Grupos Fuchsianos

Kelvyn Welsch

Novembro de 2019

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 $\overline{\mathbb{C}} \coloneqq \mathbb{C} \cup \infty$.

Proposição 1.1. *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.* □

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 $u \coloneqq \Re(\overline{\pi})$ e $v \coloneqq \Im(\overline{\pi})$, 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:

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

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

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 1.2. *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 1.2.1. *$\overline{\mathbb{C}}$ 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 1.3. *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*).

2 Funções Racionais

Lembrete: uma função complexa é dita meromorfa quando é holomorfa num domínio, com exceção de um conjunto discreto de pontos, que são pólos (?).

Proposição 2.1. *Se f é meromorfa em $\overline{\mathbb{C}}$, então f é contínua em $\overline{\mathbb{C}}$* □

Teorema 2.2. *Uma função de $\overline{\mathbb{C}}$ para $\overline{\mathbb{C}}$ é meromorfa se, e somente se é uma função racional* □

Proposição 2.3. *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 $\mathbb{C}$

3 Transformações de Möbius

Definição 3.1. 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.

Proposição 3.1. *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 2.2 e a proposição 2.3 ■

Corolário 3.1.1. *Se $T \in$ Möb, então T é homeomorfismo de $\overline{\mathbb{C}}$.* □

Demonstração. Pela proposição 3.1, T é meromorfa. Pela proposição 2.1, 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. ■

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. Para tanto, verigique que $\ker\theta = \{\lambda\mathbb{I}, \lambda \in \mathbb{C}\}$, onde $\mathbb{I}$ é a matriz identidade.

Apêndice A Teoria de Grupos

A.1 Homomorfismos

Definição A.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 A.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 A.2. Sejam G e H grupos e $h : G \to H$ um homomorfismo. O *núcleo* de h é o conjunto $\ker h$ definido por $\ker h \coloneqq \{g \in G; h(g) = e_H\}$. A *imagem* de h é o conjunto Im $h \coloneqq \{b \in H; \exists g \in G$ com h(g) = b$\}$ ♣

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

A.2 Classes de Conjugação e Subgrupos Normais

Definição A.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 A.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 A.4. Seja 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 A.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 A.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.* $\square$

Definição A.5. Um grupo é dito simples quando seus únicos subgrupos normais são os triviais. ♣

Proposição A.6. *Sejam G, H grupos e $h : G \to H$ um homomorfismo. O núcleo de h é um subgrupo normal de G.* $\square$

Demonstração. Pela proposição A.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 $n \in \ker h$: $h(gng^{-1}) = h(g)e_H h(g)^{-1} = e_H$. ■

A.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 A.6. Sejam G um grupo e $H \subset G$ um subgrupo. Dado $g \in G$, o conjunto $gH \coloneqq \{gh; h \in H\}$ é chamado de *coset à esquerda de H com relação a g* e o conjunto $Hg \coloneqq \{hg; h \in H\}$ é chamado de *coset à direita de H com relação a g.* ♣

Proposição A.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 $E = [g]_E$.* $\square$

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 A.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 A.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 A.7. Seja G um grupo. A ordem de G é definida como a cardinalidade do conjunto G. ♣

Teorema A.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”.

A.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 apêndice.

Teorema A.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 A.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 A.11.2. *Se ϕ é um epimorfismo, então existe um isomorfismo ψ entre $G/\ker\phi$ e H dado por $\psi(g\ker\phi) = \phi(g)$* □

A.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 A.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 A.12. *Seja 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 A.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 A.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 A.14. *Seja 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 A.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 A.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 A.15.1. *$G/Z(G) \cong Inn(G)$.*

Demonstração. Basta aplicar as Proposições A.14 e A.15 no Corolário 2 do Teorema A.11. Existirá um isomorfismo ψ entre $G/ker\theta = G/Z(G)$ e $\mathrm{Inn}(G)$ dado por $\psi(gZ(G)) = \theta(g) = \phi_g$. ■

A.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 A.10. Seja 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 A.11. Seja 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 $y_i = \alpha(g, x_i)$, $1 \leq i \leq k$. ♣

Definição A.12. Seja 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 A.16. *Seja G um grupo e $\alpha : G \times M \to M$ uma ação de G em M. Dado $m \in M$, vale que $n \in Orb_\alpha(m) \implies Orb_\alpha(m) = Orb_\alpha(n)$.* □

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 A.16.1. *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 A.16.2. *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 A.13. Seja 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. Assim como fizemos com a transitividade, forneceremos uma equivalência para a definição de livre e efetiva:

Proposição A.17. *Seja 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 sequinte 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. ∎

Proposição A.18. *Seja 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. ∎

Definição A.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 dos elementos de G tais que os elementos de X são seus pontos fixos 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. Em símbolos: $G_{\alpha,X} \coloneqq \{g \in G; \alpha(g, x) = x, \forall x \in X\}$ ♣

Proposição A.19. *Seja 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. ∎

Proposição A.20. *Seja 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. ∎