Grupos Fuchsianos

Kelvyn Welsch

Novembro de 2019

Conteúdo

1 Introdução

Este texto visa a introduzir o conceito e algumas propriedades dos grupos fuchsianos. Especificamente, nosso objetivo é provar alguns resultados sobre a dimensão Hausdorff do conjunto limite de grupos fuchsianos de segunto tipo, resultado este devido a Patterson [ref]. Grupos fuchsianos são uma classe de grupos que possuem ligações com diversas áreas da matemática, tais quais geometria hiperbólica, geometria projetiva e análise complexa. Os grupos fuchsianos foram nomeado em homenagem a Lazarus Fuchs (1833-1902), sendo Poincaré o primeiro a se debruçar mais profundamente sobre o estudo deles.

A fim de termos um melhor aproveitamento sobre o assunto, iremos recordar alguns resultados de teoria de grupos e topologia, além de dar um panorama geral sobre geometria hiperbólica antes de lidarmos com os grupos fuchsianos propriamente ditos. Naturalmente, leitores mais confortáveis com os requisitos podem pular esta parte introdutória. De modo geral, espera-se que o leitor saiba, no mínimo, a definição de um grupo e de uma topologia.

2 Teoria de Grupos

2.1 Homomorfismos

Definição 2.1. Sejam $(G, \cdot)$, $(H, *)$ grupos. Uma função $h : G \to H$ é dita um *homomorfismo de grupos* se $h(a \cdot b) = h(a) * h(b)$, $\forall a, b \in G$. Quando um homomorfismo é injetivo, sobrejetivo e bijetivo, dizemos que é um monomorfismo, epimorfismo e isomorfismo, respectivamente. Quando o domínio e o contradomínio são idênticos, dizemos que se trata de um endomorfismo. Um automorfismo é um endomorfismo que também é um isomorfismo. ♣

Dizemos que um homomorfismo de grupos é uma função que preserva a estrutura de grupo. A razão para isto é a que se segue. Por definição, um homomorfismo preserva a operação de grupo. Além disso, a proposição abaixo nos diz que o elemento neutro e a operação de elemento inverso também são preservadas. Em outras palavras, um homomorfismo mapeia elemento neutro em elemento neutro e o homomorfismo do inverso é o inverso do homomorfismo.

A partir de agora iremos deixar de enfatizar e distinguir os símbolos das operações dos grupos, pelo bem da sanidade mental.

Proposição 2.1. *Sejam G, H grupos e $h : G \to H$ um homomorfismo. Se e_G e e_H são os elementos neutros de G e H, respectivamente, vale que $h(e_G) = e_H$. Além disso, se $g \in G$, então $h(g^{-1}) = h(g)^{-1}$.* ▫

Demonstração. Tome $g \in G$, qualquer. Teremos que $g = e_G \cdot g \implies h(g) = h(e_G) \cdot h(g) \implies h(g) \cdot h(g)^{-1} = h(e_G) \cdot h(g) \cdot h(g)^{-1} \implies e_H = h(e_G) \cdot e_H \implies e_H = h(e_G)$.

Usando isso, $e_G = g \cdot g^{-1} \implies e_H = h(g) \cdot h(g^{-1}) \implies h(g)^{-1} = h(g)^{-1} \cdot h(g) \cdot h(g^{-1}) = e_H \cdot h(g^{-1}) = h(g^{-1}) \implies h(g)^{-1} = h(g^{-1})$. ■

Definição 2.2. Sejam G e H grupos e $h : G \to H$ um homomorfismo. O *núcleo* de h é o conjunto $\ker h$ definido por $\ker h := \{g \in G; h(g) = e_H\}$. A *imagem* de h é o conjunto Im $h := \{b \in H; \exists g \in G \text{ com h(g) = b}\}$ ♣

Proposição 2.2. *Sejam G e H grupos e $h : G \to H$ um homomorfismo. Vale que* $\ker h$ *é subgrupo de G e Im h é subgrupo de H.* □

Demonstração. Vejamos que $\ker h$ é subgrupo de G. Basta mostrarmos que, se $g, f \in \ker h$, arbitrários, então $gf \in \ker h$ e $g^{-1} \in \ker h$. Pela proposição 2.1, $e_H = h(e_G) = h(gg^{-1}) = h(g)h(g^{-1})$. Mas $h(g) = e_H$, donde $e_H = e_H h(g^{-1}) \implies h(g^{-1}) = e_H$ e assim $g^{-1} \in \ker h$. Se, ainda, $f \in \ker h$ então $h(gf) = h(g)h(f) = e_H e_H = e_H \implies h(gf) = e_H$, donde $gf \in \ker h$. Vejamos agora que Im h é subgrupo de H. Seja $g \in$ Im h. Então existe $a \in G$ tal que $g = h(a)$. Ora, $h(a^{-1}) = h(a)^{-1} = g^{-1}$, donde existe um elemento de G (a saber, a^{-1})) tal que g^{-1} é sua imagem. E portanto $g^{-1} \in$ Im h. Suponhamos, ainda, que $f \in$ Im h. Mostrarei que $gf \in$ Im h. Por definição, existe um $b \in G$ tal que $h(b) = f$. Teremos: $h(ab) = h(a)h(b) = gf$. Assim, existe um elemento de G (a saber, ab) tal que $h(ab) = gf$, e portanto $gf \in$ Im h. Desta forma, concluímos a nossa demonstração. ■

Proposição 2.3. *Sejam G e H grupos e $\theta : G \to H$ um homomorfismo. Dado $M, N \in G$, vale que $\theta(M) = \theta(N) \iff MN^{-1} \in \ker \theta$.* □

Demonstração. $\theta(M) = \theta(N) \iff \theta(M)\theta(N)^{-1} = e_H \iff \theta(MN^{-1}) = e_H \iff MN^{-1} \in \ker \theta$. ■

2.2 Classes de Conjugação e Subgrupos Normais

Definição 2.3. Seja G um grupo. Dois elementos $a, b \in G$ são ditos *conjugados* se existe $g \in G$ tal que $gag^{-1} = b$ ♣

Proposição 2.4. *Seja G um grupo. A relação $\sim$ tal que $a \sim b$ se, e somente se a e b forem conjugados é uma relação de equivalência. As classes de equivalência por tal $\sim$ são chamadas de* classes de conjugação. □

Demonstração. (i) Reflexividade. Dado $a \in G$, para ver que $a \sim a$, basta tomarmos $g = e$. Daí $eae^{-1} = eae = a$. (ii) Simetria. Sejam $a, b \in G$ tais que $a \sim b$. Então existe $g \in G$ tal que $gag^{-1} = b$. Mas daí, $ga = bg$ e $a = g^{-1}bg$. Tomando $h = g^{-1}$ teremos $hbh^{-1} = a$, donde $b \sim a$. (iii) Transitividade. Suponhamos que $a \sim b$ e $b \sim c$. Então existem $g, h \in G$ tais que $gag^{-1} = b$ e $hbh^{-1} = c$. Então teremos $(hg)a(hg)^{-1} = hgag^{-1}h^{-1} = hbh^{-1} = c$, donde $a \sim c$. ■

Elementos conjugados de um grupo costumam possuir propriedades semelhantes. No caso dos grupos estudados por nós, elementos conjugados se relacionam, por exemplo, quanto aos seus pontos fixos (lembre-se de que são funções). Destacamos que os elementos conjugados de um grupo de matrizes são chamados de matrizes semelhantes. É fácil ver também que, em um grupo abeliano, as classes de conjugação são conjuntos unitários, uma vez que, $\forall g \in G$, $gag^{-1} = gg^{-1}a = a$.

Definição 2.4. Sejam G um grupo e $N \subset G$ um subgrupo. Dizemos que N é um *subgrupo normal* se, $\forall g \in G$, $\forall n \in N$, $gng^{-1} \in N$. ♣

Da definição, segue diretamente que qualquer subgrupo de grupos abelianos é normal. Este resultado também pode ser enunciado como corolário da proposição 2.5 a seguir. Além disso, é trivial ver que, em qualquer grupo G, os subgrupos $\{e_G\}$ e o próprio G são subgrupos normais. Estes subgrupos normais são chamados de subgrupos triviais.

Como pode se esperar, o conceito de subgrupo normal está intimamente relacionado ao conceito de elementos conjugados. Se $n \in N$ (N normal), então todos os seus elementos conjugados também pertencem a N. Em outras palavras, $[n] \subset N$, onde $[n]$ é a classe de conjugação de N. Com esta observação, fica evidente provar a seguinte proposição:

Proposição 2.5. *Sejam G um grupo e $N \subset G$ um subgrupo. Então N é normal se, e somente se, é a união de classes de conjugação de G.* □

Definição 2.5. Um grupo é dito simples quando seus únicos subgrupos normais são os triviais. ♣

Proposição 2.6. *Sejam G, H grupos e $h : G \to H$ um homomorfismo. O núcleo de h é um subgrupo normal de G.* □

Demonstração. Pela proposição 2.2, já sabemos que $\ker h$ é um subgrupo. Falta provarmos que é normal. Queremos provar que, dado $n \in \ker h$ e $g \in G$, $h(gng^{-1}) = e_H$. Ora, $h(gng^{-1}) = h(g)h(n)h(g)^{-1}$. Usando que $n \in \ker h$: $h(gng^{-1}) = h(g)e_H h(g)^{-1} = e_H$. ■

2.3 Cosets e Grupo Quociente

Dado um subgrupo H de G, podemos criar classes de equivalência em G. Estas classes de equivalência se fazem "transladando" H com elementos de G. Estas classes de equivalência são chamadas de *cosets*. Como a operação de grupo não necessariamente é comutativa, podemos ter cosets à direita ou cosets à esquerda. Esta noção, unida com a de subgrupo normal, irá nos conduzir ao conceito de grupo quociente, muito importante neste texto. Precisamente, temos a seguinte

Definição 2.6. Sejam G um grupo e $H \subset G$ um subgrupo. Dado $g \in G$, o conjunto $gH := \{gh; h \in H\}$ é chamado de *coset à esquerda de H com relação a g* e o conjunto $Hg := \{hg; h \in H\}$ é chamado de *coset à direita de H com relação a g.* ♣

Proposição 2.7. *Sejam G um grupo e $H \subset G$ um subgrupo. Sejam também $\sim_D$ e $\sim_E$ as relações em G tais que $x \sim_D y$ se, e somente se existe $h \in H$ tal que $x = hy$ e $x \sim_E y$ se, e somente se existe $h \in H$ tal que $x = yh$. Então vale que ambas são relações de equivalência e além disso, $D \subset G$ é coset à direita de H se e somente se existe $g \in G$ tal que $D = [g]_D$ e $E \subset G$ é coset à esquerda de H se, e somente se existe $g \in G$ tal que $E = [g]_E$.* □

Demonstração. Provemos que $\sim_D$ é uma relação de equivalência: (i) (reflexiva) Tome $g \in G$. Como H é subgrupo, $e_G \in H$. Assim, existe $h \in H$ tal que $g = gh$ (a saber, $h = e_G$), donde $g \sim_D g$. (ii) (simétrica) Sejam $x, y \in G$ tais que $x \sim_D y$. Então existe $h \in H$ tal que $x = yh$. Como H é subgrupo, $h^{-1} \in H$. Assim, $x = yh \implies xh^{-1} = y$, donde $y \sim_D x$. (iii) (transitiva) Sejam $x, y, z \in G$ tais que $x \sim_D y$ e $y \sim_D z$. Então existem $g, h \in H$ tais que $x = yg$ e $y = zh$. Estas duas igualdades implicam $x = (zh)g = z(hg)$. Ora, $hg \in H$, por motivos óbvios, donde $x \sim_D z$.

Se D é coset à direita de H, por definição, existe $g \in G$ tal que $D = gH$. Assim, $x \in D$ se, e somente se, existe $h \in H$ tal que $x = gh$, que é equivalente a dizer que $x \sim_D g$, e portanto $x \in D$ se, e somente se $x \in [g]_D$. Portanto, $D = [g]_D$.

Os casos para cosets à esquerda e $\sim_E$ se faz de modo análogo. ■

Sob certas hipóteses, os cosets à direita e à esquerda coincidem. Nestes casos, o conjunto dos cosets forma um grupo. Este grupo, derivado das classes de equivalências, é chamado de grupo quociente. As hipóteses suficientes e necessárias para que isto ocorra é que H seja um subgrupo normal de G. (vemos aqui, finalmente, a utilidade da definição de subgrupo normal). Estes resultados estão formalmente enunciados a seguir:

Proposição 2.8. *Sejam G um grupo e N um subgrupo de G. Uma condição necessária e suficiente para que $gN = Ng$, $\forall g \in G$ é que N seja um subgrupo normal de G.* □

Demonstração. Por definição, $x \in gN$ se, e somente se existe $n \in N$ tal que $x = gn$. Isto, porém, é verdade se, e somente se $xg^{-1} = gng^{-1}$. Mas $x \in Ng$ se, e somente se existe $m \in N$ tal que $xg^{-1} = m$, ou seja, se, e somente se $xg^{-1} = gng^{-1} \in N$. Concluímos que $gN = Ng$ se, e somente se $gng^{-1} \in N$, $\forall g \in G$, $\forall n \in N$, que é precisamente a definição de N ser normal. ■

Proposição 2.9. *Sejam G um grupo e N um subgrupo normal de G. Então o conjunto $G/N = \{gN = Ng; g \in G\}$, munido da operação $(gN)(hN) = ghN$ forma um grupo, chamado de* grupo quociente de G por N, *onde $e_G N = N$ é o elemento neutro e $g^{-1}N$ é o elemento inverso de gN.* □

Aqueles que estão mais habituados com álgebra linear hão de perceber a semelhança entre as definições de grupo quociente e espaço quociente. Perceberão também o quão mais fácil é definir o segundo (sem necessidade de recorrer a objetos análogos aos cosets à esquerda e à direita). Isto se deve ao fato de, num espaço vetorial, as operações serem comutativas.

Além de útil na definição de grupo quociente, os cosets desempenham papel fundamental na demonstração do Teorema de Lagrange, que será enunciado aqui apenas à título de informação.

Definição 2.7. Seja G um grupo. A ordem de G é definida como a cardinalidade do conjunto G. Um grupo G é dito finito se tem ordem finita ♣

Teorema 2.10. *(Teorema de Lagrange) Sejam G um grupo finito e $H \subset G$ um subgrupo. Então a ordem de G é múltipla da ordem de H.* ▫

Enfatizo que "ordem de um elemento"é um conceito diferente de "ordem de um grupo"e será tratada na seção 2.9.

2.4 Homomorfismo Revisitado

Existem alguns tipos de grupos quocientes que são de particular interesse. Um deles é aquele quocientado pelo núcleo de um homomorfismo. Este caso possui um resultado importante que será contemplado pelo Primeiro Teorema de Isomorfismos. Antes dele, vejamos um teorema mais geral, que é um dos resultados mais importantes deste capítulo.

Teorema 2.11. *(Teorema Fundamental de Homomorfismos). Sejam G e H grupos e $\phi : G \to H$ um homomorfismo. Seja N um subgrupo normal de G tal que $N \subset \ker \phi$. Então a função $\psi : G/N \to H$ definida por $\psi(gN) = \phi(g)$ é um homomorfismo.* ▫

Corolário 2.11.1. *(Primeiro Teorema de Isomorfismos). Existe um isomorfismo ψ entre $G/\ker \phi$ e Im ϕ dado por $\psi(g \ker \phi) = \phi(g)$* ▫

Corolário 2.11.2. *Se ϕ é um epimorfismo, então existe um isomorfismo ψ entre $G/\ker \phi$ e H dado por $\psi(g \ker \phi) = \phi(g)$* ▫

2.5 Comutatividade

O objetivo desta seção é usar as ferramentas que já temos para medir o quão abeliano um grupo é. Começaremos definindo o centro de um grupo (ou centralizador).

Definição 2.8. Seja G um grupo. O *centro de G* é o subconjunto de G definido por: $Z(G) := \{z \in G; zg = gz, \forall g \in G\}$. ♣

Em palavras, o centro de um grupo é o conjunto dos elementos que comutam com todos os outros. Enfatizo que este conjunto nunca é vazio, pois contém sempre o elemento neutro de G. Mais ainda:

Proposição 2.12. *Sejam G um grupo e $Z(G)$ seu centro. Vale que $Z(G)$ é um subgrupo normal de G.* ▫

Demonstração. Suponha que $x, y \in Z(G)$. Quero provar que $xy \in Z(G)$. Para tanto, tome $g \in G$ arbitrário. Pela associatividade, e como $y \in Z(G)$, $xyg = xgy$. Como $x \in Z(G)$, $xgy = gxy$. Assim, $(xy)g = g(xy)$. Pela arbitrariedade de g, resta-nos que $xy \in Z(G)$. Provaremos também que $x^{-1} \in Z(G)$. Ora, $xg = gx \implies g = x^{-1}gx \implies gx^{-1} = x^{-1}g$. Concluímos que $Z(G)$ é de fato subgrupo de G.

Falta provar que $Z(G)$ é normal. Ora, dados $z \in Z(G)$ e $g \in G$, $gzg^{-1} = gg^{-1}z = z \in Z(G)$. Isto completa nossa demonstração. ∎

Como o leitor pode imaginar, enfatizar que o centro de um grupo é um subgrupo normal revela que iremos tomar o quociente do grupo pelo centro em algum momento. O leitor está correto. Antes disto, porém, enunciaremos uma definição que nos permitirá entender melhor o significado de $G/Z(G)$.

Definição 2.9. Seja G um grupo. Dado $g \in G$, a função $\phi_g : G \to G$ definida por $\phi_g(h) = ghg^{-1}$ é chamada de *automorfismo interno*. O conjunto de todos automorfismo internos de um grupo G é denotado por $\mathrm{Inn}(G)$. ♣

Proposição 2.13. *Os automorfismos internos de um grupo G são de fato automorfismos. Além disso, Inn(G) é um grupo sob a operação de composição.* □

Demonstração. Precisamos mostrar que, dado $g \in G$, ϕ_g é um isomorfismo. Primeiramente, vamos mostrar que $\phi_g(xy) = \phi_g(x)\phi_g(y)$. De fato, por definição, $\phi_g(xy) = gxyg^{-1} = gxeyg^{-1}$, onde e é o elemento neutro. Como $g^{-1}g = e$, $\phi_g(xy) = gxg^{-1}gyg^{-1} = (gxg^{-1})(gyg^{-1}) = \phi_g(x)\phi_g(y)$. Agora já sabemos que ϕ_g se trata de um endomorfismo. Só falta ver que ϕ_g é uma bijeção. Seja $y \in G$. Tome $x = g^{-1}yg \in G$. Então $\phi_g(x) = y$. De fato, $\phi_g(x) = gg^{-1}ygg{-}1 = eye = y$, e portanto ϕ_g é sobrejetiva. Suponha agora que $x \neq y$. Então $gx \neq gy \implies gxg^{-1} \neq gyg^{-1} \implies \phi_g(x) \neq \phi_g(y)$, donde ϕ_g é injetiva e, portanto, um automorfismo.

Falta mostrar que $\mathrm{Inn}(G)$ é um grupo. Inicialmente, mostraremos que a operação de composição está bem definida neste conjunto. Seja ϕ_g e ϕ_h elementos de $\mathrm{Inn}(G)$. Note que $\phi_g \circ \phi_h : G \to G$ é dada por $x \mapsto ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \phi_{gh}(x)$, donde $\phi_g \circ \phi_h = \phi_{gh} \in \mathrm{Inn}(G)$. Automaticamente temos que esta operação é associativa, pois a composição de funções o é. Afirmamos que ϕ_e (onde e é o elemento neutro de G) é o elemento neutro de $\mathrm{Inn}(G)$. De fato, como vimos, $\phi_g \circ \phi_e = \phi_{ge} = \phi_g = \phi_{eg} = \phi_e \circ \phi_g$. Finalmente, dado $\phi_g \in \mathrm{Inn}(G)$, mostraremos que seu elemento oposto é ϕ_h, onde $h = g^{-1}$. Ora, $\phi_g \circ \phi_h = \phi_{gh} = \phi_e$, o elemento neutro. ∎

Proposição 2.14. *Sejam G um grupo e Inn(G) o grupo de automorfismos internos de G. Então a função $\theta : G \to$ Inn(G) que associa a cada $g \in G$ o automorfismo interno ϕ_g, isto é, $\theta(g) = \phi_g$, é um epimorfismo.* □

Demonstração. Para provar que é um homomorfismo, basta ver que $\theta(gh) = \phi_{gh} = \phi_g \circ \phi_h$ (a última igualdade está provada na demonstração da proposição 2.13). Ademais, por definição de $\mathrm{Inn}(G)$, temos que se $f \in \mathrm{Inn}(G)$, então existe $g \in G$ tal que $f = \phi_g = \theta(g)$, por definição de θ. E portanto, θ é sobrejetiva. ∎

Proposição 2.15. *Seja G um grupo. $g \in Z(G) \iff \phi_g = \phi_e$. Em outras palavras,* $\ker\theta = Z(G)$. ▫

Demonstração. $g \in Z(G) \implies \phi_g(x) = gxg^{-1} = gg^{-1}x = x = exe^{-1} = \phi_e(x)$. Reciprocamente, $\phi_g = \phi_e \implies \phi_g(x) = x$, $\forall x \in G \implies gxg^{-1} = x \implies gx = xg$, $\forall x \in G$.

A segunda afirmação se prova com a seguinte sequências de desigualdades: $g \in \ker\theta \iff \theta(g) = \phi_e \iff \phi_g = \phi_e \iff g \in Z(G)$. ■

A proposição acima mostra que um elemento de G faz parte do centro se, e somente se o homomorfismo θ definido anteriormente o mapeia para a identidade (i.e. para o elemento neutro de $\mathrm{Inn}(G)$). Vemos então que, quanto mais abeliano um grupo é, maior é seu centro e mais elementos são mapeados por θ para a identidade. Uma outra forma de ver isto é a seguinte: quanto menos abeliano é um grupo, mais automorfismos internos existem (distintos da identidade). Desta forma, o tamanho do centro de um grupo é "inversamente proporcional" ao tamanho do grupo de automorfismos internos deste. A intuição nos diz, então, que deve existir uma certa relação entre $G/Z(G)$ e $\mathrm{Inn}(G)$ e é precisamente isto que o corolário abaixo diz. Esta relação é, na verdade, um isomorfismo!

Corolário 2.15.1. *$G/Z(G) \cong Inn(G)$.*

Demonstração. Basta aplicar as Proposições 2.14 e 2.15 no Corolário 2 do Teorema 2.11. Existirá um isomorfismo ψ entre $G/ker\theta = G/Z(G)$ e $\mathrm{Inn}(G)$ dado por $\psi(gZ(G)) = \theta(g) = \phi_g$. ■

2.6 Ações de Grupos

O cerne do estudo dos grupos é "simetria". Este fato é bem conhecido mas, à primeira vista, a definição de um grupo não parece estar nitidamente relacionada com simetria. Isto porque os elementos de um grupo, a grosso modo, são as transformações de simetria em si, desprovidas do objeto a qual se referem. Esta é a motivação da definição de ação de um grupo. A ação de um grupo é a razão de ser de um grupo, aquilo para o qual ele foi construído. Como o nome indica, a ação de um grupo torna explícito a atuação de um grupo num objeto que possui simetrias. Novamente, devido ao fato de um grupo não ser necessariamente comutativo, podemos ter dois tipos de ação, à esquerda e à direita. Sem mais delongas, passemos à definição formal.

Definição 2.10. Sejam M um conjunto não-vazio e G um grupo. Seja $\alpha : G \times M \to M$ uma função. Considere as seguintes propriedades:

1) Dado $g \in G$, a função $\alpha(g, \cdot) : M \to M$ é bijetiva

2) Se e é o elemento neutro de G, então a função $\alpha(e, \cdot) : M \to M$ é a identidade. Ou seja, $\alpha(e, x) = x$, $\forall x \in M$.

3e) Vale $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$, $\forall g, h \in G$, $\forall x \in M$

3d) Vale $\alpha(g, \alpha(h, x)) = \alpha(hg, x)$, $\forall g, h \in G$, $\forall x \in M$

Se α satisfaz 1, 2 e 3e, então é α é dita ser uma ação à esquerda de G. Se for 1, 2, 3d, α é dita ser uma ação à direita de G. ♣

Note que se G é comutativo, ações à direita e à esquerda empatam. Quando dissermos apenas "ação", estará subentendido que pode se tratar de uma ação à direta ou à esquerda.

Vamos olhar com mais atenção a esta definição e extrair o significado intuitivo de cada propriedade. Dado um elemento g do grupo, a função $\alpha(g, \cdot) : M \to M$ se torna uma transformação de simetria de M. Nada mais justo do que ser bijetiva. A condição 2 apenas impõe que a transformação de simetria que não faz nada (a identidade), corresponda ao elemento neutro. A terceira condição é a mais interessante. Ela diz que realizar uma transformação de simetria por g em M já transformado por h deve corresponder à transformação de simetria composta gh ou hg. Em outras palavras, aplicar h e depois aplicar g deve empatar com aplicar gh (ou hg) de uma vez só.

Existem algumas características de ações que são importantes de serem vistas. Uma delas é a transitividade:

Definição 2.11. Sejam G um grupo e $\alpha : G \times M \to M$ uma ação de G em M. α é dita *transitiva* se, $\forall x, y \in M$, existir $g \in G$ tal que $y = \alpha(g, x)$. Será dita *simplesmente transitiva* quando tal g for único. Mais ainda, α é dita ser *k-transitiva* se, para todo par de k-uplas $(x_1, ..., x_k)$ e $(y_1, ..., y_k)$ com elementos distintos dois a dois, existir um $g \in G$ tal que $y_i = \alpha(g, x_i)$, $1 \leqslant i \leqslant k$. ♣

Definição 2.12. Sejam G um grupo e $\alpha : G \times M \to M$ uma ação de G em M. Dado $m \in M$, a *órbita de m pela ação de α* é o conjunto $Orb_\alpha(m) := \{\alpha(g, m); g \in G\}$. ♣

Em palavras, a órbita de m por α é o conjunto dos pontos de M que m pode assumir, considerando todas as transformações de simetria que G pode oferecer através de α. A proposição seguinte abrirá o caminho para uma definição alternativa de ação transitiva.

Proposição 2.16. *Sejam G um grupo e $\alpha : G \times M \to M$ uma ação de G em M. Dado $m \in M$, vale que $n \in Orb_\alpha(m) \implies Orb_\alpha(n) = Orb_\alpha(m)$.* ▫

Demonstração. Suponhamos que α seja uma ação à esquerda. Mostraremos inicialmente que $Orb_\alpha(n) \subset Orb_\alpha(m)$. Seja $x \in Orb_\alpha(n)$. Então existe $g \in G$ tal que $\alpha(g, n) = x$. Por outro lado, como $n \in Orb_\alpha(m)$, então existe $h \in G$ tal que $\alpha(h, m) = n$. Ora, substituindo uma coisa na outra, $x = \alpha(g, \alpha(h, m)) = \alpha(gh, m)$, em que usamos a definição de ação à esquerda. A última igualdade mostra que $x \in Orb_\alpha(m)$.

Veja que mostramos a seguinte implicação: $n \in Orb_\alpha(m) \implies Orb_\alpha(n) \subset Orb_\alpha(m)$. Trocando o papel das letras, teremos: $m \in Orb_\alpha(n) \implies Orb_\alpha(m) \subset Orb_\alpha(n)$. Assim, se mostramos que $n \in Orb_\alpha(m) \implies m \in Orb_\alpha(n)$, obteremos automaticamente a igualdade desejada. Novamente, a hipótese nos leva a crer que existe $h \in G$ com $\alpha(h, m) = n$. Pela definição de ação, $\alpha(e, m) = m$. Donde $\alpha(h^{-1}h, m) = m \implies \alpha(h^{-1}, \alpha(h, m)) = m \implies \alpha(h^{-1}, n) = m$ e portanto $m \in Orb_\alpha(n)$.

Para ações à direita, a demonstração é análoga. ∎

Corolário 2.16.1. *A relação definida por* $m \sim n$ *se, e somente se* $m \in Orb_\alpha(n)$ *é uma relação de equivalência. (e portanto as órbitas formam classes de equivalência em* M*)*

Corolário 2.16.2. *Se existe* $m \in M$ *tal que* $Orb_\alpha(m) = M$*, então* $Orb_\alpha(n) = M$*,* $\forall n \in M$*.* ▫

Demonstração. Dado $n \in M$, como $Orb_\alpha(m) = M$, então $n \in Orb_\alpha(m)$. Pela proposição, $Orb_\alpha(n) = Orb_\alpha(m) = M$. ■

Corolário 2.16.3. *Uma ação* α *é transitiva se, e somente se existir* $m \in M$ *tal que* $Orb_\alpha(m) = M$ ▫

Demonstração. Pelo corolário acima, existir $m \in M$ tal que $Orb_\alpha(m) = M$, é equivalente a dizer que $Orb_\alpha(x) = M$, $\forall x \in M$. Dados $x, y \in M$ arbitrários, pelo que foi dito, $Orb_\alpha(x) = M$, donde $y \in Orb_\alpha(x)$, donde existe $g \in G$ tal que $y = \alpha(g, x)$. Pela arbitrariedade de x e y, concluímos que α é transitiva. Reciprocamente, sendo α transitiva e, fixado um $x \in M$, para todo $y \in M$, existe $g \in G$ tal que $y = \alpha(g, x)$, e portanto $y \in Orb_\alpha(x)$, $\forall y \in M$ e, portanto, $Orb_\alpha(x) = M$. ■

Definição 2.13. Sejam G um grupo e $\alpha : G \times M \to M$ uma ação de G em M. α é dita *efetiva* se dados $g, h \in G$, $g \neq h \implies \exists x \in M; \alpha(g, x) \neq \alpha(h, x)$. Tal α também costuma ser dita *fiel*. α é dita *livre* se, dados $g, h \in G$, $g \neq h \implies \alpha(g, x) \neq \alpha(h, x), \forall x \in M$. ♣

Apesar de parecidas, não se engane: a definição de ação efetiva e livre são diferentes, sendo a última mais forte, ou seja, toda ação livre é efetiva mas não vale a recíproca. Em palavras, uma ação é efetiva se transformações de simetria diferentes fazem algum ponto ficar diferente. Ou, se duas transformações de simetria deixam o espaço igual, então os elementos correspondentes do grupo são iguais. Assim como fizemos com a transitividade, forneceremos uma equivalência para a definição de livre e efetiva:

Proposição 2.17. *Sejam* G *um grupo e* $\alpha : G \times M \to M$ *uma ação de* G *em* M*. Então* α *é efetiva se, e somente se* $\alpha(g, x) = x$*,* $\forall x \in M \implies g = e$*. Além disso,* α *é livre se, e somente se* $\exists x \in M$*;* $\alpha(g, x) = x \implies g = e$*.* ▫

Demonstração. Suponha, primeiramente, que valha a implicação: $\alpha(a, y) = y$, $\forall y \in M \implies a = e$. Provarei a contrapositiva da tese. Tome $g, h \in G$ arbitrários e ponha $a = gh^{-1}$ e $y = \alpha(h, x)$. Daí $\alpha(gh^{-1}, \alpha(h, x)) = \alpha(h, x)$, $\forall x \in M \implies gh^{-1} = e \implies g = h$. Note que não há perda de generalidade ao tomarmos $\alpha(h, x)$ no lugar de y pois $\alpha(h, \cdot)$ é uma bijeção por definição (e portanto alcança todos $y \in M$). Mas, por definição de ação, $\alpha(gh^{-1}, \alpha(h, x)) = \alpha(g, x)$. E portanto temos a seguinte implicação: $\alpha(g, x) = \alpha(h, x), \forall x \in M \implies g = h$. A tese segue da arbitrariedade na escolha de g e h. Reciprocamente, suponhamos que α seja efetiva. Suponhamos também que, para algum g, $\alpha(g, x) = x$, $\forall x \in M$. Quero provar que $g = e$. Para tanto, notemos que $\alpha(e, x) = x$, $\forall\ inM$, pela definição de ação. Assim, a hipótese acima enunciada pode ser reescrita como: $\alpha(g,x) = \alpha(e,x)$, $\forall x \in M$. Ora, da efetividade de α segue que $g = e$.

Em segundo lugar, suponhamos que α seja livre. Isto é, que se existe $x \in M$ tal que $\alpha(g,x) = \alpha(h,x)$, então $g = h$. Suponhamos também que existe $x \in M$ tal que $\alpha(g,x) = x$. Provemos que $g = e$. Note que, por definição de ação, $x = \alpha(e,x)$. Daí, existe $x \in M$ tal que $\alpha(g,x) = \alpha(e,x)$. Mas como a ação é livre, chegamos que $g = e$. Reciprocamente, suponhamos que valha a implicação: $\exists x \in M; \alpha(g,x) = x \implies g = e$. Suponhamos também que exista x tal que $\alpha(g,x) = \alpha(h,x)$. Quero provar que $g = h$. Note que $\alpha(g,x) = \alpha(h,x) \implies \alpha(gh^{-1}, \alpha(h,x)) = \alpha(h,x)$. Por hipótese, isso nos dá $gh^{-1} = e$, donde $g = h$, concluindo nossa demonstração. ■

Essa proposição nos dá, em palavras, o seguinte: o uma ação é efetiva se a única transformação que deixar *tudo* igual for a identidade; uma ação é livre se a única transformação que deixar *alguma coisa* igual for a identidade.

Proposição 2.18. *Sejam G um grupo e $\alpha : G \times M \to M$ uma ação de G em M. α é simplesmente transitiva se, e somente se α é transitiva e livre.* □

Demonstração. Suponha que α é transitiva e livre. Então, dados $x, y \in M$, existe $g \in G$ tal que $\alpha(g,x) = y$. Daí, se $\alpha(h,x) = y$, teremos $\alpha(g,x) = \alpha(h,x)$, para algum x. Como α é livre, isso nos dá $g = h$, donde g é o único elemento tal que $\alpha(g,x) = y$, o que demonstra ser α transitiva.

Reciprocamente, suponha que α é simplesmente transitiva. Isto é, dados $x, y \in M$, se $\alpha(g,x) = y$ e $\alpha(h,x) = y$, então $g = h$ (além do mais, tal g sempre existe). Ora, que α é transitiva é óbvio. Dado $x \in M$ e $g \in G$, tome $y = \alpha(g,x)$. Daí valerá que se $\alpha(h,x) = y$, isto é, que se $\alpha(g,x) = \alpha(h,x)$ para algum x, então $g = h$, donde α é livre. ■

Definição 2.14. (grupo de isotropia). Seja G um grupo e $\alpha : G \times M \to M$ uma ação de G em M. Se $g \in G$ e $m \in M$ tais que $\alpha(g,m) = m$, então m é dito ser um ponto fixo de g. Seja $X \subset M$. O conjunto $\{g \in G; \alpha(g,x) \in X, \forall x \in X\}$ é chamado de *grupo estabilizador de G com relação a X* ou *grupo de isotropia* e denotado por $G_{\alpha,X}$ ou G_X quando a ação estiver subentendida.

♣

Proposição 2.19. *Sejam G um grupo, $\alpha : G \times M \to M$ uma ação de G em M e $X \subset M$. Então G_X é um subgrupo de G.* □

Demonstração. Suponha que $g, h \in G_X$. Então $\alpha(g,x) = x$, $\forall x \in X$ e também $\alpha(h,x) = x$, $\forall x \in X$. Daí, dado $x \in X$ arbitrário, $\alpha(gh,x) = \alpha(g, \alpha(h,x)) = \alpha(g,x) = x$, donde $gh \in G_X$. Ainda, $\alpha(e,x) = x \implies \alpha(g^{-1}g, x) = x \implies \alpha(g^{-1}, \alpha(g,x)) = \alpha(g^{-1}, x) = x$. ■

Proposição 2.20. *Sejam G um grupo e $\alpha : G \times M \to M$ uma ação de G em M. A ação α é livre se, e somente se $G_x = \{e_G\}$, $\forall x \in X$.* □

Demonstração. Suponha que α é livre. Dado $g \in G_X$, temos que $\alpha(g,x) = x$. Porém, pela proposição 2.17, como α é livre, isto implica que $g = e$, donde $G_X = \{e\}$.

Reciprocamente, suponha que temos $G_X = \{e\}$. Então $\alpha(g,x) = x$ implica que $g \in G_X$ e portanto $g = e$. Temos então a implicação $\alpha(g,x) = x \implies g = e$, que pela proposição 2.17 é o mesmo que dizer que α é livre. ■

A partir de agora, usaremos a notação mais simplificada: $gx = \alpha(g,x)$.

2.7 Ações descontínuas em espaços topológicos

Veremos agora algumas definições importantes para o conceito de grupo fuchsiano.

Definição 2.15. Sejam G um grupo, X um espaço topológico

2.8 Grupos de Simetria

Definição 2.16. Seja M um conjunto. O conjunto de todas as bijeções de M para M forma um grupo sob a operação de composição e é chamado de grupo de simetria de M, denotado por $\mathrm{Sym}(M)$. Um subgrupo de um grupo de simetria é chamado de grupo de permutação.

Na verdade, o grupo de simetria de um objeto matemático é o grupo de funções que preservam a estrutura deste objeto. Por exemplo, se for um espaço métrico, o grupo de simetria é o grupo de isometria. Se for um espaço topológico, é o grupo de homeomorfismos, se for uma variedade diferenciável, é o grupo de difeomorfismos... E assim por diante.

2.9 Geradores

Antes de passarmos para a próxima definição, convém lembrarmos que a intersecção arbitrária de subgrupos de um grupo ainda é um subgrupo. Notamos também que o mesmo não vale para uniões de subgrupos. Entretanto, até o final desta seção.

Definição 2.17. Seja G um grupo e $X \subset G$ um subconjunto. O *subgrupo de G gerado por X* e denotado por $\langle X \rangle$ é definido como:

$$\langle X \rangle := \bigcap_{S < G;\, X \subset S} S$$

O subgrupo gerado por $X = \emptyset$ é $\langle X \rangle = \{e\}$.

♣

Como a intersecção arbitrária de subgrupos é subgrupo, temos automaticamente que $\langle X \rangle$ é subgrupo de G.

Agora, trabalharemos para apresentar uma definição equivalente de subgrupo gerado, começando com a definição de *palavra*:

Definição 2.18. Sejam G um grupo e $X \subset G$ um subconjunto não-vazio. Um elemento de G é dito uma palavra de X quando pode ser escrito como $x_1...x_n$, onde x_i ou x_i^{-1} pertence a X, para todo i natural entre 1 e n. ♣

Isso nos dá a seguinte:

Proposição 2.21. *Sejam G um grupo e X um subconjunto não vazio de G. Vale que $\langle X \rangle$ é o conjunto de todas as palavras de X.* □

Demonstração. Seja W o conjunto de todas as palavras de X. É simples ver que W forma um subgrupo. Mais trivial ainda é ver que este subgrupo contém X. Portanto, $\langle X \rangle \subset W$, por definição. Reciprocamente, seja $w \in W$ arbitrário. Dado um subgrupo S que contém X, por ser em particular um grupo, é fechado com relação a operação de grupo e de elemento oposto. Como w é justamente formada por elementos de X (e portanto de S) e seus elementos inversos, então teremos $w \in S$. Pela arbitrariedade de w e S temos que W está contido na interseção de todos os subgrupos que contenham X. Isto é, $W \subset \langle X \rangle$. ■

Definição 2.19. Seja G um grupo e $X \subset G$. Se $\langle X \rangle = G$, dizemos que X *gera* G e que os elementos de X são *geradores* de G. Se existe algum X finito que gera G, dizemos que G é finitamente gerado.

Definição 2.20. Seja G um grupo. Se existir $x \in G$ tal que $G = \langle x \rangle$, dizemos que G é um grupo cíclico.

Definição 2.21. Seja G um grupo e $x \in G$ um elemento. Então a ordem de x é definida como a ordem do grupo $\langle x \rangle$.

Proposição 2.22. *Seja G um grupo. $x \in G$ tem ordem infinita se, e somente se todas as potências de x são distintas (pela proposição anterior, o conjunto das potências de x empata com $\langle x \rangle$).*

Demonstração. Se todas as potências de x são distintas, $\langle x \rangle$ é obviamente infinito. Reciprocamente, iremos provar a contra-positiva. Isto é, supondo que existam potências iguais, digamos $x^m = x^l$, provaremos que $\langle x \rangle$ é finito. Sem perda de generalidade, consideremos $m > l$. Então teremos que $x^{m-l} = e_G$. Daí, o conjunto dos naturais tais que $x^k = e_G$ é não vazio. Pelo princípio da boa ordenação, podemos achar o menor natural que valha a igualdade. Denotaremos este natural por n. Pelo algoritmo da divisão, tomando um inteiro m qualquer, podemos reescrevê-lo como $m = nq + r$, com $0 \leqslant r \leqslant n - 1$. Então $x^m = (x^n)^q + x^r = (e_G)^q + x^r = x^r$, o que mostra que $\langle x \rangle = \{e_G, x, ..., x^{n-1}\}$, donde x tem ordem finita. ■

Corolário 2.22.1. *Se G é um grupo finito, então, dado $x \in G$, existe um inteiro positivo n tal que $x^n = x^{-1}$.*

Demonstração. Basta ver que, como G é finito e como $\langle x \rangle \leqslant G$, devem existir m, l tais que $x^m = x^l$. Pelo que foi falado na demonstração da proposição, concluiremos que $\langle x \rangle = \{e_G, x, ..., x^{n-1}\}$. Como $x^{-1} \in \langle x \rangle$, segue a asserção. ■

Corolário 2.22.2. *Se G é um grupo finito, vale que $\langle x \rangle$ é o conjunto cujos elementos são da forma $x_1^{\epsilon_1}...x_n^{\epsilon_n}$, com $\epsilon_i \geqslant 0$, para todo i.*

2.10 Grupos Livres

Definição 2.22. Sejam F um grupo, X um conjunto não-vazio e $\sigma : X \to F$ uma função. Então (F, σ) é dito livre em X se, para todo grupo G e toda função $\alpha : X \to G$, existir e for único um homomorfismo $\beta : F \to G$ tal que $\alpha = \beta \circ \sigma$.

Esta definição pode parecer muito estranho a uma primeira vista. Gastaremos um tempo buscando uma intuição para ela. Para tanto, faremos uma analogia com espaços vetoriais.

A base de espaço vetorial possui uma característica singular. Qualquer transformação linear fica unicamente determinada uma vez que se sabe o valor que esta assume nos elementos de uma base. Isto significa que há a total *liberdade* de escolhermos os valores da transformação nos vetores da base, sem correr o risco de chegar numa inconsistência. Isto se deve ao fato de que os vetores de uma base não satisfazem relações desnecessárias, só satisfazem as relações impostas pela definição de espaço vetorial. Este fato é sinônimo do fato de que os vetores são linearmente *independentes*. Por exemplo, se os vetores u, v, w satisfizerem a relação de dependência $2u + v + 3w = 0$, então não podemos escolher arbitrariamente os valores de uma transformação linear $T(u), T(v), T(w)$ sem corrermos o risco de sermos contraditórios. $T(u), T(v), T(w)$ devem necessariamente satisfazer a mesma relação. Agora, basta trocarmos "espaço vetorial"por grupo e "transformação linear"por homomorfismo. Assim, um grupo F é livre sobre um conjunto de geradores X se qualquer homomorfismo de domínio F fica unicamente determinado pelos valores que assume nos elementos de X (que podem ser escolhidos "livremente"). Isso é análogo a X ser uma base de F. Ser "livre"significa que os elementos de X são "livres"de relações desnecessárias, isto é, que não aquelas impostas pelo fato de F ser grupo.

A principal diferença reside no fato de que todo espaço vetorial possui uma base, enquanto que nem todo grupo é livre sobre algum conjunto de geradores. Quanto um grupo é livre, então é possível traçar um análogo de "dimensão"no caso de espaços vetoriais, e que é chamado de posto.

Esta questão possui algumas facilidades de ser tratadas no caso de grupos abelianos. Isto decorre do fato de que um grupos abelianos podem ser vistos como módulos sobre $\mathbb{Z}$, isto é, são "quase"espaços vetoriais. Daí, um grupo abeliano livre de posto n é isomorfo a $\mathbb{Z}^n$.

Note que, implicitamente, esta discussão supôs que $X \subset F$. Na verdade, esta suposição não é exatamente injustificada. Sempre que um grupo for livre em um conjunto X, há, no mínimo, uma cópia de X dentro de F, que difere no máximo pela natureza dos elementos. Formalmente, a função $\sigma : X \to F$ é injetiva:

Proposição 2.23. *Se G é um grupo livre em X, então a função $\sigma : X \to F$ da definição é injetiva.*

Demonstração. Será por absurdo. Suponha que σ não é injetiva. Então existem $x_1, x_2, \in X$ distintos tais que $y = \sigma(x_1) = \sigma(x_2)$. Tome $G = \{g_1, g_2\}$ composto de dois elementos distintos e uma função $\alpha : X \to G$ tal que $\alpha(x_1) = g_1$ e

$\alpha(x_2) = g_2$. Tomemos β tal que $\beta \circ \sigma = \alpha$, que existe pela definição de grupo livre. Entretanto, $(\beta \circ \sigma)(x_1) = \beta(\sigma(x_1)) = \beta(\sigma(x_2)) = (\beta \circ \sigma)(x_2)$, o que é um absurdo, pela definição de α. ■

Não é difícil ver, a partir daí, que F seria livre também em $\Im\sigma$, substituindo σ pela função inclusão $i : \Im\sigma \to F$, donde todo grupo livre é livre sobre algum subconjunto. É possível mostrar que $\Im\sigma$ gera F. Mais que isso, um outro aspecto importante sobre um grupo ser livre é que F é, em certo sentido, o "maior"grupo que $\Im\sigma$ pode gerar. Enunciaremos o teorema sem demonstrá-lo, pois a demonstração possui diversos detalhes técnicos chatos, apesar de que a ideia da demonstração é simples, e sera dada.

Proposição 2.24. *Seja X um conjunto não-vazio. Então existe um grupo F e uma função $\sigma : X \to F$ tal que (F, σ) é livre em X e $F = \langle \Im\sigma \rangle$*

A demonstração é completamente por construção. Primeiro, devemos tomar um conjunto X^{-1}, disjunto a X e com a mesma cardinalidade, de forma que a cada elemento de X, corresponderemos um de X^{-1} para cumprir o papel de seu elemento inverso. Daí, tomaremos o conjunto S de todas as palavras (isto é, sequências finitas de elementos) de $X \cup X^{-1}$, sendo que a palavra "vazia"cumprirá o papel de identidade. O produto de duas palavras é definida como a concatenação delas e o inverso se faz trocando cada elemento da palavra pelo seu inverso e invertendo também a ordem. S é quase F. Temos que fazer apenas mais um ajuste. Do jeito que construímos, palavras como $x^{-1}xa$, $xx^{-1}a$ e a são diferentes uma da outra, enquanto que num grupo, elas seriam iguais. O resto do trabalho agora se reduz a unir palavras assim formando classes de equivalência, definindo operações da forma natural, provando que tudo está bem definido e de fato forma um grupo. F será o conjunto das classes de equivalência.

Por fim, deve-se provar que a função $\sigma : X \to F$ por $\sigma(x) = [x]$ faz de (F, σ) livre. Dada uma função $\alpha : X \to G$, construamos primeiro uma função $\overline{\beta} : S \to G$, do conjunto de todas as palavras, mapeando uma palavra $x_1...x_n$ para $g_1...g_n$, onde $g_i = \alpha(x_i)$. É fácil ver que elementos na mesma classe de equivalência serão mapeados para o mesmo elemento em G, donde definimos $\beta : F \to G$ por $\beta([w]) = \overline{\beta(w)}$. É fácil mostrar que tal β se torna um homomorfismo.

3 Topologia

Nesta seção abordaremos, primeiramente, formas típicas de construir topologias, como inicial, final, quociente e produto.

Construções do tipo "topologia inicial"e "topologia final"são muito comuns na matemática, principalmente no que se refere a uma álgebra de conjuntos. Prova disso é o conceito de $\sigma-$álgebra inicial e final. Devido ao fato deste tipo de construção ser tão comum e tão semelhante nos diversos casos, antes de partirmos para as definições formais, generalizaremos informalmente esta construção para estruturas quaisquer onde esta faz sentido.

Sejam A e B conjuntos e $f : A \to B$. Se pudermos construir uma "estrutura"a partir de B (por "estrutura", pode-ser ler topologia, $\sigma-$álgebra ou outros), digamos $\mathcal{B}$, então f induzirá naturalmente uma "estrutura"em A, chamada de "estrutura"inicial e definida como $\mathcal{A} := f^{-1}(\mathcal{B})$. A "estrutura"inicial é a menor estrutura que torna a função f um "morfismo"entre $(A, \mathcal{A})$ e $(B, \mathcal{B})$. (Por morfismo, pode-se ler função contínua no caso de topologia ou função mensurável no caso de $\sigma-$álgebra).

Se, por outro lado, tivermos uma "estrutura"a partir de "A"e não em B, então f pode induzir naturalmente uma "estrutura"em B chamada de "estrutura"final e definida por $\mathcal{B} := \{Y \subset B; f^{-1}(Y) \in \mathcal{A}\}$. Esta é a maior "estrutura"em B que torna f um "morfismo"entre $(A, \mathcal{A})$ e $(B, \mathcal{B})$.

Passemos às definições formais para o caso específico de topologia.

Definição 3.1. Seja X, Y conjuntos, τ_Y uma topologia em Y e $f : X \to Y$ uma função. O conjunto $f^{-1}(\tau_Y) := \{f^{-1}(U), U \in \tau_Y\}$ é chamado de *topologia inicial induzida por* f. Mais geralmente, seja $(Y_i, \tau Y_i)$ uma família arbitrária de espaços topológicos indexadas por I e (f_i) uma família de funções indexadas pelo mesmo conjunto tal que $f_i : X \to Y_i$, para todo $i \in I$. Então, a *topologia inicial induzida por* $(f_i)_{i \in I}$ é definida como $\tau_X := \{f_i(U), U \in \tau_{Y_i}, i \in I\}$. ♣

Definição 3.2. Seja X, Y conjuntos, τ_X uma topologia em X e $f : X \to Y$ uma função. O conjunto $\{U \subset Y; f^{-1}(U) \in \tau_X\}$ é chamado de *topologia final induzida por* f. Mais geralmente, seja $(X_i, \tau X_i)$ uma família arbitrária de espaços topológicos indexadas por I e (f_i) uma família de funções indexadas pelo mesmo conjunto tal que $f_i : X_i \to Y$, para todo $i \in I$. Então, a *topologia final induzida por* $(f_i)_{i \in I}$ é definida como $\tau_Y := \{U \subset Y; f_i^{-1}(U) \in \tau_{X_i}, i \in I\}$.♣

É fácil ver que as topologias inicial e final são de fato topologias, pela forma como pré-imagens preservam uniões e intersecções. Além disso, também não é difícil ver que a topologia inicial é a menor topologia que torna f contínua (ou todas as funções de uma família (f_i) contínuas); já a topologia final é a maior topologia que torna f contínua ((ou todas as funções de uma família (f_i) contínuas).

Estas definições nos permitirão manejar melhor outras, como o conceito de topologia induzida, quociente e produto, apresentados ambos a seguir.

Definição 3.3. Seja (X, τ) um espaço topológico e $S \subset X$. A topologia induzida por τ em X é definida por $\tau_S := \{S \cap U, U \in \tau\}$.

Proposição 3.1. *Seja (X, τ) um espaço topológico e $S \subset X$. Então a topologia induzida em S corresponde à topologia inicial induzida pela função inclusão $i : S \to X$, $i(x) = x$.*

Definição 3.4. Sejam (X, τ_X) um espaço topológico e $\sim$ uma relação de equivalência em X. Então o espaço quociente de (X, τ_X) por $\sim$ é definido como (Y, τ_Y) onde $Y = X/\sim$, isto é, $Y = \{[x] := \{v \in X; v \sim\}; x \in X\}$ e onde $\tau_Y = \{U \subset Y; \bigcup_{[x] \in U} [x] \in \tau_X\}$. ♣

Em um certo sentido, a topologia do espaço quociente é mais "grossa". Primeiro, note que, se um certo conjunto é um aberto do espaço quociente, então também é um aberto do espaço original, ("abrindo"as classes de equivalência). Por outro lado, a topologia quociente exclui os abertos que possuem elementos sem possuir toda a classe de equivalência deste elemento. (lembre-se que, no espaço quocientado, um elemento e sua classe de equivalência se confundem). Um exemplo fácil é o seguinte. Considere o plano com a topologia usual. Considere a relação de equivalência que quocienta o plano em linhas verticais, isto é, dois pontos estão na mesma classe de equivalência se, e somente se suas abscissas forem iguais. Uma faixa do plano sem a fronteira é um aberto tanto do plano quanto do espaço quociente. Entretanto, bolas abertas não são abertos do espaço quociente pois este conjunto não contém nenhuma classe de equivalência, isto é, nenhuma linha vertical, deixando de fazer sentido falar até mesmo que esse conjunto é subconjunto do espaço quociente. De certa maneira, podemos dizer que a topologia quociente é a maior topologia "contida"na topologia usual e que os abertos façam sentido para o espaço quocientado. Esta afirmação pode ser rigorosamente expressa na seguinte proposição:

Proposição 3.2. *Sejam (X, τ_X) um espaço topológico e (Y, τ_Y) o espaço quociente de (X, τ_X) por uma relação de equivalência $\sim$. Seja $q : X \to Y$ a projeção canônica de $\sim$, isto é, a função que mapeia um elemento $x \in X$ na sua respectiva classe de equivalência $[x] \in Y$. Então τ_Y empata com a topologia final induzida por q.*

Demonstração. Seja $\mathcal{F}$ a topologia final induzida por q. Tome $U \subset Y$. Temos que $\bigcup_{[x]\in U}[x] := \{a \in X; a \in [x], \text{ para algum } [x] \in U\} = \{a \in X; [a] \in U\}$. De fato, se a está no segundo conjunto, então $[a] \in U$. Em particular, existe $[x] \in U$ tal que $a \in [x]$, a saber, $[x] = [a]$. Se, por outro lado, a está no primeiro conjunto, então existe $[x] \in U$ tal que $a \in [x]$. Por outro lado, pelo fato de serem classes de equivalência, temos que $[a] = [x]$. Assim, $[a] \in U$ e portanto a está no segundo conjunto. Pois bem. Com isso em mãos, para completarmos a prova basta considerarmos as seguintes equivalências: $U \in \mathcal{F} \iff q^{-1}(U) \in \tau_X \iff \{x \in X; q(x) \in U\} \in \tau_X \iff \{x \in X; [x] \in U\} \in \tau_X \iff \bigcup_{[x]\in U}[x] \in \tau_X \iff U \in \tau_Y$. ■

Nosso objetivo agora é de definir uma topologia para o espaço definido como produto cartesiano de espaços topológicos. A forma mais natural seria a de considerar a topologia gerada pelo conjunto de todos os produtos cartesianos de abertos de cada topologia. Esta construção de fato existe, é chamada de topologia das caixas e é bastante adequada para o produto cartesiano de um número finito de espaços. Entretanto, ela passa a não se tornar mais tão adequada no caso de um produto infinito. Uma construção melhor é chamada de "topologia produto". Esta topologia empata com a topologia das caixas no caso finito, e é mais adequada no caso infinito. De fato, a topologia produto é sempre mais "grossa"(isto é, possui um número menor de abertos) do que a topologia das caixas. Passemos às definições formais.

Definição 3.5. Seja $(X_i, \tau_i)_{i \in I}$ uma coleção arbitrária de espaços topológicos. O espaço produto desta coleção é definido como (X, τ) tal que

$$X = \bigtimes_{i \in I} X_i$$

e τ é a topologia inicial induzida pela família de funções $\pi_i : X \to X_i$ contínuas, onde π_i são as projeções canônicas.

Não é difícil ver que esta topologia empata com a topologia gerada por elementos da forma $\bigtimes_{i \in I} U_i$, onde $U_i \neq X_i$, apenas para um número finito de índices.

A construção da topologia produto é análogo a muitas outras construções "produto"na matemática.

Por fim, relembremos alguns conceitos que serão importantes para a definição de grupo fuchsiano.

Definição 3.6. Seja (X, τ) um espaço topológico. Dado um subconjunto $S \subset X$, $x \in S$ é dito *ponto isolado* se existe um aberto $U \in \tau$ tal que $S \cap U = \{x\}$. Se todo ponto de S é isolado, S é chamado de conjunto discreto.

Proposição 3.3. *Seja (X, τ) um espaço topológico. Um subconjunto $S \subset X$ é discreto se, e somente se a topologia induzida por τ em S for a topologia discreta de S (isto é, todo subconjunto de S estiver na topologia).*

Demonstração. Suponha que S é discreto. Dado $x \in S$, tomemos U_x tal que $U_x \cap S = \{x\}$. Daí, $\{x\}$ são abertos da topologia induzida, por definição. Como topologias são fechadas por uniões arbitrárias, segue que todo subconjunto de S é aberto e portanto a topologia induzida empata com a topologia discreta de S. Reciprocamente, suponha que a topologia induzida em S seja a discreta. Então, dado $x \in S$, $\{x\} \in \tau_S$. Ora, pela definição de topologia induzida, há de haver um aberto U de τ tal que $S \cap U = \{x\}$, donde x é isolado. Pela arbitrariedade de x, segue que S é discreto. ■

4 Grupos Topológicos

Um grupo topológico é só um conjunto que possuem tanto estrutura de grupo quanto de espaço topológico e, além disso, estas estruturas conversam bem entre si. (especificamente, as operações de grupo são contínuas).

Definição 4.1. Uma tripla $(G, +, \tau)$ é dita um grupo topológico se $(G, +)$ é um grupo, (G, τ) é um espaço topológico e se as funções $+ : G \times G \to G$ e $- : G \to G$ tais que $+(g, h) = g + h$ e $-(g) = -g$ são contínuas, onde entende-se implicitamente que $G \times G$ está munido com a topologia produto.

Proposição 4.1. *G é um grupo topológico se, e somente se, a função $f : G \times G \to G$ definida por $f(g, h) = gh^{-1}$ é contínua.*

A demonstração segue de fatos básicos sobre continuidade de funções e sobre a topologia produto.

Dado $g \in G$, G grupo topológico, não é difícil ver que a função $m_g(x) : G \to G$ definida por $m_g(x) = gx$ é uma bijeção contínua, sendo $m_{g^{-1}}$ sua função inversa (também contínua). Assim, m_g é um homeomorfismo, para todo $g \in G$. Dados $x, y \in G$ arbitrários, então $m_{x^{-1}y}(x) = y$, o que indica que o grupo de homeomorfismos de um grupo topológico é transitivo (no linguajar de topologia, G é um espaço homogêneo). Isto é, qualquer ponto de G é topologicamente semelhante a qualquer outro ponto. Mais que isso, toda vizinhança é homeomorfa a alguma vizinhança do elemento neutro:

Proposição 4.2. *Seja G um espaço topológico, $g \in G$ e U uma vizinhança aberta de g. Então existe V vizinhança aberta de e (elemento neutro) tal que U e V são homeomorfos.*

Demonstração. Considere a função m_g como definida acima. Seja $V := m_g^{-1}(U)$. É fácil ver que V de fato é uma vizinhança aberta de e. Pela bijetividade de m_g, vale que $m_g(V) = U$. Defina então $f : V \to m_g(V) = U$ por $f(x) = m_g(x)$. f será um homeomorfismo. É fácil ver que f será bijetiva e contínua, por ser restrição de função contínua, e também é fácil ver que f^{-1} é restrição de $m_g^{-1} = m_{g^{-1}}$, contínua, donde f^{-1} é contínua. ■

Esta semelhança entre as várias partes de um grupo topológico permite-nos encontrar um critério mais simples para decidir se um grupo é discreto, basta ver se apenas um elemento é isolado.

Proposição 4.3. *Sejam G um grupo topológico, H um subgrupo de G e $g \in H$. Então H é um subgrupo discreto se, e somente se, g for um ponto isolado de H.*

Demonstração. Se H é discreto, segue trivialmente que existe g isolado (tome por exemplo a identidade) Por outro lado, seja U um aberto tal que $U \cap H = \{g\}$. Tome $h \in H$ arbitrário e tome o homeomorfismo $m_{gh^{-1}}$. Note que $m_{gh^{-1}}(h) = g$, donde $V := m_{gh^{-1}}^{-1}(U)$ é uma vizinhança aberta de h. Mostraremos, agora, que $V \cap H = \{h\}$. Seja $x \in V \cap H$. Pela definição de V, temos que $m_{gh^{-1}}(x) = gh^{-1}x \in U$. Por construção, $gh^{-1}x \in H$, donde devemos ter $gh^{-1}x = m_{gh^{-1}}(x) = g$ necessariamente, por hipótese. Entretanto, como $m_{gh^{-1}}$ é bijetiva e $m_{gh^{-1}}(h) = g$, devemos ter necessariamente $h = x$, portanto h é um ponto isolado. Pela arbitrariedade de h, concluímos que H é um subgrupo discreto. ■

Corolário 4.3.1. *Seja G um grupo topológico. Então G é discreto se, e somente se, existir um aberto da topologia contendo apenas um elemento do grupo.*

Demonstração. Se G é discreto, obviamente haverá abertos contendo apenas um elemento. Por outro lado, suponha que $\{g\}$ é um aberto, para algum $g \in G$. então g é um ponto isolado de G, donde G é discreto, pela proposição. ■

5 Alguns Grupos de Matrizes

5.1 O grupo SL(2, $\mathbb{R}$)

Nesta seção estudaremos algumas propriedades algébricas e topológicas do grupo SL(2, $\mathbb{R}$). Por exemplo, a decomposição de Iwasawa, além de nos fornecer um conjunto gerador para SL(2, $\mathbb{R}$), nos permitirá ver que este grupo é homeomorfo ao produto de um círculo pelo semiplano, que implicará que o mesmo grupo é homeomorfo ao produto de um círculo pelo plano, ou de um círculo por um disco, que corresponde a um toro sólido sem a casca.

5.2 O grupo PSL(2, $\mathbb{R}$)

Este grupo pode ser definido de diversas formas. Seu nome herda sua ligação com geometria projetiva, mas não iremos nos importar muito com isto agora. Uma maneira relativamente comum de definir é a seguinte:

Definição 5.1. Seja n um inteiro positivo e F um corpo. Definimos $PSL(n, F) = SL(n, F)/(\lambda\mathbb{I}_n \cap SL(n, F))$, onde $\lambda \in F$ e $\mathbb{I}_n$ é a matriz identidade $n \times n$.

Com esta definição, fica evidente que $PSL(2, \mathbb{R}) = SL(2, \mathbb{R})/G$, onde G é o grupo formado pelas matrizes $\mathbb{I}$ e $-\mathbb{I}$. Daí, podemos escrever os elementos de $PSL(2, \mathbb{R})$ como conjuntos da forma $\{-g, g\}$, com $g \in SL(2, \mathbb{R})$. Este grupo será isomorfo a Möb$_+(\mathbb{R})$, que é o grupo das transformações de Möbius com coeficientes reais e tais que $ad - bc > 0$. Alguns autores inclusive definem $PSL(2, \mathbb{R})$ como Möb$_+(\mathbb{R})$. Valerá que $PGL(n, F) \cong PSL(n, F)$ se, e somente se todo elemento do corpo possui uma raiz n-ésima.

6 Análise Complexa

6.1 A Esfera de Riemann

Há algumas vantagens em usar o corpo dos números complexos. Uma delas é de que os complexos são algebricamente fechados. Outra, é de que uma função que é diferenciável uma vez em um domínio[1] é diferenciável infinitas vezes neste domínio e, para todo ponto dele, podemos escrever a função como uma série de potências convergente em uma determinada vizinhança do ponto (são as chamadas funções *holomorfas* ou *analíticas*). Duas desvantagens dos complexos são: não poder dividir por zero e $\mathbb{C}$ não ser compacto (e portanto poder haver sequências sem nenhuma subsequência convergente). Estas duas desvantagens podem ser ambas dribladas acrescentando ∞ aos complexos. Este novo conjunto será chamado de *plano complexo estendido*, e denotado por $\overline{\mathbb{C}} := \mathbb{C} \cup \infty$. Para os leitores preocupados, a natureza do elemento ∞ não importa - a princípio, pode tomar qualquer objeto que não pertença a $\mathbb{C}$.

[1]Neste texto, domínio será sinônimo de aberto conexo.

Proposição 6.1. *Seja $S^2 \subset \mathbb{R}^3$ a esfera unitária de centro em $(0,0,0)$. A projeção estereográfica $\overline{\pi} : S^2/(0,0,1) \to \mathbb{C}$ é um homeomorfismo.* $\square$

Demonstração. A projeção estereográfica é dada por:

$$\overline{\pi}(x,y,z) = \frac{x}{1-z} + i\frac{y}{1-z} \tag{1}$$

Para ver que a projeção é contínua, basta ver que cada uma das funções coordenadas são contínuas (nunca se tem $z = 1$).

Falta ver que a função inversa é contínua. Para tanto, achemos agora uma expressão para esta. Definindo $u := \Re(\overline{\pi})$ e $v := \Im(\overline{\pi})$, temos:

$$u^2 + v^2 + 1 = \frac{x^2 + y^2 + (1-z)^2}{(1-z)^2} = \frac{x^2 + y^2 + z^2 + 1 - 2z}{(1-z)^2}$$

Como $(x,y,z) \in S^2$, $x^2 + y^2 + z^2 = 1$ e daí:

$$u^2 + v^2 + 1 = \frac{2 - 2z}{(1-z)^2} = \frac{2}{1-z}$$

Por (1), temos que:

$$u = \frac{x}{1-z} \implies x = u(1-z) = \frac{2u}{2/(1-z)} = \frac{2u}{u^2+v^2+1}$$

Analogamente:

$$y = \frac{2v}{u^2+v^2+1}$$

Para achar z em função de u e v, veja que:

$$u^2 + v^2 + 1 = \frac{2}{1-z} \implies 1 - z = \frac{2}{u^2+v^2+1} \implies z = 1 - \frac{2}{u^2+v^2+1}$$

$$\implies z = \frac{u^2+v^2+1-2}{u^2+v^2+1} \implies z = \frac{u^2+v^2-1}{u^2+v^2+1}$$

Com isto, chegamos finalmente que:

$$\overline{\pi}^{-1}(u,v) = \left(\frac{2u}{u^2+v^2+1}, \frac{2v}{u^2+v^2+1}, \frac{u^2+v^2-1}{u^2+v^2+1}\right) \tag{2}$$

Que é evidentemente contínua pois cada função coordenada é contínua. ■

Podemos construir uma bijeção $\pi : S^2 \to \overline{\mathbb{C}}$ estendendo $\overline{\pi}$ de forma que $\pi(0,0,1) = \infty$. A semelhança entre $\overline{\mathbb{C}}$ e S^2 se estende também para a topologia, por isso os dois objetos costumam ser identificados e costumamos chamar $\overline{\mathbb{C}}$ de *esfera de Riemann*.

Definiremos a topologia de $\overline{\mathbb{C}}$ como as imagens por π de abertos de S^2, e teremos:

Proposição 6.2. *π é um homeomorfismo.* ◻

Demonstração. Seja A um aberto de $\overline{\mathbb{C}}$. Quero mostrar que $\pi^{-1}(A)$ é aberto de S^2. Ora, por definição de aberto em $\overline{\mathbb{C}}$, existe B aberto de S^2 tal que $A = \pi(B)$. Como π é uma bijeção, $\pi^{-1}(A) = \pi^{-1}(\pi(B)) = B$, que é aberto de S^2. Está provado que π é contínua.

Agora, dado B aberto de S^2, quero provar que $\tau^{-1}(B)$ é aberto de $\overline{\mathbb{C}}$, onde τ é a função inversa de π. Ora, a imagem inversa da função inversa de uma função, coincide com sua imagem direta, donde $\tau^{-1}(B) = \pi(B)$, que é aberto por definição. ■

Corolário 6.2.1. *$\overline{\mathbb{C}}$ é compacto* ◻

Demonstração. S^2 é compacto e $\overline{\mathbb{C}}$ é a imagem de S^2 sob π. Como π é homeomorfismo, em particular é contínua. Como a imagem de compactos por funções contínuas é compacto, a proposição segue. ■

Proposição 6.3. *Todo aberto de $\overline{\mathbb{C}}$ ou é um aberto de $\mathbb{C}$, ou é o complementar de um compacto de $\mathbb{C}$ unido com ∞* ◻

O processo que acabamos de fazer é o caso particular de uma técnica mais geral conhecida como compactificação de espaços topológicos (mais especificamente, *compactificação de Alexandrov*).

6.2 Círculos e Retas

6.3 Funções Racionais

Ao transformar o plano complexo na esfera de Riemann, o conceito de holomorfismo pode ser generalizado. Agora, funções com certas singularidades podem se tornar bem definidas, se definirmos o valor da função na singularidade como sendo infinito. Por questões de bom comportamento, estas singularidades devem ser pólos e devem ser isoladas. Uma função complexa holomorfa em todo plano exceto em um conjunto discreto de pontos que são pólos é chamada de função meromorfa. Assim, "holomorfismo"na esfera de Riemann passa a ser uma adaptação das funções meromorfas no plano. Alguns autores chamam esta generalização de "holomorfismo"para a esfera de Riemann de holomorfismo de fato, enquanto outros ainda usam o termo meromorfismo. Usaremos o segundo.

Assim como holomorfismo no plano implicava em continuidade, a proposição seguinte nos garante que:

Proposição 6.4. *Se f é meromorfa em $\overline{\mathbb{C}}$, então f é contínua em $\overline{\mathbb{C}}$* ◻

Diferentemente das funções holomorfas no plano, é possível descrever a forma de todas as funções meromorfas:

Teorema 6.5. *Uma função de $\overline{\mathbb{C}}$ para $\overline{\mathbb{C}}$ é meromorfa se, e somente se é uma função racional* ◻

E além disso:

Proposição 6.6. *Uma função racional $f : \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ é injetiva se, e somente se for composta por polinômios de grau igual a 1.*

O conjunto das funções meromorfas em $\overline{\mathbb{C}}$ forma um corpo $\mathbb{C}(z)$. Este corpo possui um subcorpo isomorfo a $\mathbb{C}$ (o das funções constantes) e portanto, $\mathbb{C}(z)$ pode ser considerado uma extensão de $\mathbb{C}$

6.4 Transformações de Möbius

Definição 6.1. Uma função $T : \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ é dita ser uma *Transformação de Möbius* se existem $a, b, c, d \in \mathbb{C}$ com $ad - bc \neq 0$ tais que:

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

$\forall z \in \overline{\mathbb{C}}$. ♣

É fácil ver que as transformações de Möbius formam um grupo sob a operação de composição. Este grupo será denotado por Möb. Nesta seção, iremos nos dedicar a estudar as transformações de Möbius enquanto grupo, analisando isomorfismos com outros grupos, geradores, etc.

As transformações de Möbius são precisamente os automorfismos da esfera de Riemann. Isto significa que estas transformações preservam a estrutura de variedade complexa da esfera. Sem entrar em muitos detalhes agora, mas preservar a estrutura de variedade complexa significa que a transformação é uma bijeção meromorfa com inversa também meromorfa. A proposição seguinte demonstra isto, juntamente com o fato já conhecido que Möb é um grupo.

Uma questão interessante a se pensar: quais são os "automorfismos"do plano enquanto variedade diferenciável real?

Proposição 6.7. *Uma função $T : \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ pertence a Möb se, e somente se T é uma bijeção meromorfa* □

Demonstração. Basta usar em conjunto o teorema 5.5 e a proposição 5.6. ■

Corolário 6.7.1. *Se $T \in$ Möb, então T é homeomorfismo de $\overline{\mathbb{C}}$.* □

Demonstração. Pela proposição 5.7, T é meromorfa. Pela proposição 5.4, T é contínua em $\overline{\mathbb{C}}$. Como Möb é um grupo, $T^{-1} \in$ Möb, donde T^{-1} é meromorfa e portanto contínua. A afirmação segue. ■

A proposição acima diz que preservar a estrutura de variedade complexa nos dá automaticamente que a topologia também é preservada.

Existe uma identificação natural entre $GL(2, \mathbb{C})$ e Möb, $\theta : GL(2, \mathbb{C}) \to$ Möb, dada por:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{az + b}{cz + d}$$

Não é difícil ver que se $M, N \in GL(2,\mathbb{C})$ e $T, U \in$ Möb tais que $T = \theta(M)$ e $N = \theta(U)$, então $\theta(NM) = U \circ T = \theta(N) \circ \theta(M)$, donde θ é um homomorfismo. Mais que isso, θ é sobrejetivo e, portanto, é um epimorfismo. Mas θ não é um isomorfismo pois não é injetiva. De fato:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{az+b}{cz+d}$$

$$\begin{pmatrix} 2a & 2b \\ 2c & 2d \end{pmatrix} \mapsto \frac{2az+2b}{2cz+2d} = \frac{2(az+b)}{2(cz+d)} = \frac{az+b}{cz+d}$$

As duas matrizes acima, em geral, são diferentes (a não ser que todos os elementos sejam nulos) mas as imagens por θ são iguais.

Busquemos um grupo similar a $GL(2,\mathbb{C})$ que seja isomorfo a Möb, e não apenas epimorfo. Uma maneira de lidar com este problema é saber quando duas matrizes $M, N \in GL(2,\mathbb{C})$ determinam o mesmo elemento de Möb. Invocando a proposição 2.3, vemos que isso ocorre se, e somente se $MN^{-1} \in \ker\theta$. Não é difícil ver que $\ker\theta = \{\lambda\mathbb{I}, \lambda \in \mathbb{C}^* := \mathbb{C}\backslash\{0\}\}$, onde $\mathbb{I}$ é a matriz identidade (este conjunto também corresponde ao centro de $GL(2,\mathbb{C})$). Assim, pelo Colorário 2 do Teorema 2.11, teremos $GL(2,\mathbb{C})/\ker\theta = GL(2,\mathbb{C})/\lambda\mathbb{I} \cong$ Möb. Denotaremos $PGL^2(2,\mathbb{C}) := GL(2,\mathbb{C})/\lambda\mathbb{I}$. Em palavras, $PGL(2,\mathbb{C})$ é o grupo das classes de equivalência de elementos de $GL(2,\mathbb{C})$ onde dois elementos fazem parte da mesma classe de equivalência se for possível obter um a partir do outro multiplicado por uma constante não-nula.

Lembro que $\det(MN) = \det(M)\det(N)$, donde a função $\det : GL(2,\mathbb{C}) \to$ é um homomorfismo. O núcleo deste homomorfismo é denotado por $SL(2,\mathbb{C})$. Afirmo que esta função é na verdade um epimorfismo. Pelo Corolário 2 do Teorema 2.11, existe um isomorfismo entre $\mathbb{C}^*$ e $GL(2,\mathbb{C})/SL(2,\mathbb{C})$.

Note que, dado $N \in GL(2,\mathbb{C})$, podemos achar $M \in SL(2,\mathbb{C})$ tal que $N = \lambda M$, onde $\lambda^2 = \det(N)$. De fato, tome $M = (\lambda\mathbb{I})^{-1}N$. (lembre-se de que $\lambda \neq 0$). Daí $\det(M) = \det(\lambda\mathbb{I})^{-1}\det(N) = \det(N)/\lambda^2 = 1$ e verdadeiramente teremos $M \in SL(2,\mathbb{C})$. Além disso, $\lambda M = (\lambda\mathbb{I})(\lambda\mathbb{I})^{-1}N = N$, como havíamos dito. Como $N = \lambda M$ e pelo que foi dito acima, teremos $\theta(N) = \theta(M)$. Assim, para todo $T \in$ Möb, podemos achar $M \in SL(2,\mathbb{C})$ tal que $\theta(M) = T$. Em outras palavras, toda transformação de Möbius pode ser escrita como:

$$\frac{az+b}{cz+d} \tag{3}$$

Onde $ad - bc = 1$.

Definimos $PSL(2,\mathbb{C}) := SL(2,\mathbb{C})/(\lambda\mathbb{I} \cap SL(2,\mathbb{C}))$. E assim, já provamos parcialmente o seguinte:

Proposição 6.8. *Möb* $\cong PGL(2,\mathbb{C}) \cong PSL(2,\mathbb{C})$ □

[2] derivado de “projective general linear group”, por suas relações com transformações projetivas

Observação: Se definíssemos $PSL(2,\mathbb{C})$ como a imagem direta de $SL(2,\mathbb{C})$ pela aplicação quociente $\rho : GL(2,\mathbb{C}) \to PGL(2,\mathbb{C})$, daí teríamos $PGL(2,\mathbb{C}) = PSL(2,\mathbb{C})$. Esta afirmação pode ser facilmente demonstrada com o que foi falado acima. Preferimos definir do outro jeito para ser compatível com a definição generalizada (futura definição 8.1).

Busquemos agora um gerador para Möb. A proposição seguinte nos fornece isto.

Proposição 6.9. *Sejam R_θ definida por $R_\theta(z) = e^{i\theta}z$, J definida por $J(z) = 1/z$, S_r definida por $S_r(z) = rz$ e T_t definida por $T_t(z) = z + t$ funções da esfera de Riemann na esfera de Riemann. O conjunto $X = \{R_\theta, S_r, T_t, J | \theta \in \mathbb{R}, r \in \mathbb{R}^+, t \in \mathbb{C}\}$ gera Möb.*

Devido a esta proposição, há uma interpretação geométrica bacana para transformações de Möbius. Imagine que temos uma esfera em cima de um plano e uma lâmpada em cima da esfera, que gera uma projeção estereográfica sobre o plano. Então as transformações de Möbius correspondem a uma composição das seguintes operações com a esfera: i) rotação sobre o eixo vertical (R_θ), ii) rotação sobre o eixo horizontal que passa por 1 e -1 (J), iii) contração ou expansão da esfera (S_r), iv) translações da esfera (T_t).

Uma outra característica importante das transformações de Möbius é o que se segue:

Teorema 6.10. *Uma transformação da esfera de Riemann em si mesma é um homeomorfismo conforme que preserva orientação se, e somente se, é uma transformação de Möbius.*

Transformações de Möbius diferentes da identidade possuem no máximo dois pontos fixos. Isto é, se uma transformação de Möbius deixa três pontos fixos, então é a identidade. Podemos usar a interpretação acima e então este fato pode ser expresso nos seguinte termos: é impossível fazer quaisquer movimentos numa esfera fixando três dedos nela (em pontos diferentes).

7 Geometria Hiperbólica

7.1 O Espaço Hiperbólico

Lembremos que os cinco axiomas de Euclides permaneceram por muito tempo sendo os princípios norteadores da geometria. O quinto axioma, que é equivalente a dizer: "dada uma reta e um ponto fora da reta, há apenas uma outra reta paralela à primeira que passa pelo ponto"ou ainda, "a soma dos ângulos internos de um triângulo é 180°", era o axioma menos natural de ser aceito sem demonstração, e muitas pessoas tentaram provar que este axioma podia ser provado a partir dos outros quatro. Na primeira metade do século XIX, Gauss provou que isto não era possível, construindo uma geometria consistente sem utilizar o quinto axioma e com triângulos podendo ter a soma interna de seus ângulos menor do que 180°. Apesar de Gauss não ter publicado, anos mais tarde, os matemáticos Lobachevsky e Bolyai publicaram versões semelhantes, dando origem ao embrião do que seria a geometria hiperbólica.

O ambiente natural para tratar de geometria hiperbólica é o espaço hiperbólico. O espaço hiperbólico aparece naturalmente ao se fazer a classificação das variedades riemannianas completas, simplesmente conexas e de curvatura seccional constante. Há apenas três tipos de variedades assim: $\mathbb{R}^n$, com curvatura nula, a esfera, com curvatura positiva, e o espaço hiperbólico, com curvatura negativa.

Um modo natural de se construir o espaço hiperbólico é como uma esfera num espaço de Minkowski. Estes detalhes, necessitam de uma ampla dose de geometria diferencial, por isso não abordaremos o espaço hiperbólico desta maneira neste texto. Iremos utilizar construções conhecidas como "modelos"do espaço hiperbólico, que são nada mais, nada menos do que objetos isométricos ao espaço hiperbólico e nos quais será relativamente mais fácil trabalhar. A despeito disto, durante o texto poderão haver alguns comentários relacionando construções nos modelos com construções no espaço hiperbólico propriamente dito, a fim de esclarecer construções obscuras, sanar a curiosidade dos leitores interessados ou que possuem os requisitos para tal.

Os modelos mais famosos são: o semiplano superior do plano complexo e o disco unitário, conhecido como "disco de Poincaré"neste contexto.

Como iremos ver, a geometria hiperbólica é completamente diferente da euclidiana e causa disto é a diferença na definição de distância em cada geometria. A construção dos modelos e das distâncias neles pode parecer arbitrária, à primeira vista. Por isso, optamos por introduzir brevemente sobre o modo usual de definir distância numa variedade riemanniana, para motivar a definição de distância no nossos modelos

7.2 Distância em Variedades Riemannianas

O modo de definir distância numa variedade riemanniana reflete muito sobre a estrutura deste objeto, por isto gastaremos um tempo falando disto. Para os leitores menos habituados, uma variedade, é uma generalização do conceito de superfície (se for diferenciável, é uma superfície onde faz sentido falar de coisas como derivadas e diferenciabilidade). Uma variedade riemanniana é uma variedade que possui uma estrutura a mais, chamada de métrica riemanniana. Esta estrutura é semelhante a um produto interno, dando portanto noção de comprimentos e ângulos e não deve ser confundida com métrica no sentido de espaço métrico[3]. Para ser mais exato, a métrica riemanniana é um objeto que a cada ponto da variedade associa um produto interno no espaço tangente a este ponto e que também deve satisfazer a um certo critério de suavidade. Esta estrutura não nos permite calcular distâncias diretamente, mas ela nos induz uma norma em cada espaço tangente, que pode ser usada para calcular comprimento de vetores tangentes a uma curva, e portanto comprimentos de curvas na nossa

[3]Para não confundir, passaremos a nos referir a métrica no sentido de espaço métrico como distância.

variedade. Explicitamente, seja (M, g) uma variedade riemanniana e $\gamma : I \to M$ uma curva em M, então o comprimento de γ pode ser obtido assim:

$$L(\gamma) = \int_I ||\gamma'(t)||dt = \int_I \sqrt{g_{\gamma(t)}(\gamma'(t), \gamma'(t))}dt$$

É possível mostrar que esta integral é invariante por parametrizações diferentes.

Queremos que a distância entre dois pontos tome o menor valor, considerando todas as formas de partir de um e chegar no outro. Assim, podemos definir a distância entre dois pontos como o ínfimo dos comprimentos de curvas ligando ambos. Vale considerar um critério de suavidade, como curvas diferenciáveis por partes ou de classe $\mathcal{C}^1$ por partes. Construiremos distância justamente assim, o ínfimo do comprimento de curvas ligando dois pontos, depois observaremos que isto de fato constitui-se como uma métrica. Ainda, provaremos que existe e é única a curva que liga quaisquer dois pontos e cujo comprimento coincide com a distância (chamaremos de geodésica), sendo curvas análogas a retas, no caso euclidiano. Construiremos distância assim nos nossos modelos, deixando clara a estrutura de variedade riemanniana herdada do espaço hiperbólico.

Vale uma observação: esta definição só faz sentido em variedades conexas, para que haja pelo menos uma curva ligando dois pontos.

Uma outra observação, agora um pouco mais técnica, é a seguinte. A definição formal de variedade demanda que esta seja um espaço topológico. É possível provar que a topologia induzida pela distância da forma como a construímos empata com a topologia que começamos, isto é, da variedade enquanto espaço topológico, e isto vale para toda variedade riemanniana (Hausdorff).

7.3 Revisão de Geometria Euclidiana

Antes de começarmos, é interessante ponderar um pouco sobre o significado do termo "geometria". Felix Klein, dentro do programa de Erlangen, define geometria da seguinte forma: "Dado um conjunto munido de uma estrutura e de um grupo de transformações que preservam tal estrutura, geometria é o estudo dos objetos que são invariantes por tais transformações. No caso da geometria euclidiana, o conjunto é $\mathbb{R}^2$ (ou n, mais geralmente). Neste caso específico, apesar de também ser uma variedade riemanniana, o plano possui uma estrutura natural de espaço métrico e portanto há um jeito fácil de escrever a métrica sem recorrer a ínfimo de comprimentos. O grupo é o de isometrias e usualmente denotado por $\text{Isom}(\mathbb{R}^2)$. O grupo de isometrias que preservam orientação é denotado por $\text{Isom}^+(\mathbb{R}^2)$ e composto por rotações e translações, sendo subgrupo de $\text{Isom}(\mathbb{R}^2)$. Falaremos mais sobre as isometrias depois de um instante.

Em nome da consistência, iremos nos esquecer por um momento da estrutura de espaço métrico do plano e lidarmos como ele apenas enquanto variedade riemanniana. Então, definiremos distância da forma como havíamos falado e provaremos que esta distância empata com a usual.

(em breve)

Um assunto interessante, e que será de especial interesse neste estudo, é a chamada *tesselação*. Isto não é nada mais do que um ladrilhamento do plano, isto é, cobrir o plano com polígonos de forma que os polígonos não se superponham e de forma que vértices se encontrem com vértices. Caso os polígonos sejam regulares, as únicas tesselações possíveis do plano são com triângulos, quadrados ou hexágonos. Na geometria hiperbólica, entretanto, há um número infinito de tesselações possíveis, revelando uma estrutura mais rica do que a da geometria euclidiana. Os grupos fuchsianos, pelos quais estamos interessados, serão ferramentas importantes no estudo das tesselações do plano hiperbólico. Há uma associação entre uma tesselação e um grupo de isometria (o grupo de isometria que preserva a tesselação), conectando assim álgebra com geometria. E, no caso da geometria hiperbólica, estes grupos serão os fuchsianos.

7.4 Modelo do Semiplano Superior

Partiremos agora, de fato, para a geometria hiperbólica. Começaremos considerando o modelo do semiplano complexo superior.

O primeiro modelo de espaço hiperbólico que utilizaremos será o semiplano complexo superior. Na verdade, iremos trabalhar com o plano complexo estendido. Isto é, definimos $\mathbb{H} := \{z \in \mathbb{C}; \mathrm{Im}(z) > 0\}$, e . Rapidamente nota-se que $\mathbb{H}$ corresponde a um dos hemisférios da esfera de Riemann.

8 Geometria Projetiva

9 Grupos Fuchsianos

Há duas maneiras comuns (e equivalentes) de definir um grupo fuchsiano. Ambas, dizem que um grupo fuchsiano é um tipo particular de subgrupo de $PSL(2, \mathbb{R})$. Uma delas diz que grupo fuchsiano é um subgrupo discreto de $PSL(2, \mathbb{R})$, enquanto a outra diz que grupo fuchsiano é um grupo que age descontinuamente.