V Bienal da SBM
Sociedade Brasileira de Matemática
UFPB - Universidade Federal da Paraíba
18 a 22 de outubro de 2010

Ações de grupos e geometria

Eliezer Batista *

Resumo: Um dos conceitos mais importantes na matemática moderna certamente é o conceito de grupo. Podemos ver a ubiqüidade dos grupos em quase todas as áreas da matemática, como na própria álgebra, na geometria, nas equações diferenciais, na teoria de números, bem como nas ciências naturais, como a física e a química. A idéia principal que confere aos grupos esta importância capital é a noção de simetria. Sempre em ciência tentamos reconhecer padrões e simetrias em nossos objetos de estudo, sejam eles uma molécula, um pêndulo físico, uma equação diferencial, um sólido geométrico, as raízes de uma equação polinomial, etc. A partir do momento em que identificamos as simetrias de nosso sistema, estamos introduzindo um grupo de transformações, ou uma ação de grupo. Uma ação de um grupo em um conjunto é uma função do grupo no conjunto das bijeções daquele conjunto dado de forma que as operações do grupo sejam compatíveis com a composição de funções no conjunto. O grupo é uma abstração deste conjunto de bijeções neste conjunto específico, podemos falar dos elementos de um grupo de maneira intrínseca, auto-contida, sem qualquer referência a um conjunto externo onde ele age. Esta é a perspectiva da maioria dos livros de álgebra existentes na atualidade. No entanto, no nível das aplicações, os grupos somente são relevantes quando "encarnados", em grupos de transformações. Nosso objetivo neste minicurso é esclarecer melhor esta inter relação entre o ponto de vista abstrato, do grupo como uma estrutura existente por si própria, e o ponto de vista concreto, do grupo agindo em outros conjuntos como bijeções. Para tornarmos esta discussão interessante e motivadora, pretendemos abordar vários aspectos da geometria afim e projetiva sob o ponto de vista de ações de grupos.

1 Introdução

A primeira aparição do conceito de grupo em matemática se dá no contexto do estudo de equações polinomiais. O problema em questão era encontrar fórmulas para se determinar as raízes de um polinômio de grau maior ou igual a 5. Desde os trabalhos de Lagrange[1] as permutações das raízes de um polinômio eram consideradas importantes para a procura de métodos gerais de solução. Com o teorema de Abel[2] ficou claro que nem todas as equações polinomiais admitiam métodos de solução por radicais. A pergunta que restou era: "Quais equações polinomiais admitiam solução por radicais?". Esta pergunta foi respondida por Galois[3], que formulou muitos conceitos matemáticos inovadores para resolver este problema, inclusive o conceito de grupo. Os trabalhos de Galois somente puderam ser apreciados e entendidos postumamente, pois a primeira edição de seus trabalhos completos foi editada por Joseph Liouville em 1846.

Apenas algumas décadas mais tarde, ainda no século XIX a teoria de grupos já havia se expandido para outras áreas da matemática, isto se deve grandemente ao trabalho do matemático norueguês Sophus Lie[4]. Basicamente, Lie tentou estender a teoria de Galois para equações diferenciais, mas, diferentemente das equações algébricas, onde as simetrias envolvendo as raízes eram finitas, as simetrias das soluções das equações diferenciais eram contínuas. Pela primeira vez, além de técnicas puramente algébricas para se tratar de grupos, foram necessários várias técnicas oriundas da análise para se compreender melhor a estrutura dos grupos de Lie[5]. Os grupos de Lie são os grupos

*Universidade Federal de Santa Catarina, Florianópolis, SC, Brasil, ebatista@mtm.ufsc.br

[1]Para mais detalhes sobre a vida e obra de Lagrange, veja a página: http://en.wikipedia.org/wiki/Joseph_Louis_Lagrange

[2]Veja estas excelentes notas de aula disponíveis na internet: http://www.cds.caltech.edu/∼nair/abel.pdf

[3]http://en.wikipedia.org/wiki/Évariste_Galois

[4]Veja o texto na Wikipédia: http://en.wikipedia.org/wiki/Sophus_Lie

[5]Veja este interessante curso introdutório sobre grupos de Lie: http://www.physics.drexel.edu/∼bob/LieGroups.html

mais utilizados em aplicações desde ramos da matemática pura, como equações diferenciais, geometria diferencial, até aplicações em ciências físicas como mecânica clássica, física quântica, teoria de campos, entre outras. Particularmente em geometria, que será o tema principal destas notas de aula, a importânncia da teoria de grupos foi ressaltada pelo matemático alemão Felix Klein[6]. Em 1871, ainda em Göttingen, Klein escreveu um artigo sobre a geometria não euclidiana, dando especial atenção aos espaços projetivos. Ficou claro para ele que os grupos de transformação exercem influência capital na definição dos objetos geométricos. Isto motivou a criação, em 1872, já na universidade de Erlangen, de todo um projeto de pesquisas com o intuito de definir as geometrias como sendo o estudo dos objetos que são invariantes por grupos de transformações, este projeto é hoje conhecido como "Programa de Erlangen".

Neste minicurso, vamos mostrar os diferentes aspectos de ações de grupos em geometria. Para isto, vamos nos restringir a dois tipos especiais de geometria, a geometria afim e a geometria projetiva. Por que geometria afim? Bem, em primeiro lugar, os espaços afins são, desde a antiguidade, os ambientes mais naturais para se descrever os objetos geométricos. em segundo lugar, porque os espaços afins são a coisa mais próxima de espaços vetoriais, portanto, as técnicas e a linguagem da álgebra linear ainda podem ser adaptadas para o contexto destes espaços. E a geometria porjetiva? Também porque os espaços projetivos são definidos a partir de espaços vetoriais e porque os espaços projetivos são conjuntos quocientes, assim podemos exemplificar muitos conceitos pertinentes à teoria dos grupos, como grupos quocientes e espaços de órbitas utilizando elementos da geometria projetiva. Faremos o máximo possível para mantermos estas notas de aula autocontidas, o único pré-requisito assumido é um conhecimento elementar dos conteúdos básicos de álgebra linear, como o conceito de espaço vetorial e de transformação linear, assumimos também uma certa familiaridade com matrizes de transformações lineares, é necessário que se saiba escrever a matriz de uma transformação linear em qualquer base. Os resultados mais importantes serão todos demonstrados, no entando, alguns detalhes serão sempre deixados como exercício para se adquirir prática com a linguagem e os conceitos.

2 Grupos, Subgrupos e Homomorfismos

Definição 2.1. *Um grupo é um par $(G, \cdot)$ onde G é um conjunto não vazio e*

$$\begin{array}{rccc} \cdot : & G \times G & \to & G \\ & (a, b) & \mapsto & a \cdot b \end{array}$$

é uma função, denominada operação do grupo, satisfazendo

1. *(Associatividade) Para todos os elementos $a, b, c \in G$ temos $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
2. *(Elemento neutro) Existe um elemento $e \in G$ tal que para todo $a \in G$ tenhamos $a \cdot e = e \cdot a = a$.*
3. *(Elemento inverso) A todo elemento $a \in G$ associa-se um elemento a^{-1} tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$.*

Exercício 2.1: Mostre que existe um único elemento neutro em um grupo.

Exercício 2.2: Mostre que existe um único elemento inverso para cada elemento $a \in G$.

A operação no grupo nem sempre é comutativa, quando isto ocorre, temos uma classe particular de grupos, os grupos abelianos.

Definição 2.2. *Um grupo $(G, \cdot)$ é dito ser abeliano, ou comutativo se para todos os elementos $a, b \in G$ tivermos $a \cdot b = b \cdot a$, ou seja, a operação do grupo satisfaz À propriedade da comutatividade*

[6] http://en.wikipedia.org/wiki/Felix_Klein

Antes de irmos para os exemplos, uma última definição.

Definição 2.3. *Um subconjunto não vazio H de um grupo G é dito ser um sub-grupo de G se H com a operação de G também for um grupo.*

Exercício 2.3 mostre que se $H \subseteq G$ é subgrupo, então o elemento neutro de H é igual ao elemento neutro de G e para qualquer $a \in H$, seu inverso com relação a H é o mesmo inverso com relação a G.

Exercício 2.4: Mostre que uma condição necessária e suficiente para que $H \subseteq G$ seja subgrupo de G é que para quaisquer $a, b \in H$, tivermos que $a \cdot b^{-1} \in H$.

Exercício 2.5: Mostre que um subgrupo de um grupo abeliano também é abeliano.

Vejamos alguns exemplos de grupos e subgrupos.

Exemplo 2.1. *O conjunto dos números inteiros com a operação de adição, $(\mathbb{Z}, +)$, é um grupo abeliano,pois a soma é associativa, comutativa, o elemento neutor é o número 0 e o inverso de $n \in \mathbb{Z}$ é o seu oposto, $-n$. Os números inteiros múltiplos de um determinado $m \in \mathbb{Z}$ são subgrupos de Z com a operação adição.*

Exemplo 2.2. *Seja $n \in \mathbb{Z}$ um número inteiro positivo. O conjunto das classes de congruência módulo n, denotado por $\mathbb{Z}_n$ é um grupo, induzido pela operação de adição dos números inteiros: $\bar{k} + \bar{l} = \overline{k+l}$. Este grupo é um grupo abeliano com n elementos, que são $\bar{0}, \bar{1}, \ldots, \bar{n-1}$.*

Exemplo 2.3. *O conjunto dos números reais também com a operação de adição, $(\mathbb{R}, +)$, também é um grupo abeliano e podemos ver que $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ são subgrupos de $(\mathbb{R}, +)$.*

Exemplo 2.4. *O conjunto dos números complexos não nulos com a operação de multiplicação, $(\mathbb{C}^*, \cdot)$ é um grupo abeliano, pois a multiplicação é associativa, comutativa, o elemento neutro é o número 1 e todo número complexo não nulo possui inverso multiplicativo. Os conjuntos $(\mathbb{R}^*, \cdot)$ e $(\mathbb{Q}^*, \cdot)$ são subgrupos abelianos de $(\mathbb{C}^*, \cdot)$.*

Exemplo 2.5. *O subconjunto dos números complexos de módulo unitário, $U(1) = \{z \in \mathbb{C} \mid |z| = 1\}$ é um subgrupo de $(\mathbb{C}^*, \cdot)$. Geometricamente, este conjunto corresponde à circunferência no plano complexo de raio 1 e centro na origem. Se $z = a + bi$, então*

$$|z| = \sqrt{z\bar{z}} = \sqrt{(a+bi)(a-bi)} = \sqrt{a^2 + b^2}.$$

Se $|z| = 1$, então $z^{-1} = a - bi$ e $|z^{-1}| = |z| = 1$. Além disto, se $z, w \in U(1)$, então

$$|zw^{-1}| = |z||w^{-1}| = |z||w| = 1.$$

Portanto $zw^{-1} \in U(1)$, mostrando que $U(1)$ é subgrupo de $(\mathbb{C}^*, \cdot)$.

Exemplo 2.6. *Seja X um conjunto qualquer e $Bij(X) = \{f : X \to X \mid f \text{ é bijeção }\}$. Vamos verificar que $Bij(X)$ é um grupo com a operação dada pela composição de funções, de fato, veremos mais adiante que todo grupo pode ser visto como um subgrupo de um grupo de bijeções sobre um determinado conjunto.*

Em primeiro lugar, a composição de funções é associativa, isto é, $f \circ (g \circ h) = (f \circ g) \circ h$, sempre que for possível efetuar a composição. Em nosso caso, todas as funções possuem como domínio todo o conjunto X e seus conjuntos imagem também são o conjunto X. Também sabemos que a função identidade Id_X quando composta com qualquer função $f : X \to X$ resulta na própria f, isto é, $f \circ Id_X = Id_X \circ f = f$. Além do mais, Id_X é uma bijeção e portanto pertence a $Bij(X)$. Além disto, uma função $f : X \to X$ é bijeção se, e somente se, possuir função inversa, isto é, uma função $g : X \to X$ tal que $g \circ f = f \circ g = Id_X$, e esta inversa é também uma bijeção.

Resta-nos saber o principal, isto é, se a composta de duas bijeções também é uma bijeção para caracterizarmos $Bij(X)$ como um grupo. Para isto, tome $f, g \in Bij(X)$, então existem f^{-1} e g^{-1}, também pertencentes a $Bij(X)$. Note que

$$f \circ g \circ g^{-1} \circ f^{-1} = g^{-1} \circ f^{-1} \circ f \circ g = Id_X.$$

Portanto $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$, o que mostra que $f \circ g \in Bij(X)$. Note que, em geral, o grupo $Bij(X)$ não é abeliano.

Exemplo 2.7. *Seja $I_n = \{1, \ldots, n\}$, uma permutação em I_n é uma bijeção $\pi : I_n \to I_n$. O conjunto $S_n = \{\pi : I_n \to I_n \,|\, \pi$ é permutação $\}$ com a operação dada pela composição é um grupo, pois é um caso particular do exemplo anterior.*

Um elemento genérico do grupo de permutações S_n pode se esrito da seguinte maneira

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}.$$

Vamos exemplificar com $n = 3$. Em S_3 temos os elementos

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$\pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Este é o menor grupo não abeliano existente.

A composição de duas permutações é feita como composta de funções (leitura da direita para a esquerda[7]). Assim, por exemplo

$$\pi_1 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \pi_4.$$

Exercício 2.6: Escreva a tábua de composição do grupo de permutações S_3.

Exemplo 2.8. *Consideremos um subconjunto interessante das bijeções em $\mathbb{R}$: Sejam $a, b \in \mathbb{R}$ números reais tais que $a \neq 0$, defina $f_{a,b} : \mathbb{R} \to \mathbb{R}$ por $f_{a,b}(x) = ax + b$. Seja $Aff(\mathbb{R})$ o conjunto de tais funções (que depois veremos se tratarem das transformações afins na reta), vamos verificar que $Aff(\mathbb{R})$ é um subgrupo A composta de duas funções deste tipo é dada por*

$$f_{c,d} \circ f_{a,b}(x) = f_{c,d}(ax + b) = c(ax + b) + d = cax + (cb + d) = f_{ca,cb+d}(x).$$

Em particular, desta expressão é fácil ver que $f_{a,b}^{-1} = f_{\frac{1}{a},-\frac{b}{a}} \in Aff(\mathbb{R})$. Também podemos ver que a função identidade $Id_{\mathbb{R}}$ pode ser escrita como $Id_{\mathbb{R}} = f_{1,0} \in Aff(\mathbb{R})$. Assim, chegamos à conclusão que $Aff(\mathbb{R})$ é um subgrupo de $Bij(\mathbb{R})$.

Exemplo 2.9. *De particular interesse para o estudo da geometria são os grupos de transformações lineares e alguns de seus subgrupos. Para fixarmos as notações, seja $\mathbb{V}$ um espaço vetorial (a menos que se diga o contrário, vamos assumir que os espaços vetoriais sejam todos sobre o corpo dos reais, $\mathbb{R}$). Seja $GL(\mathbb{V})$ o conjunto de todas as transformações lineares invertíveis de $\mathbb{V}$ em $\mathbb{V}$. Certamente, este é um subconjunto do grupo de bijeções $Bij(\mathbb{V})$, como a composição de duas transformações lineares também é linear e a inversa de uma transformação linear também é linear, então temos que $GL(\mathbb{V})$ é um subgrupo de $Bij(\mathbb{V})$.*

[7] Muito embora alguns autores adotem a convenção oposta para que a leitura seja da esquerda para a direita

Exercício 2.7: Mostre que a composta de duas transformações lineares invertível é uma transformação linear invertível e que a inversa de uma transformação linear também é uma transformação linear invertível.

No caso em que o espaço vetorial $\mathbb{V}$ é de dimensão finita (digamos, $\dim(\mathbb{V}) = n$ podemos identificar as transformações lineares de $\mathbb{V}$ em $\mathbb{V}$ com matrizes quadradas $n \times n$. Para isto, basta tomarmos uma base $\{e_1, \ldots, e_n\}$ e definirmos, para uma dada transformação linear $T : \mathbb{V} \to \mathbb{V}$, a matriz $\widehat{T} = (t_{ij})_{i,j}$ tal que $T(e_j) = \sum_{i=1}^{n} t_{ij} e_i$. A condição de que $T \in GL(\mathbb{V})$ equivale, em termos matriciais, à condição $\det(\widehat{T}) \neq 0$. Geometricamente, podemos entender o determinante $\det(\widehat{T})$ como o volume (com sinal) do peralelepípedo n dimensional determinado pelos vetores $T(e_1), \ldots, T(e_n)$. Dizermos que $T : \mathbb{V} \to \mathbb{V}$ é inversível, em dimensão finita, é equivalente a dizermos que T é injetiva, ou ainda, que $T(e_1), \ldots, T(e_n)$ são linearmente independentes, o que equivale a dizer que o volume do paralelogramo determinado por estes vetores é não nulo.

Exemplo 2.10. *Definamos $GL(n, \mathbb{R})$ como o conjunto das matrizes $n \times n$ de determinante não nulo. Como você já deve ter notado, este conjunto corresponde ao grupo $GL(\mathbb{V})$ no caso em que $\dim(\mathbb{V}) = n$, portanto, também deve ser um grupo. Mais adiante tornaremos mais precisa esta noção de correpondência entre os grupos com a definição de isomorfismo. Por agora, basta-nos verificar que $GL(n, \mathbb{R})$ é um grupo, para isto, sejam $A, B \in GL(n, \mathbb{R})$, então $\det(AB) = \det(A)\det(B) \neq 0$, logo $AB \in GL(\mathbb{V})$. Também temos que $\det(I) = 1 \neq 0$ e que $\det(AA^{-1}) = \det(I) = 1$, logo $\det(A^{-1}) = \frac{1}{\det(A)} \neq 0$. Com estes resultados, temos que $GL(n, \mathbb{R})$ é um grupo.*

Exercício 2.8: Mostre que $\det(AB) = \det(A)\det(B)$.

Exemplo 2.11. *Existem alguns sub-grupos dos grupos lineares que são importantes para aplicações: O primeiro exemplo é o subgrupo linear especial $SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) \,|\, \det(A) = 1$. Para vermos que, de fato, $SL(n, \mathbb{R})$ é subgrupo de $GL(n, \mathbb{R})$, tome $A, B \in SL(n, \mathbb{R})$, temos que $\det(B^{-1}) = \frac{1}{\det(B)} = 1$ e, portanto*

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = 1.$$

Portanto $AB^{-1} \in SL(n, \mathbb{R})$.

Exemplo 2.12. *Considere agora que $\mathbb{V}$ de dimensão finita esteja munido com um produto escalar euclidiano*

$$\begin{array}{rccc} \langle \cdot, \cdot \rangle : & \mathbb{V} \times \mathbb{V} & \to & \mathbb{R} \\ & (v, w) & \mapsto & \langle v, w \rangle \end{array}$$

onde, se $v = (v^1, v^2, \ldots, v^n)$ e $w = (w^1, w^2, \ldots, w^n)$, então

$$\langle v, w \rangle = \sum_{i=1}^{n} v^i w^i.$$

O conjunto das transformações lineares que preserva o produto escalar, ou transformações ortogonais é denotado por $O(\mathbb{V})$. Um elemento de $O(\mathbb{V})$ é uma transformação linear A tal que

$$\langle Av, Aw \rangle = \langle v, w \rangle.$$

Vamos mostrar que $O(\mathbb{V})$ é um grupo. Primeiramente, se $A, B \in O(\mathbb{V})$ então

$$\langle (AB)v, (AB)w \rangle = \langle A(Bv), A(Bw) \rangle = \langle Bv, Bw \rangle = \langle v, w \rangle.$$

Portanto $AB \in O(\mathbb{V})$. Também temos que

$$\langle \mathrm{Id}v, \mathrm{Id}w \rangle = \langle v, w \rangle,$$

o que nos leva à conclusão que $\mathrm{Id} \in O(\mathbb{V})$*. Finalmente, dada a tranformação linear* $A : \mathbb{V} \to \mathbb{V}$*, definimos a adjunta da transformação linear* A *como a transformação linear* $B : \mathbb{V} \to \mathbb{V}$ *tal que*

$$\langle Av, w\rangle = \langle v, Bw\rangle, \qquad \forall v, w \in \mathbb{V}.$$

É fácil ver que a adjunta de uma transformação linear é única, portanto denominaremos por A^**. Agora, se* $A \in O(\mathbb{V})$ *então, dados quaisquer* $v, w \in \mathbb{V}$ *temos*

$$\langle v, w\rangle = \langle Av, Aw\rangle = \langle v, A^*Aw\rangle,$$

portanto

$$\langle v, (w - A^*Aw)\rangle = 0, \qquad \forall v \in \mathbb{V},$$

o que implica que $A^*Aw = w$ *para todo* $w \in \mathbb{V}$*, ou seja,* $A^*A = \mathrm{Id}$*. Um raciocínio análogo, com*

$$\langle Av, w\rangle$$

mostra que $AA^* = \mathrm{Id}$*. Portanto* $A^* = A^{-1}$ *o que nos leva à conclusão que* $O(\mathbb{V})$ *é um grupo.*

Exercício 2.9: Mostre que, realmente, a adjunta de uma transformação linear, se existir, é única.

Exercício 2.10: Considere uma base ortonormal $\{e_1, \dots e_n\}$ de $\mathbb{V}$ com produto interno euclidiano e uma tranformação linear $A : \mathbb{V} \to \mathbb{V}$ uma transformação linear qualquer. Construa explicitamente a adjunta A^*. Mostre que a matriz de A^* na base acima é a transposta da matriz de A, isto é, $\widehat{A^*} = A^T = (a_{ji})_{i,j}$.

Exercício 2.11: Mostre que $(AB)^* = B^*A^*$ e que isto, matricialmente, implica em $(\widehat{AB})^T = \widehat{B}^T\widehat{A}^T$.

Exercício 2.12: Mostre que a matriz de uma transformação ortogonal A satifaz $\widehat{A}^T = \widehat{A}^{-1}$.

Você percebeu que com a mesma associação que fizemos de cada transformação linear à sua matriz de transformação linear, as transformações ortogonais estarão associadas a matrizes que satisfarão a propriedade do exercício 2.12. Estas matrizes são chamadas matrizes ortogonais. Também você já desconfia que o conjunto das matrizes ortogonais $n \times n$, denotado por $O(n)$, também será um grupo, de fato será subgrupo de $GL(n, \mathbb{R})$.

Exercício 2.13: Mostre que o determinante de uma matriz ortogonal só pode assumir os valores 1 e -1.

Exemplo 2.13. *O conjunto das matrizes ortogonais de terminante* 1*, denotado por* $SO(n) = SL(n, \mathbb{R}) \cap O(n)$ *também é um grupo, denominado grupo ortogonal especial, pois trata-se da intersecção de dois subgrupos de* $GL(n, \mathbb{R})$*.*

Exercício 2.14: Mostre que, de fato, a interscção de dois subgrupos de um grupo G também é um subgrupo de G.

Com esta coleção de exemplos suficientemente ampla para nos fornecer intuição, podemos avançar um pouco mais na teoria de forma a entendermos as interrelações entre diversos grupos. Para relacionarmos grupos distintos, precisamos definir funções entre eles que sejam compatíveis com as suas operações internas, estas funções são denominadas homomorfismos.

Definição 2.4. *Dados dois grupos* G *e* H*, uma função* $\varphi : G \to H$ *é dita ser um homomorfismo de grupos se* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$*, para todos os elementos* $a, b \in G$*. Se o homomorfismo é injetivo, dizemos que ele é um monomorfismo. Se o homomorfismo é sobrejetivo, dizemos que ele é um epimorfismo. Se o homomorfismo é bijetivo, dizemos que ele é um isomorfismo.*

Denotaremos $G \cong H$ quando os grupos G e H forem isomorfos.

Definição 2.5. *Um homomorfismo sobre o mesmo grupo é denominado um endomorfismo. Um endomorfismo bijetor, isto é um isomorfismo sobre o mesmo grupo é denominado um automorfismo.*

Exercício 2.15: Mostre que, se $\varphi : G \to H$ é um homomorfismo de grupos, então

1. $\varphi(e_G) = e_H$.

2. Para qualquer $a \in G$, temos que $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

Exercício 2.16: Mostre que, se $\phi : G \to H$ é um homomorfismo de grupos e $K \subseteq G$ é um subgrupo, então $\phi(K) \subseteq H$ também é um subgrupo. Mstre também que de K é um subgrupo abeliano de G, então $\phi(K)$ também é subgrupo abeliano de H.

O primeiro grande resultado que vamos mostrar é que todo grupo é isomorfo a um subgrupo de um grupo de bijeções.

Teorema 2.1. *Todo grupo G é isomorfo a um sub-grupo do grupo das bijeções em G.*

Demonstração: Seja $a \in G$, defina a função

$$\begin{array}{rccc} L_a: & G & \to & G \\ & b & \mapsto & a \cdot b \end{array}$$

Vejamos que L_a é injetiva. De fato, se $L_a(b) = L_a(c)$, isto significa que $a \cdot b = a \cdot c$. Multiplicando esta última igualdade à esquerda por a^{-1}, teremos $a^{-1} \cdot a \cdot b = a^{-1} \cdot a \cdot c$, e portanto, $b = c$, o que implica que L_a é injetiva.

Para vermos que L_a é sobrejetiva, tome $b \in G$, podemos escrever $b = a \cdot a^{-1} \cdot b$, ou seja, $b = L_a(a^{-1} \cdot b)$. Portanto L_a é sobrejetiva.

Disto concluimos que $L(G) \subseteq \text{Bij}(G)$. Sejam agora $a, b, c \in G$, temos que

$$L_a \circ L_b(c) = L_a(b \cdot c) = a \cdot (b \cdot c) = (a \cdot b) \cdot c = L_{a \cdot b}(c).$$

Temos também que, para todo elemento $a \in G$

$$L_e(a) = e \cdot a,$$

portanto, $L_e = \text{Id}_G$. Finalmente, temos que para todo $a \in G$,

$$L_{a^{-1}} \circ L_a = L_{a^{-1} \cdot a} = L_e = \text{Id}_G,$$

de maneira análoga, podemos mostrar que $L_a \circ L_{a^{-1}} = \text{Id}_G$. Portanto $L_{a^{-1}} = (L_a)^{-1}$.

Sejam $a, b \in G$, temos que

$$L_a \circ (L_b)^{-1} = L_a \circ L_{b^{-1}} = L_{a \cdot b^{-1}} \in L(G),$$

logo $L(G)$ é sub-grupo de $\text{Bij}(G)$. Resta-nos mostrar que G está em correspondência 1 a 1 com $L(G)$, ou seja, falta-nos verificar que a função

$$\begin{array}{rccc} L: & G & \to & L(G) \subseteq \text{Bij}(G) \\ & a & \mapsto & L_a \end{array},$$

que é um homomorfismo de grupos, conforme foi mostrado, também é bijetiva.

Para a injetividade de L, suponha que $L_a = L_b$, isto significa que, para qualquer $c \in G$ temos $L_a(c) = L_b(c)$, ou ainda $a \cdot c = b \cdot c$. Em particular, para $c = e$, o elemento neutro de G, temos $a = a \cdot e = b \cdot e = b$. A sobrejetividade sobre $L(G)$ é óbvia, pois toda bijeção em $L(G)$ é da forma L_a para algum $a \in G$. Portanto G é isomorfo ao subgrupo $L(G)$ em $\text{Bij}(G)$ e portanto, pode ser identificado com este subgrupo. ■

Um corolário muito famoso do teorema acima é o chamado teorema de Cayley, que caracteriza todos os grupos finitos como subgrupos do grupo de permutação:

Corolário 2.1. *(Teorema de Cayley) Todo grupo finito é isomorfo a um subgrupo de um grupo de permutações.*

Para a verificação da injetividade dos homomorfismos, podemos estabelecer um critério muito útil, análogo ao critério para decidir de uma transformação linear é injetiva ou não:

Definição 2.6. *Dado um homomorfismo de grupos $\phi : G \to H$, definimos o kernel de ϕ, como o subconjunto*

$$\ker(\phi) = \{g \in G \,|\, \phi(g) = e_H\}.$$

Exercício 2.17: Mostre que o kernel do homomorfismo $\phi : G \to H$, é um subgrupo de G.

Proposição 2.1. *O homomorfismo $\phi : G \to H$ é injetivo se, e somente se* $\ker(\phi) = \{e_G\}$.

Demonstração: ($\Rightarrow$) Se ϕ é injetiva e $g \in \ker(\phi)$ então $\phi(g) = e_H = \phi(e_G)$, então, pela injetividade, temos que $g = e_G$.

($\Leftarrow$) Considere $g, h \in G$ tais que $\phi(g) = \phi(h)$, então

$$e_H = \phi(g)(\phi(h))^{-1} = \phi(g)\phi(h^{-1}) = \phi(gh^{-1}),$$

ou seja, $gh^{-1} \in \ker(\phi)$. Como $\ker(\phi) = \{e_G\}$ então $gh^{-1} = e_G$, o que implica em $g = h$. ■

Exercício 2.18: Seja $\mathbb{V}$ um espaço vetorial de dimensão n, com uma base $\{e_1, \ldots, e_n\}$ e dada uma transformação linear $A : \mathbb{V} \to \mathbb{V}$, denotemos por $\widehat{A}$ a matriz da transformação linear nesta base escolhida. Mostre que a aplicação

$$\begin{array}{rccc} \widehat{\cdot}: & GL(\mathbb{V}) & \to & GL(n,\mathbb{R}) \\ & A & \mapsto & \widehat{A} \end{array}$$

é um isomorfismo de grupos.

Exercício 2.19: Dado o isomorfismo do exercício anterior, e supondo que $\mathbb{V}$ é um espaço com produto interno e que a base escolhida é ortonormal com relação a este produto interno, mostre que $O(\mathbb{V}) \cong O(n)$.

Exemplo 2.14. *Para darmos nosso próximo exemplo de isomorfismo. Consideremos o caso particular do grupo $SO(2)$, que é o grupo das matrizes ortogonais 2×2. Se $A \in SO(2)$ então*

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

tal que

$$A^T = \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = A^{-1}.$$

Portanto $a = d$ e $b = -c$, o que reduz a matriz à forma

$$A = \begin{pmatrix} a & -c \\ c & a \end{pmatrix}.$$

A condição $\det(A) = 1$ *nos fornece a igualdade*

$$a^2 + c^2 = 1,$$

o que nos leva à conclusão que existe $\theta \in \mathbb{R}$ tal que $a = \cos\theta$ e $c = \sin\theta$, ou seja,

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Esta é a matriz de rotação de um ângulo θ no plano, que denominaremos de R_θ.

Defina agora a aplicação

$$\begin{array}{rccc} \phi: & U(1) & \to & SO(2) \\ & e^{i\theta} & \mapsto & R_\theta \end{array}.$$

É fácil ver que esta aplicação é realmente um homomorfismo de grupos (verifique os detalhes como exercício). Para verificarmos a injetividade, considere $e^{i\theta} \in \ker(\phi)$*, então*

$$R_\theta = \mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{pmatrix}.$$

Portanto $\cos\theta = \cos 0$ *e* $\sin\theta = \sin 0$*, o que nos leva a* $\theta = 0$*, ou seja* $e^{i\theta} = e^{i.0} = 1$*, que é o elemento neutro do grupo* $U(1)$*. Portanto,* ϕ *é um morfismo injetor. Para a sobrejetividade, seja* $A \in SO(2)$*. Como vimos, existe um número real* θ *tal que* $A = R_\theta = \phi(e^{i\theta})$*.*

Exemplo 2.15. *A aplicação*

$$\begin{array}{rccc} \det: & GL(n,\mathbb{R}) & \to & \mathbb{R}^* \\ & A & \mapsto & \det(A) \end{array}$$

onde $\mathbb{R}^*$ *é o grupo multiplicativo dos reais não nulos, é um homomorfismo de grupos, devido à propriedade multiplicativa dos determinantes. Note que o kernel da aplicação determinante é o conjunto das matrizes de determinante igual a* 1*, ou seja,* $\ker(\det) = SL(n,\mathbb{R})$*.*

Exemplo 2.16. *Considere o grupo* $Aff(\mathbb{R})$ *e a aplicação*

$$\begin{array}{rccc} \phi: & Aff(\mathbb{R}) & \to & GL(2,\mathbb{R}) \\ & f_{a,b} & \mapsto & \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \end{array}.$$

Vamos verificar que ϕ *é um monomorfismo. Primeiramente*

$$\phi(f_{a,b} \circ f_{c,d}) = \phi(f_{ac,ad+b}) = \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix}.$$

Por outro lado,

$$\phi(f_{a,b})\phi(\circ f_{c,d}) = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix},$$

o que mostra que ϕ *é homomorfismo. Para provarmos a injetividade, seja* $f_{a,b} \in \ker(\phi)$*, então*

$$\phi(f_{a,b}) = \mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

o que nos leva à conclusão que $a = 1$ *e* $b = 0$*, ou seja,* $f_{a,b} = f_{1,0} = \mathrm{Id}$*, o que significa que* ϕ *é injetivo.*

Exercício 2.20: Utilizando o mesmo homomorfismo do exemplo acima, determine o subgrupo de $GL(2,\mathbb{R})$ que é isomorfo ao grupo aditivo dos reais.

Exercício 2.21: O grupo diedral D_3 é o grupo das simetrias do triângulo equilátero, seus elementos são mostrados na figura a seguir:

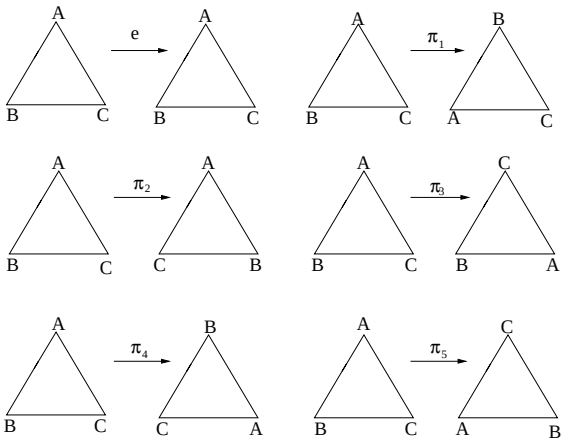

Figura 2.1: Simetrias do triângulo equilátero.

Construa um isomorfismo entre S_3 e D_3.

Como um último tópico a ser abordado nesta seção, mostraremos como um sub-grupo H de um grupo G pode introduzir uma relação de equivalência em G.

Exercício 2.22: Seja G um grupo e H um subgrupo. Mostre que as relações $g \sim_L h \Leftrightarrow g^{-1}h \in H$ e $g \sim_R h \Leftrightarrow gh^{-1} \in H$, são relações de equivalência em G.

Definição 2.7. *Dado um sub-grupo H de um grupo G e um elemento $g \in G$, definimos a classe lateral à esquerda de g associada a H como o conjuunto*

$$gH = \{k \in G | k \sim_L g\}.$$

Similarmente, a classe lateral à direita de g em relação a H é o conjunto

$$Hg = \{k \in G | k \sim_R g\}.$$

Podemos também caracterizar a classe lateral à esquerda gH como o conjunto dos elementos $k \in G$ tais que podem ser escritos como $k = g \cdot h$ para algum $h \in H$. Durante toda nossa discussão, utilizaremos classes laterais à esquerda, a menos que se diga o contrário.

Proposição 2.2. *Duas classes laterais à esquerda g_1H e g_2H ou são disjuntas ou são iguais*

Demonstração: Suponha que exista um elemento $k \in g_1H \cap g_2H$, então existem $h_1, h_2 \in H$ tais que

$$k = g_1 \cdot h_1 = g_2 \cdot h_2.$$

Multiplicando-se esta última igualdade à direita por h_1^{-1}, temos que

$$g_1 = g_2 \cdot h_2 \cdot h_1^{-1} \in g_2H.$$

Logo para qualquer $g_1 \cdot h \in g_1H$ concluímos que

$$g_1 \cdot h = g_2 \cdot h_2 \cdot h_1^{-1} \cdot h \in g_2H.$$

Analogamente, podemos provar também que $g_2H \subseteq g_1H$ e portanto, as duas classes são iguais. ■

Uma outra propriedade importante das classes laterais à esquerda é que elas estão em bijeção com o sub-grupo H.

Exercício 2.23: Mostre que a aplicação $L_g : H \to gH$ é uma bijeção (não homomorfismo) entre H e gH.

No caso de grupos finitos, temos um importante resultado sobre a ordem das classes laterais, o teorema de Lagrange.

Teorema 2.2. *Seja G um grupo finito e H um sub-grupo e sejam $|G|$ e $|H|$ suas respectivas ordens (número de elementos). Então a quantidade de classes laterais relativas e H é igual a*

$$\#C = \frac{|G|}{|H|}.$$

Demonstração: Pela proposição anterior, podemos ver que as classes laterais são disjuntas duas a duas. Então, escolhamos um representante para cada classe: $g_1, g_2, \ldots, g_n$, o que queremos saber é qual o valor deste número n. Pelo exercício anterior, verificamos que todas as classes g_1H, g_2H, ..., g_nH estão em bijeção com H, logo o número de elementos de cada classe é igual à ordem do sub-grupo H. Assim, a ordem do grupo G pode ser escrita como o produto do número de classes laterais pelo número de elementos em cada classe lateral, ou seja $|G| = n|H|$, sendo assim,

$$\#C = n = \frac{|G|}{|H|}. \qquad \blacksquare$$

Como corolário imediato do teorema de Lagrange, podemos enunciar que

Corolário 2.2. *A ordem de um sub-grupo de um grupo finito é sempre um divisor da ordem do grupo.*

Note que, se um grupo G não é abeliano, e H é um subgrupo qualquer, nem sempre ocorrerá de as classes laterais À esquerda coincidirem com as classes laterais à direita.

Exercício 2.24: Considere o grupo S_3 e o subgrupo $H = \{e, \pi_1\}$. Construa as classes laterais à esquerda e à direita.

Definição 2.8. *Seja G um grupo e $H \subseteq G$ um subgrupo. Se as classes laterais à esquerda e à direita de H coincidirem, diremos que H é um subgrupo normal de G, denotado como $H \trianglelefteq G$.*

Proposição 2.3. *Seja G um grupo e $H \subseteq G$ um subgrupo. Então são equivalentes as seguintes afirmativas:*

(i) H é subgrupo normal.

(ii) Para qualquer $g \in G$, temos que $gHg^{-1} = H$.

(iii) Para qualquer $g \in G$, temos que $gHg^{-1} \subseteq H$.

Demonstração: (i)⇒(ii) Seja $g \in G$ e considere as duas classes laterais gH e Hg. Por hipótese, estes dois conjuntos são iguais, isto é, para todo $h \in H$ existe $k \in H$ tal que $gh = kg$, assim, seja $ghg^{-1} \in gHg^{-1}$, temos que $ghg^{-1} = kgg^{-1} = k \in H$, portanto temos que $gHg^{-1} \subseteq H$. Por outro lado, seja $h \in H$, então $h = gg^{-1}hgg^{-1}$, de novo, existe $l \in H$ tal que $hg = gl$, então

$$h = gg^{-1}hgg^{-1} = gg^{-1}glg^{-1} = glg^{-1} \in gHg^{-1},$$

o que implica em que $H \subseteq gHg^{-1}$. Portanto, os dois subconjuntos são iguais.

(ii)⇒(iii) Óbvio.

(iii)⇒(i) Considere as classes laterais gH e Hg. Seja $gh \in gH$, mas $gh = ghg^{-1}g$ e como $gHg^{-1} \subseteq H$, temos que existe $k \in H$ tal que $k = ghg^{-1}$. Portanto $gh = ghg^{-1}g = kg \in Hg$. Semelhantemente, seja $hg \in Hg$, mas $hg = gg^{-1}hg$ e como $g^{-1}Hg \subseteq H$, temos que existe $k \in H$ tal que $k = g^{-1}hg$. Portanto $hg = gg^{-1}hg = gk \in gH$. Portanto as duas classes são iguais, o que faz com qu e$H \trianglelefteq G$. $\blacksquare$

Exemplo 2.17. *Considere $\phi : G \to H$ um homomorfismo de grupos. Podemos verificar que o kernel deste homomorfismo é um subgrupo normal de G. De fato, seja $g \in G$ e $h \in \ker(\phi)$, então*

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g)e_H(\phi(h))^{-1} = e_H.$$

Portanto $ghg^{-1} \in \ker(\phi)$, ou ainda $g(\ker(\phi))g^{-1} \subseteq \ker(\phi)$.

O fato de um subgrupo H de G ser normal faz com que o conjunto quociente, G/H, seja munido de uma estrutura de grupo. De fato, dadas duas classes (indiferentemente se à esquerda ou à direita, pois o subgrupo é normal) g_1H e g_2H, podemos definir seu produto como $g_1H.g_2H = g_1g_2H$. Para mostrarmos que esta operação está bem definida, suponha que $g_1H = {g'}_1H$ e $g_2H = {g'}_2H$, isto significa que ${g'}_1^{-1}g_1 \in H$ e ${g'}_2^{-1}g_2 \in H$, então

$$ {g'}_1{g'}_2H = {g'}_1{g'}_2{g'}_2^{-1}g_2H = {g'}_1g_2H = {g'}_1Hg_2 = {g'}_1{g'}_1^{-1}g_1Hg_2 = g_1Hg_2 = g_1g_2H, $$

onde na terceira e na sexta igualdades utilizamos o fato de as classes à esquerda serem iguais às classes à direita. Com isto, verificamos que a operação de grupo em G/H está bem definida. A as outras propriedades de grupos são facilmente verificadas a partir das propriedades da operação em G.

Exercício 2.25: Seja G um grupo e $h \trianglelefteq G$. Mostre que a aplicação canônica,

$$ \begin{array}{rccc} \pi: & G & \to & G/H \\ & g & \mapsto & gH \end{array}, $$

é um epimorfismo.

Com isto, podemos finalizar esta seção com um grande teorema sobre homomorfismos de grupos e grupos quocientes, o teorema do homomorfismo.

Teorema 2.3. *Seja $\phi : G \to H$ um homomorfismo de grupos, então existe um único isomorfismo $\overline{\phi} : g/\ker(\phi) \to \mathrm{Im}(\phi)$ tal que o diagrama abaixo comute*

$$ \begin{array}{ccc} G & \xrightarrow{\phi} & H \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ G/\ker(\phi) & \xrightarrow[\overline{\phi}]{} & \mathrm{Im}(\phi) \end{array} $$

Onde $i : \mathrm{Im}(\phi) \to H$ é a inclusão canônica.

Demonstração: Defina a aplicação $\overline{\phi} : g/\ker(\phi) \to \mathrm{Im}(\phi)$ como, $\overline{\phi}(g\ker(\phi)) = \phi(g)$. Por construção, uma vez verificado que a aplicação está bem definida e é um homomorfismo, teremos a comutatividade do diagrama. Primeiramente, temos que verificar que esta função está bem definida. Para isto, considere $g\ker(\phi) = g'\ker(\phi)$, isto significa que $g^{-1}g' \in \ker(\phi)$, logo

$$ \overline{\phi}(g'\ker(\phi)) = \phi(g') = \phi(gg^{-1}g') = \phi(g)\phi(g^{-1}g') = \phi(g) = \overline{\phi}(g\ker(\phi)), $$

o que implica que a aplicação $\overline{\phi}$ está bem definida.

O segundo passo é mostrar que $\overline{\phi}$ é, de fato, um homomorfismo de grupos. Isto pode ser facilmente verificado:

$$ \overline{\phi}(g\ker(\phi)h\ker(\phi)) = \overline{\phi}(gh\ker(\phi)) = \phi(gh) = \phi(g)\phi(h) = \overline{\phi}(g\ker(\phi))\overline{\phi}(h\ker(\phi)). $$

Por último, precisamos verificar a injetividade e sobrejetividade do homomorfismo. Para a injetividade, considere $g\ker(\phi) \in \ker(\overline{\phi})$, então

$$ \overline{\phi}(g\ker(\phi)) = \phi(g) = e, $$

o que significa que $g \in \ker(\phi)$, ou ainda, que $g\ker(\phi) = e\ker(\phi)$. Portanto o homomorfismo é injetivo. A sobrejetividade decorre direto do fato que dado qualquer $\phi(g) \in \mathrm{Im}(\phi)$, então $\phi(g) = \overline{\phi}(g\ker(\phi)) \in \mathrm{Im}(\overline{\phi})$. O que conclui a demonstração do teorema. ■

O corolário abaixo será muito útil na obtenção de isomorfismos em vários contextos no decorrer deste trabalho.

Corolário 2.3. *Se $\phi : G \to H$ é um epimorfismo, então $H \cong G/\ker(\phi)$.*

3 Ações de Grupos

Como vimos na seção anterior, todo grupo é isomorfo a um sub-grupo de um grupo de bijeções em um conjunto (em particular, das bijeções no próprio grupo). As situações onde um grupo pode ser visto como grupo de bijeções são as que realmente aparecem nas aplicações da teoria. É somente agindo como um grupo de bijeções que o grupo se concretiza, se incorpora e pode ser utilizado como uma ferramenta poderosa para o estudo das simetrias.

Definição 3.1. *Uma ação à esquerda de um grupo G em um conjunto X é um homomorfismo de G no grupo das bijeções em X, que será denotado por* $\mathrm{Bij}(X)$.

Neste trabalho, lidaremos apenas com ações à esquerda, mas também é possível definirmos ações à direita. Para isto, primeiramente precisamos definir o grupo oposto.

Definição 3.2. *Dado um grupo G, definimos o seu grupo oposto, G^{op} como o conjunto G munido com uma operação dada como:*

$$\begin{array}{rccc} \bullet: & G\times G & \to & G \\ & (g,h) & \mapsto & g\bullet h = hg \end{array}.$$

Definição 3.3. *Uma ação à direita de um grupo G em um conjunto X é um homomorfismo de G^{op} no grupo das bijeções em X.*

Vamos fixar as notações: Vamos denotar uma ação (à esquerda, a menos que se diga o contrário) por

$$\begin{array}{rccc} \alpha: & G & \to & \mathrm{Bij}(X) \\ & g & \mapsto & \alpha_g \end{array}$$

e portanto α_g é uma bijeção no conjunto X, qua associa a cada elemento $x \in X$ outro elemento $\alpha_g(x)$. Como α é um homomorfismo, então temos que

1. $\alpha_g(\alpha_h(x)) = \alpha_{gh}(x)$ para todos elementos $g, h \in G$ e $x \in X$.
2. $\alpha_e = \mathrm{Id}_X$, ou seja, $\alpha_e(x) = x$ para todo $x \in X$.
3. $\alpha_g^{-1} = \alpha_{g^{-1}}$ para todo $g \in G$ (isto, na verdade, é facilmente concluído a partir dos dois ítens anteriores).

Antes de mostrarmos exemplos de ações de grupos sobre conjuntos, vamos a mais algumas definições adicionais

Definição 3.4. *Seja α uma ação de um grupo G sobre um conjunto X e considere um elemento $x \in X$. Definimos a órbita do elemento x como sendo o conjunto*

$$\mathcal{O}_x = \{\alpha_g(x) | g \in G\}.$$

Proposição 3.1. *Uma ação α de um grupo G sobre um conjunto X introduz uma relação de equivalência em X.*

Demonstração De fato, diremos que dois elementos $x, y \in X$ serão relacionados, denotando por $x \sim y$, se existir $g \in G$ tal que $y = \alpha_g(x)$. É fácil ver que esta é uma relação de equivalência:

REFLEXIVA: Para qualquer $x \in X$, temos que $x = \alpha_e(x)$, portanto $x \sim x$.

SIMÉTRICA: Sejam $x, y \in X$ tais que $x \sim y$, então, existe $g \in G$ tal que $y = \alpha_g(x)$. Mas $\alpha_{g^{-1}}(y) = \alpha_{g^{-1}}(\alpha_g(x)) = x$, portanto $y \sim x$.

TRANSITIVA: Sejam $x, y, z \in X$ tais que $x \sim y$ e $y \sim z$, então existem $g, h \in G$ tais que $y = \alpha_g(x)$ e $z = \alpha_h(y)$. Portanto $z = \alpha_h(y) = \alpha_h(\alpha_g(x)) = \alpha_{hg}(x)$, o que implica emque $x \sim z$. ■

As classes de equivalência, neste caso, serão dadas pelas órbitas dos elementos.

Proposição 3.2. *Duas órbitas pela ação de um grupo ou são disjuntas ou coincidentes.*

Demonstração: Suponha que $\mathcal{O}_x \cap \mathcal{O}_y \neq \emptyset$. Então existe $z \in \mathcal{O}_x \cap \mathcal{O}_y$, ou seja existem $g, h \in G$ tais que $z = \alpha_g(x) = \alpha_h(y)$. Mas desta igualdade obtemos que $x = \alpha_{g^{-1}h}(y)$ e $y = \alpha_{h^{-1}g}(x)$. Considere $w \in \mathcal{O}_x$ então, existe $k \in G$ tal que $w = \alpha_k(x)$, ou seja $w = \alpha_k(x) = \alpha_k(\alpha g^{-1}h(y)) = \alpha_{kg^{-1}h}(y)$, o que nos leva à conclusão que $w \in \mathcal{O}_y$. Analogamente, seja $t \in \mathcal{O}_y$ então, existe $l \in G$ tal que $t = \alpha_l(y)$, ou seja $t = \alpha_l(y) = \alpha_l(\alpha h^{-1}g(x)) = \alpha_{lh^{-1}g}(x)$, o que nos leva à conclusão que $t \in \mathcal{O}_x$. Portanto $\mathcal{O}_x = \mathcal{O}_y$. ■

O resultado mostrado na proposição anterior nos leva à conclusão que o conjunto quociente do conjunto X pela relação de equivalência definida pela ação do grupo G é igual ao conjunto das órbitas dos elementos de X. Denotaremos este quociente por X/G. Além do quociente, muitas vezes é importante reconhecer subconjuntos de X que contenham apenas um representante de cada órbita definida pela ação, estes subcon juntos são denominados domínios fundamentais.

Definição 3.5. *Seja X um conjunto e α uma ação de um grupo G sobre X. Um subconjunto $F \subseteq X$ é dito ser um domínio fundamental se, para todo $x \in X$, existem únicos $y \in F$ e $g \in G$ tal que $x = \alpha_g(y)$.*

Note que, segundo esta definição, não ode haver dois elementos da mesma órbita no domínio fundamental e todas as órbitas devem estar contempladas neste domíni, pois por definição deve ser possível atingir qulquer outro ponto de X agindo sobre pontos de F. Vejamos alguns exemplos para conseguirmos distinguir as definições de conjunto quociente e domínio fundamental.

Exemplo 3.1. *Seja o grupo aditivo $\mathbb{Z}$ agindo sobre a reta real $\mathbb{R}$ da seguinte maneira: $\alpha_n(x) = x + n$. É fácil ver que α é uma ação, pois $\alpha_n(\alpha_m(x)) = \alpha_n(x + m) = x + m + n = \alpha_{n+m}(x)$ e $\alpha_0(x) = x + 0 = x$. Dado um elemento $x \in \mathbb{R}$, sua órbita será o conjunto*

$$\mathcal{O}_x = \{x + n \,|\, n \in \mathbb{Z}\}.$$

Assim, se tomarmos um intervalo da forma $[n, n + 1[$, com $n \in \mathbb{Z}$ certamente teremos um domínio fundamental, pois para quaisquer dois pontos, x, y deste intervalo, temos que $|x - y| < 1$, portanto não podem existir dois pontos da mesma órbita neste intervalo. Por outro lado, seja $x \in \mathbb{R}$ um número qualquer, então

$$x = n + x - n = n + (x - n - \lfloor x - n \rfloor) + \lfloor x - n \rfloor = \alpha_{\lfloor x-n \rfloor}(n + (x - n - \lfloor x - n \rfloor)),$$

onde $\lfloor a \rfloor$ denota o maior inteiro menor que a, e $a - \lfloor a \rfloor \in [0, 1[$ é a parte fracionária do número a. Assim, o número x é a ação do número inteiro $\lfloor x - n \rfloor$ sobre $n + (x - n - \lfloor x - n \rfloor) \in [n, n + 1[$, o que mostra que este intervalo é um domínio fundamental.

Por outro lado, o quociente é o conjunto das órbitas, podemos caracterizá-lo como a circunferência unitária através da função

$$\begin{array}{rccc} f: & \mathbb{R}/\mathbb{Z} & \to & \mathbb{S}^1 \\ & \mathcal{O}_x & \mapsto & (\cos 2\pi x, \sin 2\pi x) \end{array}.$$

Esta aplicação está bem definida, pois se $\mathcal{O}_x = \mathcal{O}_y$ isto significa que $y = x + n$, para algum número inteiro n. Então

$$f(\mathcal{O}_y) = (\cos 2\pi y, \sin 2\pi y) = (\cos 2\pi(x + n), \sin 2\pi(x + n)) = (\cos 2\pi x, \sin 2\pi x) = f(\mathcal{O}_x).$$

Também podemos ver a injetividade, pois se $f(\mathcal{O}_y) = f(\mathcal{O}_x)$, então $(\cos 2\pi y, \sin 2\pi y) = (\cos 2\pi x, \sin 2\pi x)$, o que implica que $\cos 2\pi y = \cos 2\pi x$ e $\sin 2\pi y = \sin 2\pi x$. Isto somente ocorre quando existe um inteiro n tal que $y = x + n$, ou ainda, quando $y \in \mathcal{O}_x$, que equivale a dizer que $\mathcal{O}_x = \mathcal{O}_y$. A sobrejetividade decorre imediatamente do fato que todo ponto $p \in \mathcal{S}^1$ possui coordenadas $p = (\cos\theta, \sin\theta)$, para $\theta \in [0, 2\pi[$, assim $p = f(\mathcal{O}_{\frac{\theta}{2\pi}})$.

Exemplo 3.2. *Um exemplo análogo ao exemplo anterior é o da ação do grupo aditivo $\mathbb{Z} \times \mathbb{Z}$ sobre o plano $\mathbb{R}^2$ dada por $\alpha_{(m,n)}(x, y) = (x + m, y + n)$. Também é fácil verificar que α é, de fato, uma ação e que um domínio fundamental pode ser dado, por exemplo, pelo quadrado $[0, 1[\times[0, 1[$, as verificações podem ser feitas coordenada por coordenada conforme fizemos no exemplo anterior.*

Já o quociente do plano por esta ação pode ser caracterizado pelo toro, $\mathbb{T}^2 = \mathbb{S}^1 \times \mathbb{S}^1$ através da aplicação

$$\begin{array}{rccc} f: & \mathbb{R}^2/\mathbb{Z}^2 & \to & \mathbb{T}^2 \\ & \mathcal{O}_{(x,y)} & \mapsto & (\cos 2\pi x, \sin 2\pi x, \cos 2\pi y, \sin 2\pi y) \end{array}.$$

Note que este toro está imerso no espaço quadridimensional $\mathbb{R}^4$. as verificações dos detalhes são deixadas como exercício.

Exemplo 3.3. *Considere a ação do grupo multiplicativo $(\mathbb{R}^*, \cdot)$ sobre o plano $\mathbb{R}^2$, excluído a origem, dado por $\alpha_\lambda(x,y) = (\lambda x, \lambda y)$. Verifica-se facilmente que se trata de uma ação de grupo. De fato, $\alpha_\lambda(\alpha_\mu(x,y)) = \alpha_\lambda(\mu x \mu y) = (\lambda\mu x \lambda\mu y) = \alpha\lambda\mu(x,y)$ e $\alpha_1(x,y) = 1.x, 1.y) = (x,y)$. Dado um ponto no plano $(x,y) \in \mathbb{R}^2\backslash\{(0,0)\}$, sua órbita é dada pelo conjunto*

$$\mathcal{O}_{(x,y)} = \{(\lambda x, \lambda y) \,|\, \lambda \in \mathbb{R}^*\},$$

ou seja, a órbita de um ponto é a reta que passa pela origem, $(0,0)$ e pelo ponto dado, excluída a origem. Um domínio fundamental pode ser dado pelo conjunto

$$F = \{(\cos\theta, \sin\theta) \in \mathbb{R}^2 \,|\, 0 \leq \theta < \pi\},$$

isto é, a semi-circunferência de raio 1 ao redor da origem, excluído o ponto $(-1,0)$. É claro que cada reta que passa pela origem cruza o conjunto F apenas uma vez, portanto, não há dois pontos pertencentes à mesma órbita em F. Por outro lado, temos que todo $(x,y) \in \mathbb{R}^2\backslash\{(0,0)\}$, com $y \neq 0$ pode ser escrito como

$$\begin{aligned} (x,y) &= (sign(y)\sqrt{x^2+y^2}\frac{x}{sign(y)\sqrt{x^2+y^2}}, sign(y)\sqrt{x^2+y^2}\frac{y}{sign(y)\sqrt{x^2+y^2}}) = \\ &= \alpha_{sign(y)\sqrt{x^2+y^2}}(\frac{x}{sign(y)\sqrt{x^2+y^2}}, \frac{y}{sign(y)\sqrt{x^2+y^2}}), \end{aligned}$$

onde $(\frac{x}{sign(y)\sqrt{x^2+y^2}}, \frac{y}{sign(y)\sqrt{x^2+y^2}}) \in F$. Se $y = 0$ temos que $(x,0) = \alpha_x(1,0)$.

Por outro lado, o quociente pode ser caracterizado como a circunferência unitária pela aplicação

$$\begin{array}{rccc} f: & \mathbb{R}^2\backslash\{(0,0)\}/\mathbb{R}^* & \to & \mathbb{S}^1 \\ & \mathcal{O}_{(x,y)} & \mapsto & (\cos 2\theta, \sin 2\theta) \end{array},$$

onde θ é o ângulo que define a órbita do ponto no domínio fundamental. A boa definição e a injetividade decorre naturalmente do fato de a aplicação f ser definida a partir do domínio fundamental. A sobrejetividade pode ser verificada pois qualquer ponto $(\cos\varphi, \sin\varphi) \in \mathbb{S}^1$ pode ser visto como $f(\mathcal{O}_{(\cos\frac{\varphi}{2}, \sin\frac{\varphi}{2})})$. Discutiremos com mais detalhes este tipo de exemplo quando discutirmos os espaços projetivos, na seção 5.

Dada uma ação de um grupo G sobre um conjunto X, podemos definir outros subconjuntos que caracterizarão tipos específicos de ações.

Definição 3.6. *Considere uma ação α de um grupo G sobre um conjunto X. O sub-grupo estabilizador de um elemento $x \in X$ é definido como*

$$Stab_x = \{g \in G | \alpha_g(x) = x\}$$

Exercicio 3.1: Mostre que $Stab_x$ é, de fato, um sub-grupo de G.

De forma semelhante, podemos falar do sub-grupo estabilizador de um sub-conjunto $Y \subseteq X$

$$Stab_Y = \{g \in G | \alpha_g(Y) \subseteq Y\}.$$

Note que os elementos de um sub-conjunto não precisam ficar fixos pela ação do grupo, apenas que suas órbitas precisam estar contidas neste sub-conjunto. Quando $\text{Stab}_Y = G$, dizemos que $Y \subseteq X$ é um sub-conjunto invariante pela ação do grupo G.

Uma definição dual é o conjunto dos pontos fixos pela ação de um determinado elemento ou sub-grupo de G.

Definição 3.7. *O sub-conjunto dos pontos fixos de um elemento $g \in G$ é o conjunto*

$$Fix_g = \{x \in X | \alpha_g(x) = x\}.$$

Se $H \subseteq G$ é um sub-grupo de G, o conjunto dos pontos fixos pela ação de H é definido por

$$Fix_H = \{x \in X | \alpha_g(x) = x,\ \forall g \in H\}.$$

Definição 3.8. *Uma ação α de G em X é dita ser*

1. *Fiel, se dado $g \in G$ tal que $Fix_g = X$, então $g = e$.*
2. *Livre, se dado $g \in G$ tal que $Fix_g \neq \emptyset$, então $g = e$.*
3. *Transitiva, se $\mathcal{O}_x = X$, para todo elemento $x \in X$. Ou, equivalentemente, se $x, y \in X$ então existe $g \in G$ tal que $y = \alpha_g(x)$.*

Exemplo 3.4. *Seja $G = \mathbb{R}$ o grupo aditivo dos reais. Considere $\mathbb{V}$ um espaço vetorial e $\mathbf{v} \in \mathbb{V}$ um vetor neste espaço. Então podemos indicar as translações em $\mathbb{V}$ na direção de V como a ação $T^{(\mathbf{v})}$ de $\mathbb{R}$ em $\mathbb{V}$ dada por $T_x^{(\mathbf{v})}(\mathbf{w}) = \mathbf{w} + x\mathbf{v}$.*

Exemplo 3.5. *Na mesma linha do exemplo anterior, Considere $\mathbb{A}$ um conjunto e uma ação T do grupo aditivo de um espaço vetorial $\mathbb{V}$ em $\mathbb{A}$ por translações. Se T é livre e transitiva, então dizemos que o conjunto $\mathbb{A}$, junto com o espaço $\mathbb{V}$ e a ação T forma um espaço afim. Se a dimensão de $\mathbb{V}$ é igual a n, dizemos que o espaço afim tem dimensão n. Discutiremos melhor a estrutura dos espaços afins na seção seguinte.*

Exemplo 3.6. *Considere o grupo*

$$Aff(\mathbb{R}) = \{f_{a,b} : \mathbb{R} \to \mathbb{R} \,|\, f_{a,b}(x) = ax + b, \quad a \neq 0\},$$

e o conjunto

$$X = \{(x, 1) \,|\, x \in \mathbb{R}\}.$$

Uma ação de $Aff(\mathbb{R})$ sobre X pode ser dada por

$$\alpha_{f_{a,b}}(x, 1) = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = (f_{a,b}(x), 1).$$

Esta ação não é livre, pois se $a \neq 1$ temos que $\alpha_{f_{a,b}}\left(\frac{b}{1-a}, 1\right) = \left(\frac{b}{1-a}, 1\right)$. É fácil verificar que a ação é transitiva pois $(y, 1) = \alpha_{f_{1,y-x}}(x, 1)$.

Exemplo 3.7. *O grupo multiplicativo $(\mathbb{R}^*, \cdot)$ pode agir sobre qualquer espaço vetorial, excluído o vetor nulo, pela ação $\alpha_\lambda(v) = \lambda v$, para $v \neq 0$. Este tipo de ação é que vai definir, como veremos adiante, todos os espaços projetivos.*

Exemplo 3.8. *Um grupo G pode agir sobre um espaço vetorial através de transformações lineares invertíveis, ou seja, através de um homomorfismo de grupos $\rho : G \to GL(\mathbb{V})$, este tipo especial de ação de grupos é chamado de representação linear de um grupo. O estudo das representações lineares de grupos constitui-se em uma ferramenta poderosa tanto em matemática pura como também nas aplicações, pois associa as técnicas e resultados oriundos da teoria de grupos com técnicas de álgebra linear.*

Exemplo 3.9. *Seja G um grupo. Este grupo pode agir sobre si mesmo de várias maneiras, dentre as quais destacamos duas de particular interesse:*

(a) A ação regular à esquerda: $L_g(h) = gh$, para todo $g, h \in G$.

(b) A ação adjunta: $Ad_g(h) = ghg^{-1}$, para todo $g, h \in G$.

Exercício 3.2: Mostre que a ação regular à esquerda é livre e transitiva.

Exercício 3.3: Mostre que, na ação adjunta, para todo $g \in G$ a aplicação $Ad_g : G \to G$ é um isomorfismo do grupo G nele mesmo. Mostre também que, para todo $g \in G$, Ad_g é um automorfismo de G.

Exercício 3.4: Se um automorfismo $\phi : G \to G$ é tal que existe $g \in G$ de forma que $\phi(h) = Ad_g(h)$ para todo $h \in G$, então ele é dito ser um automorfismo interno. denote por $Inn(G)$ o conjunto de todos os automorfismos internos de G. Mostre que $Inn(G) \trianglelefteq Aut(G)$.

Exercício 3.5: Faça explicitamente com o grupo S_3 o cálculo da ação adjunta, verifique as órbitas, os pontos fixos, os estabilizadores, etc.

Exercício 3.6: Mostre que $h \in G$ é um ponto fixo de Ad_g, se, e somente se, h comuta com g. mostre também que um subconjunto $H \subseteq G$ invariante pela ação adjunta é um subgrupo normal de G.

Exemplo 3.10. *Seja $G = \mathbb{Z}$ o grupo aditivo dos inteiros e $X = \mathbb{S}^1$ a circunferência unitária no plano (também denotado na seção anterior por $U(1)$)*

$$\mathbb{S}^1 = \{(\cos\theta, \sin\theta) \in \mathbb{R}^2 | \theta \in \mathbb{R}\}.$$

Para cada $\alpha \in \mathbb{R}$ podemos definir uma ação de $\mathbb{Z}$ em $\mathbb{S}^1$ por rotações da seguinte forma:

$$R_n^{(\alpha)} \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} = \begin{pmatrix} \cos n\alpha & -\sin n\alpha \\ \sin n\alpha & \cos n\alpha \end{pmatrix} \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} = \begin{pmatrix} \cos(\theta + n\alpha) \\ \sin(\theta + n\alpha) \end{pmatrix}$$

Exercício 3.7: Mostre que, se $\frac{\alpha}{2\pi} = \frac{p}{q} \in \mathbb{Q}$, a órbita de cada ponto de $\mathbb{S}^1$ é um polígono regular de q lados.

Exercício 3.8: Mostre que se $\frac{\alpha}{2\pi} \in \mathbb{R}\backslash\mathbb{Q}$ então a ação é livre.

Este último caso, o das rotações por um ângulo incomensurável com 2π é um conhecido exemplo na teoria de sistemas dinâmicos e possui a propriedade que todo ponto possui uma órbita densa, isto é, em qualquer intervalo da circunferêancia, por menor que seja, existem infinitos pontos de qualquer órbita.

Quando temos um grupo G agindo sobre um grupo H por automorfismos, podemos construir um novo grupo, que codifica em si a estrutura do grupo G, a estrutura do grupo H e a ação α de G em H, o produto semidireto:

Teorema 3.1. *Seja α uma ação de um grupo G sobre um grupo H por automorfismos. Então, o produto cartesiano $H \times G$ pode ser munido com uma operação dada por*

$$(h_1, g_1) \cdot (h_2, g_2) = (h_1 \alpha_{g_1}(h_2), g_1 g_2).$$

Com esta operação, o produto cartesiano é investido de uma estrutura de grupo, denotado por $H \rtimes_\alpha G$ e denominado produto semidireto de H por G. Além disto

(i) As inclusões

$$i_1 : \begin{array}{ccc} H & \to & H \rtimes_\alpha G \\ h & \mapsto & (h, e_G) \end{array}, \quad e \quad i_2 : \begin{array}{ccc} G & \to & H \rtimes_\alpha G \\ g & \mapsto & (e_H, g) \end{array}$$

são monomorfismos de grupo.

(ii) O subgrupo $i_1(H)$ é subgrupo normal.

(iii) A ação de G em H é escrita como um automorfismo interno de $H \rtimes_\alpha G$, isto é, $i_1(\alpha_g(h)) = i_2(g) \cdot i_1(h) \cdot (i_2(g))^{-1}$

Por outro lado, se K é um grupo tal que

(a) Os grupos G e H são subgrupos de K e $H \trianglelefteq K$.

(b) Para todo $k \in K$ existem $g \in G$ e $h \in H$ tal que $k = hg$, isto é, $K = HG$.

(c) Para todo $g \in G$ e todo $h \in H$, temos que $gh = \alpha_g(h)g$.

então $K \cong H \rtimes_\alpha G$.

Demonstração: Vamos primeiramente verificar que o produto cartesiano $H \times G$ com a operação $\cdot$ é, de fato, um grupo:

ASSOCIATIVIDADE:

$$\begin{aligned}(h_1, g_1) \cdot ((h_2, g_2) \cdot (h_3, g_3)) &= (h_1, g_1) \cdot (h_2\alpha_{g_2}(h_3), g_2g_3) = \\ &= (h_1\alpha_{g_1}(h_2\alpha_{g_2}(h_3)), g_1(g_2g_3)) = \\ &= (h_1\alpha_{g_1}(h_2)\alpha_{g_1}(\alpha_{g_2}(h_3)), (g_1g_2)g_3) = \\ &= (h_1\alpha_{g_1}(h_2)\alpha_{g_1g_2}(h_3), (g_1g_2)g_3) = \\ &= (h_1\alpha_{g_1}(h_2), g_1g_2) \cdot (h_3, g_3) = \\ &= ((h_1, g_1) \cdot (h_2, g_2)) \cdot (h_3, g_3).\end{aligned}$$

ELEMENTO NEUTRO: O elemento $(e_H, e_G) \in H \rtimes_\alpha G$ é o elemento neutro do produto semidireto. De fato, dado qualquer $(h, g) \in H \rtimes_\alpha G$ temos que

$$(e_H, e_G) \cdot (h, g) = (e_H\alpha_{e_G}(h), e_Gg) = (h, g),$$

e

$$(h, g) \cdot (e_H, e_G) = (h\alpha_g(e_H), ge_G) = (he_H, g) = (h, g).$$

ELEMENTO INVERSO: Seja $(h, g) \in H \rtimes_\alpha G$, vamos verificar que $(h, g)^{-1} = (\alpha_{g^{-1}}(h^{-1}), g^{-1})$: Primeiramente

$$(\alpha_{g^{-1}}(h^{-1}), g^{-1}) \cdot (h, g) = (\alpha_{g^{-1}}(h^{-1})\alpha_{g^{-1}}(h), g^{-1}g) = (\alpha_{g^{-1}}(h^{-1}h), e_G) = (\alpha_{g^{-1}}(e_H), e_G) = (e_H, e_G).$$

Por outro lado,

$$(h, g) \cdot (\alpha_{g^{-1}}(h^{-1}), g^{-1}) = (h\alpha_g(\alpha_{g^{-1}}(h^{-1}), gg^{-1}) = (h\alpha_{e_G}(h^{-1}), e_G) = (hh^{-1}, e_G) = (e_H, e_G).$$

Portanto, $(H \rtimes_\alpha G, \cdot)$ é um grupo. Agora resta-nos verificar os ítens (i), (ii) e (iii):

(i) Verifiquemos, primeiramente que i_1 é homomorfismo:

$$i_1(h_1) \cdot i_1(h_2) = (h_1, e_G) \cdot (h_2, e_G) = (h_1\alpha_{e_G}(h_2), e_Ge_G) = (h_1h_2, e_G) = i_1(h_1h_2).$$

A injetividade de i_1 é facilmente verificada, pois se $h \in \ker(i_1)$ então $(h, e_G) = (e_H, e_G)$ o que nos leva à conclusão que $h = e_H$.

Para a aplicação i_2 temos

$$i_2(g_1) \cdot i_2(g_2) = (e_H, g_1) \cdot (e_H, g_2) = (e_H\alpha_{g_1}(e_H), g_1g_2) = (e_H, g_1g_2).$$

A injetividade de i_2 segue um raciocínio análogo ao utilizado para i_1.

(ii) Seja $k \in H$ e $(h, g) \in H \rtimes_\alpha G$, então

$$\begin{aligned}(h, g) \cdot i_1(k) \cdot (h, g)^{-1} &= (h, g) \cdot (k, e_G) \cdot (\alpha_{g^{-1}}(h^{-1}), g^{-1}) = \\ &= (h, g) \cdot (k\alpha_{e_G}(\alpha_{g^{-1}}(h^{-1})), e_Gg^{-1}) = \\ &= (h, g) \cdot (k\alpha_{g^{-1}}(h^{-1}), g^{-1}) = \\ &= (h\alpha_g(k\alpha_{g^{-1}}(h^{-1})), gg^{-1}) = \\ &= (h\alpha_g(k)\alpha_{gg^{-1}}(h^{-1}), e_G) = \\ &= (h\alpha_g(k)h^{-1}, e_G) \in i_1(H).\end{aligned}$$

Portanto $i_1(H)$ é subgrupo normal do produto semidireto.

(iii) Seja $h \in H$ e $g \in G$, então

$$\begin{aligned} i_2(g) \cdot i_1(h) \cdot (i_2(g))^{-1} &= (e_H, g) \cdot (h, e_G) \cdot (e_H, g)^{-1} = \\ &= (e_H, g) \cdot (h, e_G) \cdot (\alpha_{g^{-1}}(e_H), g^{-1}) = \\ &= (e_H, g) \cdot (h\alpha_{e_G}(e_H), e_G g^{-1}) = \\ &= (e_H, g) \cdot (h, g^{-1}) = \\ &= (e_H \alpha_g(h), g g^{-1}) = \\ &= (\alpha_g(h), e_G) = i_1(\alpha_g(h)). \end{aligned}$$

Por outro lado, seja K um grupo satisfazendo os ítens (a), (b) e (c) do enunciado. É fácil ver que $e_K = e_H e_G$. agora defina a aplicação

$$\begin{array}{rccc} \Phi: & K & \to & H \rtimes_\alpha G \\ & hg & \mapsto & (h, g) \end{array}.$$

Podemos ver que Φ é um homomorfismo de grupos, pois

$$\Phi(h_1 g_1) \cdot \Phi(h_2 g_2) = (h_1, g_1) \cdot (h_2, g_2) = (h_1 \alpha_{g_1}(h_2), g_1 g_2)$$

e

$$\Phi((h_1 g_1)(h_2 g_2)) = \Phi(h_1 \alpha_{g_1}(h_2) g_1 g_2) = (h_1 \alpha_{g_1}(h_2), g_1 g_2),$$

o que mostra que $\Phi(h_1 g_1) \cdot \Phi(h_2 g_2) = \Phi((h_1 g_1)(h_2 g_2))$. A injetividade de Φ pode ser obtida facilmente, tomando $hg \in \ker(\Phi)$, então $\Phi(hg) = (h, g) = (e_H, e_G)$ o que nos leva à conclusão que $h = e_H$ e $g = e_G$, ou seja $hg = e_H e_G = e_K$. Finalmente, a sobrejetividade de Φ é óbvia, pois para qualquer $(h, g) \in H \rtimes_\alpha G$ temos que $(h, g) = \Phi(hg)$. Portanto $K \cong H \rtimes_\alpha G$. ■

Exemplo 3.11. *O primeiro exemplo de produto semidireto é o trivial, o produto direto. Se G age sobre H com a ação trivial, isto é, se $\alpha_g = \mathrm{Id}(H)$ para todo $g \in G$, então $H \rtimes_\alpha G = H \times G$ e o produto é dado por $(h_1 g_1) \cdot (h_2, g_2) = (h_1 h_2, g_1 g_2)$.*

Exemplo 3.12. *Se G age sobre si mesmo pela ação adjunta, então $G \rtimes_{Ad} G \cong G \times G$. Este isomorfismo é dado pela aplicação*

$$\begin{array}{rccc} \Psi: & G \times G & \to & G \rtimes_{Ad} G \\ & (g, h) & \mapsto & (gh^{-1}, h) \end{array}.$$

Para a verificação de homomorfismo, temos que

$$\begin{aligned} \Psi(g_1, h_1) \cdot \Psi(g_2, h_2) &= (g_1 h_1^{-1}, h_1) \cdot (g_2 h_2^{-1}, h_2) = \\ &= (g_1 h_1^{-1} Ad_{h_1}(g_2 h_2^{-1}), h_1 h_2) = \\ &= (g_1 h_1^{-1} h_1 g_2 h_2^{-1} h_1^{-1}, h_1 h_2) = \\ &= (g_1 g_2 (h_1 h_2)^{-1}, h_1 h_2) = \\ &= \Psi(g_1 g_2, h_1 h_2) = \Psi((g_1, h_1)(g_2, h_2)). \end{aligned}$$

A injetividade é verificada tomando-se $(g, h) \in \ker\Psi$, então $\Psi(g, h) = (gh^{-1}, h) = (e_G, e_G)$. Assim, $h = e_G$, e por conseguinte $g = e_G$, o que implica em $(g, h) = (e_G, e_G)$, que é equivalente a dizer que Ψ é injetiva. A sobrejetividade advém do fato que $(g, h) = (ghh^{-1}, h) = \Psi(gh, h)$. Isto conclui a demonstração do isomorfismo.

Exemplo 3.13. *Como um último exemplo desta seção, consideremos o grupo diedral D_n, ou seja o grupo das simetrias de um polígono regular de n lados. Para caracterizarmos estas simetrias como transformações no plano, podemos colocar os vértices do polígono sobre as raízes n-ésimas da unidade, ou seja, sobre os pontos*

$$p_k = \left(\cos \frac{2k\pi}{n}, \sin \frac{2k\pi}{n} \right)$$

para $k \in \{0, \ldots, n-1\}$. As simetrias são geradas por duas tranformações:

1. *Uma rotação no sentido anti-horário de um ângulo de $\frac{2\pi}{n}$. Vamos denominar esta transformação de a. é fácil ver que $a^n = \mathrm{Id}$.*

2. *Uma reflexão com respeito ao eixo x, isto é, uma transformação no plano que associa ao ponto (x, y) o ponto $(x, -y)$. Denotemos esta transformação por b. é fácil ver que $b^2 = \mathrm{Id}$.*

Assim, o grupo D_n é um grupo de ordem $2n$ cujos elementos são $\mathrm{Id}, a, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b$. Deixamos como exercício a verificação que $ba^k = a^{n-k}b$, para todo $k \in \{0, \ldots n-1\}$.

Agora, consideremos a ação do grupo aditivo $\mathbb{Z}_2$ sobre o grupo aditivo $\mathbb{Z}_n$ dada por $\alpha_{\bar{0}}(\bar{k}) = \bar{k}$ e $\alpha_{\bar{1}}(\bar{k}) = \overline{n-k}$. Podemos utilizar a segunda parte do teorema para mostrarmos que $D_n \cong \mathbb{Z}_n \rtimes_\alpha \mathbb{Z}_2$. De fato, temos os subgrupos $H = \{\mathrm{Id}, a, \ldots a^{n-1}\} \cong \mathbb{Z}_n$ e $G = \{\mathrm{Id}, b\} \cong \mathbb{Z}_2$ e é fácil ver que $H \trianglelefteq D_n$. Também, por construção, temos que $D_n = HG$. A ação de $\mathbb{Z}_2$ sobre $\mathbb{Z}_n$ pode, essencialmente, ser traduzida como $\alpha_b(a^k) = a^{n-k}$. Finalmente a relação $ba^k = a^{n-k}b = \alpha_b(a^k)b$ nos fornece a última condição para garantirmos o isomorfismo. Portanto, $D_n \cong \mathbb{Z}_n \rtimes_\alpha \mathbb{Z}_2$.

4 Geometria Afim

A geometria teve sua primeira estruturação com a obra de Euclides. Todos os objetos geométricos podiam ser representados em qualquer lugar do plano, sem qualquer posição privilegiada. Com o advento da geometria analítica, com Descartes, um ponto privilegiado foi introduzido no plano, a origem do sistema de coordenadas. Pela primeira vez, os objetos geométricos podiam ser descritos por meio de equações algébricas, o que abria um sem número de possibilidades no que se refere ao aspecto computacional. A evolução natural da geomeria analítica levou ao surgimento da álgebra linear, originando a estrutura de espaço vetorial. Em todo espaço vetorial, existe um ponto privilegiado, uma origem, que é o vetor nulo. Por isto, embora a estrutura de espaço vetorial permita uma versatilidade muito grande em termos de cálculos, os espaços vetoriais não são apropriados para descrever objetos ou espaços que apresentem uma homogeneidade espacial. Era necessária uma nova estrutura geométrica que unificasse os dois aspectos, de um lado, a homogeneidade do espaço existente na geometria euclidiana, de outro lado, a estrutura algébrica de espaço vetorial. A estrutura que vem suprir a esta necessidade é a estrutura de espaço afim.

Definição 4.1. *Um espaço afim (real) é uma tripla $(\mathbb{A}, \mathbb{V}, T)$, onde $\mathbb{A}$ é um conjunto, $\mathbb{V}$ é um espaço vetorial (sobre o corpo dos reais) e T é uma ação livre e transitiva do grupo aditivo do espaço vetorial $\mathbb{V}$ sobre o conjunto $\mathbb{A}$.*

Algumas observações decorrentes da definição de espaço afim:

1. O espaço afim por um abuso de notação, acaba sendo denotado por $\mathbb{A}$.

2. A ação do espaço vetorial $\mathbb{V}$ sobre o espaço afim $\mathbb{A}$ é dita ser uma ação por translações. E o grupo aditivo de $\mathbb{V}$ é chamado o grupo de tranlações do espaço afim.

3. A dimensão do espaço afim é, por definição, a dimensão do espaço vetorial que nele age livre e transitivamente.

4. Sendo $p \in \mathbb{A}$ e $v \in \mathbb{V}$, costuma-se denotar a translação $T_v(p)$ por $p + v$, lembrando que este sinal de adição não implica que o espaço afim seja munido de uma operação, apenas este sinal está representando o transladado de p pelo vetor v.

5. Como a ação é transitiva, dados quaisquer dois pontos $p, q \in \mathbb{A}$ existe $v \in \mathbb{V}$ tal que $q = T_v(p)$. Neste caso, também costuma-se denotar o vetor v por $p - q$, deixando claro que esta não é uma subtração, apenas um símbolo para denotar o vetor que translada o ponto p no ponto q.

6. Ainda dentro desta notação, podemos ver que $T_v(x) - x = v$, para qualquer $x \in \mathbb{A}$ e qualquer $v \in \mathbb{V}$, e $T_{(y-x)}(x) = y$ para quaisquer $x, y \in \mathbb{A}$.

Exercício 4.1: Mostre que, se $x, y, z, t \in \mathbb{A}$, então $(x - y) + (z - t) = (x - t) + (z - y)$.

Exemplo 4.1. *Um espaço vetorial $\mathbb{V}$ agindo sobre si mesmo pela soma, isto é, $T_v(w) = w+v$ faz com que $(\mathbb{V}, \mathbb{V}, +)$ seja um exemplo de espaço afim. As propriedades de ação decorrem diretamente das propriedades da soma no espaço vetorial. O fato de a ação ser livre também é direto, pois se $v + w = w$ para algum $w \in \mathbb{V}$, então $v = 0$. Por fim, a transitividade da ação vem do fato que se $v, w \in \mathbb{V}$, então $w = v + (w - v) = T_{w-v}(v)$.*

Como caso particular, temos que a reta real $\mathbb{R}$ agindo sobre si mesma pela soma torna a reta $(\mathbb{R}, \mathbb{R}, +)$ um exemplo de espaço afim

Exemplo 4.2. *O hiperplano $H \subseteq \mathbb{R}^n$ descrito pela equação*

$$a_1x^1 + a_2x^2 + \cdots + a_nx_n = b$$

é um outro exemplo de espaço afim. O espaço vetorial subjacente é o kernel do funcional linear $f : \mathbb{R}^n \to \mathbb{R}$ dado por

$$f(x^1, \ldots, x^n) = a_1x^1 + \cdots + a_nx^n,$$

e a ação é dada pela soma vetorial em $\mathbb{R}^n$. De fato, seja $p = (y^1, \ldots, y^n) \in H$ e seja $v = (x^1, \ldots, x^n) \in \ker(f)$, vamos verificar que $T_v(p) = p + v \in H$, para isto, uma vez que $p + v = (y^1 + x^1, \ldots, y^n + x^n)$, temos que

$$\begin{aligned} a_1(y^1 + x^1) + \cdots + a_n(y^n + x^n) &= a_1y_1 + \cdots + a_ny^n + a_1x^1 + \cdots + a_nx^n = \\ &= a_1y_1 + \cdots + a_ny^n + f(v) = p. \end{aligned}$$

Portanto $p + v \in H$. As propriedades de ação decorrem das propriedades da soma vetorial em $\mathbb{R}^n$. O fato de a ação ser livre pode ser visto facilmente, pois se $p + v = p$ para algum $p \in H$ e $v \in \ker(f)$, então coordenada por coordenada teremos $y^i + x^i = y^i$, o que implica em $x^i = 0$, e portanto $v = 0$. A transitividade da ação também é facilmente deduzida: Considere dois pontos $p = (y^1, \ldots, y^n) \in H$ e $q = (z^1, \ldots, z^n) \in H$. Podemos escrever $q = p+(q-p)$, pois estamos no espaço ambiente $\mathbb{R}^n$, resta-nos verificar que $q-p \in \ker(f)$, que decorre diretamente de

$$a_1(z^1 - y^1) + \cdots + a_n(z^n - y^n) = a_1z_1 + \cdots + a_nz^n - a_1y^1 - \cdots - a_ny^n = p - p = 0.$$

Portanto $(H, \ker(f), +)$ é um espaço afim.

Exemplo 4.3. *Seja $\mathbb{V}$ um espaço vetorial, $\mathbb{W} \subseteq \mathbb{V}$ um subespaço vetorial e $v_0 \in \mathbb{V}$ um vetor fixado. Vamos mostrar que $\mathbb{A} = \mathbb{W} + v_0$ é um espaço afim cujo espaço vetorial subjacente é $\mathbb{W}$ e a ação é dada pela soma vetorial no espaço ambiente $\mathbb{V}$. Este é o exemplo paradigmático de espaço afim. Seja $p \in \mathbb{A}$, portanto, existe $w \in \mathbb{W}$ tal que $p = w + v_0$, considere também $v \in \mathbb{W}$. Assim, $p + v = w + v_0 + v = (w + v) + v_0 \in \mathbb{A}$. Novamente, as propriedades de ação decorrem das propriedades da adição no espaço ambiente $\mathbb{V}$. A ação é livre, pois se $v + p = p$, isto implica que $v + w + v_0 = w + v_0$, resultando em $v = 0$. A transitividade da ação também é facilmente demonstrada, pois se $p, q \in \mathbb{A}$, então $p = w + v_0$ e $q = t + v_0$, com $w, t \in \mathbb{W}$, assim, $q = p + q - p = w + v_0 + (t - w) = T_{t-w}(w + v_0)$. Portanto, a tripla $(\mathbb{W} + v_0, \mathbb{W}, +)$ constitui-se em um espaço afim.*

Em matemática, toda vez que definimos uma estrutura, torna-se necessário definir os morfismos desta estrutura, isto é, as funções entre os objeto que são compatíveis com a estrutura dada. Por exemplo, para os espaços vetoriais, definimos as transformações lineares, para os grupos, definimos os homomorfismos de grupo, para os espaços topológicos, definimos as funções contínuas, etc. Portanto, para o caso dos espaços afins, precisamos definir corretamente as funções entre espaços afins que sejam compatíveis com a estrutura afim, estas são as transformações afins.

Definição 4.2. *Uma transformação afim entre dois espaços afins,* $(\mathbb{A}, \mathbb{V}, T)$ *e* $(\mathbb{B}, \mathbb{W}, S)$ *é um par* (f, Df) *onde* $f : \mathbb{A} \to \mathbb{B}$ *é uma função e* $Df : \mathbb{V} \to \mathbb{W}$ *é uma transformação linear tal que para qualquer par de pontos* $x, y \in \mathbb{A}$ *tenhamos* $f(y) - f(x) = Df(y - x)$*. A transformação linear* Df *é denominada derivada de* f*.*

Uma forma equivalente de definir transformação afim é dizermos que é um par (f, Df) tal que para qualquer ponto $x \in \mathbb{A}$ e qualquer $v \in \mathbb{V}$, temos que

$$f(T_v(x)) = S_{Df(v)} f(x).$$

De fato, seja $y = T_v(x)$, isto quer dizer que $v = y - x$. Então, a fórmula acima se escreve como

$$f(y) = f(T_v(x)) = S_{Df(y-x)} f(x),$$

o que significa que

$$f(y) - f(x) = Df(y - x),$$

que garante que (f, Df) é uma transformação afim. Por outro lado, seja $v = y - x$, então

$$f(y) - f(x) = Df(y - x),$$

de onde temos que

$$f(y) = S_{Df(y-x)} f(x) \quad \Rightarrow \quad f(T_v(x)) = S_{Df(y-x)} f(x).$$

Proposição 4.1. *Uma transformação afim está unicamente determinada pela função* $f : \mathbb{A} \to \mathbb{B}$*.*

Demonstração: Suponha que os pares $(f, D_1 f)$ e $(f, D_2 f)$ definam duas transformações afins. Vamos mostrar que as transformações lineares $D_1 f$ e $D_2 f$ são iguais. Fixe $x_0 \in \mathbb{A}$ e tome qualquer $v \in \mathbb{V}$, então

$$D_1 f(v) = f(T_v(x_0)) - f(x_0) = D_2 f(v).$$

Portanto $D_1 f(v) = D_2 f(v)$, $\forall v \in \mathbb{V}$ o que implica na igualdade entre as derivadas. ■

Este resultado nos permite referir à transformação afim apenas pela função $f : \mathbb{A} \to \mathbb{B}$.

Exemplo 4.4. *Toda transformação constante* $f : \mathbb{A} \to \mathbb{B}$*, onde* $f(x) = a \in \mathbb{B}$*,* $\forall x \in \mathbb{A}$*, é uma transformação afim com sua derivada,* Df*, sendo a transformação linear identicamente nula. De fato*

$$f(y) - f(x) = a - a = 0 = Df(y - x).$$

Exemplo 4.5. *Seja* $(\mathbb{A}, \mathbb{V}, T)$ *um espaço afim. A função* $\mathrm{Id}_{\mathbb{A}}$ *é uma transformação afim e* $D\mathrm{Id}_{\mathbb{A}} = \mathrm{Id}_{\mathbb{V}}$*. Sejam* $x, y \in \mathbb{A}$ *então*

$$\mathrm{Id}_{\mathbb{A}}(y) - \mathrm{Id}_{\mathbb{A}}(x) = y - x = \mathrm{Id}_{\mathbb{V}}(y - x)$$

Exemplo 4.6. *Uma vez que todo espaço vetorial é um espaço afim sobre si mesmo, com a ação dada pela soma, toda transformação linear* $f : \mathbb{V} \to \mathbb{W}$ *é uma transformação afim com* $Df = f$*. De fato, sejam* $v, w \in \mathbb{V}$*, então*

$$f(v) - f(w) = f(v - w) = Df(v - w),$$

onde a primeira igualdade foi obtida devido à linearidade de f*.*

Exemplo 4.7. *Seja* $(\mathbb{A}, \mathbb{V}, T)$ *um espaço afim e* $v \in \mathbb{V}$*, então a translação por* v*, isto é, a função*

$$\begin{array}{rccc} T_v : & \mathbb{A} & \to & \mathbb{A} \\ & p & \mapsto & T_v(p) \end{array}$$

é uma transformação afim, com $DT_v = \mathrm{Id}_{\mathbb{V}}$*. Para verificarmos esta afirmação, tomemos* $x, y \in \mathbb{A}$*, definamos* $w = y - x$ *e* $z = T_v(x)$ *então*

$$T_v(y) - T_v(x) = T_v(T_w(x)) - z = T_{v+w}(x) - z = T_w(T_v(x)) - z = T_w(z) - z = w = y - x = \mathrm{Id}(y - x).$$

Portanto, obtemos o resultado enunciado.

Exemplo 4.8. *As funções $f_{a,b} : \mathbb{R} \to \mathbb{R}$, apresentadas na seção 2, são também trasnformações afins no espaço afim $(\mathbb{R}, \mathbb{R}, +)$, neste caso, a derivada $Df_{a,b}$, é a multiplicação por a, ou seja, $Df_{a,b}(x) = ax$. Para vermos este fato, sejam $x, y \in \mathbb{R}$, então*

$$f_{a,b}(y) - f_{a,b}(x) = ay + b - (ax + b) = ay - ax = a(y - x)$$

Proposição 4.2. *(Regra da Cadeia) Sejam $f : \mathbb{A}_1 \to \mathbb{A}_2$ e $g : \mathbb{A}_2 \to \mathbb{A}_3$ duas transformações afins. Então, a composta $g \circ f : \mathbb{A}_1 \to \mathbb{A}_3$ também é uma transformação afim e $D(g \circ f) = Dg \circ Df$.*

Demonstração: Sejam $x, y \in \mathbb{A}_1$ então

$$f(y) - f(x) = Df(y - x).$$

Temos, portanto, que

$$g \circ f(y) - g \circ f(x) = g(f(y)) - g(f(x)) = Dg(f(y) - f(x)) = Dg(Df(y - x)) = Dg \circ Df(y - x),$$

o que conclui a demonstração. ■

Proposição 4.3. *Sejam $(\mathbb{A}, \mathbb{V}, T)$ e $(\mathbb{B}, \mathbb{W}, S)$ dois espaços afins e seja $f : \mathbb{A} \to \mathbb{B}$ uma transformação afim que é bijetiva como função. Então*

1. *$Df : \mathbb{V} \to \mathbb{W}$ é um isomorfismo de espaços vetoriais.*
2. *$f^{-1} : \mathbb{B} \to \mathbb{A}$ é uma trasnformação afim.*
3. *$D(f^{-1}) = (Df)^{-1}$.*

Demonstração: (1) Seja $v \in \ker Df$ e fixe $x \in \mathbb{A}$, então

$$f(T_v(x)) - f(x) = Df(T_v(x) - x) = Df(v) = 0.$$

Logo, temos que

$$f(T_v(x)) = S_0(f(x)) = f(x).$$

Pela injetividade de f, concluimos que

$$T_v(x) = x,$$

mas como T é uma ação livre, então se v deixa algum ponto fixo, temos que $v = 0$, portanto Df é uma transformação linear injetiva.

Para a sobrejetividade, seja $w \in \mathbb{W}$, fixe $y \in \mathbb{B}$, pela sobrejetividade de f, temos que $y = f(x)$ para algum $x \in \mathbb{A}$ assim como $T_w(y) = f(z)$ para algum $z \in \mathbb{A}$, assim

$$w = T_w(y) - y = f(z) - f(x) = Df(z - x).$$

Portanto, Df é uma transformação linear sobrejetiva. Concluimos, assim que Df é um isomorfismo entre $\mathbb{V}$ e $\mathbb{W}$.

(2) e (3) Sejam $y_1, y_2 \in \mathbb{B}$, então

$$y_2 - y_1 = f(f^{-1}(y_2)) - f(f^{-1}(y_1)) = Df(f^{-1}(y_2) - f^{-1}(y_1)).$$

Por outro lado, temos que

$$y_2 - y_1 = Df((Df)^{-1}(y_2 - y_1)).$$

Juntando estas duas informações, temos que

$$Df(f^{-1}(y_2) - f^{-1}(y_1)) = Df((Df)^{-1}(y_2 - y_1)).$$

Do ítem (1), vimos que Df é injetiva, isto nos leva à igualdade

$$f^{-1}(y_2) - f^{-1}(y_1) = (Df)^{-1}(y_2 - y_1),$$

mostrando que f^{-1} é uma transformação afim e que $D(f^{-1}) = (Df)^{-1}$. ■

Definição 4.3. *Diremos que $(\mathbb{A}, \mathbb{V}, T)$ e $(\mathbb{B}, \mathbb{W}, S)$ são dois espaços afins isomorfos se existir $f : \mathbb{A} \to \mathbb{B}$ uma transformação afim bijetiva entre eles. Este transformação afim será denominada um isomorfismo de espaços afins.*

Exemplo 4.9. *Um exemplo de isomorfismo entre espaços afins é o isomorfismo existente entre o espaço afim e seu espaço vetorial subjacente. este exemplo será importante para que posteriormente possamos falar em coordenadas em um espaço afim. Seja $(\mathbb{A}, \mathbb{V}, T)$ um espaço afim e considere o espaço vetorial $\mathbb{V}$ com sua estrutura afim: $(\mathbb{V}, \mathbb{V}, +)$. Fixemos um ponto $a \in \mathbb{A}$ e definamos*

$$f_a : \begin{array}{ccc} \mathbb{A} & \to & \mathbb{V} \\ x & \mapsto & x - a \end{array}.$$

Esta função é uma função afim com $Df_a = \mathrm{Id}_{\mathbb{V}}$. Isto pode ser facilmente visto, pois, dados $x, y \in \mathbb{A}$ temos

$$f_a(y) - f_a(x) = (y - a) - (x - a) = y - x = \mathrm{Id}_{\mathbb{V}}(y - x).$$

Também podemos ver que f_a é bijetiva, pois podemos calcular sua inversa, que é a função

$$g : \begin{array}{ccc} \mathbb{V} & \to & \mathbb{A} \\ v & \mapsto & T_v(a) \end{array}.$$

Para verificarmos que $g = f_a^{-1}$ sejam $x \in \mathbb{A}$ e $v \in \mathbb{V}$, então

$$g \circ f_a(x) = g(f_a(x)) = g(x - a) = T_{(x-a)}(a) = x$$

e

$$f_a \circ g(v) = f_a(T_v(a)) = T_v(a) - a = v.$$

Portanto, f_a é uma transformação afim bijetiva, o que caracteriza um isomorfismo de espaços afins.

Em particular, quando $\mathbb{V}$ é um espaço vetorial real de dimensão n, ele em si é isomorfo a $\mathbb{R}^n$. Vamos denotar por $\mathbb{A}^n$ o espaço afim isomorfo, como espaço afim, a $\mathbb{R}^n$.

Tendo em vista o isomorfismo entre o espaço afim $\mathbb{A}$ e seu espaço vetorial subjacente, $\mathbb{V}$, visto como espaço afim, podemos introduzir coordenadas para os pontos de $\mathbb{A}$. Fixado um ponto $a \in \mathbb{A}$ e uma base $\{e_1, \ldots, e_n\}$ de $\mathbb{V}$, para todo ponto $x \in \mathbb{A}$ podemos escrever

$$f_a(x) = x - a = \sum_{i=1}^{n} (x - a)^i e_i = \sum_{i=1}^{n} v^i e_i.$$

Assim, o ponto x pode ser descrito como

$$x = f_a^{-1}(f_a(x)) = f_a^{-1}(\sum_{i=1}^{n} v^i e_i) = a + \sum_{i=1}^{n} v^i e_i,$$

onde o sinal de adição representa a translação pelo vetor dado. Assim, as coordenadas afins do ponto x, uma vez escolhida a origem no ponto a, são dadas pela n-upla $(v^1, \ldots v^n)$.

Vamos agora demonstrar dois resultados que caracterizam as transformações afins. Basicamente, uma transformação afim pode ser unicamente determinada conhecidos o seu valor em um ponto fixado e sua derivada.

Teorema 4.1. *(Teorema da reconstrução) Sejam $(\mathbb{A}, \mathbb{V}, T)$ e $(\mathbb{B}, \mathbb{W}, S)$ dois espaços afins. Para todo par de pontos $x \in \mathbb{A}$ e $y \in \mathbb{B}$ e para toda transformação linear $g : \mathbb{V} \to \mathbb{W}$, existe uma única transformação afim $f : \mathbb{A} \to \mathbb{B}$ tal que $f(x) = y$ e $Df = g$.*

Demonstração: Suponha dados $x \in \mathbb{A}$, $y \in \mathbb{B}$ e $g : \mathbb{V} \to \mathbb{V}$ uma transformação linear. Associe para todo $z \in \mathbb{A}$ o elemento

$$f(z) = S_{g(z-x)}(y) \in \mathbb{B}.$$

Vamos verificar que a aplicação

$$\begin{array}{rccc} f: & \mathbb{A} & \to & \mathbb{B} \\ & z & \mapsto & f(z) \end{array}.$$

é uma transformação afim e que $Df = g$. De fato, sejam $z, t \in \mathbb{A}$, então

$$\begin{aligned} f(z) - f(t) &= S_{g(z-x)}(y) - S_{g(t-x)}(y) = \\ &= S_{g(z-t+t-x)}(y) - S_{g(t-x)}(y) = \\ &= S_{g(z-t)+g(t-x)}(y) - S_{g(t-x)}(y) = \\ &= S_{g(z-t)}(S_{g(t-x)}(y)) - S_{g(t-x)}(y) = \\ &= g(z-t). \end{aligned}$$

Para verificarmos a unicidade, suponha que existe outra transformação afim $F : \mathbb{A} \to \mathbb{B}$ tal que $F(x) = y$ e $DF = g$, então, tomando qualquer $z \in \mathbb{A}$ temos

$$w = F(z) - y = F(z) - F(x) = DF(z-x) = g(z-x) = f(z) - f(x) = f(z) - y.$$

Assim, $F(z) = f(z) = S_w(y)$, como esta igualdade vale para todo $z \in \mathbb{A}$ temos que $F = f$. ■

Corolário 4.1. *Sejam $(\mathbb{A}, \mathbb{V}, T)$ e $(\mathbb{B}, \mathbb{W}, S)$ dois espaços afins. Duas transformações afins $f_1, f_2 : \mathbb{A} \to \mathbb{B}$ possuem a mesma derivada se, e somente se, existir um vetor $w \in \mathbb{W}$ tal que $f_2 = S_w \circ f_1$.*

Demonstração: ($\Rightarrow$) Suponha que $Df_1 = Df_2$. Seja $x \in \mathbb{A}$ e considere os pontos $y_1 = f_1(x)$ e $y_2 = f_2(x)$ em $\mathbb{B}$. Vamos verificar que $f_2 = S_w \circ f_1$, onde $w = y_2 - y_1$. De fato, se $z \in \mathbb{A}$, então

$$f_2(z) - f_2(x) = Df_2(z-x) = Df_1(z-x) = f_1(z) - f_1(x).$$

Assim

$$f_2(z) - y_2 = f_1(z) - y_1 = f_1(z) - y_1 + y_2 - y_2 = f_1(z) + w - y_2$$

Portanto

$$T_w(f_1(z)) = f_1(z) + w = T_{(f_2(z)-y_2)}(y_2) = f_2(z),$$

o que conclui a demonstração. ■

Este corolário nos auxilia a caracterizarmos uma transformação afim basicamente por uma transformação linear e uma translação. Isto nos permite escrever uma transformação afim em coordenadas:

Sejam $(\mathbb{A}, \mathbb{V}, T)$ e $(\mathbb{B}, \mathbb{W}, S)$ dois espaços afins. Fixe um ponto $a \in \mathbb{A}$ e um ponto $\bar{a} \in \mathbb{B}$ como sendo as respectivas origens do sistema de coordenadas. Fixe, ainda, uma base $\{e_1, \ldots, e_n\}$ em $\mathbb{V}$ e uma base $\{f_1, \ldots, f - m\}$ em $\mathbb{W}$. Assim, para qualquer $x \in \mathbb{A}$ temos que

$$x - a = v = \sum_{i=1}^{n} v^i e_i.$$

Considere agora uma transformação afim $f : \mathbb{A} \to \mathbb{B}$, então podemos escrever para qualquer $x \in \mathbb{A}$

$$f(x) - \bar{a} = f(x) - \bar{a} + f(a) - f(a) = f(x) - f(a) + f(a) - \bar{a} = Df(x-a) + f(a) - \bar{a} = Df(v) + b,$$

onde $b = f(a) - \bar{a} \in \mathbb{W}$. Com o auxílio das duas bases, podemos escrever a matriz da transformação linear Df, que será denotada por $A = (a_{ij})_{i,j} \in M_{m \times n}(\mathbb{R})$ de forma que

$$Df(e_j) = \sum_{i=1}^{m} a_{ij} f_i.$$

Portanto

$$\begin{aligned} f(x) &= \bar{a} + Df(v) + b = \bar{a} + \sum_{j=1}^{n} v^j Df(e_j) + \sum_{i=1}^{n} b^i f_i = \\ &= \bar{a} + \sum_{i=1}^{n} (\sum_{j=1}^{m} a_{ij} v^j + b^i) f_i, \end{aligned}$$

ou seja, em coordenadas afins, temos que

$$f(x)^i = \sum_{j=1}^{m} a_{ij} v^j + b^i.$$

Isto é, uma transformação afim é, essencialmente, uma transformação linear mais uma translação.

Exercício 4.2: Seja $\mathbb{A}^n$ o espaço afim de dimensão n. Mostre que $\mathbb{A}^n$ é isomorfo ao hiperplano $x^{n+1} = 1$ em $\mathbb{R}^{n+1}$.

Exercício 4.3: Ainda dentro do contexto do isomorfismo do exercício anterior, fixe como origem do espaço afim $\mathbb{A}^n$, visto como subespaço afim de $\mathbb{R}^{n+1}$, o ponto $(0, 0, \ldots, 0, 1)$. Mostre que, com isto, que toda transformação afim $f : \mathbb{A}^n \to \mathbb{A}^n$ pode ser vista como uma transformação linear em $\mathbb{R}^{n+1}$ cuja matriz é da forma

$$\left(\begin{array}{c|c} A & b \\ \hline 0 & 1 \end{array}\right)$$

Finalmente, estamos em condições de apresentarmos o grupo das transformações afins de um determinado espaço afim. Seja $(\mathbb{A}, \mathbb{V}, T)$ um espaço afim, denotaremos por $Aff(\mathbb{A})$ o grupo das transformações afins bijetivas em $\mathbb{A}$. Como vimos anteriormente, se $f \in aff(\mathbb{A})$, então sua derivada, Df é um isomorfismo no espaço vetorial $\mathbb{V}$, ou seja $Df \in GL(\mathbb{V})$. Denotando também por $\mathbb{V}$ o grupo abeliano aditivo do espaço vetorial $\mathbb{V}$, temos o seguinte resultado:

Proposição 4.4. *Seja $(\mathbb{A}, \mathbb{V}, T)$ um espaço afim, e $Aff(\mathbb{A})$ o grupo das transformações afins bijetivas em $\mathbb{A}$. Então $Aff(\mathbb{A})/\mathbb{V} \cong GL(\mathbb{V})$.*

Demonstração: Pela regra da cadeia, demonstrada anteriormente, temos que a aplicação

$$\begin{array}{rccc} D: & Aff(\mathbb{A}) & \to & GL(\mathbb{V}) \\ & f & \mapsto & Df \end{array}$$

é um homomorfismo de grupos. Pelo Teorema da reconstrução, dado qualquer isomorfismo linear $g \in GL(\mathbb{V})$ é possível construir uma infinidade de transformações afins f tais que $Df = g$, bastando escolher um par de pontos $a, b \in \mathbb{A}$ de forma que $f(a) = b$. Deixamos como exercício a verificação de que qualquer uma destas transformações afins assim construídas são bijetivas, ou seja, que $f \in Aff(\mathbb{A})$. Portanto, D é um epimorfismo. O corolário do teorema do homomorfismo de grupos nos afirma que neste caso $GL(\mathbb{V}) \cong Aff(\mathbb{A})/\ker(D)$. Resta-nos calcular o kernel do homomorfismo D. Para isto, tome $f \in \ker(D)$, ou seja, $Df = \mathrm{Id}_{\mathbb{V}}$, fixe um ponto $a \in \mathbb{A}$ e denote po b sua imagem pela função f, isto é, $b = f(a)$. Mostraremos que $f = T_{(b-a)}$, de fato para qualquer $x \in \mathbb{A}$

$$\begin{aligned} f(x) - x &= f(x) - x + (a - f(a)) + (f(a) - a) = \\ &= (f(x) - f(a)) + (a - x) + (b - a) = \\ &= Df(x - a) + (a - x) + (b - a) = \\ &= (x - a) + (a - x) + (b - a) = \\ &= b - a. \end{aligned}$$

Portanto $f(x) = T_{b-a}(x)$, e como isto vale para qualquer ponto, então $f = T_{b-a}$. O mesmo cálculo acima mostra também que poderíamos ter iniciado com qualquer ponto $c \in \mathbb{A}$ para definirmos o vetor de tranlação, uma vez que $f(c) - c = f(a) - a$. Identificando um vetor $v \in \mathbb{V}$ com sua translação T_v mostramos, com o que foi exposto acima que $\ker(D) \subseteq \mathbb{V}$. Por outro lado, vimos que toda translação possui como derivada a função $\mathrm{Id}_{\mathbb{V}}$, o que implica que $\mathbb{V} \subseteq \ker(D)$. Isto prova que $\mathbb{V} = \ker(D)$, e, como consequência, que $Aff(\mathbb{A})/\mathbb{V} \cong GL(\mathbb{V})$. ■

Teorema 4.2. *Seja $(\mathbb{A}, \mathbb{V}, T)$ um espaço afim, e $Aff(\mathbb{A})$ o grupo das transformações afins bijetivas em $\mathbb{A}$. Então $Aff(\mathbb{A}) \cong \mathbb{V} \rtimes GL(\mathbb{V})$.*

Demonstração: Fixemos $a \in \mathbb{A}$ como a origem do espaço afim. Então, para qualquer $f \in Aff(\mathbb{A})$ defina $v_f = f(a) - a$. Defina a aplicação

$$\begin{array}{rccc} \Phi: & Aff(\mathbb{A}) & \to & \mathbb{V} \rtimes GL(\mathbb{V}) \\ & f & \mapsto & (v_f, Df) \end{array}$$

Esta aplicação está bem definida, pois dada uma transformação afim f, sua derivada e o valor do ponto a por f estão unicamente definidos.

Vamos verificar que Φ é homomorfismo de grupos: Sejam $f, g \in Aff(\mathbb{A})$, então, primeiramente, pela regra da cadeia, sabemos que $D(g \circ f) = Dg \circ Df$ e

$$\begin{aligned} v_{g\circ f} &= g \circ f(a) - a = g(f(a)) - a + (g(a) - g(a)) = \\ &= (g(f(a)) - g(a)) + (g(a) - a) = Dg(f(a) - a) + v_g = \\ &= Dg(v_f) + v_g. \end{aligned}$$

Assim

$$\Phi(g \circ f) = (v_g + Dg(v_f), Dg \circ Df) = (v_g, Dg) \cdot (v_f, Df) = \Phi(g) \cdot \Phi(f),$$

o que significa que Φ é homomorfismo de grupos.

Para mostrarmos a injetividade, seja $f \in \ker(\Phi)$, então $\Phi(f) = (0, \mathrm{Id}_{\mathbb{V}})$. Deste fato, concluimos que $Df = \mathrm{Id}_{\mathbb{V}}$. Como visto anteriormente, existe $v \in \mathbb{V}$ tal que $f = T_v$. Por outro lado, como $v_f = 0$, temos que

$$0 = v_f = f(a) - a = T_v(a) - a = v.$$

Assim $f = T_0$, ou seja, para qualquer $x \in \mathbb{A}$ tem-se que $f(x) = T_0(x) = x = \mathrm{Id}_{\mathbb{A}}(x)$. Portanto $f = \mathrm{Id}_{\mathbb{A}}$.

A sobrejetividade de Φ decorre do teorema da reconstrução, pois dado um elemento $(v, g) \in \mathbb{V} \rtimes GL(\mathbb{V})$ existe uma única transformação linear $F \in Aff(\mathbb{A})$ tal que $DF = g$ e $F(a) = T_v(a)$. Com isto, temos o isomorfismo. ■

Exercício 4.4: Considere o espaço afim $(\mathbb{A}^n, \mathbb{R}^n, +)$ e defina uma distância em $\mathbb{A}^n$ dada pelo produto escalar em $\mathbb{R}^n$, isto é, dados dois pontos $x, y \in \mathbb{A}^n$ sua distância é dada por

$$d(x, y) = \sqrt{\langle y - x, y - x \rangle}.$$

Uma isometria em $\mathbb{A}^n$, é uma transformação afim $f : \mathbb{A}^n \to \mathbb{A}^n$ tal que para qualquer par de pontos $x, y \in \mathbb{A}^n$ tenhamos

$$d(f(x), f(y)) = d(x, y)$$

1. Mostre que o conjunto das isometrias, $\mathrm{ISO}(\mathbb{A}^n)$ é um subgrupo de $Aff(\mathbb{A}^n)$.

2. Mostre que as tranlações são isometrias.

3. Mostre que a derivada de uma isometria é uma transformação ortogonal.

4. Mostre que $\mathrm{ISO}(\mathbb{A}^n) \cong \mathbb{R}^n \rtimes O(n)$.

5 Geometria Projetiva

A geometria projetiva tem sua origem mais remota na renascença, com o surgimento da perspectiva na pintura. Basicamente, nossa visão das coisas depende dos raios de luz incidentes sobre nossas retinas. Uma pintura seria a intersecção deste feixe convergente de raiso de luz com a superfície da tela. Portanto, os objetos fundamentais, ao invés de serem os pontos seriam os raios de luz, ou semirretas, todas convergindo para um único ponto. Esta idéia simples nos leva abstratamente à noção de espaço projetivo, muito embora, historicamente, este conceito matemático ainda levou quatro séculos para se consolidar. Há duas maneiras equivalentes de se construir um espaço projetivo: A primeira é por adição de pontos no infinito em um espaço afim, de modo que todo feixe de reas paralelas no espaço afim possua um ponto em comum no infinito. A segunda maneira é através do feixe de ratas em um espaço vetorial que passa pela origem. Esta segunda construção está mais adequada ao nosso contexto de ações de grupos, como veremos a seguir. Primeiramente, vamos revisitar um exemplo 3.7 da seção 3 sobre a ação do grupo multiplicativo do reais sobre um espaço vetorial.

Proposição 5.1. *Seja $\mathbb{V}$ um espaço vetorial real. Então existe uma ação livre do grupo multiplicativo $(\mathbb{R}^*, \cdot)$ sobre o conjunto $\mathbb{V}\backslash\{0\}$ dada por $\alpha_\lambda(v) = \lambda v$.*

Demonstração: Os axiomas de espaço vetorial asseguram que α é, de fato, uma ação. Para vermos que é livre, considere $\lambda \in \mathbb{R}^*$ tal que exista um vetor $v \neq 0$ satisfazendo $\alpha_\lambda(v) = \lambda v = v$. Disto temos que $(\lambda - 1)v = 0$ e como v não é um vetor nulo, obrigatoriamente temos que $\lambda - 1 = 0$, ou seja, $\lambda = 1$. ■

A órbita de qualquer vetor $v \in \mathbb{V}$ é a reta que passa pela origem na direção de v, excluida a origem, ou seja

$$\mathcal{O}_v = \{\lambda v \,|\, \lambda \neq 0\}.$$

Definição 5.1. *Seja $\mathbb{V}$ um espaço vetorial real e α uma ação do grupo multiplicativo do números reais não nulos sobre $\mathbb{V}\backslash\{0\}$. O espaço projetivo real associado a $\mathbb{V}$ é o quociente $P(\mathbb{V}) = (\mathbb{V}\backslash\{0\})/\mathbb{R}^*$.*

Apenas para fixarmos a notação, dado $v \in \mathbb{V}$ denotaremos sua órbita pela ação do grupo $(\mathbb{R}^*, \cdot)$ por $[v]$. Quando o espaço vetorial em questão é $\mathbb{R}^{n+1}$, então o espaço projetivo associado a este espaço vetorial, $P\mathbb{R}^{n+1}$ é mais comumente denotado como $\mathbb{RP}^n$, e denominado espaço projetivo real n dimensional. A primeira vista, parece estranho que o espaço projetivo associado a um espaço n dimensional tenha dimensão n. Para podermos ver melhor esta situação, temos que introduzir coordenadas no espaço projetivo. Considere uma base $\{e_1, \dots e_{n+1}\}$ em $\mathbb{V}$, assim qualquer vetor $v \in \mathbb{V}$ pode ser escrito como

$$v = \sum_{i=1}^{n} x^i e_i = (x^1, \dots, x^{n+1}),$$

então, o elemento associado em $P(\mathbb{V})$ será denotado da forma

$$[v] = [x^1, \dots, x^{n+1}].$$

Estas são as coordenadas homogêneas do ponto $[v] \in P(\mathbb{V})$. Mas esta não é toda a história, uma vez que existe uma redundância infinita na descrição deste ponto, pois para qualquer $\lambda \in \mathbb{R}^*$ temos que

$$[v] = [x^1, \dots, x^{n+1}] = [\lambda x^1, \dots, \lambda x^{n+1}].$$

Não existe uma maneira única de associar coordenadas a um ponto do espaço projetivo, o que podemos fazer é determinar vizinhanças em $P(\mathbb{V})$ para as quias exista uma correspondência um a um com um espaço vetorial com uma dimensão a menos que o espaço vetorial $\mathbb{V}$. Para cada $i \in \{1, \dots, n+1\}$, defina

$$U_i = \{[x^1, \dots, x^{n+1}] \in P(\mathbb{V}) \,|\, x^i \neq 0\}.$$

Quem sabe um pouco de topologia, reconhecerá imediatamente que estes subconjuntos do espaço projetivo são abertos. Devido ao escopo e interesse destas notas, não entraremos nos detalhes topológicos envolvidos. Agora defina duas aplicações

$$\begin{array}{rccc} \phi: & U_i & \to & \mathbb{R}^n \\ & [x^1, \dots x^{n+1}] & \mapsto & \left(\frac{x^1}{x^i}, \cdots, \frac{x^{i-1}}{x^i}, \frac{x^{i+1}}{x^i}, \dots, \frac{x^{n+1}}{x^i}\right) \end{array},$$

e

$$\begin{array}{rccc} \psi: & \mathbb{R}^n & \to & U_i \\ & (x^1, \dots x^n) & \mapsto & [x^1, \dots, x^{i-1}, 1, x^{i+1}, \dots, x^n] \end{array}.$$

É fácil ver que ambas as aplicações são contínuas, verificando, portanto, que estas aplicações são mutuamente inversas, chagaremos à conclusão que estes conjuntos são homeomorfos, vistos como espaços topológicos. Em linguagem topológica, dizemos que o espaço projetivo $P(\mathbb{V})$ é localmente homeomorfo a $\mathbb{R}^n$. Esta é a razão de dizermos que a dimensão do espaço projetivo é uma dimensão a menos que o espaço vetorial que lhe deu origem. Vamos, então, verificar que estas duas aplicações são mutuamente inversas: Seja $[x^1, \dots, x^{n+1}] \in U_i$, então

$$\begin{aligned} \psi \circ \phi([x^1, \dots, x^{n+1}]) &= \psi\left(\frac{x^1}{x^i}, \cdots, \frac{x^{i-1}}{x^i}, \frac{x^{i+1}}{x^i}, \dots, \frac{x^{n+1}}{x^i}\right) = \\ &= \left[\frac{x^1}{x^i}, \cdots, \frac{x^{i-1}}{x^i}, 1, \frac{x^{i+1}}{x^i}, \dots, \frac{x^{n+1}}{x^i}\right] = \\ &= [x^1, \dots, x^{i-1}, x^i, x^{i+1}, \dots, x^{n+1}], \end{aligned}$$

sendo que, na última igualdade, multiplicamos por x^i que é um número diferente de 0. Seja agora $(x^1, \dots x^n)$, então

$$\begin{aligned} \phi \circ \psi(x^1, \dots x^n) &= \phi[x^1, \dots, x^{i-1}, 1, x^i, \dots, x^n] = \\ &= (x^1, \dots, x^{i-1}, x^i, \dots, x^n), \end{aligned}$$

o que conclui a verificação

Os espaços projetivos não são particularmente interessantes do ponto de vista puramente algébrico, pois não são fechados por nenhuma operação algébrica. Por outro lado, os espaços projetivos constituem uma fonte riquíssima de exemplos de espaços com propriedades topológicas interessantes. Vejamos alguns exemplos:

Exemplo 5.1. *Como vimos no exemplo 3.3 da seção 3, o conjunto dos vetores não nulos do espaço vetorial $\mathbb{R}^2$ sob a ação do grupo multiplicativo dos reais não nulos dá origem ao espaço projetivo unidimensional, ou reta projetiva $\mathbb{RP}^1$. Muito embora tenha este nome, a reta projetiva não é uma reta, mas já vimos que está em bijeção com uma circunferência, conforme ilustrado na figura abaixo.*

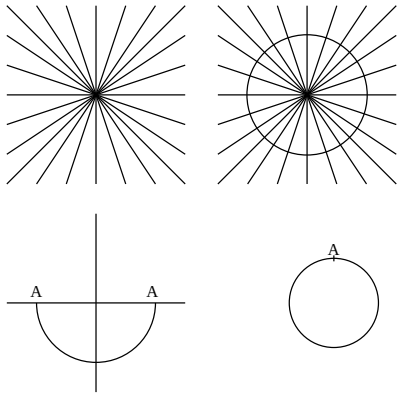

Figura 5.1: *Representação da reta projetiva como uma circunferência no plano.*

Para caracterizarmos um espaço projetivo como algum espaço topológico mais conhecido, primeiramente notemos que a esfera n dimensional,

$$\mathbb{S}^n = \{(x^1, \ldots, x^{n+1}) \in \mathbb{R}^{n+1} \,|\, (x^1)^2 + \cdots + (x^{n+1})^2 = 1\,\},$$

Intersecta exatamente duas vezes qualquer reta que passe pela origem, e esta intersecção se dá sempre em pontos antípodas, isto é, se $x = (x^1, \ldots, x^{n+1}) \in \mathbb{S}^n$ é o ponto de intersecção da esfera com uma reta que passa pela origem, então o ponto $-x = (-x^1, \ldots, -x^{n+1})$, que também pertence a $\mathbb{S}^n$, é o outro ponto de intersecção da esfera com a mesma reta. Portanto, o espaço projetivo $\mathbb{RP}^n$ pode ser caracterizado como uma esfera $\mathbb{S}^n$ com seus pontos antípodas identificados. Sendo mais precisos, podemos definir uma ação do grupo multiplicativo $\mathbb{Z}_2 = \{1, -1\}$ sobre a esfera $\mathbb{S}^n$ da maneira óbvia: $\alpha_{-1}(x) = -x$. assim a órbita de qualquer ponto da esfera é o par de pontos antípodas por ele determinado. O quociente $\mathbb{S}^n/\mathbb{Z}_2$ está, portanto, em correspondência um a um com o espaço projetivo, ou seja $\mathbb{S}^n/\mathbb{Z}_2 \cong \mathbb{RP}^n$, onde o símbolo $\cong$ aqui representa mais do que simplesmente bijeção, representa um homeomorfismo entre espaços topológicos. Nestas notas de aula, por questão de tempo, não vamos abordar os aspectos topológicos envolvidos no estudo dos espaços projetivos.

Exemplo 5.2. *O plano projetivo, $\mathbb{RP}^2$ é, basicamente, a esfera $\mathbb{S}^2$ com os pontos antípodas identificados, ou ainda, podemos pensar um dos hemisférios com os pontos antípodas do equador identificados, conforme ilustrado na figura abaixo.*

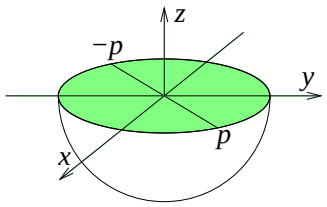

Figura 5.2: *Hemisfério com o spontos antípodas do equador identificados como uma representação do plano projetivo $\mathbb{RP}^2$.*
Este é um exemplo de superfície bidimensional não orientável, como a faixa de Möbius ou a garrafa de Klein. É impossível mergulhar o plano projetivo, como uma superfície no espaço tridimensional sem que haja auto- intersecções. Uma das múltiplas formas de se representar o plano projetivo é tomar uma faixa de Möbius, cujo bordo é uma circunferência, e um disco, cujo bordo também é uma circunferência, e identificar as duas circunferências que correspondem aos bordos destas duas superfícies. O resultado final será o plano projetivo.

Exemplo 5.3. *O espaço projetivo tridimensional, $\mathbb{RP}^3$ pode ser identificado com o grupo das rotações em $\mathbb{R}^3$, o grupo $SO(3)$. Para melhorarmos nossa percepção, retornemos ao caso de $\mathbb{RP}^2$. Como vimos, $\mathbb{RP}^2$ também pode ser entendido como um hemisfério com os pontos antípodas do equador identificados. Mas todo hemisfério é homeomorfo a um disco. Por exemplo, o hemisfério norte da esfera $\mathbb{S}^2$, denotado por*

$$U_N = \{(x, y, z) \in \mathbb{R}^3 | x^2 + y^2 + z^2 = 1\ ,\ z \geq 0\},$$

é homeomorfo ao disco

$$D = \{(x, y) \in \mathbb{R}^2 | x^2 + y^2 \leq 1\},$$

pela aplicação

$$f: \begin{array}{ccc} D & \to & \mathbb{S}^2 \\ (x,y) & \mapsto & (x, y, \sqrt{1-x^2-y^2}) \end{array},$$

cuja aplicação inversa é a projeção nas primeiras duas coordenadas. Assim, o plano projetivo é, ainda, homeomorfo ao disco unitário com os pontos antípodas da borda identificados. Da mesma forma, um hemisfério de $\mathbb{S}^3$ pode ser

visto como homeomorfo a um disco tridimensional (uma bola). Vejamos: o hemisfério norte de $\mathbb{S}^3$*,*

$$U_N = \{(x, y, z, t) \in \mathbb{R}^4 | x^2 + y^2 + z^2 + t^2 = 1 \ , \ t \geq 0\},$$

é homeomorfo à bola

$$D = \{(x, y, z) \in \mathbb{R}^3 | x^2 + y^2 + z^2 \leq 1\},$$

pela aplicação

$$\begin{array}{rccc} f: & D & \to & \mathbb{S}^3 \\ & (x,y,z) & \mapsto & (x,y,,z,\sqrt{1-x^2-y^2-z^2}) \end{array} \quad ,$$

cuja aplicação inversa é a projeção nas primeiras três coordenadas. Como $\mathbb{RP}^3$ *é homeomorfo a* $\mathbb{S}^3$ *com os pontos antípodas identificados, também podemos caracterizá-lo como um hemisfério de* $\mathbb{S}^3$ *com os pontos antípodas da borda (que é homeomorfa a uma esfera* $\mathbb{S}^2$*) identificados. E através deste homeomorfismo de um hemisfério de* $\mathbb{S}^3$ *com uma bola, podemos finalmente ver o espaço projetivo* $\mathbb{RP}^3$ *como uma bola tridimensional com os pontos antípodas de sua borda identificados.*

Como este espaço está relacionado com o grupo $SO(3)$*? Bem, podemos estabelecer uma aplicação de* $\mathbb{R}^3$ *em* $SO(3)$ *associando a cada vetor* $v \in \mathbb{R}^3$ *uma rotação cujo eixo é dado pelo vetor unitário* $\hat{v} = \frac{v}{\|v\|}$ *e com ângulo dado por* $\|v\|$*. Está claro que esta aplicação é contínua, sobrejetiva e que dois vetores corresponderão à mesma rotação se, e somente se, forem co-lineares e a sua diferença for um múltiplo inteiro de* 2π*. Portanto, se tomarmos a restrição desta aplicação à bola fechada* $\overline{B(0,\pi)}$*, teremos uma aplicação contínua entre um espaço compacto (a bola fechada* $\overline{B(0,\pi)}$*) e um espaço Haussdorff (o grupo* $SO(3)$*, pois a sua topologia é herdada da topologia métrica existente no espaço das matrizes* $M_3(\mathbb{R}) \cong \mathbb{R}^9$*), logo aberta*[8]*. Podemos identificar os pontos antípodas da superfície da bola* $\overline{B(0,\pi)}$ *que representa o grupo de rotações, isto é feito pois uma rotação de* π *cujo eixo é um vetor unitário* v *é o mesmo que uma rotação de* $-\pi$ *com respeito ao eixo* $-v$*. Temos, então uma aplicação contínua, aberta, injetiva e sobrejetiva entre* $\mathbb{RP}^3$ *(que é homeomorfo à bola com os pontos antípodas da borda identificados), e o grupo* $SO(3)$*, isto é o mesmo que dizer que* $\mathbb{RP}^3$ *é homeomorfo ao grupo* $SO(3)$*. O que conclui nossa discussão sobre a estrutura topológica do grupo* $SO(3)$*. Para mais detalhes, veja a referência [4].*

Para apresentarmos o próximo exemplo e seus desdobramentos posteriores, termos que introduzir a noção de espaço projetivo complexo.

Definição 5.2. *Seja* $\mathbb{V}$ *um espaço vetorial sobre o corpo dos números complexos. Definimos o espaço projetivo complexo* $P(\mathbb{V})$ *como o conjunto das órbitas determinadas pela ação do grupo multiplicativo* $(\mathbb{C}^*, \cdot)$ *sobre o conjunto* $\mathbb{V}\backslash\{0\}$*, dada por* $\alpha_z(v) = zv$*.*

Se considerarmos o espaço vetorial complexo $\mathbb{C}^{n+1}$ então o espaço projetivo correspondente será denotado por $\mathbb{CP}^n$. A maioria das notações e convenções acima são análogas ao caso real, a diferença está na interpretação, pois a órbita de cada vetor dada pela ação dos números complexos não nulos é um plano complexo que passa pela origem de $\mathbb{C}^{n+1}$, que como espaço vetorial real tem dimensão $2n+2$. O espaço projetivo real tem dimensão complexa n, o que significa que sua dimensão sobre os reais é igual a $2n$.

Exemplo 5.4. *O nosso último exemplo de espaço projetivo será o espaço projetivo complexo unidimensional* $\mathbb{CP}^1$*. Que o conjunto de todos os planos complexos passando pela origem de* $\mathbb{C}^2$*. Se olharmos sua dimensão sobre* $\mathbb{R}$*, veremos que este terá dimensão* 2*, isto é, será uma superfície real. Vamos ver que,* $\mathbb{CP}^1$ *é homeomorfo à esfera* $\mathbb{S}^2$*. Para isto, precisamos, primeiramente, entender a projeção estereográfica, que promove um homeomorfismo entre a esfera bidimensional* $\mathbb{S}^2$*, menos um ponto, e o plano complexo. Vejamos como isto se processa: Tomemos o ponto* $N = (0, 0, 1)$ *sobre* $\sim^2$*, que chamaremos de polo norte, e associarmos a cada ponto* $P = (x, y, z) \in \mathbb{S}^2$ *o ponto* $Z = \rho(P) = X + \imath Y \in \mathbb{C}$ *que é a intersecção da semirreta* $\overrightarrow{NP}$ *com o plano* x, y*, conforme mostrado na figura abaixo.*

[8]Um teorema importante em topologia nos garante que toda aplicação contínua entre um espaço compacto e um espaço Haussdorff é aberta, isto é, que a imagem de um aberto é um aberto

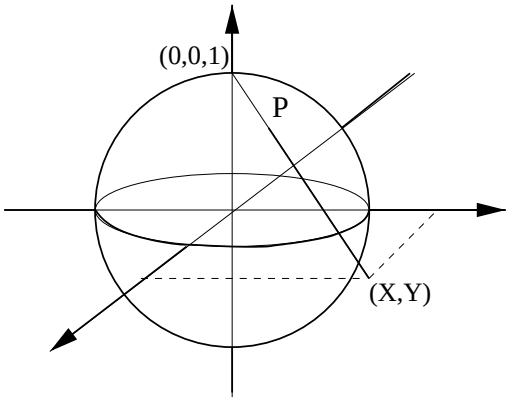

Figura 5.3: *Projeção estereográfica.*

Em coordenadas, podemos calcular facilmente a projeção estereográfica considerando as semelhanças de triângulos existentes nos planos x, z e y, z, conforme mostrado na Figura a seguir:

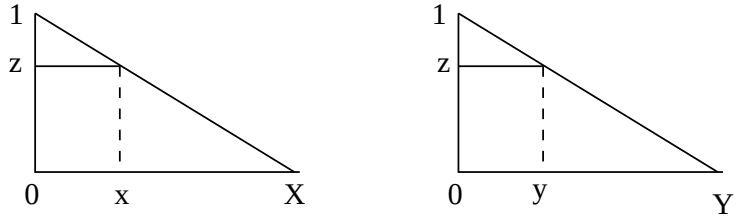

Figura 5.4: *Cálculo em coordenadas da projeção estereográfica.*

Assim, temos

$$\begin{aligned} \frac{X}{x} = \frac{1}{1-z} \qquad &\Rightarrow \quad X = \frac{x}{1-z} \\ \frac{Y}{y} = \frac{1}{1-z} \qquad &\Rightarrow \quad Y = \frac{y}{1-z}, \end{aligned}$$

e portanto $Z = \rho(x, y, z) = \frac{x+\imath y}{1-z}$.

A inversa da projeção estereográfica também pode ser facilmente calculada, pois, dado $Z = X + \imath Y \in \mathbb{C}$ *podemos encontrar um ponto sobre* $\mathbb{S}^2$ *com coordenadas* (x, y, z)*, tais que*

$$x = X(1-z), \qquad y = Y(1-z),$$

disto temos que

$$x^2 + y^2 = (X^2 + Y^2)(1-z)^2.$$

Mas, lembrando que $x^2 + y^2 + z^2 = 1$*, vemos que* $x^2 + y^2 = 1 - z^2$*, o que resulta na igualdade*

$$1 - z^2 = (X^2 + Y^2)(1-z)^2 \quad \Rightarrow 1 + z = (X^2 + Y^2)(1-z).$$

Desenvolvendo esta última igualdade, temos que

$$z = \frac{X^2 + Y^2 - 1}{X^2 + Y^2 + 1}.$$

E como $x = X(1-z)$ *e* $y = Y(1-z)$*, concluímos que*

$$x = \frac{2X}{X^2 + Y^2 + 1}, \qquad y = \frac{2Y}{X^2 + Y^2 + 1},$$

e portanto

$$\rho^{-1}(X+\imath Y)=\left(\frac{2X}{X^2+Y^2+1},\frac{2Y}{X^2+Y^2+1},\frac{X^2+Y^2-1}{X^2+Y^2+1}\right).$$

Deixamos com exercício a verificação de que ρ e ρ^{-1} são, de fato, mutuamente inversas. Estas aplicações também são contínuas, assim a esfera menos o polo norte é homeomorfa ao plano complexo.

Temos também que a aplicação

$$\begin{array}{rccc}\tilde{\rho}: & \mathbb{S}^2\backslash(0,0,-1) & \to & \mathbb{C} \\ & (x,y,z) & \mapsto & \frac{x-\imath y}{1+z}\end{array},$$

pode ser vista como uma projeção estereográfica a partir do polo sul mas compatível com a orientação do plano complexo. Esta plicação também é inversível e constitui-se um homeomorfismo entre a esfera menos o polo sul e o plano complexo. Exceto os polos norte e sul, todos os outros pontos da esfera estão nos domínios das aplicações ρ e $\tilde{\rho}$. Pode-se mostrar facilmente que, para $P=(x,y,z)\in\mathbb{S}^2$ temos $\tilde{\rho}(P)=\frac{1}{\rho(P)}$.

Em vista do que foi exposto acima, temos que a esfera $\mathbb{S}^2$ pode ser coberta por dois abertos $U_S=\mathbb{S}^2\backslash(0,0,-1)$ e $U_N=\mathbb{S}^2\backslash(0,0,1)$, cada um deles homeomorfo ao plano complexo $\mathbb{C}$ e na intersecção entre estes dois abertos, a composta $\tilde{\rho}\circ\rho^{-1}:\mathbb{C}\to\mathbb{C}$ produz a inversão no plano complexo, isto é, $\tilde{\rho}\circ\rho^{-1}(z)=\frac{1}{z}$.

Vejamos que $\mathbb{CP}^1$ também possui as mesmas propriedades que $\mathbb{S}^2$, isto é, pode ser coberta por dois abertos homeomorfos ao plano complexo e que na intersecção entre eles produz a inversão no plano complexo: Os abertos são

$$V_N=\{[z,w]\in\mathbb{CP}^1|w\neq 0\},\qquad V_S=\{[z,w]\in\mathbb{CP}^1|z\neq 0\},$$

onde $[z,w]$ é a órbita do ponto $(z,w)\in\mathbb{C}^2$.

As bijeções, ou melhor, os homeomorfismos são, análogas às aplicações definidas no caso real, e são, respectivamente

$$\begin{array}{rccc}\phi_N: & V_N & \to & \mathbb{C} \\ & [z,w] & \mapsto & \frac{z}{w}\end{array},$$

e

$$\begin{array}{rccc}\phi_S: & V_S & \to & \mathbb{C} \\ & [z,w] & \mapsto & \frac{w}{z}\end{array}.$$

E suas inversas se escrevem como

$$\begin{array}{rccc}\phi_N^{-1}: & \mathbb{C} & \to & V_N \\ & z & \mapsto & [z,1]\end{array},$$

e

$$\begin{array}{rccc}\phi_S^{-1}: & \mathbb{C} & \to & V_S \\ & z & \mapsto & [1,z]\end{array}.$$

É fácil ver que, realmente, todas estas aplicações são contínuas e que ϕ_N e ϕ_N^{-1} e ϕ_S e ϕ_S^{-1} são, de fato, mutuamente inversas. Também temos que $\phi_S\circ\phi_N^{-1}(z)=\frac{1}{z}$, ou seja, estas aplicações funcionam da mesma maneira que as projeções estereográficas. Compondo, portanto, estes homeomorfismos entre abertos de $\mathbb{CP}^1$ e o plano com as inversas das transformações estereográficas, teremos um homeomorfismo entre $\mathbb{CP}^1$ e $\mathbb{S}^2$, conforme anunciado previamente.

Definição 5.3. *Sejam $\mathbb{V}$ e $\mathbb{W}$ dois espaços vetoriais e $P(\mathbb{V})$ e $P(\mathbb{W})$ seus respectivos espaços projetivos para cada transformação linear $f:\mathbb{V}\to\mathbb{W}$ definimos a transformação projetiva associada $P(f):P(\mathbb{V})\to P(\mathbb{W})$ dada por $P(f)([v])=[f(v)]$.*

O próximo resultado é necessário para garantir que as transformações projetivas estão bem definidas e que elas se comportam bem sob composição.

Proposição 5.2. *Sejam $\mathbb{U}$, $\mathbb{V}$ e $\mathbb{W}$ espaços vetoriais (reais ou complexos) e $P(\mathbb{U})$, $P(\mathbb{V})$ e $P(\mathbb{W})$ seus espaços projetivos associados. Então*

(1) Se $f : \mathbb{U} \to \mathbb{V}$ é uma transformação linear, então $P(f)$ está bem definida.

(2) Se $f : \mathbb{U} \to \mathbb{V}$ e $g : \mathbb{V} \to \mathbb{W}$ são duas transformações lineares, então $P(g \circ f) = P(g) \circ P(f)$.

(3) Temos que $P(\mathrm{Id}_{\mathbb{V}}) = \mathrm{Id}_{P(\mathbb{V})}$. E o mesmo vale para qualquer espaço vetorial.

(4) Se $f : \mathbb{U} \to \mathbb{V}$ é um isomorfismo, então $P(f)$ também é bijetiva e $P(f)^{-1} = P(f^{-1})$.

Demonstração: (1) Sejam dois vetores $v, w \in \mathbb{U}$ tais que $[v] = [w]$, isto significa, em particular que existe um escalar λ (real ou complexo, conforme for o caso) tal que $w = \lambda v$. Então

$$P(f)([w]) = [f(w)] = [f(\lambda v)] = [\lambda f(v)] = [f(v)] = P(f)([v]).$$

(2) Seja $[v] \in \mathbb{U}$, então

$$P(g) \circ P(f)([v]) = P(g)(P(f)([v])) = P(g)([f(v)]) = [g(f(v))] = [g \circ f(v)] = P(g \circ f)([v]).$$

(3) Seja $v \in \mathbb{V}$, logo

$$P(Id_{\mathbb{V}})([v]) = [Id_{\mathbb{V}}(v)] = [v] = Id_{P(\mathbb{V})}[v].$$

(4) Dos ítens (2) e (3) temos

$$P(f^{-1}) \circ P(f) = P(f^{-1} \circ f) = P(Id_{\mathbb{U}}) = Id_{P(\mathbb{U})}$$

e

$$P(f) \circ P(f^{-1}) = P(f \circ f^{-1}) = P(Id_{\mathbb{V}}) = Id_{P(\mathbb{V})}.$$

Portanto, $P(f)$ é inversível e $P(f)^{-1} = P(f^{-1})$. ■

Exercício 5.1: Mostre que uma transformação projetiva $P(f)$ é inversível, se, e somente se, f é inversível.

A partir deste resultado, temos condições de analisar a estrutura do grupo de transformações projetivas inversíveis.

Teorema 5.1. *Seja $\mathbb{V}$ um espaço vetorial (real ou complexo). Então o grupo das transformações projetivas inversíveis em $P(\mathbb{V})$, denotado por $PGL(\mathbb{V})$, é isomorfo a $GL(\mathbb{V})/\mathbb{K}^*\mathrm{Id}$, onde $\mathbb{K}$ é o corpo subjacente ($\mathbb{K} = \mathbb{R}$, ou $\mathbb{K} = \mathbb{C}$, conforme o caso).*

Demonstração: Devido à proposição acima, podemos definir a aplicação

$$\begin{array}{rccc} P: & GL(\mathbb{V}) & \to & PGL(\mathbb{V}) \\ & g & \mapsto & P(g) \end{array}.$$

O ítem (3) da proposição anterior nos garante que P está bem definida. O exercício acima nos garante que a aplicação é sobrejetiva e o ítem (1) da proposição anterior nos garante que P é um homomorfismo de grupos. Logo, pelo teorema do homomorfismo, temos que $PGL(\mathbb{V}) \cong GL(\mathbb{V})/\ker(P)$, resta-nos, tão somente, determinarmos $\ker(P)$. Seja $f \in \ker(P)$ então, $P(f) = \mathrm{Id}_{P(\mathbb{V})}$, ou ainda, para qualquer $v \in \mathbb{V}$ temos

$$P(f)([v]) = \mathrm{Id}_{P(\mathbb{V})}([v]) = [v].$$

Por outro lado

$$P(f)([v]) = [f(v)],$$

ou seja, $[f(v)] = [v]$ para todo $v \in \mathbb{V}$. Com esta informação, concluimos que $f(v) = \lambda_v v$, isto é, f age como um fator multiplicativo, mas que, a priori, pode ser diferente para cada vetor. Vamos mostrar que não é este o caso,

isto é, a função $v \mapsto \lambda_v$ é uma função constante. Sejam $v, w \in \mathbb{V}$, vamos dividir em dois casos: o primeiro quendo v e w são linearmente independentes e o segundo quando eles são linearmente dependentes. Para o caso LI, temos

$$f(v+w) = \lambda_{v+w}(v+w),$$

e por outro lado

$$f(v+w) = f(v) + f(w) = \lambda_v v + \lambda_w w.$$

Isto implica que

$$(\lambda_{v+w} - \lambda_v)v + (\lambda_{v+w} - \lambda_w)w = 0.$$

como v e w são LI, concluimos que $\lambda_v = \lambda_w = \lambda_{v+w}$. Para o caso LD, então podemos escrever $w = \alpha v$, com $\alpha \neq 0$ uma vez que estamos tratando de vetores não nulos. Assim

$$\lambda_w \alpha v = \lambda_w w = f(w) = f(\alpha v) = \alpha f(v) = \alpha \lambda_v v,$$

o que nos leva à conclusão que $\lambda_w \alpha = \lambda_v \alpha$, ou ainda $\lambda_w = \lambda_v$. Com isto, mostramos que $f = \lambda \mathrm{Id}$, ou seja, $\ker(P) \subseteq \mathbb{K}^* \mathrm{Id}$. A outra inclusão é trivialmente verificada. Portanto $\ker(P) = \mathbb{K}^* \mathrm{Id}$, o que conclui a demonstração. ■

Uma propriedade importante das transformações projetivas decorrente deste isomorfismo é que, dada uma transformação projetiva $P(g) \in PGL(\mathbb{V})$, sempre podemos escolher como transformação linear representante desta transformação projetiva uma transformação linear cujo determinante é igual a 1. por isto, é verdade que $PGL(\mathbb{V}) = PSL(\mathbb{V})$.

Exemplo 5.5. *Considere agora o grupo $GL(2,\mathbb{C})$ das transformações lineares em $\mathbb{C}^2$. Então, a cada matriz*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2\mathbb{C}),$$

associamos a transformação projetiva

$$[z, w] \quad \mapsto \quad [az + bw, cz + dw].$$

Como $\mathbb{CP}^1$ é homeomorfo a $\mathbb{S}^2$, esta tranformação projetiva equivale a um homeomorfismo em $\mathbb{S}^2$. Adicionalmente, a esta transformação projetiva, podemos associar uma transformação no plano complexo, por exemplo, se $[z, w] \in V_N$ então à transformação projetiva $[z, w] \mapsto [az + bw, cz + dw]$ associamos a tranformação no plano complexo

$$\zeta \quad \mapsto \quad \frac{a\zeta + b}{c\zeta + w},$$

onde $\zeta = \psi_N([z, w]) = \frac{z}{w}$. As transformações no plano complexo definidas pela forma acima, constituem uma classe importante de funções de uma variável complexa e são chamadas transformações de Möbius.

Note que uma transformação de Möbius não está definida sobre todo o plano complexo, pois se a transformação é da forma

$$z \mapsto \frac{az + b}{cz + d}$$

então o domínio desta função é igual a $\mathbb{C} \setminus \left\{-\frac{d}{c}\right\}$ e o seu conjunto imagem não possui o ponto $\frac{a}{c}$ pois este seria a "imagem" do ponto no infinito. Esta restirção de domínios e contradomínios das transformações de Möbius impede que haja uma ação do grupo $PGL(2,\mathbb{C})$ sobre o plano complexo. Esta dificuldade técnica nos motiva a introduzirmos uma generalização do conceito de ação de grupo que venha a contemplar este importante caso: O conceito de ação parcial de grupo.

Definição 5.4. *Seja G um grupo e X um conjunto. Uma ação parcial de G sobre X é uma família $\{D_g\}_{g \in G}$ de subconjuntos de X junto com uma família $\{\alpha_g : D_{g^{-1}} \to D_g\}_{g \in G}$ de bijeções entre estes subconjuntos satisfazendo:*

(i) $D_e = X$ *e* $\alpha_e = \mathrm{Id}_X$.

(ii) $D_{h^{-1}}(D_{g^{-1}} \cap D_h) \subseteq D_{(gh)^{-1}}$

(iii) $\alpha_g(\alpha_h(x)) = \alpha_{gh}(x)$, *para todo* $x \in D_{h^{-1}}(D_{g^{-1}} \cap D_h)$

Os ítens (ii) e (iii) são necessários para garantir que a composição das bijeções parcialmente definidas, onde for possível fazer a composição, deve ser compatível com a operação de grupo, como se esperaria de uma boa ação de grupos. O estudo das ações parciais de grupos ainda é relativamente recente, tendo iniciado na década de 90 do século XX e originou muitos desenvolvimentos importantes na matemática desde então. certamente é um assunto fascinante e muito promissor para jovens matemáticos que queiram se lançar no mundo da pesquisa científica.

Exercício 5.2: Verifique que o conjunto das transformações de Möbius no plano constitui uma ação parcial do grupo $PGL(2, \mathbb{C})$ sobre o plano complexo.

Exercício 5.3: Determine as transformações de Möbius que constituem bijeções sobre todo o plano complexo.

Exercício 5.4: Mostre que o subgrupo $PSL(2, \mathbb{R})$ possui uma ação, via transformações de Möbius, sobre o semiplano superior

$$H = \{z \in \mathbb{C} \,|\, \mathcal{I}(z) > 0\},$$

onde $\mathcal{I}(z)$ é a parte imaginária do número complexo z.

com isto, encerramos estas pequenas notas, esperando que elas tenham contribuido positivamente para um enriquecimento de sua compreensão matamática e que tenham motivado você a se aprofundar neste rico e interessante assunto.

Referências

[1] S.V. Duzhin, B.D. Chebotarevskii: "Transformation Groups for Beginners", AMS (2004)

[2] A.I. Kostrikin, Yu.I. Manin: "Linear Algebra and Geometry", CRC Press (1989).

[3] J.J. Rotman: "A First Course in Abstract Algebras with Applications", Pearson Prentice Hall (2006).

[4] D.H. Sattinger, O.L. Weaver:"Lie Groups and Algebras with Applications to Physics, Geometry, and Mechanics", Springer-Verlag (1993).

[5] K. Spindler: "Abstract Algebra with Applications in Two Volumes: Volume I, Vector Spaces and Groups", Marcel Dekker (1994).