

**UNIVERSIDADE FEDERAL DE SANTA CATARINA
PÓS GRADUAÇÃO EM ENSINO DE MATEMÁTICA**

Graciela Siegloch

AÇÕES DE GRUPOS E GEOMETRIA

Foz do Iguaçu

2010

Graciela Siegloch

AÇÕES DE GRUPOS E GEOMETRIA

Monografia submetida ao Programa de Pós Graduação em Matemática – Formação do Professor da Universidade Federal de Santa Catarina para a obtenção do Grau de Especialista em Matemática - Formação do Professor.
Orientador: Prof. Dr.Eliezer Batista

Foz do Iguaçu

2010

Catálogo na fonte elaborada pela biblioteca da
Universidade Federal de Santa Catarina

A ficha catalográfica é confeccionada pela Biblioteca Central.

Tamanho: 7cm x 12 cm

Fonte: Times New Roman 9,5

Maiores informações em:

<http://www.bu.ufsc.br/design/Catalogacao.html>

Dedico este trabalho a Deus e a meus pais que com muito empenho sempre estiveram ao meu lado me apoiando e incentivando a seguir em frente.

AGRADECIMENTOS

Agradeço a Deus, ao meu orientador professor Eliezer Batista, aos meus colegas e amigos de pós-graduação, e aos meus familiares que com muita paciência me incentivaram a continuar.

Agradeço a todos que colaboraram para a conclusão desta especialização, e que pela falha da memória aqui não estão citados.

“Não há nada que dominemos inteiramente a não ser os nossos pensamentos”.

(René Descartes)

RESUMO

O conceito de grupo, sem sombra de dúvidas, pode ser considerado um dos mais importantes da matemática moderna. Tal conceito está presente em diversas áreas da matemática, como a geometria, a álgebra, a teoria dos números, em equações diferenciais, além de pontos da física e da química. Não é raro tentarmos reconhecer padrões e simetrias em formas de nosso cotidiano, desta mesma forma agimos quando analisamos algum objeto ou conceito matemático, como as raízes de uma equação polinomial, ou um sólido geométrico, entre outros diversos objetos a serem estudados, desta forma o fato principal que agrega aos grupos tal importância é a noção de simetria. Quando identificamos simetrias em nosso sistema, estamos imediatamente introduzindo um grupo de transformações, ou uma ação de grupos. Essa ação de grupos no conjunto é uma função do grupo no conjunto das bijeções do conjunto dado de tal forma que as operações do grupo sejam compatíveis com a composição de funções no conjunto. Já o grupo é uma abstração do conjunto de bijeções neste conjunto específico, onde podemos falar dos elementos de um grupo de maneira livre, sem qualquer referência a um conjunto externo onde ele age. Mas, considerando as aplicações que estudaremos, os grupos serão relevantes somente quando fizerem parte dos grupos de transformações. Desta forma nosso objetivo neste trabalho, é esclarecer 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 isso pretendemos abordar vários aspectos da geometria afim sob o ponto de vista das ações de grupo.

Palavras-chave: Grupo, Geometria.

SUMÁRIO

INTRODUÇÃO	9
OBJETIVOS	10
1. GRUPOS, SUBGRUPOS E HOMOMORFISMOS	11
2. AÇÕES DE GRUPOS	24
3. GEOMETRIA AFIM	34
CONSIDERAÇÕES FINAIS.....	45
REFERÊNCIAS	46

INTRODUÇÃO

A partir do estudo de equações polinomiais, teve-se a primeira aparição do conceito matemático de grupo. O principal problema era o de encontrar fórmulas para se determinar raízes de um polinômio de grau maior ou igual a 5. Desde os trabalhos desenvolvidos por Joseph Louis Lagrange, sabia-se que as permutações das raízes de um polinômio eram consideradas importantes para a procura geral de métodos de solução, e com o teorema de Niels Henrik Abel ficou claro que nem todas as equações polinomiais admitiam métodos de solução por radicais. Assim surgiu a seguinte questão “Quais equações polinomiais admitiam solução por radicais?”. Tal pergunta foi respondida por Évariste Galois, que dominou grandes textos matemáticos de seu tempo com facilidade e para solucionar este problema formulou conceitos inovadores, dos quais um deles é o conceito de grupo.

Grande parte das memórias e manuscritos deixados por Galois, foram publicados após sua morte por Joseph Liouville (1809-1882) em 1846 em seu *Journal Mathématique*, e mais tarde, em 1870, Camille Jordan (1838-1902) publicou uma avaliação completa de seus trabalhos em seu livro *Traité des Substitutions*.

O estudo dos grupos começou essencialmente com Galois; foi ele o pioneiro no uso (1830) da palavra “grupo” em seu sentido técnico. As pesquisas em teoria dos grupos foram então levadas adiante por Augustin-Louis Cauchy (1789-1857) e outros que se sucederam, para o caso particular dos grupos de substituições. Como o subsequente notável trabalho de Arthur Cayley (1821-1895), Ludwig Sylow (1832-1918), Sophus Lie, George Frobenius (1848-1917), Felix Klein, Henri Poincaré (1854-1912), Otto Holder (1859-1937) e outros o estudo dos grupos assumiu sua forma abstrata independente e se desenvolveu rapidamente. (EVES, 2004, p.536).

Vários estudiosos levaram a teoria desenvolvida por Galois à diante, fazendo com que a teoria dos grupos se expandisse para outras áreas da matemática. Um dos grandes colaboradores para esta expansão foi o matemático norueguês Sophus Lie. Lie tentou estender a teoria de Galois para equações diferenciais, mas as simetrias das soluções das equações diferenciais eram contínuas, ao contrário do que acontecia com as equações algébricas, onde as simetrias envolvendo raízes eram finitas. Com isso pela primeira vez foram necessárias além de técnicas puramente algébricas para se tratar de grupos, técnicas vindas da análise, para compreender melhor a estrutura dos grupos de Lie. Tais grupos são de grande relevância em aplicações de vários ramos da matemática pura, como em equações diferenciais e na geometria diferencial, e particularmente em geometria, onde focaremos nossos estudos no decorrer deste trabalho.

O matemático Félix Klein ressaltou em seus trabalhos a importância da teoria dos grupos, e em 1871, escreveu um artigo sobre a geometria não euclidiana, dando atenção principalmente aos espaços projetivos, ficando claro para ele que os grupos de transformações exercem influência capital na definição dos objetos geométricos. Com isso, em 1872 na universidade de Erlangen, motivou a criação de um projeto de pesquisa com o objetivo de definir geometrias como sendo o estudo dos objetos que são invariantes por grupos de transformações, conhecido hoje como “Programa de Erlangen”.

Neste trabalho mostraremos diferentes aspectos das ações de grupos em geometria, nos restringindo a um tipo especial da geometria: a geometria afim. Desde a antiguidade, os espaços afins são os ambientes mais naturais para se descrever objetos geométricos, sendo também muito próximo aos espaços vetoriais, assim, a técnica e a linguagem da álgebra linear pode ser trabalhada em paralelo com esses espaços.

OBJETIVOS

Neste trabalho, temos como objetivo mostrar os diferentes aspectos das ações de grupos em geometria, em especial na geometria afim. Para isso, deveremos ter o conhecimento básico dos conceitos de álgebra linear, como as transformações lineares e espaço vetorial, entre outros pontos que se tornarão necessários no decorrer de nosso estudo. Seguiremos descrevendo no primeiro capítulo as noções básicas de Grupos, Subgrupos e Homomorfismo de Grupos. Em seguida, no segundo capítulo estudaremos as ações de Grupos e suas respectivas propriedades. E enfim, no terceiro capítulo, veremos a Geometria Afim.

Esperamos com isso estabelecer relações entre a Geometria Afim e a Álgebra de maneira a mostrar ao leitor um pouco desta ligação que pode ser estabelecida nestas duas áreas em particular.

1. GRUPOS, SUBGRUPOS E HOMOMORFISMOS

Iniciamos nosso estudo descrevendo algumas definições de Grupos, Subgrupos e Homomorfismos, que se farão necessárias no decorrer deste trabalho.

Definição 1.1. Um grupo é um par (G, \cdot) em que

$$\begin{aligned} \cdot : G \times G &\rightarrow G \\ (a, b) &\mapsto a \cdot b \end{aligned}$$

é uma função, denominada operação do grupo, satisfazendo as seguintes propriedades:

1. *Associatividade:* Para quaisquer que sejam os elementos $a, b, c \in G$, temos $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
2. *Existência do Elemento Neutro:* Existe um elemento $e \in G$ tal que para todo $a \in G$ tenhamos $a \cdot e = e \cdot a = a$.
3. *Existência de Elemento Inverso:* A todo elemento $a \in G$ associa-se um elemento a^{-1} tal que $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Na prática não utilizaremos a notação de par ordenado (G, \cdot) para grupos, denotaremos um grupo apenas por G .

Proposição 1.1. Existe um único elemento neutro em um grupo.

Demonstração:

Suponhamos que e e e' sejam elementos neutros de (G, \cdot) , como G é grupo, é imediata a propriedade da associatividade, logo pela segunda propriedade de grupos verificamos que

$$e' = e \cdot e' = e' \cdot e = e$$

Logo existe um único elemento neutro no grupo. ■

Quando a operação no grupo é comutativa, temos uma classe particular de grupos, definiremos a seguir esse caso particular.

Definição 1.2. Se para todos os elementos $a, b \in G$ de um grupo (G, \cdot) tivermos $a \cdot b = b \cdot a$, dizemos que G é abeliano, ou comutativo.

Definição 1.3. Um subconjunto não vazio H de um grupo G é um sub-grupo de G se H com a operação de G também for um grupo.

Proposição 1.2. Se G é um grupo, para que um subconjunto não vazio $H \subset G$ seja subgrupo de G é necessário e suficiente que $\forall a, b \in H$, então $a \cdot b' \in H$. Onde b' é o simétrico de b .

Demonstração: $(\Rightarrow) H$ é subgrupo.

Indicaremos por e o elemento neutro de G e por e_H o elemento neutro de H . Então

$$e_H \cdot e_H = e_H = e_H \cdot e$$

Do fato de G ser regular temos que $e_H = e$.

Seja $\forall a, b \in H$. Então:

Se $b \in G \Rightarrow$ logo existe um simétrico b'

Se $b \in H \Rightarrow$ existe um simétrico b'_H em H ;

$$b'_H \cdot b = e_H = e = b' \cdot b$$

G é regular então $b'_H = b'$

Logo $\forall a, b \in H \Rightarrow a \cdot b'_H \in H \Rightarrow a \cdot b' \in H$

(\Leftarrow) Se $\forall a, b \in H$, $a \cdot b' \in H$ então H é subgrupo.

Seja $x_0 \in H$, pois H é não vazio. Então por hipótese

$$x_0 \cdot x'_0 \in H \Rightarrow e \in H \text{ (existência do elemento neutro)}$$

Dado $b \in H$ temos:

$$e \cdot b' \in H \Rightarrow b' \in H \text{ (existência do simétrico)}$$

- A operação \cdot é fechada em H . Sejam $a \cdot (b')' \in H$, por hipótese, então $a \cdot b \in H$.
- Associatividade: Sejam $a, b, c \in H$
 $(a \cdot b) \in H \Rightarrow (a \cdot b) \cdot c \in H$.
 $(b \cdot c) \in H \Rightarrow a \cdot (b \cdot c) \in H$

Como os elementos $(a \cdot b) \cdot c$ e $a \cdot (b \cdot c) \in G$, em G vale a associatividade, então temos que $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ em H . O que conclui a demonstração. ■

Exemplo 1.1. O conjunto dos números inteiros com a operação da adição, $(\mathbb{Z}, +)$, é um grupo abeliano, pois a soma é associativa, comutativa, o elemento neutro é o número 0 e o inverso de $n \in \mathbb{Z}$ é seu oposto $-n$. E ainda, os números inteiros múltiplos de um determinado $m \in \mathbb{Z}$ são subgrupos de \mathbb{Z} com a operação da adição.

Exemplo 1.2. 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: $\bar{k} + \bar{l} = \overline{k+l}$, e este é um grupo abeliano com n elementos, que são $\bar{0}, \bar{1}, \dots, \overline{n-1}$.

Exemplo 1.3. O conjunto dos números reais com a operação da adição $(\mathbb{R}, +)$ é um grupo abeliano, e podemos verificar então que $(\mathbb{Q}, +), (\mathbb{Z}, +)$ são subgrupos de $(\mathbb{R}, +)$.

Exemplo 1.4. Outro conjunto que é abeliano é o conjunto dos números complexos não nulos com a operação da multiplicação, (\mathbb{C}^*, \cdot) , pois a multiplicação é associativa, comutativa e o elemento neutro é o número 1. Todo número complexo não nulo não possui inverso multiplicativo. O conjunto dos números reais não nulos (\mathbb{R}^*, \cdot) e dos números racionais não nulos (\mathbb{Q}^*, \cdot) são subgrupos de (\mathbb{C}^*, \cdot) .

Exemplo 1.5. 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 a 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 disso, se $z, w \in U(1)$, então

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

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

Exemplo 1.6. Seja X um conjunto qualquer e $Bij(X) = \{f : X \rightarrow X \mid f \text{ é bijeção}\}$. O que iremos verificar é que $Bij(X)$ é um grupo com a operação dada pela composição de funções, de fato, veremos adiante que todo grupo pode ser visto como um subgrupo de um grupo de bijeções sobre um determinado conjunto.

A princípio, a composição de funções é associativa, pois, $f \circ (g \circ h) = (f \circ g) \circ h$, sempre que a composição seja possível. Para o nosso caso, todas as funções possuem como domínio todo o conjunto X e seus conjuntos imagem também são o conjunto X . Sabemos ainda, que a função identidade Id_X quando composta com qualquer função $f : X \rightarrow X$ resulta na própria f , ou seja, $f \circ Id_X = Id_X \circ f = f$. Além disso, Id_X é uma bijeção e, portanto pertence a $Bij(X)$. Temos ainda que uma função $f : X \rightarrow X$ é bijeção se, e somente se, possuir função inversa, isto é, uma função $g : X \rightarrow X$ tal que $g \circ f = f \circ g = Id_X$, e esta inversa também é uma bijeção.

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

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

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

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

Exemplo 1.7. Seja $I_n = \{1, \dots, n\}$. Uma permutação em I_n é uma bijeção $\pi: I_n \rightarrow I_n$. O conjunto $S_n = \{\pi: I_n \rightarrow I_n \mid \pi \text{ é permutação}\}$ 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 ser escrito da seguinte forma

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

Utilizando $n = 3$ temos o exemplo de S_3 , onde os elementos ficam

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Este é o menor grupo não abeliano existente.

A composta de duas permutações é feita como composta de funções, onde, por exemplo, temos

$$\pi_1 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \pi_3$$

Exemplo 1.8. Consideremos agora, um subconjunto interessante das bijeções em \mathbb{R} : Sejam $a, b \in \mathbb{R}$ números reais tais que $a \neq 0$, defina $f_{a,b}: \mathbb{R} \rightarrow \mathbb{R}$ por $f_{a,b}(x) = ax + b$. Seja $Aff(\mathbb{R})$ o conjunto de tais funções, que adiante veremos que se tratam das transformações afins na reta, vamos verificar que $Aff(\mathbb{R})$ é um subgrupo A composta de duas funções deste tipo é dada por

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

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

Definição 1.4. Sejam G e H grupos. Uma função $\varphi: G \rightarrow H$ é um homomorfismo de grupos se $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, para todos os elementos de $a, b \in G$. Se o homomorfismo é injetivo então o chamamos de monomorfismo. Se o homomorfismo é sobrejetivo, dizemos que ele é um epimorfismo. Se o homomorfismo for bijetor será chamado de isomorfismo.

Para facilitar a denotaremos $G \cong H$ quando os grupos G e H forem isomorfos.

Proposição 1.3. Sejam G e H grupos. Se $f: G \rightarrow H$ é homomorfismo então:

- (i). $f(e_G) = e_H$.
- (ii). $f(g') = f(g)'$

Demonstração:

$$\begin{aligned} \text{i.} \quad & f(e_G) \cdot e_H = f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G) \\ & \Rightarrow e_H = f(e_G). \end{aligned}$$

$$\begin{aligned} \text{ii.} \quad & f(g') \cdot (f(g))' = e_H = f(e_G) = f(g \cdot g') = f(g) \cdot f(g') \\ & \Rightarrow (f(g))' = f(g') \end{aligned}$$

Definição 1.5. Chamamos de endomorfismo um homomorfismo sobre o mesmo grupo. Um endomorfismo bijetor, ou seja, um isomorfismo sobre o mesmo grupo é denominado um automorfismo.

Teorema 1.1. Todo grupo G é isomorfo a um sub-grupo do grupo das bijeções em G .

Demonstração: Seja $a \in G$, e definamos a função

$$\begin{aligned} F_a: G &\rightarrow G \\ b &\mapsto a \cdot b \end{aligned}$$

Verifiquemos a injetividade de F_a .

De fato, se $F_a(b) = F_a(c)$, ou seja, $a \cdot b = a \cdot c$, e multiplicando a última igualdade á esquerda por a^{-1} temos $a^{-1} \cdot a \cdot b = a^{-1} \cdot a \cdot c$. Logo $b = c$, e conseqüentemente, F_a é injetiva.

Verifiquemos agora a sobrejetividade de F_a . Para isso tomemos $b \in G$. Podemos escrever $b = a \cdot a^{-1} \cdot b$, ou podemos escrever ainda $F_a(a^{-1} \cdot b)$. Portanto F_a é sobrejetiva.

Concluimos, então que $F(G) \subseteq \text{Bij}(G)$. Sejam agora $a, b, c \in G$. Temos que

$$F_a \circ F_b(c) = F_a(b \cdot c) = a \cdot (b \cdot c) = (a \cdot b) \cdot c = F_{a \cdot b}(c)$$

E ainda, para todo elemento de $a \in G$, $F_e(a) = e \cdot a = a$, portanto, $F_e = Id_G$. Então para todo $a \in G$ temos,

$$F_{a^{-1}} \circ F_a = F_{a^{-1} \cdot a} = F_e = Id_G,$$

De maneira análoga

$$F_a \circ F_{a^{-1}} = F_{a \cdot a^{-1}} = F_e = Id_G,$$

Portanto $F_{a^{-1}} = (F_a)^{-1}$.

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

$$F_a \circ (F_b)^{-1} = F_a \circ F_{b^{-1}} = F_{a \cdot b^{-1}} \in F(G)$$

desta forma, $F(G)$ é sub-grupo de $Bij(G)$. Agora, nos resta mostrar que G está em correspondência 1 a 1 com verificando a função

$$\begin{aligned} F : G &\rightarrow F(G) \subseteq Bij(G) \\ a &\mapsto F_a \end{aligned}$$

E como já mostramos F é um homomorfismo de grupos.

Suponhamos para a injetividade de F , que $F_a = F_b$, logo para qualquer $c \in G$ temos $F_a(c) = F_b(c)$, ou $a \cdot c = b \cdot c$. Como caso particular em que $c = e$, o elemento neutro de G , teremos $a = a \cdot e = b \cdot e = b$. A sobrejetividade sobre $F(G)$, vem do fato de toda bijeção em $F(G)$ ser da forma F_a para algum $a \in G$. Portanto G é isomorfo ao subgrupo $F(G)$ em $Bij(G)$, e por isso pode ser identificado com este subgrupo. ■

Definição 1.6. Dado um homomorfismo de grupos $\phi: G \rightarrow H$, definimos o kernel de ϕ , como o subconjunto

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

Proposição 1.4. Um homomorfismo $\phi: G \rightarrow H$ é injetivo se, e somente se, $\ker(\phi) = \{e_G\}$.

Demonstração:

(\Rightarrow) Se ϕ é injetiva e $\phi(g) = e_H = \phi(e_G)$, logo pela injetividade temos que $g = e_G$.

(\Leftarrow) Suponhamos que $g, h \in G$ 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 $g = h$. ■

Exemplo 1.9. Para este exemplo de isomorfismo consideremos o caso particular do grupo $SO(2)$, que é o grupo das matrizes ortogonais 2×2 com a operação de multiplicação de matrizes. Se $A \in SO(2)$ então

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

tal que

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

Logo $a = d$ e $b = -c$, reduzindo a matriz a forma

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

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

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

E chegamos a conclusão que existe $\theta \in \mathbb{R}$ tal que $a = \cos(\theta)$ e $c = \text{sen}(\theta)$, ou seja,

$$A = \begin{pmatrix} \cos(\theta) & -\text{sen}(\theta) \\ \text{sen}(\theta) & \cos(\theta) \end{pmatrix}$$

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

Definamos agora a aplicação

$$\begin{aligned} \phi: U(1) &\rightarrow SO(2) \\ e^{i\theta} &\mapsto R_\theta \end{aligned}$$

É fácil verificar que a aplicação é um homomorfismo de grupos. Para verificarmos a injetividade, considere $e^{i\theta} \in \ker(\phi)$. Então

$$R_\theta = Id = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \cos(0) & -\text{sen}(0) \\ \text{sen}(0) & \cos(0) \end{pmatrix}.$$

Portanto, $\cos(\theta) = \cos(0)$ e $\sin(\theta) = \sin(0)$, o que nos leva a $\theta = 0$, (ou ainda θ é múltiplo inteiro de 2π), ou seja, $e^{i\theta} = e^{i \cdot 0} = 1$, 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 $A = R_\theta = \phi(e^{i\theta})$.

Definição 1.7. Seja G um grupo e $H \subseteq G$ um subgrupo. Podemos definir duas relações de equivalência em G a partir de H

(i). Equivalência à esquerda

$$g \sim_L h \Leftrightarrow g^{-1}h \in H$$

(ii). Equivalência à direita

$$g \sim_R h \Leftrightarrow gh^{-1} \in H$$

Proposição 1.5. As relações acima definidas são, de fato, relações de equivalência.

Demonstração: Vamos verificar para a relação \sim_L , sendo que o outro caso é análogo.

Reflexiva: Como $\forall g \in G$, $g^{-1}g = e \in H$, logo $g \sim_L g$.

Simétrica: Sejam $g, h \in G$, tal que $g \sim_L h$ então $g^{-1}h \in H$, logo $h \sim_L g$.

Transitiva: Sejam $g, h, k \in G$ tal que $g \sim_L h$ e $h \sim_L k$ então $g^{-1}h \in H$ e $h^{-1}k \in H$ logo

$$g^{-1}k = (g^{-1}h)(h^{-1}k) \in H \Rightarrow g \sim_L k \quad \blacksquare$$

Proposição 1.6. Se $h \sim_L g$ então $\exists k \in H$ tal que $h = gk$.

Demonstração: $h \sim_L g \Rightarrow h^{-1}g \in H$ então $g^{-1}h \in H$ logo $\exists k \in H$ tal que $g^{-1}h = k$, multiplicando à esquerda por g temos $h = gg^{-1}h = gk$. \blacksquare

Assim todos os elementos equivalentes pela relação \sim_L a $g \in G$ podem ser escritos na forma gk para algum $k \in H$.

Analogamente para a relação \sim_R podemos verificar que se $h \sim_R g$ então $\exists k \in H$ tal que $h = kg$.

Definição 1.8. Seja $H \subseteq G$, um subgrupo do grupo G , e um elemento $g \in G$. Definamos a classe lateral à esquerda de g associada ao conjunto H como o conjunto $gH = \{k \in G \mid k \sim_L g\}$, e a classe lateral à direita de g em relação a H é o conjunto $Hg = \{k \in G \mid k \sim_R g\}$.

No decorrer deste trabalho utilizaremos classes laterais à esquerda, podendo ainda, caracterizar a classe gH como o conjunto dos elementos $k \in G$ tais que podem ser escritos como $k = g \cdot h$ para algum $h \in H$.

Proposição 1.7. Sejam g_1H e g_2H , duas classes laterais à esquerda. Então g_1H e g_2H ou são disjuntas ou são iguais.

Demonstração: Suponhamos que exista um elemento $k \in g_1H \cap g_2H$. Então existem $h_1, h_2 \in H$ tais que

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

Seguindo da última igualdade, e multiplicando à direita por h_1^{-1} , temos $g_1 = g_2 \cdot h_2 \cdot h_1^{-1} \in g_2H$. Logo para qualquer $g_1 \cdot h \in g_1H$ concluímos que $g_1 \cdot h = g_2 \cdot h_2 \cdot h_1^{-1} \cdot h \in g_2H$.

Podemos provar também, de forma análoga, que $g_2H \subseteq g_1H$ e, portanto, as duas classes são iguais.

Proposição 1.8. A aplicação $L_g : H \rightarrow gH$
 $h \mapsto gh$ é uma bijeção entre H e gH .

Demonstração:

- i. L_g é injetiva: Sejam $h, k \in H$ tal que $L_g(h) = L_g(k) \Rightarrow gh = gk$, multiplicando à esquerda por g^{-1} temos

$$gg^{-1}h = g^{-1}gk \Rightarrow h = k$$

Logo L_g é injetiva.

- ii. L_g é sobrejetiva: $\forall x \in gH, \exists h \in H$ tal que $x = gh = L_g(h)$

Portanto L_g é sobrejetiva. ■

A ordem de um elemento a é o menor valor inteiro positivo n tal que $a^n = I$ (se este valor existe). Se este valor não existe, o elemento tem ordem infinita.

Se um grupo G tem ordem finita, então todos os seus elementos x tem ordem finita, e a ordem de cada elemento divide a ordem do grupo.

A ordem de um grupo G e de um elemento a é representado por $|G|$ e $|a|$.

Teorema 1.2. (Teorema de Lagrange) Seja H um subgrupo do grupo finito G e sejam $|H|$ e $|G|$ suas respectivas ordens. Então a quantidade de classes laterais relativas de H é definida pela expressão

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

Demonstração: De uma proposição anterior temos que as classes laterais são disjuntas duas a duas. Escolhemos então um representante para cada classe podendo ser escrito como $g_1 \cdot g_2 \cdot \dots \cdot g_n$. O que pretendemos saber é qual o valor de n .

Pela proposição anterior, temos que todas as classes laterais g_1H, g_2H, \dots, g_nH estão em bijeção com H , logo o número de elementos de cada classe é igual à ordem do subgrupo H . Desta forma, a ordem de

G será o produto entre o número de classes laterais e o número de elementos de cada classe lateral, ou seja, $|G| = n|H|$, logo

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

Corolário 1.1. Seja G um grupo finito, e H subgrupo de G , então a ordem de H é sempre um divisor da ordem de G .

Exemplo 1.10. Considere o grupo diedral D_4 . Ele é gerado por dois elementos a , e b satisfazendo as relações:

$$a^4 = b^2 = e,$$

e

$$ba^k = a^{4-k}b.$$

Assim. O grupo D_4 terá 8 elementos $e, a, a^2, a^3, b, ab, a^2b, a^3b$ satisfazendo a seguinte tabela de multiplicação:

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

Exemplo 1.11. Tomemos o subgrupo $H = \{e, b\}$ e calculemos a classe lateral à esquerda $aH = \{a, ab\}$.

Mas temos que a classe lateral à direita é $Ha = \{a, a^3b\}$, logo as classes laterais são diferentes.

Podemos notar, que se um grupo G não é abeliano, e H é um subgrupo qualquer, nem sempre as classes laterais à direita e à esquerda coincidirão. Vejamos a seguir o que ocorre quando essas classes coincidem:

Definição 1.9. Seja $H \subseteq G$ um subgrupo do grupo G . Se as classes laterais à esquerda e à direita de H coincidirem, dizemos que H é subgrupo normal de G , denotado por $H \trianglelefteq G$.

Proposição 1.9. Seja $H \subseteq G$ um subgrupo do grupo G . Então são equivalentes as afirmativas:

- (i). H é subgrupo normal.
- (ii). Para qualquer $g \in G$ temos $gHg^{-1} = H$.
- (iii). Para qualquer $g \in G$, temos que $gHg^{-1} \subseteq H$.

Demonstração:

(i) \Rightarrow (ii) Consideremos as duas classes laterais gH e Hg com $g \in G$. Por hipótese para todo $h \in H$ existe $k \in H$ tal que $gh = kg$, logo, seja $ghg^{-1} \in gHg^{-1}$, temos que

$$\begin{aligned} ghg^{-1} &= kgg^{-1} = k \in H \\ &\Rightarrow gHg^{-1} \subseteq H. \end{aligned}$$

Por outro lado, seja $h = gg^{-1}hgg^{-1}$. Novamente existe $l \in H$ tal que $hg = gl$. Então

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

Logo $H \subseteq gHg^{-1}$, portanto os dois subconjuntos são iguais.

(ii) \Rightarrow (iii) É imediato.

(iii) \Rightarrow (i) Consideremos as classes laterais gH e Hg . Seja $gh \in gH$. Então temos $gh = ghg^{-1}g$ e como $gHg^{-1} \subseteq H$ existe $k \in H$ tal que $k = ghg^{-1}$. Portanto $gh = ghg^{-1}g = kg \in Hg$. Seja agora $hg \in Hg$. Como $hg = gg^{-1}hg$ e $g^{-1}Hg \subseteq H$, temos que existe $k \in H$ tal que $k = g^{-1}hg$. Portanto $hg = gg^{-1}hg = gk \in gH$. Assim, as duas classes são iguais. Logo $H \trianglelefteq G$. ■

Precisamos ainda, falar um pouco sobre Grupo Quociente, então vejamos. Se H é um subgrupo normal de G , então o quociente

$$G/H = \{gH \mid g \in G\}$$

possui estrutura de grupos com a operação

$$(g_1H) \cdot (g_2H) = g_1g_2H.$$

De fato, esta operação está bem definida, isto é, independe do representante da classe.

Sejam $\begin{matrix} xH = \tilde{x}H \\ yH = \tilde{y}H \end{matrix}$ duas classes laterais identificadas por dois representantes distintos. Vamos provar

que $xyH = \tilde{x}\tilde{y}H$.

Primeiramente inclusão $xyH \subseteq \tilde{x}\tilde{y}H$: Considere $a \in xyH$. Então $\exists h \in H$ tal que $a = xyh$.

Como H é subgrupo normal, então $yH = Hy$ o que significa que $\exists k \in H$ tal que $yh = ky$. Como $xH = \tilde{x}H$ temos que existe $l \in H$ de forma que $xk = \tilde{x}l$.

Novamente, pela condição $yH = Hy$, existe $m \in H$ tal que $y = ym$.

Finalmente, como $yH = \tilde{y}H$ existe $n \in H$ tal que $ym = \tilde{y}n$ assim

$$a = xhh = xky = \tilde{x}ly = \tilde{x}ym = \tilde{x}\tilde{y}n \in \tilde{x}\tilde{y}H.$$

Portanto $xyH \subseteq \tilde{x}\tilde{y}H$. Com raciocínio análogo podemos mostrar que $\tilde{x}\tilde{y}H \subseteq xyH$.

Teorema 1.3. Seja $\phi: G \rightarrow H$ um homomorfismo de grupos. Então existe um único isomorfismo $\bar{\phi}: G / \ker(\phi) \rightarrow \text{Im}(\phi)$ tal que o diagrama abaixo comute

$$\begin{array}{ccc} G & \xrightarrow{\phi} & H \\ \pi \downarrow & & \uparrow i \\ G / \ker(\phi) & \xrightarrow{\bar{\phi}} & \text{Im}(\phi) \end{array}$$

e $i: \text{Im}(\phi) \rightarrow H$ é a inclusão canônica.

Demonstração: Primeiro definamos a aplicação $\bar{\phi}: G / \ker(\phi) \rightarrow \text{Im}(\phi)$ como $\bar{\phi}(g \ker(\phi)) = \phi(g)$. Para verificarmos a comutatividade do diagrama precisamos verificar se a aplicação está bem definida e se é um homomorfismo. Verifiquemos, primeiramente, que a função está bem definida, para isso consideremos $g \ker(\phi) = g' \ker(\phi)$, o que significa que $g^{-1}g' \in \ker(\phi)$. Logo

$$\begin{aligned} \bar{\phi}(g' \ker(\phi)) &= \phi(g') = \phi(gg^{-1}g') \\ &= \phi(g)\phi(g^{-1}g') = \phi(g) = \bar{\phi}(g \ker(\phi)) \end{aligned}$$

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

Mostremos agora, que $\bar{\phi}$ é de fato um homomorfismo de grupos:

$$\begin{aligned} \bar{\phi}(g \ker(\phi) h \ker(\phi)) &= \bar{\phi}(gh \ker(\phi)) \\ &= \phi(gh) = \phi(g)\phi(h) = \bar{\phi}(g \ker(\phi))\bar{\phi}(h \ker(\phi)) \end{aligned}$$

E ainda, precisamos verificar a injetividade e sobrejetividade do homomorfismo de grupos. Para a injetividade, consideremos $g \ker(\phi) \in \ker(\bar{\phi})$. Então

$$\bar{\phi}(g \ker(\phi)) = \phi(g) = e.$$

Isso significa que $g \in \ker(\phi)$, ou, $g \ker(\phi) = e \ker(\phi)$. Logo o homomorfismo é injetivo, e a sobrejetividade decorre do fato de que qualquer $\phi(g) \in \text{Im}(\phi)$, e assim $\phi(g) = \bar{\phi}(g \ker(\phi)) \in \text{Im}(\bar{\phi})$, concluindo a demonstração do teorema. ■

Enunciaremos ainda um corolário que será muito útil na obtenção de isomorfismos no decorrer deste trabalho.

Corolário 1.2. Se $\phi: G \rightarrow H$ é um epimorfismo, então $H \cong G / \ker(\phi)$.

2. AÇÕES DE GRUPOS

Como já sabemos, todo grupo é isomorfo a um sub-grupo de um grupo de bijeções em um conjunto, particularmente, das bijeções do próprio grupo. Podemos verificar que as situações em que um grupo pode ser visto como grupo de bijeções são as que aparecem nas aplicações da teoria. Agindo como um grupo de bijeções o grupo realmente se concretiza, e se incorpora tornando-se uma ferramenta poderosa para o estudo das simetrias.

Definição 2.1. 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 $Bij(X)$.

Definiremos a seguir o grupo oposto, neste trabalho, lidaremos apenas com ações à esquerda, mas também é possível definirmos ações à direita.

Definição 2.2. Definimos o grupo oposto, G^{op} do grupo dado G como o conjunto G munido com uma operação dada como:

$$\begin{aligned} \bullet : G \times G &\rightarrow G \\ (g, h) &\mapsto g \bullet h = hg \end{aligned}$$

Definição 2.3. Uma ação à direita de um grupo G em um conjunto X é um homomorfismo de G^{op} no grupo das bijeções em X .

Fixemos as notações: Denotemos uma ação (à esquerda, a menos que se diga o contrário) por

$$\begin{aligned} \alpha : G &\rightarrow Bij(X) \\ g &\mapsto \alpha_g \end{aligned}$$

onde α_g é uma bijeção no conjunto X , que associa a cada elemento $x \in X$ outro elemento $\alpha_g(x)$.

Como α é um homomorfismo, então temos que

- I. $\alpha_g(\alpha_h(x)) = \alpha_{gh}(x)$ para todos os elementos $g, h \in G$ e $x \in X$.
- II. $\alpha_e = Id_X$, ou seja, $\alpha_e(x) = x$ para todo $x \in X$.
- III. $\alpha_g^{-1} = \alpha_{g^{-1}}$ para todo $g \in G$.

Definição 2.4. Considere $x \in X$ um elemento de um conjunto X , e seja α uma ação de um grupo G sobre o conjunto X . Definimos a órbita do elemento x como sendo o conjunto

$$O_x = \{\alpha_g(x) / g \in G\}.$$

Definição 2.5. Uma relação R sobre G é dita de equivalência se:

- (i). R for reflexiva: xRx .
- (ii). R for simétrica: $xRy \Rightarrow yRx$.

(iii). R for Transitiva: $xRy \in yRz \Rightarrow xRz$.

Proposição 2.1. 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 ($x \sim y$) se existir $g \in G$ tal que $y = \alpha_g(x)$. É fácil verificar que esta é uma relação de equivalência:

1. Para qualquer $x \in X$, temos que $x = \alpha_e(x)$, portanto $x \sim x$, sendo reflexiva.

2. 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 $y \sim x$. Logo é simétrica.

3. 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 $z = \alpha_h(y) = \alpha_h(\alpha_g(x)) = \alpha_{hg}(x)$, implicando em $x \sim z$. ■

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

Proposição 2.2. Duas órbitas pela ação de um grupo ou são disjuntas ou coincidentes.

Demonstração:

Suponhamos que $O_x \cap O_y \neq \emptyset$, então existe $z \in O_x \cap O_y$, ou seja existem $g, h \in G$ tais que $z = \alpha_g(x) = \alpha_h(y)$. E desta igualdade temos que $x = \alpha_{g^{-1}h}(y)$ e $y = \alpha_{h^{-1}g}(x)$.

Considerando $u' \in O_x$ temos que existe $k \in G$ tal que $w = \alpha_k(x)$, ou seja, $w = \alpha_k(x) = \alpha_k(\alpha_{g^{-1}h}(y)) = \alpha_{kg^{-1}h}(y)$, donde podemos concluir que $u' \in O_y$. Analogamente, seja $t \in O_y$ então, existe $l \in G$ tal que $t = \alpha_l(y)$, ou seja $t = \alpha_l(y) = \alpha_l(\alpha_{h^{-1}g}(x)) = \alpha_{lh^{-1}g}(x)$, donde podemos concluir que $t \in O_x$. Portanto $O_x = O_y$. ■

Pelos resultados mostrados na proposição anterior podemos concluir 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 , e 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 subconjuntos são denominado domínios fundamentais.

Definição 2.6. Seja α uma ação de um grupo G sobre um conjunto 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 $x = \alpha_g(y)$.

Podemos notar que, segundo esta definição, não pode haver dois elementos da mesma órbita no domínio fundamental e todas as órbitas devem estar contempladas neste domínio, pois por definição deve ser possível atingir qualquer outro ponto de X agindo sobre pontos de F . A seguir veremos alguns exemplos para conseguirmos distinguir as definições de conjunto quociente e domínio fundamental.

Exemplo 2.1. Seja o grupo aditivo \mathbb{Z} agindo sobre reta real \mathbb{R} da seguinte maneira: $\alpha_n(x) = x + n$. É fácil verificar que α é uma ação, pois

$$\alpha_n(\alpha_m(x)) = \alpha_n(x+m) = x+m+n = \alpha_{n+m}(x) \text{ e}$$

$$\alpha_0(x) = x+0 = x.$$

Dado um elemento $x \in \mathbb{R}$, sua órbita será o conjunto

$$O_x = \{x+n \mid n \in \mathbb{Z}\}.$$

Desta forma, tomando 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. Além disso, 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 $a - \lfloor a \rfloor \in [0, 1[$ que é a parte fracionária do número a . Desta forma, 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.

Analisando por outro ângulo, o quociente é o conjunto das órbitas, e podemos caracteriza-lo como a circunferência unitária através da função

$$f: \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{S}^1$$

$$O_x \mapsto (\cos(2\pi x), \text{sen}(2\pi x))$$

Se, $O_x = O_y$ então $y = x + n$, para algum número inteiro n . Podemos ver que esta aplicação está bem definida. De fato,

$$f(O_y) = (\cos 2\pi y, \text{sen} 2\pi y) = (\cos 2\pi(x+n), \text{sen} 2\pi(x+n))$$

$$= (\cos 2\pi x, \text{sen} 2\pi x) = f(O_x)$$

Também podemos verificar a injetividade, pois se $f(O_x) = f(O_y)$, então $(\cos 2\pi y, \text{sen} 2\pi y) = (\cos 2\pi x, \text{sen} 2\pi x)$, implicando em $\cos 2\pi y = \cos 2\pi x$ e $\text{sen} 2\pi y = \text{sen} 2\pi x$. Isto somente ocorre quando existe um n tal que $y = x + n$, ou ainda quando $y \in O_x$, que é equivalente a dizer que $O_x = O_y$. A sobrejetividade decorre imediatamente do fato de que todo ponto $p \in \mathbb{S}^1$ possui coordenadas $p = (\cos \theta, \text{sen} \theta)$, para $\theta \in [0, 2\pi[$, assim $p = f\left(\frac{O_\theta}{2\pi}\right)$.

Exemplo 2.2. Considere a ação do grupo multiplicativo (\mathbb{R}^*, \cdot) sobre o plano \mathbb{R}^2 , excluindo a origem, dado por $\alpha_\lambda(x, y) = (\lambda x, \lambda y)$. É fácil verificar que se trata de uma ação de grupo, de fato

$$\alpha_\lambda(\alpha_\mu(x, y)) = \alpha_\lambda(\mu x, \mu y) = (\lambda \mu x, \lambda \mu y) = \alpha_{\lambda\mu}(x, y)$$

$\alpha_1(x, y) = (1 \cdot x, 1 \cdot y) = (x, y)$. Dado um ponto no plano $(x, y) \in \mathbb{R}^2 \setminus \{(0, 0)\}$ sua órbita é dada pelo conjunto

$$O_{(x,y)} = \{(\lambda x, \lambda y) \mid \lambda \in \mathbb{R}^*\},$$

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

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

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

$$(x, y) = \left(\operatorname{sign}(y) \sqrt{x^2 + y^2} \frac{x}{\operatorname{sign}(y) \sqrt{x^2 + y^2}}, \operatorname{sign}(y) \sqrt{x^2 + y^2} \frac{y}{\operatorname{sign}(y) \sqrt{x^2 + y^2}} \right) =$$

$$\alpha_{\operatorname{sign}(y) \sqrt{x^2 + y^2}} \left(\frac{x}{\operatorname{sign}(y) \sqrt{x^2 + y^2}}, \frac{y}{\operatorname{sign}(y) \sqrt{x^2 + y^2}} \right),$$

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

E ainda podemos caracterizar o quociente como a circunferência unitária pela aplicação

$$f : \mathbb{R}^2 \setminus \{(0, 0)\} / \mathbb{R}^* \rightarrow \mathbb{S}^1$$

$$O_{(x,y)} \mapsto (\cos 2\theta, \sin 2\theta)$$

onde θ é o ângulo que define a órbita do ponto no domínio fundamental. A injetividade e o fato de ser bem definido decorrem naturalmente, já que a aplicação f é 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

$$f \left(O_{\left(\cos \frac{\varphi}{2}, \sin \frac{\varphi}{2} \right)} \right).$$

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

Definição 2.7. Considere uma ação α de um grupo G sobre um conjunto X . O subgrupo estabilizador de um elemento $x \in X$ é definido como $Stab_x = \{g \in G \mid \alpha_g(x) = x\}$.

Proposição 2.3. Seja G um grupo e $\alpha: G \rightarrow Bij(X)$ uma ação de G em X . Para todo $x \in X$, $Stab_x$ é subgrupo de G .

Demonstração: Sejam $g, h \in Stab_x$, primeiramente notemos que

$$x = \alpha_e(x) = \alpha_{h^{-1}h}(x) = \alpha_{h^{-1}}(\alpha_h(x)) = \alpha_{h^{-1}}(x)$$

Portanto $\alpha_{gh^{-1}}(x) = \alpha_g(\alpha_{h^{-1}}(x)) = \alpha_g(x) = x$, logo $gh^{-1} \in Stab_x$, o que mostra que $Stab_x$ é subgrupo de G . ■

Analogamente podemos falar do subgrupo estabilizador de um subconjunto $Y \subseteq X$: $Stab_Y = \{g \in G \mid \alpha_g(Y) \subseteq Y\}$.

Os elementos de um subconjunto não precisam ficar fixos pela ação do grupo, apenas suas órbitas precisam estar contidas neste subconjunto. Quando $Stab_Y = G$, dizemos que $Y \subseteq X$ é um subconjunto invariante pela ação do grupo G . Uma definição dual é o conjunto dos pontos fixos pela ação de um determinado elemento ou subgrupo de G .

Definição 2.8. O subconjunto dos pontos fixos de um elemento $g \in G$ é o conjunto $Fix_g = \{x \in X \mid \alpha_g(x) = x\}$. Se $H \subseteq G$ é um subgrupo de G , o conjunto dos pontos fixos pela ação de H é definido por $Fix_H = \{x \in X \mid \alpha_g(x) = x, \forall g \in H\}$.

Definição 2.9. Definimos uma ação α de G em X como sendo

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 $O_x = X$, para todo elemento $x \in X$. Ou, equivalente, se $x, y \in X$ então existe $g \in G$ tal que $y = \alpha_g(x)$.

Exemplo 2.3. Consideremos o grupo

$$\text{Aff}(\mathbb{R}) = \{f_{a,b}(x) = ax + b, a \neq 0 \text{ e } b \in \mathbb{R}\},$$

e o conjunto $X = \{(x,1) \mid x \in \mathbb{R}\}$.

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

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

Podemos ver que esta ação não é livre, pois se $a \neq 1$ temos que $\alpha_{f_{a,b}}\left(\frac{b}{1-a}, 1\right) = \left(\frac{b}{1-a}, 1\right)$. A ação é transitiva pois $(y,1) = \alpha_{f_{1,y-x}}(x,1)$.

Exemplo 2.4. Um grupo G pode agir sobre um espaço vetorial através de transformações lineares invertíveis, ou seja, através de um homomorfismo de grupos $\rho: G \rightarrow GL(V)$. Este tipo especial de ação de grupos é chamado de representação linear de um grupo. O estudo destas representações lineares de grupos tornou-se uma ferramenta poderosa tanto em matemática pura como também nas aplicações, pois associa técnicas e resultados oriundos da teoria dos grupos com técnicas de álgebra linear.

Teorema 2.1. Seja α uma ação de um grupo G sobre um grupo H por automorfismos, isto é $\forall g \in G, \alpha_g \in \text{Aut}(H)$. 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 $H \times_{\alpha} G$ é denominado produto semidireto de H por G . Além disso

- (i). As inclusões $i_1: H \rightarrow H \times_{\alpha} G$ e $i_2: G \rightarrow H \times_{\alpha} G$ são monomorfismos de grupo.

$$h \mapsto (h, e_G) \quad , \quad e \quad g \mapsto (e_H, g)$$
- (ii). O subgrupo $i_1(H)$ é subgrupo normal.
- (iii). A ação de G em H é escrita como um automorfismo interno de $H \times_{\alpha} G$, isto é,

$$i_1(\alpha_g(h)) = i_2(g) \cdot i_1(h) \cdot (i_2(g))^{-1}.$$

Mas 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 todo $h \in H$ 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

$$K \cong H \times_{\alpha} G.$$

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

I. Associatividade:

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

II. Elemento Neutro:

O elemento neutro do produto semidireto é $(e_H, e_G) \in H \times_\alpha G$. De fato, dado qualquer $(h, g) \in H \times_\alpha G$ teremos que

$$\begin{aligned}
 (e_H, e_G) \cdot (h, g) &= (e_H \alpha_{e_G}(h), e_G g) = (h, g), e \\
 (h, g) \cdot (e_H, e_G) &= (h \alpha_g(e_H), g e_G) = (h e_H, g) = (h, g).
 \end{aligned}$$

III. Elemento Inverso: Seja $(h, g) \in H \times_\alpha G$, vamos verificar que $(h, g)^{-1} = (\alpha_{g^{-1}}(h^{-1}), g^{-1})$, onde a princípio temos

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

Mas, por outro lado temos

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

Portanto $(H \times_\alpha G, \cdot)$ é um grupo. Agora verificaremos os itens (i), (ii) e (iii).

1. Então vamos verificar primeiramente que i_1 é homomorfismo:

$$\begin{aligned}
i_1(h_1) \cdot i_1(h_2) &= (h_1, e_G) \cdot (h_2, e_G) \\
&= (h_1 \alpha_{e_G}(h_2), e_G e_G) \\
&= (h_1 h_2, e_G) \\
&= i_1(h_1 h_2)
\end{aligned}$$

A injetividade de i_1 é facilmente verificada, pois se $h \in \ker(i_1)$ então $(h, e_g) = (e_H, e_G)$, logo $h = e_H$.

Para a aplicação i_2 temos

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

A injetividade de i_2 , segue de forma análoga a utilizada em i_1 .

2. Seja $k \in H$ e $(h, g) \in H \times_\alpha G$, então

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

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

3. Seja $k \in H$ e $(h, g) \in H \times_\alpha G$, então

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

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

$$\begin{aligned}\Phi: K &\rightarrow H \times_{\alpha} G \\ hg &\mapsto (h, g)\end{aligned}$$

Podemos verificar que Φ é um homomorfismo de grupos, pois

$$\begin{aligned}\Phi(h_1, g_1) \cdot \Phi(h_2, g_2) &= (h_1, g_1) \cdot (h_2, g_2) = (h_1 \alpha_{g_1}(h_2), g_1 g_2) \text{ e} \\ \Phi((h_1, g_1)(h_2, g_2)) &= \Phi(h_1 \alpha_{g_1}(h_2) g_1 g_2) = (h_1 \alpha_{g_1}(h_2), g_1 g_2)\end{aligned}$$

Isto mostra que $\Phi(h_1, g_1) \cdot \Phi(h_2, g_2) = \Phi((h_1, g_1)(h_2, g_2))$.

Obtemos a injetividade de Φ tomando $h, g \in \ker(\Phi)$, então

$$\Phi(hg) = (h, g) = (e_H, e_G),$$

onde podemos concluir que

$$h = e_H \text{ e } g = e_G,$$

ou seja,

$$hg = e_H e_G = e_K.$$

E enfim, a sobrejetividade de Φ é óbvia, pois para qualquer $(h, g) \in H \times_{\alpha} G$ temos que $(h, g) = \Phi(hg)$. Portanto $K \cong H \times_{\alpha} G$. ■

Exemplo 2.5. Se G age sobre H trivialmente, isto é, $\alpha_g = Id_H \forall g \in G$ então $G \times_{\alpha} H \cong G \times H$, o produto direto

$$\begin{aligned}(h_1, g_1)(h_2, g_2) &= (h_1 \alpha_{g_1}(h_2), g_1 g_2) \\ &= (h_1 h_2, g_1 g_2)\end{aligned}$$

é o exemplo mais simples de produto semidireto.

Exemplo 2.6. Se G age sobre si mesmo pela ação adjunta, então $G \times_{Ad} G \cong G \times G$. Este isomorfismo é dado pela aplicação

$$\begin{aligned}\Psi: G \times G &\rightarrow G \times_{Ad} G \\ (g, h) &\mapsto (gh^{-1}, h)\end{aligned}$$

Para verificarmos o homomorfismo, temos que

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

Verificamos a injetividade tomando $(g, h) \in \ker(\Psi)$, então

$$\Psi(g, h) = (gh^{-1}, h) = (e_G, e_G),$$

desta forma $h = e_G$, e por consequência $g = e_G$, o que implica em

$$(g, h) = (e_G, e_G),$$

o que equivale a dizer que Ψ é injetiva.

A sobrejetividade vem do fato de que

$$(g, h) = (ghh^{-1}, h) = \Psi(gh, h),$$

concluindo a demonstração do isomorfismo.

No próximo capítulo, veremos mais um exemplo de produto semidireto, o grupo afim.

3. GEOMETRIA AFIM

A primeira estruturação da geometria ocorreu com a obra de Euclides, onde 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, e 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.

Com a evolução natural da geometria analítica, houve o surgimento da álgebra linear, originando a estrutura de espaço vetorial, e disso veio que em todo espaço vetorial, existe um ponto privilegiado, uma origem, que é o vetor nulo. Desta forma, 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.

Tornou-se necessário 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. E para suprir esta necessidade apresentamos a estrutura de espaço afim.

Definição 3.1. Definimos um espaço afim (real) como uma tripla $(\mathbf{A}, \mathbf{V}, \mathbf{T})$, onde \mathbf{A} é um conjunto, \mathbf{V} é um espaço vetorial (sobre o corpo dos reais) e \mathbf{T} é uma ação livre e transitiva do grupo aditivo do espaço vetorial \mathbf{V} sobre o conjunto \mathbf{A} .

Temos a seguir algumas observações decorrentes da definição de espaço afim:

1. O espaço afim por um abuso de notação, acaba sendo denotado por \mathbf{A} .
2. A ação do espaço vetorial \mathbf{V} sobre o espaço afim \mathbf{A} é dita ser uma ação por translações. E o grupo aditivo de \mathbf{V} é chamado o grupo de translações do espaço afim.
3. Por definição, a dimensão do espaço afim é a dimensão do espaço vetorial que nele age livre e transitivamente.
4. Sendo $p \in \mathbf{A}$ e $v \in \mathbf{V}$, costuma-se denotar a translação $T_v(p)$ por $p + v$, onde o sinal de adição não implica que o espaço afim seja munido de uma operação, apenas representa o traslado de p pelo vetor v .
5. Como a ação é transitiva, dados quaisquer dois pontos $p, q \in \mathbf{A}$ existe $v \in \mathbf{V}$ tal que $q = T_v(p)$. Neste caso, também costuma-se denotar o vetor v por $q - p$, deixando claro que esta não é uma subtração, apenas um símbolo para denotar o vetor que translada o ponto p no ponto q . A unicidade da diferença $q - p$ entre os pontos p e q em um espaço afim é consequência da ação do grupo aditivo do espaço vetorial subjacente ser livre.
6. Dentro desta notação, podemos ver que $T_v(x) - x = v$ para qualquer $x \in \mathbf{A}$ e qualquer $v \in \mathbf{V}$, e $T_{(y-x)}(x) = y$ para quaisquer $x, y \in \mathbf{A}$.

Proposição 3.1. Seja $(\mathbf{A}, \mathbf{V}, \mathbf{T})$ um espaço afim. Então

- a) $\forall x, y, z \in \mathbf{A} \quad (x - y) + (x - z) = x - z,$

- b) $\forall x \in \mathbf{A} \quad x - x = 0$,
 c) $\forall x, y \in \mathbf{A} \quad y - x = -(x - y)$,
 d) $\forall x, y, z, t \in \mathbf{A} \quad (x - y) + (z - t) = (x - t) + (z - y)$.

Demonstração:

$$\begin{aligned} T_{(x-y)+(y-z)}(z) &= T_{(x-y)}(T_{(y-z)}(z)) \\ \text{a) } &= T_{(x-y)}(y) \\ &= x \\ &= T_{(x-z)}(z). \end{aligned}$$

Pelo fato de a ação T ser livre temos que $(x - y) + (y - z) = (x - z)$.

b) $T_{(x-x)}(x) = x$, novamente por T ser livre, temos que $x - x = 0$.

c) Da definição anterior temos

$$(x - y) + (y - x) = x - x = 0 = (x - y) - (x - y)$$

esta igualdade em \mathbf{V} , então subtraindo $(x - y)$ de ambos os lados, temos que $y - x = x - y$.

d) Vamos aplicar $T_{(x-y)+(z-t)}$ e $T_{(x-t)+(z-y)}$ as partes t

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

Novamente o fato de T ser livre, temos que

$$(x - y) + (z - t) = (x - t) + (z - y). \quad \blacksquare$$

Exemplo 3.1. Seja \mathbf{V} um espaço vetorial agindo sobre si mesmo da seguinte forma: $T_v(w) = w + v$. Isso faz com que $(\mathbf{V}, \mathbf{V}, +)$ seja um exemplo de espaço afim. As propriedades de ação decorrem diretamente das propriedades da soma no espaço vetorial. E o fato de a ação ser livre também é direto, pois se $v + w = w$ para algum $w \in \mathbf{V}$, então $v = 0$. A transitividade da ação decorre do fato que se $v, w \in \mathbf{V}$, então $w = v + (w - v) = T_{w-v}(v)$.

Teremos ainda, como caso particular que a reta real \mathbb{R} agindo sobre si mesma pela soma torna a reta $(\mathbb{R}, \mathbb{R}, +)$ um exemplo de espaço a fim.

Em matemática, ao definirmos uma estrutura torna-se necessário definir os morfismos desta

estrutura, ou seja as funções entre os objetos compatíveis com a estrutura dada. Por exemplo, nos espaços vetoriais, definimos as transformações lineares, para os grupos, definimos os homomorfismos de grupo, para os espaços topológicos, definimos as funções contínuas, etc. Desta forma para os espaços afins, temos a necessidade de definir corretamente as funções entre espaços afins que sejam compatíveis com a estrutura afim, estas são as transformações afins.

Definição 3.2. Uma transformação afim entre dois espaços afins, $(\mathbf{A}, \mathbf{V}, \mathbf{T})$ e $(\mathbf{B}, \mathbf{W}, \mathbf{S})$ é um par (f, Df) onde $f : \mathbf{A} \rightarrow \mathbf{B}$ é uma função e $Df : \mathbf{V} \rightarrow \mathbf{W}$ é uma transformação linear tal que para qualquer par de pontos $x, y \in \mathbf{A}$ tenhamos $f(y) - f(x) = Df(y - x)$. A transformação linear Df é denominada derivada de f .

Equivalentemente, podemos definir uma transformação afim como um par (f, Df) tal que para qualquer ponto $x \in \mathbf{A}$ e qualquer $v \in \mathbf{V}$ temos que

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

De fato, seja $y = T_v(x)$, logo $v = y - x$. Então a fórmula acima fica $f(y) = f(T_v(x)) = S_{Df(y-x)}f(x)$, o que significa que $f(y) - f(x) = Df(y - x)$, o que garante que (f, Df) é uma transformação afim. Temos por outro lado, que se $v = y - x$, então $f(y) - f(x) = Df(y - x)$, de onde vem que

$$\begin{aligned} f(y) &= S_{Df(y-x)}f(x) \\ \Rightarrow f(T_v(x)) &= S_{Df(y-x)}f(x) \\ &= S_{Df(v)}f(x) \end{aligned}$$

Proposição 3.2. Uma transformação afim está unicamente determinada pela função $f : \mathbf{A} \rightarrow \mathbf{B}$.

Demonstração: Suponha que os pares (f, D_1f) e (f, D_2f) definam duas transformações afins, mostraremos que as transformações lineares D_1f e D_2f são iguais. Fixemos $x_0 \in \mathbf{A}$ e tomemos qualquer $v \in \mathbf{V}$. Então

$$\begin{aligned} D_1f(v) &= f(T_v(x_0)) - f(x_0) \\ &= D_2f(v) \end{aligned}$$

Portanto $D_1f(v) = D_2f(v)$, $\forall v \in \mathbf{V}$, o que implica na igualdade entre as derivadas.

Observando, que este resultado nos permite referir a transformação afim apenas pela função $f : \mathbf{A} \rightarrow \mathbf{B}$. ■

Exemplo 3.2. Seja $(\mathbf{A}, \mathbf{V}, \mathbf{T})$ um espaço afim e $v \in \mathbf{V}$, então a translação por v , isto é, a função

$$\begin{aligned} T_v : \mathbf{A} &\rightarrow \mathbf{A} \\ p &\rightarrow T_v(p) \end{aligned}$$

é uma transformação afim, com $DT_v = Id_{\mathbf{V}}$. A fim de verificar a informação, tomemos $x, y \in \mathbf{A}$, e definamos $w = y - x$ e $z = T_v(x)$. Logo

$$\begin{aligned} T_v(y) - T_v(x) &= T_v(T_w(x)) - z \\ &= T_{v+w}(x) - z \\ &= T_w(T_v(x)) - z \\ &= T_w(z) - z \\ &= w \\ &= y - x \\ &= Id(y - x). \end{aligned}$$

Portanto, obtemos o resultado enunciado.

Exemplo 3.3. A identidade é uma transformação afim e $DId_{\mathbf{A}} = Id_{\mathbf{A}}$:

$$\begin{aligned} \forall x, y \in \mathbf{A} \quad Id_{\mathbf{A}}(y) - Id_{\mathbf{A}}(x) &= Id_{\mathbf{V}}(y - x) \\ &= Id_{\mathbf{V}}(y - x) \end{aligned}$$

Exemplo 3.4. Qualquer transformação linear $T : \mathbf{V} \rightarrow \mathbf{V}$, em $(\mathbf{V}, \mathbf{V}, +)$ é uma transformação afim com $DT = T$:

De fato, sejam $v, w \in \mathbf{V}$

$$T(v) - T(w) = T(v - w)$$

Exemplo 3.5. Sejam $(\mathbf{A}, \mathbf{V}, \mathbf{T})$ um espaço afim e $x_0 \in \mathbf{A}$ um ponto fixo. Tome a função

$$\begin{aligned} f : \mathbf{A} &\rightarrow \mathbf{V} \\ x &\mapsto x - x_0 \end{aligned}$$

Esta função é afim com $Df = Id_{\mathbf{V}}$.

De fato, sejam $x, y \in \mathbf{A}$

$$\begin{aligned} f(y) - f(x) &= (y - x_0) - (x - x_0) \\ &= (y - x_0) + (x_0 - x) \\ &= (y - x) + (x_0 - x_0) \\ &= (y - x) + 0 \\ &= y - x \\ &= Id_{\mathbf{V}}(y - x) \end{aligned}$$

Proposição 3.3. (Regra da Cadeia) Sejam $f : \mathbf{A}_1 \rightarrow \mathbf{A}_2$ e $g : \mathbf{A}_2 \rightarrow \mathbf{A}_3$ duas transformações afins, então a composta $g \circ f : \mathbf{A}_1 \rightarrow \mathbf{A}_3$ também é uma transformação afim e $D(g \circ f) : Dg \circ Df$.

Demonstração: Seja $x, y \in \mathbf{A}_1$, então temos

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

Logo,

$$\begin{aligned} g \circ f(y) - g \circ f(x) &= g(f(y)) - g(f(x)) \\ &= Dg(f(y) - f(x)) \\ &= Dg(Df(y - x)) \\ &= Dg \circ Df(y - x) \end{aligned}$$

concluindo a demonstração. ■

Proposição 3.4. Sejam $(\mathbf{A}, \mathbf{V}, \mathbf{T})$ e $(\mathbf{B}, \mathbf{W}, \mathbf{S})$ dois espaços afins, e seja $f : \mathbf{A} \rightarrow \mathbf{B}$ uma transformação que é uma função bijetiva. Então:

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

Demonstração:

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

$$\begin{aligned} f(T_v(x)) - f(x) &= Df(T_v(x) - x) \\ &= Df(v) \\ &= 0 \end{aligned}$$

Então $f(T_v(x)) = S_0(f(x)) = f(x)$. Pela injetividade de f , podemos concluir que $T_v(x) = x$, mas como T é uma ação livre, então v deixa algum ponto fixo, e logo, que $v = 0$, portanto Df é uma transformação linear injetiva.

Verifiquemos agora a sobrejetividade. Seja $w \in \mathbf{W}$, fixe $y \in \mathbf{B}$, pela sobrejetividade de f , temos que $y = f(x)$ para algum $x \in \mathbf{A}$, da mesma forma que $T_w(y) = f(z)$ para algum $z \in \mathbf{A}$, assim

$$\begin{aligned} w = T_w(y) - y &= f(z) - f(x) \\ &= Df(z - x) \end{aligned}$$

Assim, Df é uma transformação linear sobrejetora. Concluimos, então que Df é um isomorfismo entre \mathbf{V} e \mathbf{W} .

Vejam agora os itens (2) e (3). Sejam $y_1, y_2 \in \mathbf{B}$, então

$$\begin{aligned} y_2 - y_1 &= f(f^{-1}(y_2)) - f(f^{-1}(y_1)) \\ &= Df(f^{-1}(y_2) - f^{-1}(y_1)) \end{aligned}$$

Mas por outro lado, temos que

$$y_2 - y_1 = Df\left((Df)^{-1}(y_2 - y_1)\right),$$

Das duas informações resulta que

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

E ainda vimos no item (1) que Df é injetiva, o que nos leva a seguinte igualdade

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

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

Definição 3.3. Diremos que $(\mathbf{A}, \mathbf{V}, \mathbf{T})$ e $(\mathbf{B}, \mathbf{W}, \mathbf{S})$ são dois espaços afins isomorfos se existir $f : \mathbf{A} \rightarrow \mathbf{B}$ uma transformação bijetiva entre eles. Esta transformação afim será denominada um isomorfismo de espaços afins.

Teorema 3.1. (Teorema da Reconstrução) Sejam $(\mathbf{A}, \mathbf{V}, \mathbf{T})$ e $(\mathbf{B}, \mathbf{W}, \mathbf{S})$ dois espaços afins. Para todo par de pontos $x \in \mathbf{A}$ e $y \in \mathbf{B}$ e para toda transformação linear $g : \mathbf{V} \rightarrow \mathbf{W}$, existem uma única transformação afim $f : \mathbf{A} \rightarrow \mathbf{B}$ tal que $f(x) = y$ e $Df = g$.

Demonstração: Suponhamos $x \in \mathbf{A}$ e $y \in \mathbf{B}$ e $g : \mathbf{V} \rightarrow \mathbf{W}$ uma transformação linear. Associe para todo $z \in \mathbf{A}$ o elemento

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

Iremos verificar que a aplicação

$$\begin{aligned} f : \mathbf{A} &\rightarrow \mathbf{B} \\ z &\mapsto f(z), \end{aligned}$$

é uma transformação afim e que $Df = g$. De fato, sejam $z, t \in \mathbf{A}$, 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 vamos supor que existe outra transformação afim $F : \mathbf{A} \rightarrow \mathbf{B}$ tal que $F(x) = y$ e $DF = g$, então, tomando qualquer $z \in \mathbf{A}$ temos

$$\begin{aligned}
w = F(z) - y &= F(z) - F(x) \\
&= DF(z-x) \\
&= g(z-x) \\
&= f(z) - f(x) \\
&= f(z) - y
\end{aligned}$$

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

Corolário 3.1. Sejam $(\mathbf{A}, \mathbf{V}, \mathbf{T})$ e $(\mathbf{B}, \mathbf{W}, \mathbf{S})$ dois espaços afins. Duas transformações afins $f_1, f_2 : \mathbf{A} \rightarrow \mathbf{B}$ possuem a mesma derivada se, e somente se, existir um vetor $w \in \mathbf{W}$ tal que $f_2 = S_w \circ f_1$.

Demonstração:

(\Rightarrow) Suponhamos que $Df_1 = Df_2$. Fixemos $x \in \mathbf{A}$, e sejam $y_1 = f_1(x)$ e $y_2 = f_2(x)$. Vamos mostrar que $f_2 = S_w \circ f_1$ onde $w = y_2 - y_1$.

Tome $z \in \mathbf{A}$, existe $v \in \mathbf{V}$ tal que $z = T_v(x)$ então

$$\begin{aligned}
f_2(z) &= f_2(T_v(x)) \\
&= S_{Df_2(v)}f_2(x) \\
&= S_{Df_1(v)}S_{f_2(x)-f_1(x)}(f_1(x)) \\
&= S_{Df_1(v)+w}(f_1(x)) \\
&= S_w(S_{Df_1(v)}f_1(x)) \\
&= S_w(f_1(T_v(x))) \\
&= S_w(f_1(z))
\end{aligned}$$

(\Leftarrow) Se $f_2 = S_w \circ f_1$, então fixamos $x \in \mathbf{A}, \forall v \in \mathbf{V}$

$$\begin{aligned}
Df_2(v) &= Df_2(T_v(x) - x) \\
&= f_2(T_v(x)) - f_2(x) \\
&= S_w(f_1(T_v(x))) - S_w(f_1(x)) \\
&= DS_w(f_1(T_v(x)) - f_1(x)) \\
&= f_1(T_v(x)) - f_1(x) \\
&= Df_1(T_v(x) - x) \\
&= Df_1(v)
\end{aligned}$$

■

O corolário que acabamos de ver nos auxilia na caracterização de uma transformação afim basicamente por uma transformação linear e uma translação. Este fato nos permite escrever uma transformação afim em coordenadas:

Sejam $(\mathbf{A}, \mathbf{V}, \mathbf{T})$ e $(\mathbf{B}, \mathbf{W}, \mathbf{S})$ dois espaços afins, fixe um ponto $a \in \mathbf{A}$ e um ponto $\bar{a} \in \mathbf{B}$ como sendo as respectivas origens de um sistema de coordenadas. Fixemos ainda, uma base $\{e_1, \dots, e_n\}$ em \mathbf{V} e uma base $\{f_1, \dots, f_m\}$ em \mathbf{W} . Desta forma, para qualquer $x \in \mathbf{A}$ temos que

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

Considere agora uma transformação afim $f : \mathbf{A} \rightarrow \mathbf{B}$. Então podemos escrever para qualquer $x \in \mathbf{A}$

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

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

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

Portanto temos que

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

e em coordenadas afins teremos que

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

Ou seja, uma transformação afim, essencialmente, uma transformação linear mais uma translação.

Proposição 3.5. Seja $(\mathbf{A}, \mathbf{V}, \mathbf{T})$ um espaço afim, e $\text{Aff}(\mathbf{A})$ o grupo das transformações afins bijetivas em \mathbf{A} . Então $\text{Aff}(\mathbf{A}) / \mathbf{V} \cong GL(\mathbf{V})$.

Demonstração: Como demonstramos anteriormente, pela regra da cadeia temos que

$$\begin{aligned}
D: \text{Aff}(\mathbf{A}) &\rightarrow GL(\mathbf{V}) \\
f &\mapsto Df
\end{aligned}$$

é um homomorfismo de grupos, e pelo teorema da reconstrução, dado qualquer isomorfismo linear $g \in GL(\mathbf{V})$ é possível construir uma infinidade de transformações afins f tais que $Df = g$, escolhendo um par de pontos $a, b \in \mathbf{A}$ de forma que $f(a) = b$. Podemos afirmar ainda que qualquer uma destas transformações afins assim construídas são bijetivas, ou seja, que $f \in \text{Aff}(\mathbf{A})$. Portanto, D é um epimorfismo. E neste caso o corolário do teorema de homomorfismos de grupos nos afirma que $GL(\mathbf{V}) \cong \text{Aff}(\mathbf{A}) / \ker(D)$. O que nos resta é calcular o kernel do homomorfismo D . Para isto, tomemos $f \in \ker(D)$, ou seja, $Df = Id_{\mathbf{V}}$, fixemos um ponto $a \in \mathbf{A}$ e denotemos por b sua imagem pela função f , isto é, $b = f(a)$. Mostraremos que $f = T_{(b-a)}$, de fato para qualquer $x \in \mathbf{A}$

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

Assim $f(x) = T_{(b-a)}(x)$, e como isso vale para qualquer ponto, então $f = T_{b-a}$. Seguindo o mesmo cálculo feito acima mostra que poderíamos ter iniciado com qualquer ponto $c \in \mathbf{A}$ para definirmos o vetor de

translação, uma vez que $f(c) - c = f(a) - a$. Identificando um vetor $v \in \mathbf{V}$ com sua translação T_v , mostramos com o que foi exposto acima que $\ker(D) \subseteq \mathbf{V}$. Mas por outro lado, vimos que toda translação possui como derivada a função $Id_{\mathbf{V}}$ implicando em $\mathbf{V} \subseteq \ker(D)$. O que prova que $\mathbf{V} = \ker(D)$, e consequentemente $Aff(\mathbf{A}) / \mathbf{V} \cong GL(\mathbf{V})$. ■

Teorema 3.2. Seja $(\mathbf{A}, \mathbf{V}, \mathbf{T})$ um espaço afim, e $Aff(\mathbf{A})$ o grupo das transformações afins bijetivas em \mathbf{A} . Então $Aff(\mathbf{A}) \cong \mathbf{V} \times GL(\mathbf{V})$, onde este grupo é o produto semidireto de \mathbf{V} por $GL(\mathbf{V})$ com a ação de $GL(\mathbf{V})$ sobre \mathbf{V} por transformações lineares.

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

$$\begin{aligned} \Phi: Aff(\mathbf{A}) &\rightarrow \mathbf{V} \times GL(\mathbf{V}) \\ f &\mapsto (v_f, Df) \end{aligned}$$

Verificamos que esta aplicação está bem definida, pois dada uma transformação afim f , sua derivada e o valor do ponto a por f estão unicamente definidos pelo teorema da reconstrução.

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

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

Assim

$$\begin{aligned} \Phi(g \circ f) &= (v_g + Dg(v_f), Dg \circ Df) \\ &= (v_g, Dg) \cdot (v_f, Df) \\ &= \Phi(g) \cdot \Phi(f) \end{aligned}$$

o que significa que Φ é homomorfismo de grupos.

Para mostrarmos a injetividade, seja $f \in \ker(\Phi)$, então $\Phi(f) = (0, Id_{\mathbf{V}})$. Disso, concluímos que $Df = Id_{\mathbf{V}}$. Como vimos anteriormente, existe $v \in \mathbf{V}$ tal que $f = T_v$. Por outro lado, como $v_f = 0$, temos que

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

desta forma, $f = T_0$, ou seja, para qualquer $x \in \mathbf{A}$ tem-se que $f(x) = T_0(x) = x = Id_{\mathbf{A}}(x)$. Portanto $f = Id_{\mathbf{A}}$.

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

CONSIDERAÇÕES FINAIS

Com a contemplação dos conhecimentos básicos dos conceitos de álgebra linear, seguindo pela descrição das noções básicas de Grupos, Subgrupos e Homomorfismo de Grupos, passamos para as Ações de Grupos e suas propriedades, chegando enfim na Geometria Afim. Com isso encerramos nosso estudo e esperamos ter contribuído positivamente para o enriquecimento da compreensão matemática, motivando o leitor a aprofundar seus estudos neste assunto.

REFERÊNCIAS

BATISTA, Elieser. **Ações de Grupos e Geometria**. V Bienal da Sociedade Brasileira de Matemática – Universidade Federal da Paraíba – 18 a 22 de outubro de 2010.

EVES, Howard; tradução: DOMINGUES, Hygino H. **Introdução à História da Matemática**. Campinas, SP: Editora da Unicamp, 2004.

DOMINGUES, Hyguino H. **Álgebra Moderna** - 4ª. ed. reform. – São Paulo, SP: Atual, 2003.

ALVES, Maria Bernardete Martins; ARRUDA, Susana Margareth. **Como fazer referências**: bibliográficas, eletrônicas e demais formas de documento. Florianópolis: Universidade Federal de Santa Catarina, Biblioteca Universitária, c2001. Disponível em: <<http://www.bu.ufsc.br/design/framerefer.php>>. Acesso em: 19 fev. 2010.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 10520**: informação e documentação: citações em documentos: apresentação. Rio de Janeiro, 2002.

DUZHIN, S.V.; CHEBOTAREVSKII, B.D. **Transformation Groups for Beginners**. AMS (2004).

KOSTRIKIN, A.I.; MANIN, Yu. I. **Linear Algebra and Geometry**. CRC Press (1989)

ROTMAN, J.J. **A First Course in Abstract Algebras with Applications**. Person Prentice Hall (2006).

SATTINGER; D.H.; WEAVER, O.L.; **Lie Groups and Algebras with Applications to Physics, Geometry, and Mechanics**. Springer – Verlag (1993).

SPINDLER, K.; **Abstract Algebra with Applications in Two Volumes: Volume I, Vector Spaces and Groups**. Marcel Dekker (1994).