UNIVERSIDADE FEDERAL DE SANTA CATARINA

MAYCON ANTONIO PEREIRA

# AÇÕES DE GRUPOS EM AUTOMORFISMOS DE ANÉIS

Blumenau

2018

**Maycon Antonio Pereira**

# AÇÕES DE GRUPOS EM AUTOMORFISMOS DE ANÉIS

Trabalho de Conclusão de Curso submetido ao Curso de Licenciatura em Matemática da Universidade Federal de Santa Catarina para a obtenção do Grau de Licenciado em Matemática.

**Orientador**: Prof. Dr. Felipe Vieira

Blumenau

2018

Catalogação na fonte pela Biblioteca Universitária da Universidade Federal de Santa Catarina.

Arquivo compilado às 01:31h do dia 27 de junho de 2018.

Maycon Antonio Pereira
Ações de Grupos em Automorfismos de Anéis : / Maycon Antonio Pereira; Orientador, Prof. Dr. Felipe Vieira; , - Blumenau, 01:31, 21 de junho de 2018.
69 p.

Trabalho de Conclusão de Curso - Universidade Federal de Santa Catarina, Departamento de Matemática (MAT), Centro de Blumenau, Curso de Licenciatura em Matemática.

Inclui referências

1. Anéis. 2. Grupos. 3. Ações de grupos. I. Prof. Dr. Felipe Vieira II. III. Curso de Licenciatura em Matemática IV. Ações de Grupos em Automorfismos de Anéis

CDU 02:141:005.7

Maycon Antonio Pereira

**AÇÕES DE GRUPOS EM AUTOMORFISMOS DE ANÉIS**

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de Licenciado em Matemática, e aprovado em sua forma final pelo Curso de Licenciatura em Matemática do Departamento de Matemática (MAT), Centro de Blumenau da Universidade Federal de Santa Catarina.

Blumenau, 21 de junho de 2018.

---

**Prof. Dr. André Vanderlinde da Silva**
Coordenador do Curso de Licenciatura em Matemática

**Banca Examinadora:**

---

**Prof. Dr. Felipe Vieira**
Orientador
Universidade Federal de Santa Catarina – UFSC

---

**Prof. Dr. Bruno Tadeu Costa**
Universidade Federal de Santa Catarina – UFSC

---

**Prof. Dr. Rafael Aleixo de Carvalho**
Universidade Federal de Santa Catarina – UFSC

*Este trabalho é dedicado àqueles que ousam acreditar em seus sonhos, pois para esses, o tempo é apenas um detalhe.*

## AGRADECIMENTOS

Meus principais agradecimentos são para minha família, em especial meus pais, Lino Pereira e Zeli C. Pereira, pessoas de uma sabedoria sem igual, que nunca deixaram de me apoiar. Agradeço pelo amor incondicional em todos os momentos. Às minhas irmãs, Maria e Conceição pela importante parcela de minha educação, sempre com firmeza mas nunca sem amor.

Agradeço também aos meu colegas, Leonardo, Nayara, Eduardo e Edionara, que me acolheram como um irmão. Os momentos que vivemos ficarão para sempre em minha memória.

Não poderia deixar de agradecer àqueles que são responsáveis por minha formação, nossos mestres, sempre tão atenciosos e dispostos a compartilhar todo seu conhecimento conosco. Não seria possível chegar até aqui não fossem esses seres iluminados.

E, por fim, à minha namorada, Ana, pessoa especial que chegou e rapidamente se transformou em meu porto seguro.

*"Ninguém ignora tudo. Ninguém sabe tudo. Todos nós sabemos alguma coisa. Todos nós ignoramos alguma coisa. Por isso aprendemos sempre."*
Paulo Freire

*"A resposta certa não importa nada: o essencial é que as perguntas estejam certas ."*
Mario Quintana

## RESUMO

O objetivo principal deste trabalho foi apresentar as ações de grupos sobre automorfismos de anéis. Inicialmente, fez-se um estudo básico sobre anéis e grupos, com as propriedades principais e alguns exemplos. Apresentou-se principalmente os exemplos que foram explorados no último capítulo, onde apresentou-se as ações. Além de definilas, estudou-se e, através de exemplos e demonstrações de propriedades importantes, desmistificou-se sua importância na matemática. Por fim, fez-se um pequeno estudo sobre a órbita de um elemento.



**Palavras-chaves**: Anéis. Grupos. Ações de grupos.

## ABSTRACT

The main goal of this work is to present group actions over ring automorphisms. Initially, I introduce the basics about rings and groups, the main properties and some examples. I explore some examples which will be used again in the last chapter, where we study the actions. Besides the definitions, we study and show some important properties. To finish, we present and briefly study the orbit of an element.



**Keywords**: Rings. Groups. Group actions.

## LISTA DE TABELAS



## SUMÁRIO

# 1 INTRODUÇÃO

Os conceitos relacionados a grupos estão ligados ao estudo de equações polinomiais, mais especificamente à determinação de raízes dos polinômios com grau igual ou maior que 5, visto que desde Lagrange, as permutações das raízes de um polinômio eram consideradas importantes no intuito de se conseguir um método geral para solução. Galois, além de vários outros resultados, formularia então o conceito de grupo. Anos mais tarde, ainda no século $XIX$, graças aos trabalhos de Sophus Lie, a teoria de grupos se expandiria consideravelmente. O conceito moderno de grupo foi introduzido por Arthur Cayley, mas foi apenas no início do século $XX$, com a contribuição de diversos matemáticos, que a teoria se desenvolveria mais rapidamente. A teoria de grupos têm papel importante no presente trabalho, pois estão ligadas diretamente às ações que foram estudadas.

O objetivo desse trabalho foi estudar as ações de grupos agindo sobre anéis, os quais restringiu-se aos automorfismos desses anéis. Outro ponto importante do trabalho foram as demonstrações feitas passo a passo, buscando proporcionar um melhor entendimento ao leitor. Os exemplos iniciais de ações levaram ao caso geral (teorema 4.3), assim como exemplos de outras naturezas também foram apresentados. Por fim, estudou-se brevemente a órbita de um elemento.

Os Capítulos 2 e 3 tiveram o objetivo de fundamentar as teorias necessárias para o andamento do trabalho. No Capítulo 2 foram mostradas as definições de anéis e subanéis. Foram trazidos exemplos variados e alguns tiveram sua demonstração detalhada, visando fugir de demonstrações com saltos que os estudantes muitas vezes têm dificuldade de entender. Sempre que se utilizar frases do tipo, *"é fácil ver que$\cdots$"*, *"analogamente$\cdots$"*, ou outras similares, estas estarão acompanhadas das demonstrações, tentando facilitar ao máximo a experiência do leitor. O Capítulo 3, a exemplo do que acontece na estrutura do segundo capítulo, traz então as definições e propriedades acerca da teoria dos grupos e subgrupos. Novamente,

exemplos detalhados estão presentes, como o estudo do grupo das matrizes, visto que é utilizado no capítulo seguinte na formação de uma ação. Encerrada esta parte, o básico para o estudo das ações propostas nesse trabalho está posto e pode-se, então, seguir ao capítulo final, foco principal da presente pesquisa.

No Capítulo 4 fez-se uso dos conceitos abordados para introduzir as definições sobre as ações de grupos. Vale lembrar que o conjunto utilizado na definição geral de ação exige apenas um conjunto não vazio. Para esse trabalho, restringiu-se essa definição aos automorfismos de um anel, ou seja, estudar-se-á as ações de grupos agindo sobre automorfismos de anéis. Foram mostrados exemplos e um teorema, generalizando um certo tipo de ação. Já no final do Capítulo, foram estudados os conceitos envolvendo a órbita de um elemento.

Tentar-se-á fornecer, na medida do possível, o máximo de conceitos necessários para o acompanhamento dos temas abordados. Porém, é indicado que haja um conhecimento básico de álgebra e de técnicas de demonstração. Algumas notações foram fixadas, como o caso da unidade dos conjuntos tratados, nesse caso denotada por 1, lembrando que não necessariamente este seja o número 1, mas sim a estrutura que representa a unidade dentro de um determinado conjunto. As ações de grupos foram representadas por letras gregas, elementos de conjuntos por letras minúsculas do alfabeto brasileiro, enquanto os conjuntos foram denotados por letras maiúsculas.

# 2 ANÉIS

## 2.1 DEFINIÇÕES E EXEMPLOS

Um determinado conjunto, quando munido de duas operações e obedecendo algumas propriedades, será denominado anel. Nesta seção serão abordados os conceitos referentes às propriedades citadas, apresentados alguns exemplos e demonstrações de modo a mostrar o funcionamento desta estrutura matemática.(GONÇALVES, 2015)

**Definição 2.1.** Seja $A$, um conjunto não vazio. Sejam definidas em $A$ duas operações, as quais serão chamadas, respectivamente, de *soma* e *produto* em $A$. Denotar-se-á tais operações pelos seus símbolos usuais, $+$ e $\cdot$.

Desta forma, temos:

$$\begin{aligned} + : A \times A &\to A \\ (a, b) &\mapsto a + b \end{aligned}$$

e

$$\begin{aligned} \cdot : A \times A &\to A \\ (a, b) &\mapsto a \cdot b. \end{aligned}$$

Assim, o conjunto $A$ será chamado *anel*, caso as 6 propriedades apresentadas a seguir sejam verificadas, para quaisquer $a, b, c \in A$.

**A1)** Associatividade da soma:

$$(a + b) + c = a + (b + c).$$

**A2)** Elemento neutro da soma (existência):

$$\exists\ 0 \in A, \text{ tal que } a + 0 = 0 + a = a.$$

**A3)** Elemento oposto:

$$\forall\ a \in A \text{ existe } d \in A, \text{ tal que } a + d = d + a = 0.$$

**A4)** Comutatividade da soma:

$$a + b = b + a.$$

**A5)** Associatividade do produto:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

**A6)** Distributividade:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

e

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

Respeitadas tais 6 propriedades, o conjunto já é chamado de *anel*, porém, ainda existem outras 4 propriedades que podem ser verificadas. De acordo com cada uma dessas, os anéis serão classificados com nomenclaturas específicas para cada situação. Na sequência ver-se-á quais são elas.

**A7)** Elemento neutro do produto:

$\exists\ 1 \in A$, onde $0 \neq 1$, tal que $a \cdot 1 = 1 \cdot a = a$, $\forall\ a \in A$. Este 1 é chamado de unidade do anel.

**A8)** Comutatividade do produto:

$$\forall\ a, b \in A,\ a \cdot b = b \cdot a.$$

**A9)** Não existência de divisores de zero:

Se $a, b \in A$ e $a \cdot b = 0$, então ou $a = 0$, ou $b = 0$.

**A10)** Elemento inverso:

$\forall\ a \in A$, com $a \neq 0$, $\exists\ b \in A$ tal que $a \cdot b = b \cdot a = 1$.

*Observação* 1. No caso de valer $A1 - A6$ e $A7$, diz-se que $(A, +, \cdot)$ *é um anel com unidade.*

*Observação* 2. Quando valem $A1 - A6$ e $A8$, chamamos $(A, +, \cdot)$ de *anel comutativo.*

*Observação* 3. Quando valem $A1 - A6$ e $A9$ $(A, +, \cdot)$ *é um anel sem divisores de zero.* Quando as propriedades $A1 - A9$ valem, então o anel $(A, +, \cdot)$ *é um domínio de integridade.*

*Observação* 4. Caso um domínio de integridade satisfaça também $A10$, então $(A, +, \cdot)$ *é um corpo.*

Segundo Domingues e Iezzi (2003), a ideia sobre *corpos* já havia aparecido em trabalhos de Niels Henrik Abel, matemático norueguês por volta de 1820. Porém, essa ideia só seria formalizada com a introdução dos corpos de números de grau finito estudados por Dedekind.

Tanto para o elemento neutro $(A2)$ quanto para o elemento oposto $(A3)$, note-se que são dadas pelas propriedades, as condições de existência. A seguir demonstra-se a unicidade desses elementos.

**Proposição 2.1.** *O elemento neutro do anel é único.*

*Demonstração.* Suponha que $0$ e $\overline{0}$ sejam elementos neutros do anel, então $a + 0 = a$ e $a + \overline{0} = a$. Assim temos que:

$$\begin{aligned}
a + 0 &= a + \overline{0} && \\
-a + (a + 0) &= -a + (a + \overline{0}) && \text{(soma do elemento oposto)} \\
(-a + a) + 0 &= (-a + a) + \overline{0} && \text{(A1)} \\
0 + 0 &= \overline{0} + \overline{0} && \text{(A3)} \\
0 &= \overline{0}. && \text{(A2)}
\end{aligned}$$

Logo, está provada a unicidade do elemento neutro. ■

Quando não houver chances de confusão devido às notações utilizadas, este elemento neutro será denotado por 0.

**Proposição 2.2.** *Dado $a \in A$, o elemento oposto é único.*

*Demonstração.* Seja $a \in A$ e suponha $b$ e $\overline{b}$ elementos opostos de $a$. Se $b$ e $\overline{b}$ são elementos opostos de $a$, então pode-se afirmar que $b + a = 0$ e $a + \overline{b} = 0$. Agora, vejamos:

$$b = b + 0 = b + (a + \overline{b}) = (b + a) + \overline{b} = 0 + \overline{b} = \overline{b}$$

ou seja, conclui-se que $b = \overline{b}$ e provamos que o elemento oposto é único. ■

Denotaremos o elemento oposto de $a \in A$ por $-a$. Dessa implicação resulta imediatamente que vale a Lei do cancelamento da adição, como provado abaixo.

**Proposição 2.3.** *Dados $a, b, c \in A$ tais que $a + b = a + c$, então $b = c$.*

*Demonstração.*

$$\begin{aligned} a + b = a + c &\Rightarrow -a + (a + b) = -a + (a + c) \\ &\Rightarrow (-a + a) + b = (-a + a) + c \\ &\Rightarrow b = c. \end{aligned}$$

■

A seguir, apresentar-se-ão alguns exemplos de anéis, ou seja, conjuntos onde as primeiras propriedades $A1 - A6$ valem. Há exemplos em que outras propriedades também podem ser verificadas e serão devidamente mencionadas, seja pelo número da propriedade em questão ou mesmo pela nomenclatura dada ao anel, naquele caso específico. A maioria dos exemplos apresentaram apenas a notação referente ao anel, ou seja, conjunto e operações. Porém, para auxiliar no entendimento do restante deste documento, haverá exemplificações de como é feita a verificação de cada propriedade, independentemente dela ser válida ou não.

**Exemplo 2.1.1.** Anéis numéricos

Note-se que, para os exemplos a seguir, foram utilizadas as operações usuais de soma e produto.

- Anel dos números inteiros $(\mathbb{Z}, +, \cdot)$;
- Anel dos números racionais $(\mathbb{Q}, +, \cdot)$;
- Anel dos números reais $(\mathbb{R}, +, \cdot)$;
- Anel dos números complexos $(\mathbb{C}, +, \cdot)$.

*Observação* 5. No caso dos anéis acima, esses são todos anéis comutativos.

*Observação* 6. Note-se que $(\mathbb{N}, +, \cdot)$, onde $+, \cdot$ são as operações de soma e produto usuais, não é um anel. Isso deve-se ao fato de todo número positivo não possuir elemento oposto.

**Exemplo 2.1.2.** Anel das classes de resto módulo $n$

Seja $n \in \mathbb{N}$, com $n > 1$. Considere $a \in \mathbb{N}$ e, caso tenha-se $a \geq n$ ou $a < 0$, denota-se $\overline{a} = \overline{r}$, onde $r$ é o resto da divisão euclidiana de $a$ por $n$ (de fato, $0 \leq r < n$). Dessa forma, define-se:

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\},$$

onde as operações são definidas como segue, $\forall \overline{a}, \overline{b} \in \mathbb{Z}_n$:

$$\overline{a} + \overline{b} = \overline{a+b}$$

e

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

*Observação* 7. No caso dos anéis $\mathbb{Z}_n$ é importante observar que o zero deste anel é a classe $\overline{0}$ e o elemento oposto de $\overline{a}$ é a classe $\overline{n-a}$.

Do exemplo 2.1.2 decorre um outro exemplo, no qual não vale a propriedade $A9$, ou seja, o anel irá conter divisores de zero. Vejamos:

**Exemplo 2.1.3.** Anel com divisores de zero

Dado o anel $\mathbb{Z}_8$, munido das operações usuais, vamos verificar a validade da propriedade $A9$.

Observemos que pela notação do exemplo 2.1.2, temos que:

$$\mathbb{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}.$$

Temos então que $\overline{2} \cdot \overline{4} = \overline{8}$, mas $\overline{8} = \overline{0}$, ou seja, em $\mathbb{Z}_8$, $\overline{2}$ e $\overline{4}$ são divisores de zero. Logo não vale a propriedade $A9$ e este não se trata de um domínio de integridade.

**Exemplo 2.1.4.** Anéis de Matrizes

Importante recordar de que no caso dos anéis têm-se sempre duas operações, logo ambas devem satisfazer simultaneamente as propriedades de $A1$ a $A6$. Desta forma, um anel de matrizes precisa conter somente matrizes quadradas de mesma dimensão. Assim, provar-se-á que $M_2(\mathbb{Z})$ é um anel com unidade. Sejam dadas as matrizes

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \qquad \begin{bmatrix} e & f \\ g & h \end{bmatrix}, \qquad \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

e considere as operações usuais de matrizes:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$$

e

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}.$$

**A1)** Associatividade da soma:

$$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix}\right) + \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$
$$= \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$
$$= \begin{bmatrix} a+e+i & b+f+j \\ c+g+k & d+h+l \end{bmatrix};$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix}\right)$$
$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e+i & f+j \\ g+k & h+l \end{bmatrix}$$
$$= \begin{bmatrix} a+e+i & b+f+j \\ c+g+k & d+h+l \end{bmatrix}.$$

Observe-se que nas duas situações chega-se ao mesmo resultado, logo vale a igualdade e $A1$ foi verificada.

**A2)** Existência do elemento neutro em relação à soma:

Provar-se-á que $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ é o elemento neutro da soma:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a+0 & b+0 \\ c+0 & d+0 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix};$$
$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0+a & 0+b \\ 0+c & 0+d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Logo vale $A2$.

**A3)** Existência do elemento oposto aditivo:

Dada $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, segue que $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$ é a matriz oposta:

$$\begin{aligned}\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} &= \begin{bmatrix} a+(-a) & b+(-b) \\ c+(-c) & d+(-d) \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}; \\ \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} &= \begin{bmatrix} -a+a & -b+b \\ -c+c & -d+d \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.\end{aligned}$$

**A4)** Comutatividade da soma:

$$\begin{aligned}\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} &= \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} \\ &= \begin{bmatrix} e+a & f+b \\ g+c & h+d \end{bmatrix} \\ &= \begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}.\end{aligned}$$

**A5)** Associatividade do produto:

$$
\begin{aligned}
&\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix}\right) \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix} \\
&= \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix} \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix} \\
&= \begin{bmatrix} aei+bgi+afk+bhk & aej+bgj+afl+bhl \\ cei+dgi+cfk+dhk & cej+dgj+cfl+dhl \end{bmatrix} \\
&= \begin{bmatrix} aei+afk+bgi+bhk & aej+afl+bgj+bhl \\ cei+cfk+dgi+dhk & cej+cfl+dgj+dhl \end{bmatrix} \\
&= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \left(\begin{bmatrix} ei+fk & ej+fl \\ gi+hk & gj+hl \end{bmatrix}\right) \\
&= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix}\right).
\end{aligned}
$$

**A6)** Distributividade:

$$
\begin{aligned}
&\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix}\right) \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix} \\
&= \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix} \\
&= \begin{bmatrix} (a+e)i+(b+f)k & (a+e)j+(b+f)l \\ (c+g)i+(d+h)k & (c+g)j+(d+h)l \end{bmatrix} \\
&= \begin{bmatrix} ai+ei+bk+fk & aj+ej+bl+fl \\ ci+gi+dk+hk & cj+gj+dl+hl \end{bmatrix};
\end{aligned}
$$

$$
\begin{aligned}
&\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix}\right) + \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix}\right) \\
&= \begin{bmatrix} ai+bk & aj+bl \\ ci+dk & cj+dl \end{bmatrix} + \begin{bmatrix} ei+fk & ej+fl \\ gi+hk & gj+hl \end{bmatrix} \\
&= \begin{bmatrix} ai+ei+bk+fk & aj+ej+bl+fl \\ ci+gi+dk+hk & cj+gj+dl+hl \end{bmatrix}.
\end{aligned}
$$

Dessa forma, provou-se a distributividade à esquerda. Analogamente, prova-se a distributividade à direita.

**A7)** Existência do elemento neutro em relação ao produto:

Provar-se-á que $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ é o elemento neutro do produto:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a+0 & 0+b \\ c+0 & 0+d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix};$$
$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a+0 & b+0 \\ 0+c & 0+d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Logo vale $A7$. Assim, $(M_2(\mathbb{Z}), +, \cdot)$ é um anel com unidade.

Pode-se generalizar o resultado acima e provar-se que, dado qualquer $n \in \mathbb{N}^*$, $(M_n(\mathbb{Z}), +, \cdot)$ é um anel com unidade.

Outro fato significativo com demonstração análoga, é que se o conjunto $A$ é um anel, independentemente de quais sejam os seus elementos, é possível obter-se um anel $(M_n(A), +, \cdot)$, $\forall\ n \geq 1$, como sendo o anel das matrizes de ordem $n \times n$ sobre $A$, também com as operações usuais. Assim sendo, seguem alguns exemplos de anéis de matrizes:

- $(M_n(\mathbb{Q}), +, \cdot)$ (anel das matrizes com coeficientes racionais);
- $(M_n(\mathbb{R}), +, \cdot)$ (anel das matrizes com coeficientes reais);
- $(M_n(\mathbb{C}), +, \cdot)$ (anel das matrizes com coeficientes complexos);
- $(M_n(\mathbb{Z}_3), +, \cdot)$ (anel das matrizes com coeficientes sendo as classes de $\mathbb{Z}_3$).

**Exemplo 2.1.5.** Anéis de Funções

No exemplo a seguir foram detalhadas as verificações de cada propriedade. Para tal, tornou-se necessário que as operações envolvidas fossem devidamente definidas, assim como a notação utilizada para nomear as funções.

Seja $A = \mathscr{F}(\mathbb{R})$ o conjunto de todas as funções $f : \mathbb{R} \to \mathbb{R}$. Sejam $f, g, h \in A$ e estejam definidas as seguintes operações:

$$\begin{aligned} + : A \times A &\to A \\ (f, g) &\mapsto f + g \quad \text{onde} \quad (f+g)(x) = f(x) + g(x) \end{aligned}$$

e ainda

$$\begin{aligned} \cdot : A \times A &\to A \\ (f, g) &\mapsto f \cdot g \quad \text{onde} \quad (f \cdot g)(x) = f(x) \cdot g(x). \end{aligned}$$

Agora, testar-se-á todas as propriedades da Definição 2.1, seguindo a mesma numeração dada anteriormente.

**A1)** Associatividade da soma:

Seja $x \in \mathbb{R}$:

$$\begin{aligned} [(f+g)+h](x) &= (f+g)(x) + h(x) \\ &= (f(x) + g(x)) + h(x) \\ &= f(x) + (g(x) + h(x)). \end{aligned}$$

Note que na equação acima é utilizada a associatividade de $\mathbb{R}$. Por outro lado, temos que:

$$\begin{aligned} [f+(g+h)](x) &= f(x) + (g+h)(x) \\ &= f(x) + (g(x) + h(x)). \end{aligned}$$

Observe-se que em ambas as situações chega-se ao mesmo resultado, logo vale a igualdade e $A1$) foi verificada.

**A2)** Existência do elemento neutro em relação à soma:

Seja a seguinte função constante:

$$\begin{aligned} 0 : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto 0. \end{aligned}$$

Assim, $\forall x \in \mathbb{R}$,

$$\begin{aligned}(f+0)(x) &= f(x)+0(x)\\ &= f(x)+0\\ &= f(x).\end{aligned}$$

Analogamente, mostra-se que $(0+f)(x) = f(x)$, logo vale a segunda propriedade.

**A3)** Existência do elemento oposto aditivo:

Quer-se provar neste caso, que $\forall\ f \in A$, $\exists\ -f \in A$, em que $f+(-f) = (-f)+f = 0$. Então vejamos:

Seja $f \in A$. Defina $(-f)(x) = -f(x)$. Então, $\forall\ x \in \mathbb{R}$, temos:

$$\begin{aligned}(f+(-f))(x) &= f(x)+(-f(x))\\ &= f(x)-f(x)\\ &= 0\\ &= 0(x).\end{aligned}$$

Analogamente, por meio da comutatividade da soma, a qual ver-se-á na próxima propriedade, é simples demonstrar que $(-f+f)(x) = 0(x)$.

**A4)** Comutatividade da soma:

Temos que $\forall\ x \in \mathbb{R}$ o seguinte ocorre:

$$\begin{aligned}(f+g)(x) &= f(x)+g(x)\\ &= g(x)+f(x)\\ &= (g+f)(x)\end{aligned}$$

pois a adição é comutativa em $\mathbb{R}$.

**A5)** Associatividade do produto:

Seja $x \in \mathbb{R}$:

$$\begin{aligned}[(f \cdot g) \cdot h](x) &= (f \cdot g)(x) \cdot h(x) \\ &= (f(x) \cdot g(x)) \cdot h(x) \\ &= f(x) \cdot (g(x) \cdot h(x))\end{aligned}$$

por outro lado, temos que:

$$\begin{aligned}[f \cdot (g \cdot h)](x) &= f(x) \cdot (g \cdot h)(x) \\ &= f(x) \cdot (g(x) \cdot h(x)).\end{aligned}$$

**A6)** Distributividade:

$f \cdot (g + h) = f \cdot g + f \cdot h$ (Distributividade à esquerda)
Dado um $x \in \mathbb{R}$, temos que:

$$\begin{aligned}[f \cdot (g + h)](x) &= f(x) \cdot [(g + h)(x)] \\ &= f(x) \cdot [g(x) + h(x)] \\ &= f(x) \cdot g(x) + f(x) \cdot h(x).\end{aligned}$$

Analogamente:

$(f + g) \cdot h = f \cdot h + g \cdot h$ (Distributividade à direita)
Dado um $x \in \mathbb{R}$, temos que:

$$\begin{aligned}[(f + g) \cdot h)](x) &= [(f + g)(x)] \cdot h(x) \\ &= [f(x) + g(x)] \cdot h(x) \\ &= f(x) \cdot h(x) + g(x) \cdot h(x).\end{aligned}$$

Como valem as seis primeiras propriedades, pode-se afirmar que o conjunto das funções sobre $\mathbb{R}$, com as operações definidas acima, forma um anel. Logo em seguida foram verificadas as demais propriedades.

**A7)** Existência do elemento neutro em relação ao produto:

Considere-se a função constante $g(x) = 1$, $\forall x \in \mathbb{R}$. De fato, $g(x) \neq 0$ e, $\forall\ x \in \mathbb{R}$:

$$\begin{aligned}(f \cdot g)(x) &= f(x) \cdot g(x) \\ &= f(x) \cdot 1 \\ &= f(x).\end{aligned}$$

Mostra-se de modo análogo que $g \cdot f = f$.

**A8)** Comutatividade do produto:

Dado $x \in \mathbb{R}$:

$$\begin{aligned}(f \cdot g)(x) &= f(x) \cdot g(x) \\ &= g(x) \cdot f(x) \\ &= (g \cdot f)(x).\end{aligned}$$

**A9)** Divisores de zero:

Seja uma função $f : \mathbb{R} \to \mathbb{R}$ definida da seguinte maneira:

$$f(x) = \begin{cases} 0, & se \quad x < 0 \\ x, & se \quad x \geq 0 \end{cases}$$

e $g : \mathbb{R} \to \mathbb{R}$:

$$g(x) = \begin{cases} x^2, & se \quad x < 0 \\ 0, & se \quad x \geq 0. \end{cases}$$

Nota-se que $f \neq 0$ e $g \neq 0$, onde 0 é o elemento neutro em relação à adição, definido em $A2$). Porém $f \cdot g = 0$, ou seja, o anel das funções possui divisores de zero e não é, portanto, um domínio de integridade, pois não vale $A9$).

**A10)** Inverso multiplicativo.

Nesse caso, para que a propriedade fosse verdadeira, seria necessário que todas as funções admitissem inversa, o que não é

verdade. Uma função inversível não pode anular-se e no anel em questão têm-se infinitas funções que não satisfazem essa necessidade. Por exemplo, seja $f(x) = x - 2$. Para qualquer outra função $g(x)$, a função $(f \cdot g)(x)$ anular-se-á em $x = 2$. Ou seja, será diferente de 1, que é o elemento neutro do produto. Sendo assim, a décima e última propriedade a ser verificada não vale para as funções.

Levando em conta que as primeiras 8 propriedades foram verificadas como verdadeiras, diz-se que $A = \mathscr{F}(\mathbb{R})$ é um **anel comutativo com unidade**.

## 2.2 SUBANÉIS

**Definição 2.2.** Sejam $(A, +, \cdot)$ um anel e $B$ um subconjunto não vazio de $A$. Suponha que $B$ seja fechado para as operações de soma e produto $(+, \cdot)$ de $A$, ou seja:

1. $a, b \in B \Rightarrow a + b \in B$;
2. $a, b \in B \Rightarrow a \cdot b \in B$.

Caso isso ocorra, então consideramos que $(+, \cdot)$ são operações também de $B$. Então, se $B$ for um anel com essas operações, dizemos que $B$ é subanel de $A$.

**Proposição 2.4.** *Seja $A, +, \cdot$ um anel e seja $B$ um subconjunto de $A$. Então $B$ é um subanel de $A$ se e somente se as três seguintes condições são verificadas:*

**SA1)** $0 \in B$ *(o elemento neutro de $A$ pertence a $B$);*

**SA2)** $a, b \in B \Rightarrow a - b \in B$ *($B$ é fechado pela diferença);*

**SA3)** $a, b \in B \Rightarrow a \cdot b \in B$ *($B$ é fechado pelo produto).*

*Demonstração.* ($\Rightarrow$) Seja $B$ um subanel de $A$, então vamos provar que se cumprem as condições $SA1$, $SA2$ e $SA3$:

**SA1)** Note que o elemento neutro de $B$, o qual denotaremos por $\overline{0}$ é o mesmo elemento neutro presente em $A$, neste caso o 0. Isso porque, se $b \in B$, temos que $b \in A$ e, portanto:

$$\overline{0} = b + (-b) = 0.$$

Daí, podemos concluir que $\overline{0} = 0 \in B$.

**SA2)** $a, b \in B \Rightarrow -b \in B$, pois é subanel. Como é fechado pela soma, segue que

$$a - b = a + (-b) \in B.$$

**SA3)** $B$ subanel implica em ser fechado pelo produto.

($\Leftarrow$) Agora, suponha $B \subset A$ e que $SA1$, $SA2$ e $SA3$ sejam satisfeitas.

De ($SA1$), temos que $B \neq \emptyset$, pois tem pelo menos o elemento neutro de $A$.

Também, note que, pelo item $SA2$:

$$a \in B \Rightarrow -a = 0 - a \in B. \tag{2.1}$$

Por $SA2$ e pela equação 2.1 temos que, se $a, b \in B$, então $a + b = a - (-b) \in B$, ou seja, $B$ é fechado para a soma. Por $SA3$) temos que $B$ é fechado pelo produto. O fato de $B$ ser subconjunto de $A$ implica diretamente na herança das propriedades relacionadas às operações, isto é, associatividade, comutatividade e distributividade.

Segue que, de fato, $B$ é subanel de $A$.

■

Quando $B$ for subanel de $A$, denotaremos:

$$B \leq A.$$

A seguir, alguns exemplos de subanéis.

**Exemplo 2.2.1.** Vamos provar que

$$\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Z}\}$$

é subanel de $\mathbb{R}$, onde $p$ é um número primo, com $p \geq 2$, provando $SA1$, $SA2$ e $SA3$ (Proposição 2.4).

Note que o elemento neutro do conjunto é denotado por $0 + 0\sqrt{p} = 0$, que é o mesmo de $A$. Logo, vale $SA1$.

Agora tome $x = a + b\sqrt{p}$ e $y = c + d\sqrt{p}$ em $\mathbb{Z}[\sqrt{p}]$.

$$x - y = (a + b\sqrt{p}) - (c + d\sqrt{p}) = (a - c) + (b - d)\sqrt{p} \in \mathbb{Z}[\sqrt{p}].$$

$$x \cdot y = (a + b\sqrt{p}) \cdot (c + d\sqrt{p}) = (ac + pdb) + (bc + ad)\sqrt{p} \in \mathbb{Z}[\sqrt{p}].$$

Note que as duas equações acima verificam $SA2$ e $SA3$. Anteriormente já havia sido verificada também a primeira dessas, assim $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Z}\}$ é um subanel de $\mathbb{R}$.

**Exemplo 2.2.2.** Seja $A = M_2(\mathbb{R})$, o conjunto das matrizes $2\times2$ com coeficientes reais e seja $B = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in \mathbb{R} \right\}$. Assim definidos esses dois conjuntos, é possível afirmar que $B \leq A$, pela Proposição 2.4.

De fato, neste caso, quando $a = 0 \in \mathbb{R}$, temos a matriz nula, $0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, ou seja, o elemento neutro de $A$ pertence a $B$. Facilmente verifica-se que $B$ é fechado para a diferença e para o produto como apresentado abaixo. Para tal, note que $a - b$ e $a \cdot b$, com $a, b \in \mathbb{R}$, também estarão no conjunto dos reais:

$$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a - b & 0 \\ 0 & 0 \end{bmatrix}$$

e ainda,

$$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a \cdot b & 0 \\ 0 & 0 \end{bmatrix}.$$

*Observação* 8. É importante observar que apesar do elemento neutro ser o mesmo para $A$ e $B$, isso não ocorre para a unidade dos conjuntos. Note que no caso do conjunto $A$, $1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ e no conjunto $B$, temos que $\overline{1} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. Mais ainda, $1 \notin B$.

Entre outros exemplos que poderiam ser citados estão:

**a)** $n\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C} \leq \mathbb{H}$, com $n \in \mathbb{N}$, $n \geq 1$;

**b)** $n\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Z}[\sqrt{p}] \leq \mathbb{Q}[\sqrt{p}] \leq \mathbb{R}$, com $n \in \mathbb{N}$, $n \geq 1$ e $p$ um número primo positivo.

*Observação* 9. O anel $(\mathbb{H}, +, \cdot)$, é chamado de anel dos Quaternios, e é assim definido:

$$\mathbb{R}^4 = \{(a, b, c, d) : a, b, c, d \in \mathbb{R}\}, \text{ onde}$$

$$(a, b, c, d) = (a', b', c', d') \Leftrightarrow a = a', b = b', c = c' \text{ e } d = d'.$$

Vamos definir as operações de soma e produto em $\mathbb{H}$:

soma:

$$(a, b, c, d) + (a', b', c', d') = (a + a', b + b', c + c', d + d');$$

produto:

$$(a, b, c, d) \cdot (a', b', c', d') = (aa' - bb' - cc' - dd', ab' + ba' + cd' - c'd, ac' + a'c + db' - d'b, ad' + da' + bc' - b'c).$$

Veja as seguintes identificações:

$$a \leftrightarrow (a, 0, 0, 0)$$
$$i \leftrightarrow (0, 1, 0, 0)$$
$$j \leftrightarrow (0, 0, 1, 0)$$
$$k \leftrightarrow (0, 0, 0, 1).$$

Com essas identificações pode-se visualizar $\mathbb{H}$ como o conjunto:

$$\{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}.$$

# 3 GRUPOS

## 3.1 DEFINIÇÕES

**Definição 3.1.** Seja um conjunto $G \neq \emptyset$ e uma operação denotada por $*$, assim definida:

$$\begin{aligned} * : G \times G &\to G \\ (f, g) &\mapsto f * g. \end{aligned}$$

O conjunto $(G, *)$ será dito **grupo** quando as seguintes propriedades forem válidas para quaisquer $f, g, h \in G$:

**G1)** Associatividade:

$f * (g * h) = (f * g) * h$.

**G2)** Elemento neutro:

$\exists\ e \in G$ tal que $f * e = e * f = f$.

**G3)** Inverso:

$\forall\ f \in G, \exists\ k \in G$ tal que $f * k = k * f = e$.

Como supracitado, quando essas 3 propriedades são válidas, então $(G, *)$ é um grupo. Há ainda uma quarta propriedade que pode ser verificada, isso quando as anteriores valerem e já se tiver a garantia que trata-se de um grupo. Tal propriedade adicional consiste no seguinte:

**G4)** Comutatividade:

$f * g = g * f, \forall\ f, g \in G$.

**Definição 3.2.** Quando a propriedade $G4$ é válida, diz-se que $(G, *)$ é um **grupo abeliano**.

Esse nome foi dado como uma homenagem ao matemático norueguês Niels Henrik Abel (1802 – 1829).

**Proposição 3.1.** *Seja $(G, *)$ um grupo. Então a identidade de $(G, *)$ é única.*

*Demonstração.* Suponha $e, \overline{e} \in G$ elementos neutros em relação à operação de $G$. Assim, temos que:

$$e = e * \overline{e} = \overline{e}.$$

Logo, a identidade é única, como querer-se-ia demonstrar. ■

**Proposição 3.2.** *Seja $(G, *)$ um grupo. Então o elemento inverso é único.*

*Demonstração.* Sejam $g, h_1, h_2$ elementos do grupo e suponha $h_1$ e $h_2$ inversos de $g$ em relação à operação. Então, temos que:

$$g * h_1 = h_1 * g = e$$

e

$$g * h_2 = h_2 * g = e.$$

Daí segue que:

$$h_1 = e * h_1 = (h_2 * g) * h_1 = h_2 * (g * h_1) = h_2 * e = h_2. \quad (3.1)$$

Da equação 3.1 concluímos que $h_1 = h_2$ e portanto, o inverso é único. ■

*Observação* 10. Visto que é único, denotaremos o inverso de $f$ por $f^{-1}$.

## 3.2 GRUPOS IMPORTANTES E EXEMPLOS

Se em um grupo $(G, *)$ o conjunto $G$ for finito, então esse será denominado *grupo finito*. Quando isso ocorre, é dado o nome de *ordem* do grupo ao número de elementos do mesmo. A ordem de um grupo é denotada por $|G|$.

O matemático Arthur Cayley (1821-1899) introduziu, ainda, uma outra forma de representação para os grupos, a tábua da operação $*$, chamada de *tábua do grupo*.

**Exemplo 3.2.1.** Tábua do grupo.

Seja $H = \{-1, 0, 1\}$ um grupo, onde a operação é o produto usual herdado de $\mathbb{Z}$. A quantidade de elementos de $H$ é 3, logo a ordem de $H$ é 3. A tábua desse grupo é a seguinte:

Tabela 3.1 – Tábua da operação de $H$.

| $*$ | $\mathbf{0}$ | $\mathbf{1}$ | $\mathbf{-1}$ |
|---|---|---|---|
| $\mathbf{0}$ | 0 | 0 | 0 |
| $\mathbf{1}$ | 0 | 1 | $-1$ |
| $\mathbf{-1}$ | 0 | $-1$ | 1 |

Assim como no capítulo anterior, foram mostrados exemplos, com a verificação completa das propriedades em um destes. Quando a operação não for usual, será devidamente definida em cada exemplo.

**Exemplo 3.2.2.** $\mathbb{Z}, +$ (Grupo aditivo dos inteiros).

Este grupo é formado pelo conjunto dos inteiros munido da adição usual. Veja que a adição no conjunto dos inteiros é associativa e comutativa. O número 0 é seu elemento neutro e mais: $\forall\ f \in \mathbb{Z}$, $\exists\ -f \in \mathbb{Z}$, tal que $f + (-f) = -f + f = 0$, ou seja, existe o inverso em relação à operação. Trata-se então de um grupo abeliano (DOMINGUES; IEZZI, 2003).

**Exemplo 3.2.3.** Se $n \geq 1$ for um número inteiro, então o conjunto $\mathbb{Z}_n$ (inteiros módulo $n$) é um grupo aditivo finito e contém exatamente $n$ elementos.

**Exemplo 3.2.4.** $\mathbb{Q}, +$ (Grupo aditivo dos racionais).

Este grupo é formado pelo conjunto dos números racionais com a soma usual. Assim como no exemplo 3.2.2, pode-se mostrar que valem as propriedades necessárias para que seja de fato um grupo. Logo, como esse grupo é comutativo trata-se também de um grupo abeliano.

**Exemplo 3.2.5.** $\mathbb{R}, +$ (Grupo aditivo dos reais).

O conjunto dos números reais com a operação de adição usual é também, pelo mesmo motivo apresentado no exemplo 3.2.2, um grupo abeliano.

**Exemplo 3.2.6.** $\mathbb{C}, +$ (Grupo aditivo dos complexos).

Sejam dois números complexos, $z = a + bi$ e $w = c + di$. A soma desses números é dada por $z + w = (a + b) + (c + d)i$. É simples verificar que vale a associatividade dessa operação. O conjunto possui também um elemento neutro, definido como $0 = 0 + 0i$. Pode-se ainda mostrar que para todo complexo $z = a + bi$, $-z = (-a) + (-b)i$ é seu oposto. Sendo assim, o conjunto dos complexos com a operação de soma usual é um grupo. Como a operação de soma dos complexos envolve a soma de números reais e, essa é comutativa, segue que a operação em $\mathbb{C}$ também é comutativa. Assim, o grupo é abeliano.

**Exemplo 3.2.7.** Grupo das Permutações do conjunto $S$.

Seja $S$ um conjunto, tal que $S \neq \emptyset$ e $G$ assim definido:

$$G = \{f : S \to S : f \text{ bijetiva}\}.$$

Defina a operação $*$ como sendo a composição de funções:

$$\begin{aligned} * : G \times G &\to G \\ (g, f) &\mapsto g \circ f. \end{aligned}$$

Então, segundo Gonçalves (2015) $G$ é claramente um grupo e sua identidade é a seguinte:

$$\begin{aligned} I_s : S &\to S \\ f &\mapsto f. \end{aligned}$$

Tal grupo é denominado **grupo das permutações do conjunto** $S$. Se o conjunto $S$ for da forma $S = \{1, 2, \cdots, n\}$, o grupo será denotado por $S_n$.

Até aqui todos os exemplos foram de grupos abelianos. No próximo exemplo ver-se-á que os grupos $S_n$, $n \geq 3$ são exemplos de grupos não abelianos.

**Exemplo 3.2.8.** Sejam $f, g \in S_n$, $n \geq 3$, definidas da seguinte maneira:

$$f : \{1, 2, 3, \cdots, n\} \to \{1, 2, 3, \cdots, n\}$$

$$f(1) = 2,\ f(2) = 1,\ f(x) = x,\ 3 \leq x \leq n;$$

$$g : \{1, 2, 3, \cdots, n\} \to \{1, 2, 3, \cdots, n\}$$

$$g(1) = 2,\ g(2) = 3,\ g(3) = 1 \text{ e se } n \geq 4,\ g(x) = x,\ 4 \leq x \leq n.$$

Então vejamos:

$$\begin{aligned} (g \circ f)(1) &= g(f(1)) = g(2) = 3 \\ (f \circ g)(1) &= f(g(1)) = f(2) = 1. \end{aligned}$$

Observe que $g \circ f \neq f \circ g$, ou seja, $S_n$ é um exemplo de grupo não abeliano, visto que não é comutativo. A notação utilizada para os elementos do grupo $S_n$ é dada da seguinte forma:

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}.$$

Observe que, em particular, $S_3$ tem exatos 6 elementos:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e^{-1}$$

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_1^{-1}$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_2^{-1}$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_3^{-1}$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_5^{-1}$$

$$f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_4^{-1}.$$

**Exemplo 3.2.9.** Matrizes inversíveis.

Seja $GL_2(\mathbb{R})$ o conjunto de todas as matrizes inversíveis $2\times2$, ou seja,

$$GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} : det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq 0 \right\}.$$

Agora, esteja definida a operação produto $\cdot$ no conjunto $GL_2(\mathbb{R})$ acima. Nesse caso, a operação vai ser fixada como o produto usual entre matrizes. A seguir mostrar-se-á que, de fato, $GL_2(\mathbb{R})$ é um **grupo**.

Sejam as seguintes matrizes genéricas:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \qquad \begin{bmatrix} e & f \\ g & h \end{bmatrix}, \qquad \begin{bmatrix} i & j \\ k & l \end{bmatrix}.$$

Para verificar a associatividade da operação é preciso mostrar que

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \left( \begin{bmatrix} e & f \\ g & h \end{bmatrix} \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix} \right) \tag{3.2}$$

e

$$\left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix} \tag{3.3}$$

são iguais.

Para facilitar a visualização de cada passo, os lados esquerdo e direito da igualdade acima apresentada foram trabalhados separadamente. Primeiramente foi calculado o lado esquerdo e depois o direito, para somente após serem comparados, a fim de verificar a validade da propriedade.

$$\begin{aligned} &\left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix} \\ &= \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix} \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix} \\ &= \begin{bmatrix} a(ei+fk)+b(gi+hk) & a(ej+fl)+b(gj+hl) \\ c(ei+fk)+d(gi+hk) & c(ej+fl)+d(gj+hl) \end{bmatrix}. \end{aligned} \tag{3.4}$$

Vejamos agora o lado direito da equação:

$$\begin{aligned} &\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \left( \begin{bmatrix} e & f \\ g & h \end{bmatrix} \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix} \right) \\ &= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} ei+fk & ej+fl \\ gi+hk & gj+hl \end{bmatrix} \\ &= \begin{bmatrix} i(ae+bg)+k(af+bh) & j(ae+bg)+l(af+bh) \\ i(ce+dg)+k(cf+dh) & j(ce+dg)+l(cf+dh) \end{bmatrix}. \end{aligned} \tag{3.5}$$

Veja que as entradas dessas matrizes são números reais, ou seja, vale a associatividade e a comutatividade do produto e da soma entre os elementos, então, comparando as equações 3.4 e 3.5,

pode-se concluir que os termos correspondentes são iguais, o que implica nas matrizes serem iguais. Mas se tais resultados são idênticos, conclui-se que vale a associatividade da operação no conjunto $GL_2(\mathbb{R})$.

Verifcar-se-á, na sequência, a existência do elemento neutro. Seja a matriz identidade de ordem 2, $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, então temos:

$$\begin{aligned} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} a+0 & 0+b \\ c+0 & 0+d \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ c & d \end{bmatrix}; \end{aligned} \tag{3.6}$$

$$\begin{aligned} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} &= \begin{bmatrix} a+0 & b+0 \\ 0+c & 0+d \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ c & d \end{bmatrix}. \end{aligned} \tag{3.7}$$

Logo, vale a propriedade 2.

A propriedade 3 é trivial, visto que o conjunto escolhido contém todas as matrizes inversíveis, logo para toda matriz em $G$, sua inversa também estará no conjunto.

Sendo assim, pode-se concluir que, de fato, $GL_2(\mathbb{R})$ é um grupo.

Resta ainda saber se esse grupo é abeliano. Note que, para um grupo ser abeliano a operação precisa ser comutativa, o que não é o caso. Veja abaixo um contraexemplo:

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}. \tag{3.8}$$

Por outro lado:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}. \tag{3.9}$$

Note que o resultado da equação 3.8 é diferente do resultado da equação 3.9, ou seja, a operação não é comutativa e, portanto, o grupo não é abeliano.

Para definir ações de grupos, precisa-se definir o grupo de automorfismos de um dado anel. Para isso, apresenta-se a seguir a definição de homomorfismo.

**Definição 3.3.** Seja $(A, +, \cdot)$ um anel. Então uma função $f : A \to A$ é um homomorfismo se preserva a estrutura de $A$, ou seja:

$$\forall\ a, b \in A,\ f(a + b) = f(a) + f(b) \text{ e } f(a \cdot b) = f(a) \cdot f(b).$$

**Exemplo 3.2.10.** Seja $(A, +, \cdot)$ um anel. Defina

$$Aut(A) = \{f : A \to A : f \text{ é homomorfismo bijetor}\}.$$

Vamos provar que $Aut(A)$ é um grupo com a operação $\circ$:

$$\begin{aligned} \circ : Aut(A) \times Aut(A) &\to Aut(A) \\ (f, g) &\to f \circ g. \end{aligned}$$

Sejam $f, g$ e $h \in Aut(A)$ e $x \in A$. Primeiramente, provar-se-á que a operação está bem definida. Note que a composição de funções injetoras, é injetora:

$$(f \circ g)(x) = (f \circ g)(y) \Rightarrow f(g(x)) = f(g(y)) \Rightarrow g(x) = g(y) \Rightarrow x = y.$$

A composição de funções sobrejetoras, é sobrejetora. Tome $x \in A$. Como $f$ é sobrejetora, existe $y \in A$ tal que $f(y) = x$. Agora, como $g$ é sobrejetora, existe $z \in A$ tal que $g(z) = y$. Assim:

$$(f \circ g)(z) = f(g(z)) = f(y) = x.$$

Por fim, a composição de homomorfismos, é um homomorfismo. Sejam $x, y \in A$:

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

e

$$\begin{aligned}(f \circ g)(x \cdot y) &= f(g(x \cdot y)) = f(g(x) \cdot g(y)) = f(g(x)) \cdot f(g(y)) \\ &= (f \circ g)(x) \cdot (f \circ g)(y).\end{aligned}$$

Logo, a operação está bem definida. Agora, provar-se-á que, de fato, $(Aut(A), \circ)$ é um grupo.

**G1)** Aplicando as funções em um ponto temos:

$$\begin{aligned}[f \circ (g \circ h)](x) &= f((g \circ h)(x)) \\ &= f(g(h(x)))\end{aligned}$$

por outro lado:

$$\begin{aligned}[(f \circ g) \circ h)](x) &= (f \circ g)(h(x)) \\ &= f(g(h(x))).\end{aligned}$$

Portanto $(f \circ g) \circ h = f \circ (g \circ h)$ e então vale $G1$.

**G2)** Seja $e(x) = x$ a função identidade. Nesse caso têm-se o seguinte:

$$\begin{aligned}(f \circ e)(x) &= f(e(x)) \\ &= f(x)\end{aligned}$$

e ainda:

$$\begin{aligned}(e \circ f)(x) &= e(f(x)) \\ &= f(x).\end{aligned}$$

Assim, concluímos que vale $G2$ e que a função identidade é o elemento neutro de $Aut(A)$.

**G3)** Neste ponto, é importante observar que estar-se-á tratando de automorfismos, ou seja, as funções desse conjunto são bijetoras e portanto admitem inversa na composição. Assim, pode-se afirmar que $\forall\ f \in Aut(A)$, $\exists\ f^{-1} \in Aut(A)$, tal que, $\forall x \in A$,

$$\begin{aligned}(f \circ f^{-1})(x) &= f(f^{-1}(x)) \\ &= e(x).\end{aligned}$$

Note que $f^{-1} : A \to A$ também é um homomorfismo.

De fato, sejam $x, y \in A$. Como $f$ é bijetora, $\exists\ a, b \in A$ tal que $f(a) = x$ e $f(b) = y$. Logo:

$$\begin{aligned}f^{-1}(x+y) &= f^{-1}(f(a)+f(b)) \\ &= f^{-1}(f(a+b)) \\ &= a+b \\ &= f^{-1}(x)+f^{-1}(y).\end{aligned}$$

Também:

$$\begin{aligned}f^{-1}(x \cdot y) &= f^{-1}(f(a) \cdot f(b)) \\ &= f^{-1}(f(a \cdot b)) \\ &= a \cdot b \\ &= f^{-1}(x) \cdot f^{-1}(y).\end{aligned}$$

Desta forma vale $G3$.

Prova-se, então, que, $(Aut(A), \circ)$ é um grupo. Note que a composição de funções nem sempre é comutativa, portanto, esse grupo nem sempre é abeliano.

## 3.3 SUBGRUPOS

Sejam $G$ um grupo e $H$ um subconjunto de $G$, tal que $H \neq \emptyset$. $H$ será dito *subgrupo* de $G$ se ele próprio for um grupo com a mesma

operação de $G$. Então, além de satisfazer $G1, G2$ e $G3$, $H$ tem que ser fechado pela operação. Para que tal fato ocorra é preciso que se verifiquem algumas condições, as quais são apresentadas a seguir.

**Proposição 3.3.** *Seja $(G, *)$ um grupo e $H$ um subconjunto de $G$. Então, são equivalentes as condições a seguir:*

**SG1)** *$H$ é um subgrupo de $G$.*

**SG2)** *(i) $e \in H$;*
*(ii) $\forall\ x, y \in H \Rightarrow x \cdot y \in H$;*
*(iii) $\forall\ x \in H \Rightarrow x^{-1} \in H$.*

**SG3)** *$H \neq \emptyset$ e $\forall\ x, y \in H$ temos que $x \cdot y^{-1} \in H$.*

*Demonstração.* $SG1 \Rightarrow SG2$: Essa implicação segue imediatamente do fato de $H$ ser um grupo e da unicidade da identidade e do inverso dos elementos de $G$.

$SG2 \Rightarrow SG1$: Pela condição $(ii)$ de $SG2$ pode-se afirmar que $H$ é fechado para a operação de $G$, ou seja, a operação de $H$ tem por herança as propriedades da operação de $G$ e será, portanto, associativa. Além disso, $(i)$ implica $SG2$ e $(iii)$ implica $SG3$.

$SG2 \Rightarrow SG3$: Observe-se que $e \in H$ e então $H \neq \emptyset$ e ainda, de $(iii)$, temos que $y \in H$ implica que $y^{-1} \in H$.

Dessa forma, sempre que $x, y \in H$, $x, y^{-1} \in H$. Então, por $(ii)$, segue que $x \cdot y^{-1} \in H$ como era o objetivo demonstrar.

$SG3 \Rightarrow SG2$: Por hipótese, $H \neq \emptyset$, logo $\exists\ x \in H$. Então é possível concluir que $e = x \cdot x^{-1} \in H$. Além disso, se $x \in H$, então $x^{-1} = e \cdot x^{-1} \in H$. Por fim, $x, y \in H$ implica $x, y^{-1} \in H$ e, portanto, $x \cdot y = x \cdot (y^{-1})^{-1} \in H$, ou seja, está concluída a demonstração da Proposição 3.3. ■

**Exemplo 3.3.1.** Sejam $H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n \subseteq H_{n+1} \subseteq \cdots$, uma quantidade infinita de subgrupos de um grupo $G$, com unidade $e$. Então,

$$H = \bigcup_{i=1}^{\infty} H_i$$

é um subgrupo de $G$.

Provar-se-á que $H$ satisfaz $SG3$. Note que $e \in H$, pois $e \in H_i \subset H$. Logo $H$ é não vazio.

Sejam $x, y \in H$. Assim, $x \in H_i$ e $y \in H_j$, onde os índices $i, j$ estão em $\{1, 2, \cdots, n, \cdots\}$. Assim, pode-se assumir, sem perda de generalidade que $i \leq j$ e daí ter-se-á $x, y \in H_j$, pois $H_i \subseteq H_j$.

Com isso, têm-se que $x \cdot y^{-1} \in H_j$ (pelo item $(ii)$ de SG2). Como $H_j \subset H$, prova-se que a união de subgrupos de um grupo é também um subgrupo desse mesmo grupo.

# 4 AÇÕES DE GRUPOS

## 4.1 DEFINIÇÕES

A definição de ação de grupo varia dependendo sobre qual tipo de conjunto o grupo age. Por exemplo, se um grupo age sobre um espaço topológico, exige-se que a ação seja feita através de funções contínuas. No presente trabalho, os grupos analisados agem sobre anéis e, por isso, a ação se dá através de automorfismos de anéis.

**Definição 4.1.** Uma ação de um grupo $(G, *)$, com unidade $e$, em um anel $(A, +, \cdot)$ é uma aplicação:

$$\begin{aligned} \alpha : G &\to Aut(A) \\ g &\mapsto \alpha_g, \end{aligned}$$

onde

$$\begin{aligned} \alpha_g : A &\to A \\ a &\mapsto \alpha_g(a), \end{aligned}$$

satisfazendo as propriedades abaixo:

**P1)** $\alpha_g(\alpha_h(a)) = \alpha_{gh}(a)$, $\forall\ g, h \in G$ e $a \in A$;

**P2)** $\alpha_e = Id_A$, ou seja, $\alpha_e(a) = a$, $\forall\ a \in A$.

Essa definição, na verdade, diz como uma ação funciona na prática, ou seja, que os grupos agem sobre certos conjuntos, modificando seus elementos de lugar. Existe mais de uma notação para as ações de grupos, porém, para evitar confundir o leitor, utilizar-se-á apenas a notação acima apresentada.

Muitas das teorias as quais deram suporte a este documento mencionam, sem qualquer demonstração uma terceira propriedade,

que é na verdade, uma implicação das duas primeiras. Para muitos que estiverem começando a estudar ações essa implicação pode não ser tão óbvia. Para que tal fato não ocorra aqui, demonstrar-se-á essa implicação a seguir.

**Proposição 4.1.** *Se $(G, *)$ é um grupo agindo em um anel $(A, +, \cdot)$, então, para todo $g \in G$, $(\alpha_g)^{-1} = \alpha_{g^{-1}}$.*

*Demonstração.* Seja $a \in A$. Vejamos primeiramente a seguinte igualdade:

$$\begin{aligned} \alpha_{g^{-1}} \circ \alpha_g(a) &= \alpha_{g^{-1}}(\alpha_g(a)) \\ &= \alpha_{g^{-1}g}(a) \\ &= \alpha_e(a) \\ &= a. \end{aligned} \tag{4.1}$$

Por outro lado temos:

$$\begin{aligned} \alpha_g \circ \alpha_{g^{-1}}(a) &= \alpha_g(\alpha_{g^{-1}}(a)) \\ &= \alpha_{gg^{-1}}(a) \\ &= \alpha_e(a) \\ &= a. \end{aligned} \tag{4.2}$$

Na segunda linha de ambas as equações foi utilizada $P1$, assim como no passo seguinte das equações pode-se ver claramente a identidade do conjunto $G$, ou seja, trata-se de $P2$. Assim podemos concluir que $(\alpha_g)^{-1} = \alpha_g^{-1}$. ■

Note que os grupos, neste caso, agem via automorfismos sobre um dado anel. Logo, $\forall\ g \in G$, $\alpha_g$ deve ser um homomorfismo bijetor.

**Proposição 4.2.** *Seja $\alpha$ uma ação do grupo $G$ sobre um domínio de integridade $A$, com unidade $1$. Então, $\forall\ g \in G$, $\alpha_g(1) = 1$.*

*Demonstração.* Dado $a \in A$ com $a \neq 0$ e $g \in G$:

$$\alpha_g(a) = \alpha_g(a \cdot 1) = \alpha_g(a) \cdot \alpha_g(1).$$

Logo,

$$\alpha_g(a) \cdot (1 - \alpha_g(1)) = 0 \Rightarrow \alpha_g(a) = 0 \text{ ou } 1 - \alpha_g(1) = 0.$$

Porém, $\alpha_g(a) \neq 0$, pois $\alpha_g$ é bijetora. Portanto

$$1 - \alpha_g(1) = 0 \Rightarrow \alpha_g(1) = 1.$$

■

## 4.2 EXEMPLOS

Ver-se-á a princípio dois exemplos desse tipo de ação de grupo.

**Exemplo 4.2.1.** Sejam $G$ um grupo, $A$ um anel e defina

$$\alpha : G \to Aut(A)$$
$$g \mapsto \alpha_g$$

onde $\alpha_g(a) = a$, $\forall\ g \in G$.

É simples notar que $\alpha_g$ é bijetora, $\forall\ g \in G$.

Note que, $\forall a \in A$ e $\forall g, h \in G$, $\alpha_g(\alpha_h(a)) = \alpha_g(a) = a$ e $\alpha_{gh}(a) = a$. Mais ainda, é fácil ver que $\alpha_e(a) = a$. Logo, $P1$ e $P2$ valem.

Como $\alpha_g$ é um homomorfismo, têm-se que:

$$\alpha_g(a + b) = a + b = \alpha_g(a) + \alpha_g(b)$$

e

$$\alpha_g(a \cdot b) = a \cdot b = \alpha_g(a) \cdot \alpha_g(b).$$

Essa ação é chamada de ação trivial.

**Exemplo 4.2.2.** Sejam $G$ o grupo aditivo $\mathbb{Z}_2$, onde $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ e

$A = \mathbb{C}$. Defina:

$$\begin{aligned} \alpha : G &\to Aut(A) \\ \overline{0} &\mapsto \alpha_{\overline{0}} \\ \overline{1} &\mapsto \alpha_{\overline{1}} \end{aligned}$$

onde temos:

$$\begin{aligned} \alpha_{\overline{0}}(a+bi) &= a+bi \\ \alpha_{\overline{1}}(a+bi) &= a-bi. \end{aligned}$$

Nesse exemplo, diferentemente dos demais, não é possível generalizar a verificação das propriedades em um único caso, logo, será necessário verificar as propriedades para todas as combinações possíveis de $\alpha$.

Primeiramente, ver-se-á se $\alpha$ está bem definida.

Sejam $z_1 = a + bi$ e $z_2 = c + di$:

$$\begin{aligned} \alpha_{\overline{0}}(z_1 + z_2) &= \alpha_{\overline{0}}(a+bi+c+di) \\ &= \alpha_{\overline{0}}[(a+c)+(b+d)i] \\ &= [(a+c)+(b+d)i] \\ &= a+c+bi+di \\ &= a+bi+c+di \\ &= \alpha_{\overline{0}}(z_1) + \alpha_{\overline{0}}(z_2); \end{aligned}$$

$$\begin{aligned} \alpha_{\overline{1}}(z_1 + z_2) &= \alpha_{\overline{1}}(a+bi+c+di) \\ &= \alpha_{\overline{1}}[(a+c)+(b+d)i] \\ &= [(a+c)-(b+d)i] \\ &= a+c-bi-di \\ &= a-bi+c-di \\ &= \alpha_{\overline{1}}(z_1) + \alpha_{\overline{1}}(z_2). \end{aligned}$$

Agora, é importante lembrar de que nos números complexos, $i^2 = -1$.

$$\begin{aligned}
\alpha_{\overline{0}}(z_1 \cdot z_2) &= \alpha_{\overline{0}}[(a+bi)\cdot(c+di)] \\
&= \alpha_{\overline{0}}[(ac-bd)+(ad+bc)i] \\
&= (ac-bd)+(ad+bc)i \\
&= (a+bi)\cdot(d+di) \\
&= \alpha_{\overline{0}}(z_1)\cdot\alpha_{\overline{0}}(z_2);
\end{aligned}$$

$$\begin{aligned}
\alpha_{\overline{1}}(z_1 \cdot z_2) &= \alpha_{\overline{1}}[(a+bi)\cdot(c+di)] \\
&= \alpha_{\overline{1}}[(ac-bd)+(ad+bc)i] \\
&= [(ac-bd)-(ad+bc)i] \\
&= ac-bd-adi-bci \\
&= ac-adi-bci-bd \\
&= \alpha_{\overline{1}}(z_1)\cdot\alpha_{\overline{1}}(z_2).
\end{aligned}$$

Dessa forma, $\alpha$ é homomorfismo, resta verificar se $\alpha$ é de fato bijetora:

**Injetora.**

$$\begin{aligned}
\alpha_{\overline{0}}(z_1) = \alpha_{\overline{0}}(z_2) &\Rightarrow (a+bi) = (c+di) \\
&\Rightarrow a = c \quad \text{e} \quad b = d \\
&\Rightarrow z_1 = z_2.
\end{aligned}$$

De modo análogo, é possível mostrar que $\alpha_{\overline{1}}$ também é injetora.

**Sobrejetora.** Para $\alpha_{\overline{0}}$ é trivial. Para $\alpha_{\overline{1}}$, dado $n = a + bi$, basta tomar $m = a - bi$. Logo $\alpha_{\overline{1}}(m) = \alpha_{\overline{1}}(a-bi) = a + bi = n$.

**P1)** $(i)$

$$\begin{aligned}
\alpha_{\overline{0}}(\alpha_{\overline{1}}(a+bi)) &= \alpha_{\overline{0}}(a-bi) = a-bi \\
&= \alpha_{\overline{1}}(a+bi) = \alpha_{\overline{0}+\overline{1}}(a+bi);
\end{aligned}$$

$(ii)$

$$\begin{aligned}\alpha_{\overline{1}}(\alpha_{\overline{0}}(a+bi)) &= \alpha_{\overline{1}}(a+bi)\\ &= \alpha_{\overline{1}+\overline{0}}(a+bi);\end{aligned}$$

$(iii)$

$$\begin{aligned}\alpha_{\overline{0}}(\alpha_{\overline{0}}(a+bi)) &= \alpha_{\overline{0}}(a+bi)\\ &= \alpha_{\overline{0}+\overline{0}}(a+bi);\end{aligned}$$

$(iv)$

$$\begin{aligned}\alpha_{\overline{1}}(\alpha_{\overline{1}}(a+bi)) = \alpha_{\overline{1}}(a-bi) &= a+bi\\ = \alpha_{\overline{0}}(a+bi) &= \alpha_{\overline{1}+\overline{1}}(a+bi).\end{aligned}$$

Assim, vale $P1$.

**P2)** Note que, nesse caso, $e = \overline{0}$, ou seja:

$$\alpha_e(a+bi) = \alpha_{\overline{0}}(a+bi) = a+bi.$$

Portanto, $P2$ vale.

Mostrou-se, então, que a aplicação $\alpha$ definida nesse exemplo trata-se de uma ação do grupo $\mathbb{Z}_2$ sobre os automorfismos do anel dos números complexos.

**Exemplo 4.2.3.** Seja $G = (GL_2(\mathbb{C}), \cdot)$ o grupo das matrizes inversíveis $2 \times 2$ com coeficientes pertencentes ao conjunto dos números complexos. Esteja definido $A = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{C} \right\}$ como o conjunto das matrizes de ordem 2 com coeficientes complexos.

Esta ação será assim definida:

$$\begin{aligned}\alpha : G &\to Aut(A)\\ g &\mapsto \alpha_g,\end{aligned}$$

onde

$$\begin{aligned} \alpha_g : A &\to A \\ n &\mapsto gng^{-1}. \end{aligned}$$

Novamente, é preciso verificar se $\alpha$ está bem definida. Em seguida, ver-se-á se, de fato, $\alpha$ é homomorfismo.

$$\begin{aligned} \alpha_g(a+b) &= g(a+b)g^{-1} \\ &= (ga+gb)g^{-1} \\ &= gag^{-1}+gbg^{-1} \\ &= \alpha_g(a)+\alpha_g(b). \end{aligned}$$

Agora, comparar-se-á as seguintes equações, onde a operação $\cdot$ é a mesma do anel.

$$\alpha_g(ab) = g(ab)g^{-1};$$

$$\begin{aligned} \alpha_g(a)\cdot\alpha_g(b) &= gag^{-1}\cdot gbg^{-1} \\ &= g(ab)g^{-1}. \end{aligned}$$

Como $\alpha_g(a)\cdot\alpha_g(b) = \alpha_g(ab)$, mostrou-se que $\alpha$ é homomorfismo.

Note que, dado $g \in G$, $\alpha_g$ é bijeção:

**Injetora**

$$\begin{aligned} \alpha_g(n) = \alpha_g(m) &\Rightarrow gng^{-1} = gmg^{-1} \\ &\Rightarrow g^{-1}(gng^{-1})g = g^{-1}(gmg^{-1})g \\ &\Rightarrow n = m. \end{aligned}$$

**Sobrejetora** Dado $m \in A$, tome $n = g^{-1}mg$. Logo, $\alpha_g(n) = m$.

**P1)**

$$\begin{aligned} \alpha_g(\alpha_h(a)) &= \alpha_g(hah^{-1}) \\ &= g(hah^{-1})g^{-1} \\ &= (gh)a(gh)^{-1} \\ &= \alpha_{gh}(a). \end{aligned}$$

Portanto, a primeira propriedade é válida.

**P2)** Para $P2$, denote $e = Id_2$, ou seja, a matriz identidade $2 \times 2$. Note ainda, que por definição, a matriz inversa de uma matriz identidade é a própria identidade. Como a operação é o produto, temos que a identidade multiplicada por uma matriz resulta na própria matriz, assim vale a propriedade $P2$. Algebricamente, têm-se:

$$\begin{aligned} \alpha_e(a) &= eae^{-1} \\ &= ae^{-1} \\ &= a. \end{aligned}$$

Dessa forma, mostrou-se que a ação atende às propriedades necessárias. Observe-se que o exemplo anterior é um caso particular da teoria.

**Teorema 4.3.** *Seja $(G, \cdot)$ um grupo e $(A, +, \cdot)$ um anel, tais que $G \subset A$. Suponha que a operação de $G$ seja a operação produto de $A$. Então:*

$$\begin{aligned} \tau : G &\to Aut(A) \\ g &\mapsto \tau_g, \end{aligned}$$

*onde*

$$\begin{aligned} \tau_g : A &\to A \\ a &\mapsto gag^{-1} \end{aligned}$$

*é uma ação de grupo.*

*Demonstração.* Primeiramente, veja que $\tau$ está bem definida.

Note que, $\forall\ g \in G$, e $a, b \in A$,

$$\begin{aligned} \tau_g(a+b) &= g(a+b)g^{-1} \\ &= gag^{-1} + gbg^{-1} \\ &= \tau_g(a) + \tau_g(b). \end{aligned}$$

$$\begin{aligned} \tau_g(a \cdot b) &= g(a \cdot b)g^{-1} \\ &= gag^{-1} \cdot gbg^{-1} \\ &= \tau_g(a) \cdot \tau_g(b). \end{aligned}$$

**Injetora:** $\tau_g(a) = \tau_g(b) \Rightarrow gag^{-1} = gbg^{-1} \Rightarrow ga = gb \Rightarrow a = b.$

**Sobrejetora:** Para um elemento $a \in A$, $\exists\ b \in A$ tal que $\tau_g(b) = a$, basta tomar $b = g^{-1}ag$. Assim, temos que:

$$\tau_g(b) = \tau_g(g^{-1}ag) = g(g^{-1}ag)g^{-1} = (gg^{-1})a(gg^{-1}) = a.$$

Agora, provar-se-á que $\tau$ é de fato uma ação do grupo $G$ agindo sobre o anel $A$.

**P1)**

$$\begin{aligned} \tau_g(\tau_h(a)) &= \tau_g(hah^{-1}) \\ &= ghah^{-1}g^{-1} \\ &= \tau_{gh}(a). \end{aligned}$$

**P2)**

$$\begin{aligned} \tau_e(a) &= eae^{-1} \\ &= ae^{-1} \\ &= a. \end{aligned}$$

Logo $\tau$ é uma ação de $G$ sobre $A$.

Logo, vale o Teorema 4.3, como querer-se-ia demonstrar. ■

**Exemplo 4.2.4.** Defina o grupo $G = (S_3, \circ)$ e o anel

$$A = (\mathbb{R}[x_1, x_2, x_3], +, \cdot),$$

como o anel de polinômios de três variáveis com soma e produtos usuais de polinômios. Dado $a \in A$, sua forma canônica é:

$$a = \sum_{i_1, i_2, i_3 = 0}^{m} a_{i_1, i_2, i_3} x_1^{i_1} x_2^{i_2} x_3^{i_3},$$

para $a_{i_1, i_2, i_3} \in \mathbb{R}$.

Agora, denote $f \in S_3$ por:

$$\begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}.$$

Definir-se-á, então:

$$\begin{aligned} \lambda : S_3 &\to Aut(A) \\ f &\mapsto \lambda_f, \end{aligned} \tag{4.3}$$

tal que

$$\lambda_f(a) = \sum_{i_1, i_2, i_3 = 0}^{m} a_{i_1, i_2, i_3} x_{f(1)}^{i_1} x_{f(2)}^{i_2} x_{f(3)}^{i_3}.$$

Para uma notação mais simples, denotar-se-á $i_1, i_2, i_3$ apenas por $i$. Também, 0 e $m$ representam o vetor com 3 entradas iguais a 0 e $m$, respectivamente.

Provar-se-á que a aplicação definida na equação 4.3 é, de fato, uma ação do grupo $S_3$ agindo sobre o anel de polinômios acima definido. Verificar-se-á, então, se $\lambda$ está bem definida.

Note que, dados dois elementos na forma genérica acima, pode-se supor, sem perda de generalidade, que o conjunto de índices é igual (se não for, basta completar com termos da forma $0x_1^{i_1} x_2^{i_2} x_3^{i_3}$

colocando $a_i = 0$).

$$\begin{aligned}
\lambda_f(a+b) &= \lambda_f\left[\left(\sum_{i=0}^{m} a_i x_1^{i_1} x_2^{i_2} x_3^{i_3}\right) + \left(\sum_{i=0}^{m} b_i x_1^{i_1} x_2^{i_2} x_3^{i_3}\right)\right] \\
&= \lambda_f\left(\sum_{i=0}^{m} (a_i + b_i) x_1^{i_1} x_2^{i_2} x_3^{i_3}\right) \\
&= \sum_{i=0}^{m} (a_i + b_i) x_{f(1)}^{i_1} x_{f(2)}^{i_2} x_{f(3)}^{i_3} \\
&= \sum_{i=0}^{m} a_i x_{f(1)}^{i_1} x_{f(2)}^{i_2} x_{f(3)}^{i_3} + \sum_{i=0}^{m} b_i x_{f(1)}^{i_1} x_{f(2)}^{i_2} x_{f(3)}^{i_3} \\
&= \lambda_f(a) + \lambda_f(b).
\end{aligned}$$

Como $a, b \in A$, pode-se separar a operação, como fez-se acima, pois são números reais. Analogamente, para o produto têm-se.

$$\begin{aligned}
\lambda_f(a \cdot b) &= \lambda_f\left[\left(\sum_{i=0}^{m} a_i x_1^{i_1} x_2^{i_2} x_3^{i_3}\right) \cdot \left(\sum_{j=0}^{m} b_j x_1^{j_1} x_2^{j_2} x_3^{j_3}\right)\right] \\
&= \lambda_f\left(\sum_{i,j=0}^{m} a_i b_j x_1^{i_1+j_1} x_2^{i_2+j_2} x_3^{i_3+j_3}\right) \\
&= \sum_{i,j=0}^{m} a_i b_j x_{f(1)}^{i_1+j_1} x_{f(2)}^{i_2+j_2} x_{f(3)}^{i_3+j_3} \\
&= \sum_{i=0}^{m} a_i x_{f(1)}^{i_1} x_{f(2)}^{i_2} x_{f(3)}^{i_3} \cdot \sum_{j=0}^{m} b_j x_{f(1)}^{j_1} x_{f(2)}^{j_2} x_{f(3)}^{j_3} \\
&= \lambda_f(a) \cdot \lambda_f(b).
\end{aligned}$$

**Injetora.**

$$\begin{aligned}
&\lambda_f(a) = \lambda_f(b) \\
&\Rightarrow \sum_{i=0}^{m} a_i x_{f(1)}^{i_1} x_{f(2)}^{i_2} x_{f(3)}^{i_3} = \sum_{i=0}^{m} b_i x_{f(1)}^{i_1} x_{f(2)}^{i_2} x_{f(3)}^{i_3} \\
&\Rightarrow a_i = b_i \\
&\Rightarrow a = b.
\end{aligned}$$

**Sobrejetora.** Dado $\sum_{i=0}^{m} a_i x_1^{i_1} x_2^{i_2} x_3^{i_3}$, basta notar que

$$\lambda_f \left( \sum_{i=0}^{m} a_i x_{f^{-1}(1)}^{i_1} x_{f^{-1}(2)}^{i_2} x_{f^{-1}(3)}^{i_3} \right) = \sum_{i=0}^{m} a_i x_1^{i_1} x_2^{i_2} x_3^{i_3}.$$

**P1)**

$$\begin{aligned} \lambda_f(\lambda_g(a)) &= \lambda_f \left( \sum_{i=0}^{m} a_i x_{g(1)}^{i_1} x_{g(2)}^{i_2} x_{g(3)}^{i_3} \right) \\ &= \sum_{i=0}^{m} a_i x_{f\circ g(1)}^{i_1} x_{f\circ g(2)}^{i_2} x_{f\circ g(3)}^{i_3} \\ &= \lambda_{f\circ g}(a). \end{aligned}$$

**P2)**

$$\begin{aligned} \lambda_e(a) &= \sum_{i=0}^{m} a_i x_{e(1)}^{i_1} x_{e(2)}^{i_2} x_{e(3)}^{i_3} \\ &= \sum_{i=0}^{m} a_i x_1^{i_1} x_2^{i_2} x_3^{i_3} \\ &= a. \end{aligned}$$

Dessa forma, provou-se que $P1$ e $P2$ valem.

Logo, conclui-se que $\lambda$ é uma ação do grupo $S3$ sobre os automorfismos do anel de polinômios em três variáveis, como querer-se-ia demonstrar.

## 4.3 A ÓRBITA DE UM ELEMENTO DO ANEL

**Definição 4.2.** Seja $\alpha$ uma ação do grupo $G$ sobre um anel não vazio $A$. A órbita de um elemento $a \in A$ é definida pelo seguinte conjunto:

$$\mathcal{O}_a = \{\alpha_g(a) | g \in G\}.$$

**Exemplo 4.3.1.** Dada a ação do Exemplo 4.2.4, a órbita de um elemento genérico é dada pelo seguinte conjunto:

$$\mathscr{O}_a = \left\{ \sum_{i=0}^{m} a_i x_{f(1)}^{i_1} x_{f(2)}^{i_2} x_{f(3)}^{i_3} | f \in S_3 \right\}.$$

Agora, dado um elemento $a = x_1 - 2x_2 + 5x_2x_3^2 \in A$, vamos mostrar sua órbita.

$$\begin{aligned}\mathscr{O}_a = \{ & x_1 - 2x_2 + 5x_2x_3^2, x_2 - 2x_1 + 5x_1x_3^2, x_1 - 2x_3 + 5x_3x_2^2, \\ & x_3 - 2x_2 + 5x_2x_1^2, x_2 - 2x_3 + 5x_3x_1^2, x_3 - 2x_1 + 5x_1x_2^2 \}.\end{aligned}$$

# 5 CONSIDERAÇÕES FINAIS

O desenvolvimento do presente trabalho possibilitou um estudo acerca das ações de grupos, não só em sua definição básica, como buscou restringir tal definição para determinados conjuntos, neste caso, os automorfismos de anéis. Foi possível ao longo do processo não só aprofundar o estudo das ações, como também explorar os exemplos de anéis e grupos, trazendo demonstrações detalhadas, que visaram contribuir os estudo de futuros estudantes na introdução do tema. Além disso, foi possível, ainda, aprofundar-se em teorias que não faziam parte da graduação, indo além do que já havia sido estudado.

Ao estudar as ações, com as restrições de definição já colocadas, foi possível verificar que assim como ocorre em outras teorias matemáticas, quanto maior o número de restrições postas, maior a dificuldade em se encontrar exemplos relevantes. Ainda assim, com a demonstração do Teorema 4.3, foi criada uma maneira de obter-se infinitos exemplos de ações, além de outros exemplos apresentados.

No geral, os objetivos foram alcançados com o estudo e aprofundamento das noções envolvendo as ações de grupos, análise e demonstração de exemplos de natureza diversificada. Obviamente, o estudo de ações vai muito além do que aqui foi apresentado. Esse trabalho buscou introduzir os principais conceitos e estudá-los com uma visão restrita ao que foi mencionado anteriormente. E é assim que, ao fazer esse estudo, abordamos outros conceitos, proporcionando ao leitor uma visão geral sobre anéis, grupos e ações.

## BIBLIOGRAFIA


ANDRETTI, Cinthia Marques Vieira. *Ações de Grupos e contagem*: Teorema de Burnside. Fev. 2011. Tese (Mestrado) – Universidade Federal de Santa Catarina, Florianópolis. Nenhuma citação no texto.

BATISTA, Eliezer Batista. Ações de grupos e geometria. *V Bienal da SBM*, v. 1, n. 1, 2010. Nenhuma citação no texto.

DOMINGUES, Hygino H.; IEZZI, Gelson. *Álgebra Moderna*. 4. ed. São Paulo: Saraiva, 2003. Citado 2 vezes nas páginas 21, 41.

GONÇALVES, Adilson. *Introdução à álgebra*. 5. ed. Rio de Janeiro: IMPA, 2015. Citado 2 vezes nas páginas 19, 43.

LANG, Serge. *Álgebra para graduação*. 2. ed. Rio de Janeiro: Ciência Moderna, 2008. Nenhuma citação no texto.

LIMA, Elon Lages. *Álgebra Linear*. 8. ed. Rio de Janeiro: IMPA, 2009. Nenhuma citação no texto.

MORANDI, Patrick J. Morandi. Group Actions. v. 1, n. 1, 2013. Nenhuma citação no texto.

MOURA FONSECA, Daila Silva Seabra de. *Grupos e seus automorfismos*. Jun. 2008. Tese (Mestrado) – Universidade Federal de Minas Gerais, Belo Horizonte. Nenhuma citação no texto.