implica que $F/Ker\beta \simeq G$. $\square$

Proposição 3.7. *Seja G um grupo gerado por um subconjunto X e seja F um grupo livre em um conjunto Y. Se $\alpha : Y \to X$ é uma sobrejeção, ela se estende para um epimorfismo de F para G. Em particular, todo grupo é a imagem de um grupo livre.*

Demonstração. Como F é livre em Y, temos que existe um homomorfismo $\beta : F \to G$. Mas, β é sobrejetora, pois $G =< X >$. $\square$

Proposição 3.8. *(A propriedade projetiva de grupos livres) Sejam F um grupo livre, G e H outros grupos. Assuma que $\alpha : F \to H$ é um homomorfismo e $\beta : G \to H$ um epimorfismo. Então, existe um homomorfismo $\gamma : F \to G$ tal que $\beta\gamma = \alpha$, ou seja, que o diagrama abaixo comuta:*

$$\begin{tikzcd} H & G \arrow[l, "\beta"'] \\ F \arrow[u, "\alpha"] \arrow[ur, dotted, "\gamma"'] & \end{tikzcd}$$

Demonstração. Seja F um grupo livre em um conjunto X. Se $x \in X$, então $\alpha(x) \in H = Im\beta$. Assim, existe algum g_x em G tal que $\beta(g_x) = \alpha(x)$. Pela propriedade de grupos livres, podemos estender a função $x \to g_x$ para um homomorfismo $\gamma : F \to G$. Como $\beta\gamma(x) = \beta(g(x)) = \alpha(x)$, $\forall x \in X$ e X gera F, segue que $\alpha = \beta\gamma$. $\square$

Definição 3.9. *Seja $\{A_\alpha\}$ uma família de grupos. Um* ***produto livre*** *de A_α é um grupo P com as seguintes propriedades:*
(i) P contém uma cópia isomorfa de cada A_α, isto é, para cada α existe um homomorfismo bijetor $i_\alpha : A_\alpha \to P$;
(ii) Para todo grupo G e toda família de homomorfismos $f_\alpha : A_\alpha \to G$, existe um único homomorfismo $\psi : P \to G$ estendendo cada f_α, isto é, para cada α, $\psi i_\alpha = f_\alpha$.

Assim como na definição de grupo livre, a definição de produto livre não garante que produto livre, de fato, existe. Para isso temos um teorema garantindo a existência, o qual enunciaremos abaixo e omitiremos sua demonstração que é similar a contrução de um grupo livre.

Teorema 3.10. *Se $\{A_\alpha\}$ é uma família de grupos, existe um produto livre de A_α.*

Proposição 3.11. ***(Critério de Klein)****: Sejam G um grupo agindo em um conjunto S, Γ_1, Γ_2 dois subgrupos de G e Γ o subgrupo gerado por eles. Assuma que Γ_1 contém pelo menos três elementos e que existem dois subconjuntos S_1, S_2 em S com S_2 não contido em S_1 tal que $\gamma(S_2) \subset S_1$ $\forall \gamma \in \Gamma_1 - \{1\}$ e $\gamma(S_1) \subset S_2$ $\forall \gamma \in \Gamma_2 - \{1\}$. Então, Γ é isomorfo ao produto livre $\Gamma_1 * \Gamma_2$.*

Demonstração. Vamos verificar que qualquer palavra reduzida não vazia w escrita com letras de $\Gamma_1 - \{1\} \cup \Gamma_2 - \{1\}$ não age como a identidade em S.

1º caso: $w = \alpha_1\beta_1\alpha_2\beta_2...\alpha_k$, com $\alpha_1, ..., \alpha_k \in \Gamma_1 - \{1\}$ e $\beta_1, ..., \beta_k \in \Gamma_2 - \{1\}$. Então, $w(S_2) \subset S_1$ e $w \neq 1$.

2º caso: $w = \beta_1\alpha_2...\alpha_k\beta_k$. Seja $\alpha \in \Gamma_1 - \{1\}$, então $w' = \alpha w \alpha^{-1} = \alpha\beta_1\alpha_2\beta_2...\alpha_k\beta_k\alpha^{-1} \neq 1$, pois $w'(S_2) \subset S_1$, o que implica $w \neq 1$.

3º caso: $w = \alpha_1\beta_1...\alpha_k\beta_k$. Seja $\alpha \in \Gamma_1 - \{1, \alpha_1^{-1}\}$. Então, $w' = \alpha w \alpha^{-1} = \alpha\alpha_1\beta_1...\alpha_k\beta_k\alpha^{-1} \neq 1$, pois $w'(S_2) \subset S_1$, o que implica $w \neq 1$.

4º caso: $w = \beta_1\alpha_2...\beta_{k-1}\alpha_k$. Seja $\alpha \in \Gamma_1 - \{1, \alpha_k^{-1}\}$. Então, $w' = \alpha w \alpha^{-1} = \alpha\beta_1\alpha_2...\beta_{k-1}\alpha_k\alpha^{-1} \neq 1$, pois $w'(S_2) \subset S_1$, o que implica $w \neq 1$. $\square$

Exemplo 3.12. ***(Um subgrupo do grupo modular)***.
Seja $G = GL(2, \mathbb{C})$ agindo pelas transformações lineares fracionárias na esfera de Riemann $\mathbb{C} \cup \{\infty\}$. Então,

$g = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ *e* $h = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ *geram um grupo livre em G.*

De fato, considere primeiro o subgrupo Γ_1 de G gerado por g: $\Gamma_1 = \left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\rangle$, o subgrupo $\Gamma_2 = \{1, j\}$ onde $j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ e o grupo Γ gerado por Γ_1 e Γ_2.
Considere também : $S_1 = \{z \in \mathbb{C} : |Re(z)| > 1\}$ e
$S_2 = \{z \in \mathbb{C} : |z| < 1\}$.
E fácil ver pelo Critério de Klein que $\Gamma = \Gamma_1 * \Gamma_2$ em $G = GL(2, \mathbb{C})$. Como $h = jgj$ e $o(g) = o(h) = \infty$ obtemos que $< g, h >$ é um subgrupo livre de $SL(2, \mathbb{C})$.

O grupo modular $\Gamma_2(\mathbb{Z}) = \{\gamma \in SL(2, \mathbb{Z}) : \gamma \equiv 1 (mod 2)\}$ é um grupo discreto(provado no capítulo 3) gerado por

$$g = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},\ h = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \text{ e } -1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

O estudo para quais $\lambda \in \mathbb{C}$ *as matrizes* $g = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$ *e* $h = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ *geram um subgrupo livre de* $SL(2, \mathbb{C})$ *tem recebido considerações relevantes; apresentaremos agora alguns resultados. Começaremos com um teorema que é, na verdade, uma reformulação do Critério de Klein.*

Teorema 3.13. ***(Macbeath)****: Seja* $G =< A, B >$ *um grupo de permutações de um conjunto infinito* Ω *gerado por dois subgrupos* A *e* B*. Suponha que* A *ou* B *tem ordem maior que dois e sejam* Γ *e* Δ *subconjuntos não-vazios disjuntos de* Γ*. Suponha agora que* $a\Gamma \subseteq \Delta$ *,* $\forall a \in A - \{1\}$ *e* $b\Delta \subseteq \Gamma$ *,* $\forall b \in B - \{1\}$*. Então,* $G = A * B$*.*

Demonstração. Suponha que $|A| > 2$ e observe que as imagens $a\Gamma$ $(a \neq 1)$ de Γ são subconjuntos não-vazios disjuntos de Δ pois, se $a\Gamma \cap a'\Gamma \neq \emptyset,\ a, a' \in A$, então $\Gamma \cap a^{-1}a'\Gamma \neq \emptyset \Rightarrow \Gamma \cap a''\Gamma \neq \emptyset \Rightarrow \Gamma \cap \Delta \neq \emptyset$; absurdo pois, por hipótese, Γ e Δ são disjuntos. Assim, $a\Gamma \subsetneq \Delta$, $\forall a \in A - \{1\}$. agora, tome as possíveis combinações para uma palavra reduzida não vazia w escrita com letras de $A - \{1\} \cup B - \{1\}$ e a demonstração é feita de maneira similar a da proposição 3.11. □

Se S *é qualquer conjunto no plano complexo estendido, escreveremos* S^N *para o interior do complemento de* S*. Note que se* S *é uma região aberta, então* S^N *também é uma região aberta e* $(S^N)^N = S$*.*

Corolário 3.14. *Seja* λ *qualquer número complexo, e seja* G *o grupo das transformações lineares fracionárias do plano complexo* Ω *gerado pelos dois elementos:*

$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ *e* $B = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$.

Sejam $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ *e* $T = JBJ$.
Sejam agora Γ *uma região aberta em* Ω, $\emptyset \neq \Gamma \neq \Omega$, *e* $\Sigma = J\Gamma^N$. *Então,* G *é um grupo livre, livremente gerado por* A *e* B*, desde que:*
(1) $A^K\Gamma \cap \Gamma =\neq$, $\forall K \neq 0$,
(2) $T^K\Sigma \cap \Sigma =\neq$, $\forall K \neq 0$.

Demonstração. Seja $\Delta = \Gamma^N$. Então,(2) é equivalente a (2'): $B^K\Delta \cap \Delta = \emptyset$, $\forall K \neq 0$.
De fato, $B^K\Delta = B^KJ^2\Delta = B^KJ(J\Delta) = B^KJ\Sigma = J(JB^KJ)\Sigma = JT^K\Sigma$. E mais, $B^K\Delta \cap \Delta = \emptyset \Leftrightarrow JB^K\Delta \cap J\Delta = \emptyset$.
Agora, (1) implica que, para $K \neq 0$, o conjunto aberto $A^K\Gamma$ está contido no complemento $\overline{\Gamma}$ de Γe consequentemente no interior Δ de $\overline{\Gamma}$. Analogamente, (2') implica que $B^K\Delta \subset (\Gamma^N)^N = \Gamma$, $\forall K \neq 0$.

$\square$

Teorema 3.15. ***(Chang, Jennings, e Ree)****: Seja* λ *um número complexo tal que* λ *não pertença a nenhum dos discos abertos de raio 1 e com centros -1, 0, +1. Então o grupo* G *gerado por:*

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \ e \ B = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$$

é um grupo livre, livremente gerado por A *e* B.

Demonstração. Procederemos fazendo escolhas para os conjuntos Γ, Δ e Σ no corolário 3.14. Escolhemos $\Gamma = \{z \in \mathbb{C} :\mid Rez \mid < 1\}$. Então, o conjunto Γ^N consiste dos conjuntos $\Delta_1 = \{z \in \mathbb{C} : Rez > 1\}$ e $\Delta_2 = \{z \in \mathbb{C} : Rez < -1\}$; assim, $\Delta = \Delta_1 \cup \Delta_2$. E, o conjunto $\Sigma = J\Delta = J\Delta_1 \cup J\Delta_2 = \Sigma_1 \cup \Sigma_2$, onde Σ_1 é o disco $\mid w - \frac{1}{2} \mid < \frac{1}{2}$ e Σ_2 é o disco $\mid w + \frac{1}{2} \mid < \frac{1}{2}$.

De fato,

$w = Jz,\ z \in \Delta_1; z = a + bi,\ a > 1.$

$w = \frac{1}{z} = \frac{a}{a^2+b^2} + \left(\frac{-b}{a^2+b^2}\right) i \Rightarrow \mid w - \frac{1}{2} \mid = \sqrt{\frac{(1-a)}{a^2+b^2} + \frac{1}{4}}$

Portanto, $\mid w - \frac{1}{2} \mid < \frac{1}{2} \Leftrightarrow a > 1 \Leftrightarrow z \in \Delta_1$. Analogamente, $\mid w + \frac{1}{2} \mid < \frac{1}{2} \Leftrightarrow a < -1 \Leftrightarrow z \in \Delta_2$.

É imediato que (1) é satisfeito para esta escolha de Γ, pois $A = z + 2$; e (2) será satisfeito se os dois discos Σ_1 e Σ_2 são disjuntos dos discos transladados $T^K\Sigma_1$ e $T^K\Sigma_2$ $\forall K \neq 0$. Agora, todos esses discos tem raio $\frac{1}{2}$ e centro da forma $K\lambda \pm \frac{1}{2}$. A condição que todos esses centros estão numa distância de pelo menos um é precisamente a hipótese do teorema. $\square$

Teorema 3.16. *Seja K a casca convexa do conjunto consistindo do círculo $|z| = 1$ e dos dois pontos $z = \pm 2$. Se o número complexo λ não está no interior de K, então G, como acima, é livremente gerado por A e B.*

Demonstração. Seja Σ como acima, a região limitada pelos dois círculos C_1 e C_2 de raio $\frac{1}{2}$ com centros $\pm\frac{1}{2}$, e seja λ satisfazendo as hipóteses do teorema 3.15. Então, sabemos que:

$$T^K\Sigma \cap \Sigma = \emptyset,\ \forall K \neq 0.$$

Para um arbitrário $\mu \neq 0$, seja:

$$U = \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix},$$

e seja

$$\Sigma^* = U\Sigma \text{e} T^* = UTU^{-1} = \begin{pmatrix} 1 & \mu\lambda \\ 0 & 1 \end{pmatrix}.$$

Segue que $T^{*K}\Sigma^* \cap \Sigma^* = \emptyset$, $\forall K \neq 0$, pois,

$T^K\Sigma \cap \Sigma = \emptyset \Leftrightarrow UT^K\Sigma \cap U\Sigma = \emptyset \Leftrightarrow UT^KU^{-1}(U\Sigma) \cap U\Sigma = \emptyset$, ou seja,

$T^{*K}\Sigma^* \cap \Sigma^* = \emptyset$.

Seja $\Delta^* = J\Sigma^*$ e $\Gamma^* = \Delta^{*N}$ (interior do complemento de Δ^*).

O grupo G^* gerado por A e $JT^*J = \begin{pmatrix} 1 & 0 \\ \mu\lambda & 1 \end{pmatrix}$ será livre desde que:

$$A^K\Gamma^* \cap \Gamma^* = \emptyset, \ \forall K \neq 0.$$

fazendo as contas vemos que Γ^* é uma faixa oblíqua limitada por duas retas paralelas $L_1 = JUC_1$ e $L_2 = JUC_2$, simétricas na origem. Como $A = 2 + z$, a condição desejada valerá desde que L_1 passe por $+1$ e L_2 passe por -1.

Se L é a reta $Rez = 1$, então $C_1 = JL$, e $L_1 = JUJL = VL$ para

$$V = JUJ = \begin{pmatrix} u^{-1} & 0 \\ 0 & 1 \end{pmatrix}$$

Note aqui que $JUJ = \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix} = \frac{z}{u} = u^{-1}z = \begin{pmatrix} u^{-1} & 0 \\ 0 & 1 \end{pmatrix}$

Agora, $+1$ em VL é equivalente a $V^{-1}(1) = u$, isto é,$Re(u) = 1$. De fato, $Re(u) = 1 \Leftrightarrow u \in L \Leftrightarrow V(u) = 1 \in V(L)$.

Isto mostra que se λ satisfaz as hipóteses do teorema 3.15, então G é livre para todo $\lambda_1 = u\lambda$, onde u está sobre a reta $Re(u) = 1$; equivalentemente, G é livre para todo λ_1 pertencente a reta passando por λ que é perpendicular a reta passando por λ e a origem. Com isto, o teorema 3.16 segue imediatamente do teorema 3.15.

$\square$

Teorema 3.17. *Seja μ_0 um número complexo tal que $\mu_0^{2n} = -4$ para algum inteiro positivo n. Então, valores de $\mu (\mu \neq 0)$ para os quais o grupo G gerado por :*

$$A = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \quad e \quad B = \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}$$

não é livre são densos no segmento de reta unindo μ_0 a origem.

Demonstração. A prova consiste em mostrar que, para um conjunto denso de valores de μ no segmento descrito, um certo comutador tem ordem finita. Seja T qualquer matriz unimodular e $T' = [A,T] = ATA^{-1}T^{-1}$. Escrevemos

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

e calculamos as entradas de

$$T' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

em termos das de T:

$$AT = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + c\mu & b + d\mu \\ c & d \end{pmatrix}$$

e

$$A^{-1}T^{-1} = \begin{pmatrix} 1 & -\mu \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d + c\mu & -b - a\mu \\ -c & a \end{pmatrix},$$

e agora, usando $ad - bc = 1$, temos:

$$T' = \begin{pmatrix} 1 + ac\mu + c^2\mu^2 & (ad - bc - a^2 - ac\mu)\mu \\ c^2\mu & 1 - ac\mu \end{pmatrix}.$$

Temos, em particular, que $c' = c^2\mu \Rightarrow c'\mu = (c\mu)^2$, e que T' tem traço $t' = 2 + c^2\mu^2 = 2 + c'\mu$.

Defina T_n recursivamente tomando

$$T_0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ e } T_{n+1} = [A, T_n].$$

Note que, embora T_0 não precise pertencer a G, temos $T_1 = AT_0A^{-1}T_0^{-1} = AB$; assim, T_n está em G para todo $n \geq 1$. Seja

$$T_n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \quad e \;\; t_n = tr(T_n).$$

Agora, $C_0 = 1$ e $C_{n+1}\mu = (c_n\mu)^2$ implica,por indução, que $c_n\mu = \mu^{2^n}$, e logo que $t_n = 2 + c_n\mu = 2 + \mu^{2^n}$.

Suponha que $\mu = r\mu_0$, onde $\mu_0^{2^n} = -4$ e $0 < r < 1$. Então,

$t_n = 2 + \mu^{2^n} = 2 + r\mu_0^{2^n} = 2 + r^{2^n}\mu_0^{2^n} = 2 - 4r^{2^n} = 2(1 - 2r^{2^n}) \in (-2, +2)$.

Se $t_n = 2cos(\theta)$, para θ múltiplo racional de π, então T_n tem ordem finita. De fato, basta observar que T_n tem como polinômio característico: $P_c(T_n) = X^2 - t_nX + 1$. Calculando os autovalores teremos os valores: $cos(\theta) + isen(\theta)$ e $cos(\theta) - isen(\theta)$. Mas, como $\theta = \frac{p}{q}\pi$ e T_n é diagonalizável com os autovalores na diagonal (observe que tomamos $r < 1$ porquê se $r = 1$, então $t_n = -2 \Rightarrow P_c(T_n) = X^2 + 2X + 1 \Rightarrow$ os autovalores de T_n são iguais e, neste caso, não poderíamos garantir a diagonalização com estes valores), segue que $(T_n)^{2q} = 1$.

Agora, dado $\alpha \in \mathbb{R}$ como $\mathbb{Q}$ é denso em $\mathbb{R}$, existe $r_n = \frac{p_n}{q_n} \in \mathbb{Q}$ tal que $r_n \to \frac{\alpha}{\pi}$. Mas, $r_n \to \frac{\alpha}{\pi} \Leftrightarrow \left(\frac{p_n}{q_n}\pi\right) \to \alpha$, ou seja, números $t = 2cos(\theta)$ para θ um múltiplo racional de π são densos no intervalo $[-2, +2]$. Desde que a aplicação levando r em t_n é um homeomorfismo do intervalo $[0, 1]$ em $[-2, 2]$, segue que os valores de r para os quais G não é livre são densos no intervalo $[0, 1]$.

$\square$

Exemplo 3.18. ***(Grupos Schottky)*** *Seja G agindo em $S = \mathbb{C} \cup \{\infty\}$ e sejam g_1 e g_2 como no exemplo 2.7. Então, g_1 e g_2 geram um grupo livre em G.*

De fato, considere $S_1 = Int(C_1) \cup Int(C_3)$ e $S_2 = Int(C_2) \cup Int(C_4)$ temos $g_1(S_2) \subset Int(C_3) \subset S_1$, $g_2(S_1) \subset Int(C_4) \subset S_2$ e S_2 não contido em S_1; aplicando novamente o Critério de Klein temos que $< g_1 > * < g_2 >$ é livre.

O grupo gerado por g_1 e g_2 é descontínuo em um subconjunto não-vazio de $\mathbb{C} \cup \{\infty\}$,como vimos no capítulo 2.

Exemplo 3.19. ***(de Hausdorff no grupo de rotações)***

Considere g uma rotação de $180°$ de $\mathbb{R}^3$, h uma rotação de $120°$ de $\mathbb{R}^3$ e o ângulo entre os eixos sendo $45°$. Então, g e h geram em $SO(3)$ um grupo isomorfo a $(\mathbb{Z}/2\mathbb{Z}) * (\mathbb{Z}/3\mathbb{Z})$; assim, $ghgh^2$ e gh^2gh geram um grupo livre de rotações em $SO(3)$.

De fato, considere coordenadas tais que:

$$g = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \text{ e } h = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{-1}{2} & \frac{\sqrt{3}}{2} \\ 0 & \frac{-\sqrt{3}}{2} & \frac{-1}{2} \end{pmatrix}$$

Para qualquer inteiro $K > 0$ e para qualquer sequência $n_1, ..., n_k$, com $n_j \in \{1, 2\}$, verificaremos indutivamente que existem inteiros pares $p_1, .., p_5$ e inteiros ímpares $q_1, ..., q_4$ com:

$$h^{n_1}gh^{n_2}g...h^{n_k}g = 2^{-k} \begin{pmatrix} p_1 & p_2 & p_3\sqrt{3} \\ q_1 & p_4 & q_2\sqrt{3} \\ q_3\sqrt{3} & p_5\sqrt{3} & q_4 \end{pmatrix}$$

Indução em n_i:

$(1°)$ $i = 1 :$ $n_1 = 1$ *ou* $n_1 = 2$

$$(2h)g = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & \sqrt{3} \\ 0 & -\sqrt{3} & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 0 \\ -1 & 0 & -\sqrt{3} \\ -\sqrt{3} & 0 & 1 \end{pmatrix}$$

$$(2h^2)g = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & -\sqrt{3} \\ 0 & \sqrt{3} & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & \sqrt{3} \\ \sqrt{3} & 0 & 1 \end{pmatrix}$$

(2°) *suponhamos que vale para $i = k$, ou seja:*

$$(2h^{n_1})g(2h^{n_2})g...(2h^{n_k})g = \begin{pmatrix} p_1 & p_2 & p_3\sqrt{3} \\ q_1 & p_4 & q_2\sqrt{3} \\ q_3\sqrt{3} & p_5\sqrt{3} & q_4 \end{pmatrix}$$

e provemos que vale para $i = k + 1$:

$$(2h^{n_1})g...(2h^{n_k})g...(2h^{n_{k+1}})g = \begin{pmatrix} p_1 & p_2 & p_3\sqrt{3} \\ q_1 & p_4 & q_2\sqrt{3} \\ q_3\sqrt{3} & p_5\sqrt{3} & q_4 \end{pmatrix} \begin{pmatrix} 0 & 2 & 0 \\ -1 & 0 & -\sqrt{3} \\ -\sqrt{3} & 0 & 1 \end{pmatrix} =$$

(para $n_{k+1} = 1$)

$$\begin{pmatrix} -p_2 - 3p_3 & 2p_1 & -\sqrt{3}p_2 + p_3\sqrt{3} \\ -p_4 - 3q_2 & 2q_1 & -\sqrt{3}p_4 + \sqrt{3}q_2 \\ -p_5\sqrt{3} - q_4\sqrt{3} & 2q_3\sqrt{3} & -3p_5 + q_4 \end{pmatrix} = \begin{pmatrix} par & par & par\sqrt{3} \\ impar & par & impar\sqrt{3} \\ impar\sqrt{3} & par\sqrt{3} & impar \end{pmatrix}.$$

Para $n_{k+1} = 2$ é análogo.

Como um inteiro impar é não zero,uma tal palavra não pode representar a rotação identidade. Qualquer palavra reduzida em g e h é como acima, digamos w, ou de uma das seguintes formas: w^{-1}, wg, gw. Temos então que o grupo gerado por g e h é isomorfo a $(\mathbb{Z}/2\mathbb{Z}) * (\mathbb{Z}/3\mathbb{Z})$, pois $o(g) = 2$, $o(h) = 3$ e como não existe relação entre g e h, $< g > * < h >$ é produto livre. Portanto, $ghgh^2$ e gh^2gh geram um subgrupo livre F em $SO(3)$.

Observação 3.20. *Em 1914, este exemplo permitiu Hausdorff provar o próximo teorema.*

O paradoxo de Hausdorff-Banach-Tarski

A demonstração de Hausdorff sobre o paradoxo consiste basicamente em fazer uma partição da esfera S^2 *em 5 subconjuntos, sendo que para isso é escolhida uma transversal muito peculiar.*

Antes de enunciarmos o teorema, explicitaremos como é feita esta partição:

Seja $F =< X, Y >$ *um grupo livre de rotações em* $SO(3)$*(o qual existe pelo exemplo 3.19). Dividimos* F *dentre os cinco conjuntos* $E, X, \overline{X}, Y, \overline{Y}$ *consistindo respectivamente da identidade e dos elementos, os quais, quando escritos na forma reduzida, começam com* x, x^{-1}, y *e* y^{-1}*.*

Observemos que temos uma partição de S^2 *dada pela equação das classes:*

Se $P_1, P_2, ..., P_n, ...$ *são pontos de* S^2 *e* $FP_1, FP_2, ..., FP_n, ...$ *são as órbitas de* $P_1, ..., P_n, ...$ *respectivamente, então:*

$$S^2 = FP_1 \cup FP_2 \cup ... \cup FP_n \cup ...,$$

sendo que essas uniões são claramente disjuntas, pois as órbitas são disjuntas.

Agora, pelo axioma da escolha, selecionamos uma transversal T*, escolhendo um ponto de* S^2 *em cada uma das distintas* F*-órbitas da ação de* F *sobre* S^2 *e mostremos que os cinco subconjuntos:*

$$T, XT, \overline{X}T, YT, \overline{Y}T$$

também formam uma partição de S^2 *:*

$$S^2 = T \cup XT \cup \overline{X}T \cup YT \cup \overline{Y}T$$

Primeiramente mostremos que a união acima é, de fato, disjunta:

$1°)T \cap XT = \emptyset$. *De fato, seja* $P \in T$. *Se* $P \in XT \Rightarrow \exists\ Q \in T; P = xQ \Rightarrow P \in FQ \Rightarrow P = Q$ *(pois na contrução foi escolhido um único ponto em cada órbita). Logo,* $x = id$ *e portanto,* $T \cap XT = \emptyset$. *De maneira análoga provamos que* $T \cap \overline{X}T = \emptyset$, $T \cap YT = \emptyset$ *e* $T \cap \overline{Y}T = \emptyset$.

$2°)$ *Mostremos que* $RT \cap ST = \emptyset$, *para* $R, S \in \{X, \overline{X}, Y, \overline{Y}\}$, *com* $R \neq S$. *De fato,* $RT \cap ST = \emptyset \Leftrightarrow T \cap (R^{-1}S)T = \emptyset$. *Mas, como* $R \neq S$ *temos* $R^{-1}S \neq E$ *e então caímos no* $1°$ *caso e obtemos que* $XT \cap \overline{X}T = \emptyset, XT \cap YT = \emptyset, XT \cap \overline{Y}T = \emptyset, YT \cap \overline{X}T = \emptyset, YT \cap \overline{Y}T = \emptyset$ *e* $\overline{Y} \cap \overline{X}T = \emptyset$.

Agora, mostremos que os 5 subconjuntos cobrem S^2*:*
Seja $P \in S^2$. *Podemos assumir que* $P \notin T$. *Logo,* $\exists\ Q \in T; P = fQ \Rightarrow P \in FQ$. *Mas,* $fQ \in EQ \cup XQ \cup \overline{X}Q \cup YQ \cup \overline{Y}Q$.

Teorema 3.21. *Não existe medida finitamente aditiva invariante por rotações definida em toda esfera $S^2 \subset \mathbb{R}^3$.*

Demonstração. Suponha, por absurdo, que existe uma tal medida. Como vimos os cinco subconjuntos $T, XT, \overline{X}T, YT, \overline{Y}T$ formam uma partição de S^2 :

$$S^2 = T \cup XT \cup \overline{X}T \cup YT \cup \overline{Y}T$$

Agora, observe que a rotação x leva $\overline{X}T$ em:

$$S^2 - XT = T \cup \overline{X}T \cup YT \cup \overline{Y}T$$

e de maneira similar, a rotação y leva $\overline{Y}T$ em:

$$S^2 - YT = T \cup XT \cup \overline{X}T \cup \overline{Y}T$$

Logo, $x\overline{X}T \cup XT = S^2 \Rightarrow \mu(x\overline{X}T \cup XT) = \mu(x\overline{X}T) + \mu(XT) = \mu(\overline{X}T) + \mu(XT) = \mu(S^2) \quad (*)$
e
$y\overline{Y}T \cup YT = S^2 \Rightarrow \mu(y\overline{Y}T \cup YT) = \mu(y\overline{Y}T) + \mu(YT) = \mu(\overline{Y}T) + \mu(YT) = \mu(S^2) \quad (**)$

De $(*)$ e $(**)$, temos:

$$\mu(XT \cup \overline{X}T \cup YT \cup \overline{Y}T) = 2\mu(S^2)$$

Absurdo, pois: $\mu(XT \cup \overline{X}T \cup YT \cup \overline{Y}T) \leq \mu(S^2)$.

□

Referências Bibliográficas

[1] A. Armando de Castro Jr., Curso de Teoria da Medida,Projeto Euclides, IMPA, 2004

[2] Alan F. Beardon, The Geometry of Discrete Groups, Springer-Verlag, Newyork Heidelberg Berlin. Graduate Texts in Mathematics 91 (1983)

[3] J. Tits, Free Groups in Linear Groups, J. of Algebra 2 [20], 1972,p.250-270

[4] Pierre Deligne and Dennis Sullivan, division Algebras and the Hausdorff-Banach-Tarski Paradox, L'Enseignement Mathematique, t.29(1983), p.145-150

[5] Pierre de La Harpe, Free groups in linear groups, L'Enseignement Mathematique, t.29(1983), p.129-144

[6] R.C.Lyndon and J.L.Ullman, Groups generated by two parabolic linear fractional transformations, Canad. J. math. 21 (1969), 1388-1403

[7] Serge Lang, Algebra, Addison-Wesley Publishing Company. Inc., 1965

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo