UNIVERSIDADE FEDERAL DE SANTA CATARINA

FERNANDA GONÇALVES AMARO

ANÉIS DE GRUPO

Blumenau

2019

Fernanda Gonçalves Amaro

ANÉIS DE GRUPO

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

Orientador: Prof. Dr. Felipe Vieira

Blumenau

2019

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

Arquivo compilado às 09h02 do dia 16 de dezembro de 2019.

Fernanda Gonçalves Amaro
Anéis de grupo : / Fernanda Gonçalves Amaro; Orientador, Prof. Dr. Felipe Vieira; , - Blumenau, , 16 de dezembro de 2019.
79 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. Anel. 2. Grupo. 3. Anel de grupo. 4. Isomorfismos. I. Prof. Dr. Felipe Vieira II. Curso de Licenciatura em Matemática III. Anéis de grupo

CDU 02:141:005.7

Fernanda Gonçalves Amaro

ANÉIS DE GRUPO

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de Licenciada 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, 16 de dezembro de 2019.

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. Eleomar Cardoso Júnior
Universidade Federal de Santa Catarina – UFSC

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

Este trabalho é dedicado a todos os estudantes de matemática que pesquisam sobre as teorias de anéis e grupos e não encontram o que precisam.

AGRADECIMENTOS

Primeiramente, gostaria de agradecer à minha mãe Sandra da Silva que é um ser iluminado, pois me apoiou nos estudos e na vida a sempre fazer o que me agradaria. Também agradeço ao meu pai Edemar Amaro, que da sua maneira de ser pai, também foi meu pilar durante os quatro anos e meio de graduação.

Agradeço imensamente aos professores e colegas da universidade que me ajudaram a seguir em frente nos estudos e na profissão. Com eles, enfrentei reprovações, e independente disso, manti-me regular no curso. Em especial, agradeço aos professores Felipe Vieira e Eleomar Cardoso Júnior, que estiveram ao meu lado desde o início do curso.

"Sorte é estar pronto quando a oportunidade vem."
Oprah Winfrey

RESUMO

O objetivo deste trabalho é apresentar e demonstrar propriedades de uma teoria aprofundada envolvendo anéis e grupos, chamada anéis de grupo. Para desenvolver essa teoria, foi necessário estudar em dois capítulos as definições, propriedades e exemplos de anéis e de grupos e então utilizar essa premissa para demonstrar no terceiro capítulo as proposições abordando o tema principal. Além disso, vamos estudar o problema do isomorfismo de anéis de grupo, famoso problema que ainda não foi solucionado completamente.

Palavras-chaves: Anel. Grupo. Anel de grupo. Isomorfismos.

ABSTRACT

The goal of this work is to show and to prove properties of a deeper theory about groups and rings, known as group ring. To develop this theory, it was necessary to study some definitions, properties and examples of ring and groups, and it was made in two chapters. It was used to prove the propositions about the main theme on the third chapter. We also briefly study the isomorphism problem of group rings, a famous problem that has no solution yet.

Keywords: Ring. Group. Group ring. Isomorphisms.

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos números naturais.
$\mathbb{Z}$	Conjunto dos números inteiros.
$\mathbb{Q}$	Conjunto dos números racionais.
$\mathbb{R}$	Conjunto dos números reais.
$\mathbb{C}$	Conjunto dos números complexos.
$(A, +, \cdot)$	Conjunto A munido com as operações $+$ e $\times$.
$(G, *)$	Conjunto G munido da operação $*$.
$A \leq B$	O anel A é subanel de B.
$G \leq H$	O grupo G é subgrupo de H.
$A \lhd B$	O subanel A é ideal do anel B.
$\sum_{i=1}^{n} a_i$	Soma dos a_i, onde i varia entre os números naturais, a partir de 1 até n, ou seja, tem-se que $\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n$.

SUMÁRIO

1 INTRODUÇÃO

O conteúdo do presente trabalho está relacionado à álgebra abstrata, abordando a teoria de anéis e teoria de grupos para ter como objetivo, o estudo de anéis de grupo. O objetivo geral desse trabalho é mostrar que é possível construir um anel a partir de um anel e de um grupo e também, provar que se dois anéis e dois grupos são isomorfos respectivamente, então os anéis de grupo também serão.

No Capítulo 2, está definido o que é um anel. Ali, estão exemplificados os conjuntos já conhecidos e vistos na educação básica, que são os conjuntos numéricos. Provadas as suas estruturas sob as operações de soma e produto, pode-se concluir que são anéis, anéis comutativos, com unidade e sem divisores de zero, ou até mesmo ser um corpo. Contudo, também estão provadas algumas proposições e teoremas que são de extrema importância nessa teoria. É um capítulo longo porém bastante objetivo, pois para compreender a definição de anel de grupo, é requisitado um conhecimento aprofundado sobre anel.

No Capítulo 3, está definido o que é um grupo. Assim como no segundo, estão provadas algumas proposições importantes. Para uma melhor visualização da validade de tais proposições presentes no capítulo, mostra-se exemplos, como o grupo linear ou o importante grupo de funções bijetoras.

O estudo de anéis e de grupos é imprescindível para o aprimoramento e conhecimento das propriedades algébricas que serão necessárias no Capítulo 4, no qual são apresentadas demonstrações de importantes resultados acerca de anéis de grupo.

Pelo fato deste assunto ser pouco conhecido dentre os matemáticos e estudantes/amadores dela, não há um grande número de trabalhos sobre anéis de grupo em português. Portanto, uma das motivações para a produção deste trabalho é que estudantes brasileiros possam pesquisar sobre o assunto e encontrar um material completo com demonstrações objetivas e detalhadas em

seu idioma. Em meio a tudo isso, esta obra oferece ao leitor a capacidade de desenvolver novas habilidades e conhecimentos no âmbito da álgebra. É uma oportunidade para quem o lê, obter um apreço por anéis de grupo.

2 ANÉIS

2.1 ANÉIS

Definição 2.1. Seja A um conjunto não vazio com duas operações:

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

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

Então, $(A, +, \cdot)$ é anel se, $\forall\ a, b, c \in A$, valem as seguintes propriedades:

1. Associatividade na soma:
   $(a + b) + c = a + (b + c)$;
2. Comutatividade na soma:
   $a + b = b + a$;
3. Existência do elemento neutro:
   $\exists\ 0 \in A : a + 0 = a = 0 + a$;
4. Existência do elemento oposto:
   $\forall\ a \in A\ \exists\ b \in A : a + b = 0 = b + a$;
5. Associatividade do produto:
   $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
6. Propriedade distributiva:

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

Exemplo 2.1.1. $\mathbb{Z}$ é anel.
Para provar que $\mathbb{Z}$ é anel, deve-se mostrar que valem para o conjunto, as 6 propriedades de anel.
Pela definição formal do conjunto $\mathbb{Z}$, foge ao ascopo deste trabalho provar que valem as propriedades 1, 2, 5 e 6.
Mas se faz necessário provar a existência de elemento oposto e elemento neutro.
Sobre a existência do elemento neutro (3), pode-se admitir que seja o número zero, pois para cada $a \in \mathbb{Z}$, $a + 0 = a = 0 + a$ e $0 \in \mathbb{Z}$.
Sobre a existência do elementro oposto (4), pode-se admitir que o elemento oposto de $a \in \mathbb{Z}$ é $-a \in \mathbb{Z}$, pois para todo $a \in \mathbb{Z}$, $a + (-a) = 0 = (-a) + a$.
Portanto, como são válidas todas as propriedades, conclui-se que $\mathbb{Z}$ é anel.

O conjunto $\mathbb{N}$ não é anel pois, embora $0 \in \mathbb{N}$ seja um elemento neutro para a soma, para qualquer $a \in \mathbb{N}$ não nulo, não existe um elemento $b \in \mathbb{N}$ tal que $a + b = 0$. P54888999 „,ortanto apenas a (4) não é satisfeita. Caso zero não fosse considerado um número natural, além de não existir elemento oposto também não existiria um elemento neutro $e \in \mathbb{N}$ tal que $a + e = a$. Assim, (3) e (4) não seriam satisfeitas.

Exemplo 2.1.2. O conjunto $\mathbb{Q}$ é anel.

Seja $\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0 \right\}$ sob as operações

$$\begin{array}{rcl} + : \mathbb{Q} \times \mathbb{Q} & \longrightarrow & \mathbb{Q} \\ \left(\frac{a}{b}, \frac{c}{d}\right) & \longmapsto & \frac{ad + cb}{bd}, \end{array}$$

$$\begin{array}{rcl} \cdot : \mathbb{Q} \times \mathbb{Q} & \longrightarrow & \mathbb{Q} \\ \left(\frac{a}{b}, \frac{c}{d}\right) & \longmapsto & \frac{ac}{bd}. \end{array}$$

Para provar que $\mathbb{Q}$ é anel, devem ser satisfeitas as seguintes propriedades com $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$:

1. Associatividade na soma:

$$\begin{aligned}\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f} &= \frac{ad+cb}{bd}+\frac{e}{f}\\ &= \frac{(ad+cb)f+e(bd)}{(bd)f}\\ &= \frac{(adf+cbf)+ebd}{bdf}\\ &= \frac{adf+(bcf+bed)}{b(df)}\\ &= \frac{a(df)+b(cf+ed)}{b(df)}\\ &= \frac{a}{b}+\frac{cf+ed}{df}\\ &= \frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right).\end{aligned}$$

2. Comutatividade na soma:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+cb}{bd}=\frac{cb+ad}{db}=\frac{c}{d}+\frac{a}{b}.$$

3. Existência do elemento neutro:
   Provar-se-á que $\frac{0}{1}\in\mathbb{Q}$ é o elemento neutro:

$$\begin{aligned}(i)\quad &\frac{a}{b}+\frac{0}{1}=\frac{a\cdot 1+0\cdot b}{b\cdot 1}=\frac{a+0}{b}=\frac{a}{b}.\\ (ii)\quad &\frac{0}{1}+\frac{a}{b}=\frac{0\cdot b+a\cdot 1}{1\cdot b}=\frac{0+a}{b}=\frac{a}{b}.\end{aligned}$$

4. Existência do elemento oposto:
   Provar-se-á que o elemento oposto de $\frac{a}{b}$ é $\frac{-a}{b}\in\mathbb{Q}$:

$$\begin{aligned}(i)\quad &\frac{a}{b}+\left(\frac{-a}{b}\right)=\frac{ab+(-a)b}{bb}=\frac{ab+(-ab)}{b^2}=\frac{0}{b^2}=0.\\ (ii)\quad &\left(\frac{-a}{b}\right)+\frac{a}{b}=\frac{(-a)b+ab}{bb}=\frac{(-ab)+ab}{b^2}=\frac{0}{b^2}=0.\end{aligned}$$

5. Associatividade do produto:

$$\begin{aligned}\left(\frac{a}{b}\cdot\frac{c}{d}\right)\cdot\frac{e}{f} &= \frac{a\cdot c}{b\cdot d}\cdot\frac{e}{f}\\ &= \frac{(a\cdot c)\cdot e}{(b\cdot d)\cdot f}\\ &= \frac{a\cdot(c\cdot e)}{b\cdot(d\cdot f)}\\ &= \frac{a}{b}\cdot\frac{c\cdot e}{d\cdot f}\\ &= \frac{a}{b}\cdot\left(\frac{c}{d}\cdot\frac{e}{f}\right).\end{aligned}$$

6. Propriedade distributiva:

$$\begin{aligned}(i)\ \frac{a}{b}\cdot\left(\frac{c}{d}+\frac{e}{f}\right) &= \frac{a}{b}\cdot\frac{cf+ed}{df}\\ &= \frac{a(cf+ed)}{b(df)}\\ &= \frac{acf+aed}{bdf}\\ &= \frac{acbf+aebd}{bdbf}\\ &= \frac{ac}{bd}+\frac{ae}{bf}\\ &= \frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{e}{f}.\end{aligned}$$

$$
\begin{aligned}
(ii)\left(\frac{a}{b}+\frac{c}{d}\right)\cdot\frac{e}{f} &= \left(\frac{ad+cb}{bd}\right)\cdot\frac{e}{f}\\
&= \frac{(ad+cb)e}{(bd)f}\\
&= \frac{ade+cbe}{bdf}\\
&= \frac{aedf+cebf}{bfdf}\\
&= \frac{ae}{bf}+\frac{ce}{df}\\
&= \frac{a}{b}\cdot\frac{e}{f}+\frac{c}{d}\cdot\frac{e}{f}.
\end{aligned}
$$

Logo, conclui-se que $\mathbb{Q}$ também é anel.

Observação 1. $\mathbb{R}$ é anel.
Foge ao escopo deste trabalho provar que $\mathbb{R}$, o conjunto dos números reais, é um anel.
Porém, seu elemento neutro é o zero e o elemento oposto de $a \in \mathbb{R}$ é $-a \in \mathbb{R}$, pois para qualquer $a \in \mathbb{R}$, $a + (-a) = 0 = (-a) + a$.

Exemplo 2.1.3. Seja $A = \mathbb{F}(\mathbb{R})$ o conjunto de todas as funções $f : \mathbb{R} \to \mathbb{R}$ e $f, g, h \in A$. $F(\mathbb{R})$ é anel com as seguintes operações:

$$
\begin{aligned}
+ : A \times A &\longrightarrow A\\
(f, g) &\longmapsto f + g
\end{aligned}
$$

no qual $(f + g)(x) = f(x) + g(x), \forall\ x \in \mathbb{R}$ e

$$
\begin{aligned}
\cdot : A \times A &\longrightarrow A\\
(f, g) &\longmapsto f \cdot g
\end{aligned}
$$

no qual $(f \cdot g)(x) = f(x) \cdot g(x), \forall\ x \in \mathbb{R}$.
Para que $F(\mathbb{R})$ seja anel, devem ser satisfeitas as seguintes propriedades com $x \in \mathbb{R}$:

1. Associatividade na soma:

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

2. Comutatividade na soma:

$$(f+g)(x) = f(x)+g(x) = g(x)+f(x) = (g+f)(x).$$

3. Existência do elemento neutro:
O elemento neutro de $F(\mathbb{R})$, será dado pela função o definida por $o(x) = 0, \forall\ x \in \mathbb{R}$:

$$(f+o)(x) = f(x)+o(x) = f(x) = o(x)+f(x) = (o+f)(x).$$

4. Existência do elemento oposto:
Define-se para $f \in A$,

$$\begin{aligned}-f : \mathbb{R} &\longrightarrow \mathbb{R}\\ x &\longmapsto -f(x).\end{aligned}$$

Então,

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

5. Associatividade do produto:

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

6. Propriedade distributiva:

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

e

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

Assim, conclui-se que $F(\mathbb{R})$ também é anel.

Exemplo 2.1.4. Seja $M_2(\mathbb{R})$ o conjunto de todas as matrizes de ordem 2 com entradas reais e com as operações usuais:

$$\begin{aligned}+:&\quad \begin{bmatrix}a_1 & b_1\\ c_1 & d_1\end{bmatrix}+\begin{bmatrix}a_2 & b_2\\ c_2 & d_2\end{bmatrix}=\begin{bmatrix}a_1+a_2 & b_1+b_2\\ c_1+c_2 & d_1+d_2\end{bmatrix}\\ \cdot:&\quad \begin{bmatrix}a_1 & b_1\\ c_1 & d_1\end{bmatrix}\cdot\begin{bmatrix}a_2 & b_2\\ c_2 & d_2\end{bmatrix}=\begin{bmatrix}a_1a_2+b_1c_2 & a_1b_2+b_1d_2\\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2\end{bmatrix}.\end{aligned}$$

Para que $M_2(\mathbb{R})$ seja anel, devem ser satisfeitas as seguintes propriedades com

$$A_1=\begin{bmatrix}a_1 & b_1\\ c_1 & d_1\end{bmatrix}, A_2=\begin{bmatrix}a_2 & b_2\\ c_2 & d_2\end{bmatrix}, A_3=\begin{bmatrix}a_3 & b_3\\ c_3 & d_3\end{bmatrix}\in M_2(\mathbb{R}):$$

1. Associatividade na soma:

$$\begin{aligned}
(A_1 + A_2) + A_3 &= \left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\right) + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \\
&= \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \\
&= \begin{bmatrix} (a_1 + a_2) + a_3 & (b_1 + b_2) + b_3 \\ (c_1 + c_2) + c_3 & (d_1 + d_2) + d_3 \end{bmatrix} \\
&= \begin{bmatrix} a_1 + (a_2 + a_3) & b_1 + (b_2 + b_3) \\ c_1 + (c_2 + c_3) & d_1 + (d_2 + d_3) \end{bmatrix} \\
&= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 + a_3 & b_2 + b_3 \\ c_2 + c_3 & d_2 + d_3 \end{bmatrix} \\
&= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}\right) \\
&= A_1 + (A_2 + A_3).
\end{aligned}$$

2. Comutatividade na soma:

$$\begin{aligned}
A_1 + A_2 &= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \\
&= \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix} \\
&= \begin{bmatrix} a_2 + a_1 & b_2 + b_1 \\ c_2 + c_1 & d_2 + d_1 \end{bmatrix} \\
&= \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \\
&= A_2 + A_1.
\end{aligned}$$

3. Existência do elemento neutro:

Seja $A_0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$:

$$\begin{aligned} A_1 + A_0 &= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} a_1 + 0 & b_1 + 0 \\ c_1 + 0 & d_1 + 0 \end{bmatrix} \\ &= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \\ &= A_1 \\ &= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \\ &= \begin{bmatrix} 0 + a_1 & 0 + b_1 \\ 0 + c_1 & 0 + d_1 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \\ &= A_0 + A_1. \end{aligned}$$

4. Existência do elemento oposto:
   Para cada $A_1 \in M_2(\mathbb{R})$, assume-se que seu elemento oposto seja
   $-A_1 = \begin{bmatrix} -a_1 & -b_1 \\ -c_1 & -d_1 \end{bmatrix} \in M_2(\mathbb{R})$:

$$\begin{aligned}
A_1 + (-A_1) &= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} -a_1 & -b_1 \\ -c_1 & -d_1 \end{bmatrix} \\
&= \begin{bmatrix} a_1 + (-a_1) & b_1 + (-b_1) \\ c_1 + (-c_1) & d_1 + (-d_1) \end{bmatrix} \\
&= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\
&= A_0 \\
&= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\
&= \begin{bmatrix} (-a_1) + a_1 & (-b_1) + b_1 \\ (-c_1) + c_1 & (-d_1) + d_1 \end{bmatrix} \\
&= \begin{bmatrix} -a_1 & -b_1 \\ -c_1 & -d_1 \end{bmatrix} + \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \\
&= (-A_1) + A_1.
\end{aligned}$$

5. Associatividade do produto:

$$\begin{aligned}
(A_1 \cdot A_2) \cdot A_3 &= \left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \right) \cdot \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \\
&= \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix} \cdot \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \\
&= \begin{bmatrix} (a_1a_2 + b_1c_2)a_3 + (a_1b_2 + b_1d_2)c_3 \\ (c_1a_2 + d_1c_2)a_3 + (c_1b_2 + d_1d_2)c_3 \\ (a_1a_2 + b_1c_2)b_3 + (a_1b_2 + b_1d_2)d_3 \\ (c_1a_2 + d_1c_2)b_3 + (c_1b_2 + d_1d_2)d_3 \end{bmatrix} \\
&= \begin{bmatrix} a_1a_2a_3 + b_1c_2a_3 + a_1b_2c_3 + b_1d_2c_3 \\ c_1a_2a_3 + d_1c_2a_3 + c_1b_2c_3 + d_1d_2c_3 \\ a_1a_2b_3 + b_1c_2b_3 + a_1b_2d_3 + b_1d_2d_3 \\ c_1a_2b_3 + d_1c_2b_3 + c_1b_2d_3 + d_1d_2d_3 \end{bmatrix} \\
&= \begin{bmatrix} a_1a_2a_3 + a_1b_2c_3 + b_1c_2a_3 + b_1d_2c_3 \\ c_1a_2a_3 + c_1b_2c_3 + d_1c_2a_3 + d_1d_2c_3 \\ a_1a_2b_3 + a_1b_2d_3 + b_1c_2b_3 + b_1d_2d_3 \\ c_1a_2b_3 + c_1b_2d_3 + d_1c_2b_3 + d_1d_2d_3 \end{bmatrix} \\
&= \begin{bmatrix} a_1(a_2a_3 + b_2c_3) + b_1(c_2a_3 + d_2c_3) \\ c_1(a_2a_3 + b_2c_3) + d_1(c_2a_3 + d_2c_3) \\ a_1(a_2b_3 + b_2d_3) + b_1(c_2b_3 + d_2d_3) \\ c_1(a_2b_3 + b_2d_3) + d_1(c_2b_3 + d_2d_3) \end{bmatrix} \\
&= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2a_3 + b_2c_3 & a_2b_3 + b_2d_3 \\ c_2a_3 + d_2c_3 & c_2b_3 + d_2d_3 \end{bmatrix} \\
&= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \cdot \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \right) \\
&= A_1 \cdot (A_2 \cdot A_3).
\end{aligned}$$

6. Propriedade distributiva:

$$\begin{aligned}
& A_1 \cdot (A_2 + A_3) \\
= \; & \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \right) \\
= \; & \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 + a_3 & b_2 + b_3 \\ c_2 + c_3 & d_2 + d_3 \end{bmatrix} \\
= \; & \begin{bmatrix} a_1(a_2 + a_3) + b_1(c_2 + c_3) & a_1(b_2 + b_3) + b_1(d_2 + d_3) \\ c_1(a_2 + a_3) + d_1(c_2 + c_3) & c_1(b_2 + b_3) + d_1(d_2 + d_3) \end{bmatrix} \\
= \; & \begin{bmatrix} a_1a_2 + a_1a_3 + b_1c_2 + b_1c_3 & a_1b_2 + a_1b_3 + b_1d_2 + b_1d_3 \\ c_1a_2 + c_1a_3 + d_1c_2 + d_1c_3 & c_1b_2 + c_1b_3 + d_1d_2 + d_1d_3 \end{bmatrix} \\
= \; & \begin{bmatrix} (a_1a_2 + b_1c_2) + (a_1a_3 + b_1c_3) \\ (c_1a_2 + d_1c_2) + (c_1a_3 + d_1c_3) \\ (a_1b_2 + b_1d_2) + (a_1b_3 + b_1d_3) \\ (c_1b_2 + d_1d_2) + (c_1b_3 + d_1d_3) \end{bmatrix} \\
= \; & \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix} + \\
& \begin{bmatrix} a_1a_3 + b_1c_3 & a_1b_3 + b_1d_3 \\ c_1a_3 + d_1c_3 & c_1b_3 + d_1d_3 \end{bmatrix} \\
= \; & \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \\
= \; & A_1 \cdot A_2 + A_1 \cdot A_3.
\end{aligned}$$

A demonstração de $(A_1 + A_2) \cdot A_3 = A_1A_3 + A_2A_3$ é similar.

Assim, utilizando o fato de $\mathbb{R}$ ser anel, conclui-se que $M_2(\mathbb{R})$ também é anel.

Definição 2.2. Se no anel $(A, +, \cdot)$

$$\exists\ 1 \in A,\ 1 \neq 0 \text{ tal que } 1 \cdot x = x = x \cdot 1\ \forall\ x \in A,$$

diz-se que A é anel com unidade.

Definição 2.3. Se no anel $(A, +, \cdot)$

$$\forall\ x, y \in A,\ x \cdot y = y \cdot x,$$

diz-se A é anel comutativo.

Definição 2.4. Se no anel $(A, +, \cdot)$

$$\forall\ x, y \in A,\ \text{com } x \cdot y = 0 \text{ então } x = 0 \text{ ou } y = 0$$

diz-se que A é anel sem divisores de zero.

Definição 2.5. Um anel comutativo com unidade e sem divisores de zero é dito um domínio de integridade.

Definição 2.6. Se no anel comutativo com unidade $(A, +, \cdot)$

$$\forall\ x \in A,\ x \neq 0\ \exists\ y \in A,\ \text{tal que } x \cdot y = 1 = y \cdot x,$$

então A é denominado um corpo e o elemento y é dito inverso de x.

Exemplo 2.1.5. $\mathbb{Z}$ é domínio de integridade mas não é corpo pois neste conjunto há elementos que não possuem inverso.

Exemplo 2.1.6. Como provado anteriormente no Exemplo 2.1.3., o conjunto $A = F(\mathbb{R})$ de funções sobre $\mathbb{R}$ é um anel.
Nota-se que A satisfaz também a definição de anel com unidade, pois sendo $a(x) = 1$ e $f(x)$ uma função qualquer de A, tem-se que

$$a(x) \cdot f(x) = 1 \cdot f(x) = f(x) = f(x) \cdot 1 = f(x) \cdot a(x).$$

Este conjunto também satisfaz a definição de anel comutativo, pois dadas duas funções $f(x), g(x)$ tem-se que

$$f(x) \cdot g(x) = g(x) \cdot f(x).$$

Por sua vez, A não é um anel comutativo sem divisores de zero, pois duas funções podem ser não nulas mas seu produto ser nulo, observe:

$$f(x) = \begin{cases} 1, & \text{se } x = 1 \\ 0, & \text{se } x \neq 1 \end{cases} \text{ e } g(x) = \begin{cases} 2, & \text{se } x = 2 \\ 0, & \text{se } x \neq 2 \end{cases}.$$

Sendo então, um conjunto com divizores de zero. Portanto, o conjunto das funções sobre $\mathbb{R}$ é um anel comutativo com unidade.

Exemplo 2.1.7. Como provado anteriormente no Exemplo 2.1.4., o conjunto das matrizes $M_2(\mathbb{R})$ é um anel. Utilizando a matriz identidade $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ e multiplicando com $A_1 = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, tem-se que

$$\begin{aligned} I \cdot A_1 &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \\ &= \begin{bmatrix} 1 \cdot a_1 + 0 \cdot c_1 & 1 \cdot b_1 + 0 \cdot d_1 \\ 0 \cdot a_1 + 1 \cdot c_1 & 0 \cdot b_1 + 1 \cdot d_1 \end{bmatrix} \\ &= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \\ &= A_1 \\ &= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \\ &= \begin{bmatrix} a_1 \cdot 1 + b_1 \cdot 0 & a_1 \cdot 0 + b_1 \cdot 1 \\ c_1 \cdot 1 + d_1 \cdot 0 & c_1 \cdot 0 + d_1 \cdot 1 \end{bmatrix} \\ &= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ &= A_1 \cdot I. \end{aligned}$$

Portanto, este conjunto é um anel com unidade. Sobre as demais definições, pode-se verificar que o produto de duas matrizes não é necessariamente comutativo, ou seja, duas matrizes A_1, A_2 podem não satisfazer $A_1 \cdot A_2 = A_2 \cdot A_1$. Também podem possuir divisores de zero, pois as matrizes $A_3 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, A_4 = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}$ são não nulas e seu produto que resulta em uma matriz nula:

$$A_3 \cdot A_4 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Exemplo 2.1.8. Seja o conjunto

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$$

para $n \in \mathbb{N}^*$ com as seguintes operações:

$$\begin{aligned} + &: nk_1 + nk_2 = n(k_1 + k_2) \\ \cdot &: nk_1 \cdot nk_2 = n(k_1 n k_2). \end{aligned}$$

Para que $n\mathbb{Z} = \{nk : n \in \mathbb{N}, k \in \mathbb{Z}\}$ seja um anel comutativo sem divisores de zero, devem ser satisfeitas as seguintes propriedades com $k_1, k_2, k_3 \in \mathbb{Z}$:

1. Associatividade na soma:

$$\begin{aligned}(nk_1 + nk_2) + nk_3 &= n(k_1 + k_2) + nk_3 \\ &= n[(k_1 + k_2) + k_3] \\ &= n[k_1 + (k_2 + k_3)] \\ &= nk_1 + n(k_2 + k_3) \\ &= nk_1 + (nk_2 + nk_3).\end{aligned}$$

2. Comutatividade na soma:

$$nk_1 + nk_2 = n(k_1 + k_2) = n(k_2 + k_1) = nk_2 + nk_1.$$

3. Existência do elemento neutro:
   Seja $k_0 = 0$:

$$nk_0 + nk_1 = nk_1 + nk_0 = n(k_1 + k_0) = n(k_1 + 0) = nk_1,$$

   então $nk_0 = n \cdot 0$ é o elemento neutro.

4. Existência do elemento oposto:
   Seja $-nk_1 = n(-k_1)$:

$$nk_1 + (-nk_1) = nk_1 + n(-k_1) = n(k_1 - k_1) = n0 = nk_0,$$

   então $-nk_1$ é o elemento oposto de nk_1.
   Por conta da comutatividade, $-nk_1 + nk_1 = 0$ também.

5. Associatividade do produto:

$$\begin{aligned}(nk_1 \cdot nk_2) \cdot nk_3 &= n(k_1 nk_2) \cdot nk_3 \\ &= n((k_1 nk_2)nk_3) \\ &= n(k_1(nk_2 nk_3)) \\ &= nk_1 \cdot n(k_2 nk_3) \\ &= nk_1 \cdot (nk_2 \cdot nk_3).\end{aligned}$$

6. Propriedade distributiva:

$$\begin{aligned} nk_1 \cdot (nk_2 + nk_3) &= nk_1(n(k_2 + k_3)) \\ &= n[k_1 n(k_2 + k_3)] \\ &= n[nk_1(k_2 + k_3)] \\ &= n(nk_1k_2 + nk_1k_3) \\ &= n(k_1nk_2 + k_1nk_3) \\ &= n(k_1nk_2) + n(k_1nk_3) \\ &= nk_1nk_2 + nk_1nk_3 \\ &= nk_1 \cdot nk_2 + nk_1 \cdot nk_3. \end{aligned}$$

A demonstração é similar para $(nk_1 + nk_2) \cdot nk_3 = nk_1 \cdot nk_3 + nk_2 \cdot nk_3$.

7. Unidade multiplicativa:
Suponha que nk_2 seja a unidade multiplicativa e seja nk_1 um elemento não nulo. Então:

$$nk_1 = nk_1 \cdot nk_2 = n(k_1nk_2)$$

ou seja,

$$\begin{aligned} nk_1 &= n(k_1nk_2) \\ nk_1 - n(k_1nk_2) &= n(k_1nk_2) - n(k_1nk_2) \\ nk_1(1 - nk_2) &= 0 \\ 1 - nk_2 &= 0 \\ nk_2 &= 1. \end{aligned}$$

Isso implica que $n = k_2 = 1$. Logo, somente $1\mathbb{Z} = \mathbb{Z}$ possui unidade multiplicativa 1.
De forma análoga, demonstra-se que $nk_1 = nk_2 \cdot nk_1$.

8. Comutatividade do produto:

$$\begin{aligned} nk_3 \cdot nk_2 &= n(k_3nk_2) \\ &= n(nk_3k_2) \\ &= n(nk_2k_3) \\ &= n(k_2nk_3) \\ &= nk_2 \cdot nk_3. \end{aligned}$$

9. Divisores de zero:
   Seja o produto $na \cdot nb = 0$. Para que o conjunto não tenha divisores de zero, $na = 0$ ou $nb = 0$.

   $$(na) \cdot (nb) = 0 \Rightarrow n(anb) = 0 \Rightarrow anb = 0.$$

   Como $n \neq 0$ e $a, b \in \mathbb{Z}$ segue que $a = 0$ ou $b = 0$. Portanto, $na = 0$ ou $nb = 0$.

Provadas as propriedades, conclui-se que o conjunto $n\mathbb{Z}$ é anel comutativo sem divisores de zero, e terá unidade multiplicativa apenas quando $n = 1$.

2.2 PROPRIEDADES

Seja $(A, +, \cdot)$ um anel.

Proposição 2.1. *Vale a lei do cancelamento para a soma, ou seja,* $a + b = a + c \Rightarrow b = c$ *com* $a, b, c \in A$.

Demonstração. Por hipótese, $a, b, c \in A$ e $a + b = a + c$. Provar-se-á que $b = c$.
Como A é anel, sabe-se que existe o elemento oposto de $a \in A$, denotado por $-a$. Então, somando $-a$ à esquerda de ambos os lados da igualdade, tem-se:

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

e pela associatividade em A, tem-se:

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

Como 0 é elemento neutro, tem-se $b = c$. ■

Proposição 2.2. *Existe apenas um elemento neutro no anel* A.

Demonstração. Seja $a \in A$ e $0', \hat{0}$ os elementos neutros de A. Então:

$$a + 0' = a = 0' + a$$

e

$$a + \hat{0} = a = \hat{0} + a.$$

Observa-se que

$$a + 0' = a = a + \hat{0} \Rightarrow a + 0' = a + \hat{0}.$$

Pela lei do cancelamento (Proposição 2.1), tem-se que $0' = \hat{0}$. ■

Proposição 2.3. *Dado $a \in A$, existe apenas um elemento oposto de a.*

Demonstração. Seja a um elemento qualquer em A e $a', \hat{a} \in A$ seus elementos opostos. Então:

$$a + a' = 0 = a' + a$$

e

$$a + \hat{a} = 0 = \hat{a} + a.$$

Observa-se que

$$a + a' = 0 = a + \hat{a} \Rightarrow a + a' = a + \hat{a}.$$

Pela lei do cancelamento, tem-se que $a' = \hat{a}$. ■

Proposição 2.4. $\forall\ a, b \in A$, *valem as seguintes propriedades:*

1. $-(a + b) = (-a) + (-b)$
2. $-(-a) = a$
3. $a \cdot 0 = 0 = 0 \cdot a$
4. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
5. $(-a) \cdot (-b) = a \cdot b.$

Demonstração. Para provar que valem essas propriedades, admite-se $a, b \in A$.

1. Seja $a + b$ um elemento em A, então $-(a + b)$ também é elemento em A e portanto

$$(a + b) + [-(a + b)] = 0.$$

Somando $-a$ à esquerda em ambos os lados, operando com a associatividade e com o elemento neutro, tem-se:

$$\begin{aligned}(-a) + (a + b) + [-(a + b)] &= (-a) + 0\\ (-a + a) + b + [-(a + b)] &= -a\\ (0 + b) + [-(a + b)] &= -a\\ b + [-(a + b)] &= -a.\end{aligned}$$

Somando $-b$ à esquerda em ambos os lados, operando com a associatividade e com o elemento neutro, tem-se:

$$\begin{aligned}(-b) + b + [-(a + b)] &= (-b) + (-a)\\ (-b + b) + [-(a + b)] &= (-b) + (-a)\\ 0 + [-(a + b)] &= (-b) + (-a)\\ -(a + b) &= (-b) + (-a).\end{aligned}$$

Pela definição de anel, a soma é comutativa, portanto

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

2. A é anel e $a \in A$, portanto $-a \in A$ e

$$a + (-a) = 0.$$

Como $-a \in A$ tem-se que $-(-a) \in A$ e também

$$(-a) + [-(-a)] = 0.$$

Então, somando a à esquerda desta última expressão:

$$\begin{aligned}a + (-a) + [-(-a)] &= a + 0\\ [a + (-a)] + [-(-a)] &= a\\ 0 + [-(-a)] &= a\\ -(-a) &= a.\end{aligned}$$

3. Para provar as igualdades, admite-se que $a \cdot 0 = a \cdot (0+0)$ pelo item do elemento neutro na definição de anel. Manipulando algebricamente, tem-se:

$$\begin{aligned} a \cdot 0 &= a \cdot (0+0) \\ a \cdot 0 &= a \cdot 0 + a \cdot 0 \\ 0 + a \cdot 0 &= a \cdot 0 + a \cdot 0 \\ 0 &= a \cdot 0 \end{aligned}$$

e

$$\begin{aligned} 0 \cdot a &= (0+0) \cdot a \\ 0 \cdot a &= 0 \cdot a + 0 \cdot a \\ 0 + 0 \cdot a &= 0 \cdot a + 0 \cdot a \\ 0 &= 0 \cdot a. \end{aligned}$$

Portanto, pelas duas expressões, conclui-se que

$$a \cdot 0 = 0 = 0 \cdot a.$$

4. Para provar a validade das igualdades, utiliza-se o item 4 da definição de anel, $(-a) + a = 0$, e então faz-se uso dos demais itens desta proposição para manipular a expressão:

$$\begin{aligned} (-a) + a &= 0 \\ [(-a) + a] \cdot b &= 0 \cdot b \\ (-a) \cdot b + a \cdot b &= 0 \\ (-a) \cdot b + a \cdot b + [-(a \cdot b)] &= 0 + [-(a \cdot b)] \\ (-a) \cdot b + \{(a \cdot b) + [-(a \cdot b)]\} &= -(a \cdot b) \\ (-a) \cdot b + 0 &= -(a \cdot b) \\ (-a) \cdot b &= -(a \cdot b) \end{aligned}$$

e

$$\begin{aligned}
(-b)+b &= 0\\
a\cdot[(-b)+b] &= a\cdot 0\\
a\cdot(-b)+a\cdot b &= 0\\
a\cdot(-b)+a\cdot b+[-(a\cdot b)] &= 0+[-(a\cdot b)]\\
a\cdot(-b)+\{a\cdot b+[-(a\cdot b)]\} &= -(a\cdot b)\\
a\cdot(-b)+0 &= -(a\cdot b)\\
a\cdot(-b) &= -(a\cdot b).
\end{aligned}$$

Portanto,

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

5. Para provar a igualdade, utiliza-se o item 4 da definição de anel, $(-a)+a=0$, e então faz-se uso dos demais itens desta proposição para manipular a expressão:

$$\begin{aligned}
(-a)+a &= 0\\
[(-a)+a]\cdot(-b) &= 0\cdot(-b)\\
(-a)\cdot(-b)+a\cdot(-b) &= 0\\
(-a)\cdot(-b)+[-(a\cdot b)]+(a\cdot b) &= 0+(a\cdot b)\\
(-a)\cdot(-b)+\{[-(a\cdot b)]+(a\cdot b)\} &= 0+(a\cdot b)\\
(-a)\cdot(-b)+0 &= a\cdot b\\
(-a)\cdot(-b) &= a\cdot b.
\end{aligned}$$

Pelas demonstrações acima, está provada a veracidade da proposição. ■

Proposição 2.5. *Dados $a,b\in A$ a única solução da equação $a+x=b$ é $x=b-a$.*

Demonstração. Por definição, o oposto de $a\in A$ é $-a$. Deste

modo:

$$\begin{aligned} a+x &= b \\ (-a)+a+x &= (-a)+b \\ [(-a)+a]+x &= b+(-a) \\ 0+x &= b-a \\ x &= b-a. \end{aligned}$$

Agora, basta provar que essa solução é única. Supõe-se que x_0 também seja solução, isto é, $a+x_0=b$, então operando de forma análoga:

$$\begin{aligned} a+x_0 &= b \\ (-a)+a+x_0 &= (-a)+b \\ [(-a)+a]+x_0 &= b+(-a) \\ 0+x_0 &= b-a \\ x_0 &= b-a. \end{aligned}$$

Portanto, a solução é única. ■

Proposição 2.6. *Se um anel for corpo então ele é um domínio de integridade.*

Demonstração. Por hipótese, como A é corpo, para todo $x \in A$ e $x \neq 0$, existe $y \in A$ tal que $x \cdot y = 1 = y \cdot x$.
Seja $a \in A$ tal que $x \cdot a = 0$ e $x \neq 0$. Multiplicando y à esquerda em ambos os lados tem-se $y \cdot x \cdot a = y \cdot 0$. Pelo item 3 da Proposição 2.4., $y \cdot 0 = 0$. Então $1 \cdot a = 0 \Rightarrow a = 0$. Portanto, se A for corpo e $x \cdot a = 0$, então $x = 0$ ou $a = 0$, logo, A é domínio de integridade. ■

Exemplo 2.2.1. Seja $\mathbb{C} = \{a+bi : a, b \in \mathbb{R}\}$ o conjunto dos números complexos com as seguintes operações:

$$\begin{aligned} + &: (a+bi)+(c+di) = (a+c)+(b+d)i \\ \cdot &: (a+bi)\cdot(c+di) = (ac-bd)+(ad+bc)i. \end{aligned}$$

Para que $\mathbb{C}$ seja corpo, devem ser satisfeitas as seguintes propriedades com $a+bi, c+di, e+fi \in \mathbb{C}$:

1. Associatividade na soma:

$$\begin{aligned}[(a+bi)+(c+di)] &+ (e+fi)\\ &= [(a+c)+(b+d)i]+(e+fi)\\ &= [(a+c)+e]+[(b+d)+f]i\\ &= [a+(c+e)]+[b+(d+f)]i\\ &= (a+bi)+[(c+e)+(d+f)i]\\ &= (a+bi)+[(c+di)+(e+fi)].\end{aligned}$$

2. Comutatividade na soma:

$$\begin{aligned}(a+bi)+(c+di) &= (a+c)+(b+d)i\\ &= (c+a)+(d+b)i\\ &= (c+di)+(a+bi).\end{aligned}$$

3. Existência do elemento neutro:
   Seja $0+0i \in \mathbb{C}$, então:

$$(a+bi)+(0+0i) = (a+0)+(b+0)i = a+bi.$$

   Analogamente, $(0+0i)+(a+bi) = a+bi$.

4. Existência do elemento oposto:
   Provar-se-á que $-(a+bi) = -a+(-b)i \in \mathbb{C}$ é o elemento oposto de $a+bi$:

$$\begin{aligned}(a+bi)+(-a+(-b)i) &= (a+(-a))+(b+(-b))i\\ &= 0+0i\\ &= ((-a)+a)+((-b)+b)i\\ &= (-a+(-b)i)+(a+bi).\end{aligned}$$

5. Associatividade do produto:

$$\begin{aligned}
& [(a+bi)\cdot(c+di)]\cdot(e+fi)\\
= \ & [(ac-bd)+(ad+bc)i]\cdot(e+fi)\\
= \ & [(ac-bd)e-(ad+bc)f]+[(ac-bd)f+(ad+bc)e]i\\
= \ & (ace-bde-adf-bcf)+(acf-bdf+ade+bce)i\\
= \ & [a(ce-df)-b(de+cf)]+[a(de+cf)+b(ce-df)]i\\
= \ & (a+bi)\cdot[(ce-df)+(de+cf)i]\\
= \ & (a+bi)\cdot[(c+di)\cdot(e+fi)].
\end{aligned}$$

6. Propriedade distributiva:

$$\begin{aligned}
& (a+bi)\cdot[(c+di)+(e+fi)]\\
= \ & (a+bi)\cdot[(c+e)+(d+f)i]\\
= \ & [a(c+e)-b(d+f)]+[a(d+f)+b(c+e)]i\\
= \ & (ac+ae-bd-bf)+(ad+af+bc+be)i\\
= \ & [(ac-bd)+(ae-bf)]+[(ad+bc)+(af+be)]i\\
= \ & [(ac-bd)+(ad+bc)i]+[(ae-bf)+(af+be)i]\\
= \ & (a+bi)\cdot(c+di)+(a+bi)\cdot(e+fi).
\end{aligned}$$

   Esta demonstração é de forma análoga para $[(a+bi)+(c+di)]\cdot(e+fi)=(a+bi)\cdot(e+fi)+(c+di)\cdot(e+fi)$.

7. Elemento neutro do produto:
   Provar-se-á que $1+0i\in\mathbb{C}$ é o elemento neutro do produto:

$$\begin{aligned}
(a+bi)\cdot(1+0i) &= (a1-b0)+(a0+b1)i\\
&= a+bi\\
&= (1a-0b)+(1b+0a)i\\
&= (1+0i)\cdot(a+bi).
\end{aligned}$$

8. Comutatividade do produto:

$$\begin{aligned}
(a+bi)\cdot(c+di) &= (ac-bd)+(ad+bc)i\\
&= (ca-db)+(cb+da)i\\
&= (c+di)\cdot(a+bi).
\end{aligned}$$

10. Existência do elemento inverso do produto:
Seja $a+bi \in \mathbb{C}$, um elemento não nulo. Nota-se que $a^2+b^2 \neq 0$ e $\frac{a}{a^2+b^2} + \left(-\frac{b}{a^2+b^2}\right) i$ é um número complexo. Então:

$$\begin{aligned}
&\left[\frac{a}{a^2+b^2} + \left(-\frac{b}{a^2+b^2}\right) i\right] \cdot (a+bi) \\
&= (a+bi) \cdot \left[\frac{a}{a^2+b^2} + \left(-\frac{b}{a^2+b^2}\right) i\right] \\
&= \left(\frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}\right) + \left(-\frac{ab}{a^2+b^2} + \frac{ba}{a^2+b^2}\right) i \\
&= 1 + 0i.
\end{aligned}$$

Portanto, para qualquer $a+bi \in \mathbb{C}$ não nulo,

$$\frac{a}{a^2+b^2} + \left(-\frac{b}{a^2+b^2}\right) i$$

é seu inverso multiplicativo.

Desta forma, está demonstrado que $\mathbb{C}$ é um corpo. Então, pela Proposição 2.6 conclui-se que este conjunto também é um domínio de integridade.

2.3 SUBANÉIS

Definição 2.7. Seja $(A, +, \cdot)$ um anel e B um subconjunto não vazio de A. Se as operações de A estiverem bem definidas em B e este for um anel, então B é subanel de A. Denota-se $B \leq A$.

Exemplo 2.3.1. O conjunto $n\mathbb{Z} = \{nk : n \in \mathbb{N}, k \in \mathbb{Z}\}$ é subconjunto de $\mathbb{Z}$ pois como $\mathbb{N} \subseteq \mathbb{Z}$ então $n \in \mathbb{Z}$, $k \in \mathbb{Z}$ e portanto $nk \in \mathbb{Z}$. Foi provado anteriormente no Exemplo 2.1.8 que $n\mathbb{Z}$ é anel. Logo, $n\mathbb{Z} \leq \mathbb{Z}$.

Proposição 2.7. *Seja $(A, +, \cdot)$ um anel e $B \subset A$. Assim, B é subanel de A se e somente se*

(i) $O_A \in B$

(ii) $\forall x, y \in B \Rightarrow x - y \in B$

(iii) $\forall x, y \in B \Rightarrow x \cdot y \in B$.

Demonstração. ($\Rightarrow$) Por hipótese, B é subanel de A, ou seja B também é anel e é subconjunto de A. Portanto por definição de anel valem os itens (i), (ii) e (iii).
($\Leftarrow$) Por hipótese, valem as propriedades (i), (ii) e (iii). Portanto, pelo item (i), segue que $B \neq \varnothing$ pois possui o elemento neutro de A e pelo item (ii) segue que para todo $x \in B$, seu oposto $-x$ está em B pois $-x = 0 - x \in B$. Por fim, B é fechado para o produto pelo item (iii) e fechado para a soma por dados $x, y \in B$ tem-se que $x + y = x - (-y) \in B$. Pelo fato de A se anel e B ser subconjunto de A, em B satisfazem as propriedades associativa para soma e produto, comutativa para soma e distributiva. Com isso, conclui-se que B é subanel de A. ■

Exemplo 2.3.2. Sejam os conjuntos

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}$$

e

$$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}.$$

Já está provado que $M_2(\mathbb{R})$ é anel. A é subanel de $M_2(\mathbb{R})$ pois é subconjunto de $M_2(\mathbb{R})$ e satisfaz a Proposição 2.7, ou seja, possui o elemento neutro de $M_2(\mathbb{R})$, é fechado para o produto e é fechado para a soma com elemento oposto. Portanto, $A \leq M_2(\mathbb{R})$.
A unidade multiplicativa do anel $M_2(\mathbb{R})$ é a matriz identidade, como vista no Exemplo 2.1.7, porém a unidade multiplicativa do anel A é

$$I' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

pois

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot a + 0 \cdot 0 & 1 \cdot 0 + 0 \cdot 0 \\ 0 \cdot a + 0 \cdot 0 & 0 \cdot 0 + 0 \cdot 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

e

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a \cdot 1 + 0 \cdot 0 & a \cdot 0 + 0 \cdot 0 \\ 0 \cdot 1 + 0 \cdot 0 & 0 \cdot 0 + 0 \cdot 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}.$$

Portanto, por meio deste exemplo, pode-se observar que um subanel pode não ter a mesma unidade multiplicativa do anel.

Proposição 2.8. *Em um domínio de integridade A com unidade 1, todo subanel B com unidade tem a mesma unidade 1.*

Demonstração. Supõe-se que a unidade de A seja 1 e a unidade de B seja $1'$. Como B é subconjunto de A, então $1' \in A$. Logo, vale que:

$$1' \cdot 1 = 1'$$

Somando o oposto de $1'$ à direita em ambos os lados da igualdade, tem-se:

$$\begin{aligned} 1' \cdot 1 + (-1') &= 1' + (-1') \\ 1' \cdot 1 - 1' &= 0 \\ 1' \cdot 1 - 1' \cdot 1' &= 0 \\ 1' \cdot (1 - 1') &= 0. \end{aligned}$$

Por hipótese, A é domínio de integridade, portanto não possui divisores de zero. Então, da igualdade anterior, vale que $1' = 0$ o que é um absurdo, ou $1 - 1' = 0$, ou seja, $1' = 1$, como esperava-se concluir. Portanto, B possui a mesma unidade de A. ■

Proposição 2.9. *No anel A com unidade e sem divisores de zero, $x^2 = x$ tem solução $x = 0$ ou $x = 1$.*

Demonstração. Nota-se que $x^2 = x$ implica em $x \cdot x = x$. Como A é anel, pode ser somado $-x$ à direita em ambos os lados da igualdade:

$$x \cdot x + (-x) = x + (-x) \Rightarrow x \cdot x - x = 0.$$

Por definição, também vale a propriedade distributiva:

$$x \cdot x - x = 0 \Rightarrow x \cdot (x - 1) = 0.$$

Por não possuir divisores de zero, $x = 0$ ou $x - 1 = 0$. Somando 1 à direita em ambos os lados de $x - 1 = 0$ tem-se

$$x + (-1) + 1 = 0 + 1 \Rightarrow x + 0 = 1 \Rightarrow x = 1.$$

Ou seja, $x = 0$ ou $x = 1$. ■

2.4 IDEAIS

Definição 2.8. Seja A anel e $I \leq A$.

(i) I é um ideal à esquerda de A se:

$$\forall\ a \in A \text{ e } \forall\ i \in I \Rightarrow a \cdot i \in I$$

(ii) I é um ideal à direita de A se :

$$\forall\ a \in A \text{ e } \forall\ i \in I \Rightarrow i \cdot a \in I.$$

- Se I é ideal à esquerda e à direita, então I é ideal de A e sua notação é $I \lhd A$.

Proposição 2.10. *Se A é comutativo, então as propriedades (i) e (ii) da Definição 2.8. são equivalentes.*

Demonstração. Seja I um ideal à esquerda de A, então para todo $a \in A$ e $i \in I$, vale que $a \cdot i \in I$. Como A é comutativo, $a \cdot i = i \cdot a \in I$. Portanto I também é um ideal à direita.
Por outro lado, seja I um ideal à direita de A, então para todo $a \in A$ e $i \in I$, vale que $i \cdot a \in I$. Como A é comutativo, $i \cdot a = a \cdot i \in I$. Portanto I também é um ideal à esquerda. ■

Portanto, se I é ideal à esquerda ou à direira de um anel comutativo A, então $I \lhd A$.

Exemplo 2.4.1. Seja A um anel. $\{0\}$ e A são ideais de A. Estes são chamados de **ideais triviais** de A.

Exemplo 2.4.2. Seja o anel $M_2(\mathbb{R})$. Então

$I = \left\{ \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} : a, c \in \mathbb{R} \right\}$ é ideal à esquerda de $M_2(\mathbb{R})$ pois, dada

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in M_2(\mathbb{R}) :$$

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} pa + qc & p0 + q0 \\ ra + sc & r0 + s0 \end{pmatrix} = \begin{pmatrix} pa + qc & 0 \\ ra + dc & 0 \end{pmatrix}.$$

E também,

$$J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\} \text{ é ideal à direita de } M_2(\mathbb{R}) \text{ pois}$$

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap + br & aq + bs \\ 0p + 0r & 0q + 0s \end{pmatrix} = \begin{pmatrix} ap + br & aq + bs \\ 0 & 0 \end{pmatrix}.$$

Proposição 2.11. *Se A possui unidade 1 e $1 \in I$ ideal de A então $I = A$.*

Demonstração. Para provar que $I = A$ devemos provar que $I \subseteq A$ e $A \subseteq I$. Então:

$I \subseteq A : i \in I \subseteq A \Rightarrow i \in A.$

$A \subseteq I$: Tome $x \in A$. Como $1 \in I$ então $x = x \cdot 1 \in I$. ■

2.5 ISOMORFISMOS DE ANÉIS

Definição 2.9. Sejam A e B anéis e a função $f : A \to B$ tal que para todo $x, y \in A$:

(i) $f(x + y) = f(x) + f(y)$

(ii) $f(x \cdot y) = f(x) \cdot f(y)$.

f é chamado de **homomorfismo**.

Para o exemplo a seguir, será utilizado $\mathbb{Z} \times \mathbb{Z}$ como um anel, com as seguintes operações:

$$\begin{aligned} + : (\mathbb{Z} \times \mathbb{Z}) \times (\mathbb{Z} \times \mathbb{Z}) &\longrightarrow \mathbb{Z} \times \mathbb{Z} \\ [(a,b),(c,d)] &\longmapsto (a+c, b+d), \end{aligned}$$

$$\begin{aligned} \cdot : (\mathbb{Z} \times \mathbb{Z}) \times (\mathbb{Z} \times \mathbb{Z}) &\longrightarrow \mathbb{Z} \times \mathbb{Z} \\ [(a,b),(c,d)] &\longmapsto (ac, bd). \end{aligned}$$

A demonstração de que $\mathbb{Z} \times \mathbb{Z}$ é anel está disponível em *Elementos de álgebra*, [6], página 11.

Exemplo 2.5.1. Sejam os anéis $\mathbb{Z}$, $(\mathbb{Z} \times \mathbb{Z})$ e a função

$$\begin{aligned} f : \mathbb{Z} &\to (\mathbb{Z} \times \mathbb{Z}) \\ n &\mapsto (n, 0) \end{aligned}$$

para todo $n \in \mathbb{Z}$. Provar-se-á que f é um homomorfismo.
Sejam $x, y \in \mathbb{Z}$, então:

1. $f(x+y) = (x+y, 0) = (x,0) + (y,0) = f(x) + f(y)$;
2. $f(x \cdot y) = (x \cdot y, 0) = (x,0) \cdot (y,0) = f(x) \cdot f(y)$.

Note também que f é injetora:

$$f(x) = f(y) \Rightarrow (x,0) = (y,0) \Rightarrow x = y.$$

Portanto, está provado que f é um homomorfismo injetor.

Definição 2.10. Se f é bijetora e também um homomorfismo, diz-se que f é **isomorfismo**.

Definição 2.11. Sejam A um anel e a função $f : A \to A$:

- Se f é homomorfismo, então f é chamado de endorfismo;
- Se f é isomorfismo, então f é chamado de automorfismo.

3 GRUPOS

3.1 GRUPO

Definição 3.1. Seja G um conjunto munido de uma operação:

$$\begin{aligned} * : G \times G &\longrightarrow G \\ (a, b) &\longmapsto a * b \end{aligned}$$

$\forall\ a, b, c \in G$ grupo, valem as seguintes propriedades:

1. Associatividade:
   $(a * b) * c = a * (b * c)$.
2. Existência de elemento neutro:
   $\exists\ e \in G : a * e = e * a = a$.
3. Existência de elemento inverso:
   $\exists\ a^{-1} \in G : a * a^{-1} = a^{-1} * a = e$.

Definição 3.2. Se $*$ é comutativa em um grupo $(G, *)$, isto é, para todo $a, b \in G$ temos $a * b = b * a$, então $(G, *)$ é chamado **grupo abeliano**.

Definição 3.3. Os grupos cuja operação é a soma usual são chamados de grupos aditivos.

Definição 3.4. Os grupos cuja operação é o produto usual são chamados de grupos multiplicativos.

Exemplo 3.1.1. O conjunto $\mathbb{Z}$ com a soma usual é grupo pois para $a, b, c \in \mathbb{Z}$:

1. $(a + b) + c = a + (b + c)$;
2. 0 é o elemento neutro pois $0 + a = a = a + 0$;
3. $-a$ é elemento oposto de a pois $-a + a = 0 = a + (-a)$.

E também, $a + b = b + a$. Portanto, este conjunto é um grupo aditivo e abeliano, denotado por $(\mathbb{Z}, +)$.

Exemplo 3.1.2. O conjunto $\mathbb{Q}$ com a soma usual é grupo pois para $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$:

1. os elementos $\frac{a}{b}, \frac{c}{d}, \frac{e}{f}$ se associam, como já foi provado no Exemplo 2.1.2.
2. $\frac{0}{1} = 0$ é o elemento neutro, pois, $0 + \frac{a}{b} = \frac{a}{b} = \frac{a}{b} + 0$.
3. $\frac{-a}{b}$ é elemento oposto de $\frac{a}{b}$ pois

$$\frac{-a}{b} + \frac{a}{b} = 0 = \frac{a}{b} + \left(\frac{-a}{b}\right).$$

E também, $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$, que já está provado no Exemplo 2.1.2. Portanto, este conjunto é um grupo aditivo e abeliano, denotado por $(\mathbb{Q}, +)$.

Exemplo 3.1.3. O conjunto $\mathbb{R}$ com a soma usual é grupo pois para $a, b, c \in \mathbb{R}$:

1. $(a + b) + c = a + (b + c)$;
2. 0 é o elemento neutro pois $0 + a = a = a + 0$;
3. $-a$ é elemento oposto de a pois $-a + a = 0 = a + (-a)$;

E também, $a + b = b + a$. Portanto, este conjunto é um grupo aditivo e abeliano, denotado por $(\mathbb{R}, +)$.

Exemplo 3.1.4. O conjunto $\mathbb{C}$ com a soma usual é grupo pois para $a + bi, c + di, e + fi \in \mathbb{C}$:

1. $[(a+bi)+(c+di)]+(e+fi) = (a+bi)+[(c+di)+(e+fi)]$, que já está provado no Exemplo 2.2.1;

2. $(0 + 0i)$ é o elemento neutro pois $(0 + 0i) + (a + bi) = (0+a)+(0+b)i = a+bi = (a+0)+(b+0)i = (a+bi)+(0+0i)$;
3. $-(a+bi)$ é elemento oposto de $a+bi$ pois $-(a+bi)+(a+bi) = 0 = (a + bi) + (-(a + bi))$.

E também, $(a+bi)+(c+di) = (c+di)+(a+bi)$ que está provado no Exemplo 2.2.1. Portanto, este conjunto é um grupo aditivo e abeliano, denotado por $(\mathbb{C}, +)$.

Exemplo 3.1.5. O conjunto $\mathbb{Z}$ com a multiplicação usual não é grupo, pois, não há um elemento inverso multiplicativo para elementos de $\mathbb{Z}$.

Exemplo 3.1.6. O conjunto $\mathbb{Q} \setminus \{0\}$ com a multiplicação usual para $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q} \setminus \{0\}$ é grupo pois:

1. Os elementos $\frac{a}{b}, \frac{c}{d}, \frac{e}{f}$ se associam, como já foi provado no Exemplo 2.1.2.
2. $\frac{1}{1} = 1$ é o elemento neutro pois $1 \cdot \frac{a}{b} = \frac{a}{b} = \frac{a}{b} \cdot 1$;
3. $\frac{b}{a}$ é elemento inverso de $\frac{a}{b}$ pois $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1} = \frac{ba}{ab} = \frac{b}{a} \cdot \frac{a}{b}$.

E também, $\frac{a}{b} \cdot \frac{c}{d} = \frac{c}{d} \cdot \frac{a}{b}$. Portanto, este conjunto é um grupo multiplicativo e abeliano, denotado por $(\mathbb{Q} \setminus \{0\}, \cdot)$.

Exemplo 3.1.7. O conjunto $\mathbb{R} \setminus \{0\}$ com a multiplicação usual é grupo pois para $a, b, c \in \mathbb{R} \setminus \{0\}$:

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
2. 1 é o elemento neutro pois $1 \cdot a = a = a \cdot 1$;
3. $\frac{1}{a}$ é elemento inverso de a pois $a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$.

E também, $a \cdot b = b \cdot a$. Portanto, este conjunto é um grupo multiplicativo e abeliano, denotado por $(\mathbb{R} \setminus \{0\}, \cdot)$.

Exemplo 3.1.8. O conjunto $\mathbb{C} \setminus \{0\}$ com a multiplicação usual é grupo pois para $a+bi, c+di, e+fi \in \mathbb{C} \setminus \{0\}$:

1. $[(a+bi)\cdot(c+di)]\cdot(e+fi) = (a+bi)\cdot[(c+di)\cdot(e+fi)]$ como no Exemplo 2.2.1;
2. $1+0i$ é o elemento neutro pois $(1+0i)\cdot(a+bi) = a+bi = (a+bi)\cdot(1+0i)$;
3. $\dfrac{a}{a^2+b^2} + \left(-\dfrac{b}{a^2+b^2}\right)i$ é seu inverso multiplicativo, conforme provado no Exemplo 2.2.1.

E também, $(a+bi)\cdot(c+di) = (c+di)\cdot(a+bi)$ que está provado no Exemplo 2.2.1. Portanto, este conjunto é um grupo multiplicativo e abeliano, denotado por $(\mathbb{C} \setminus \{0\}, \cdot)$.

Observação 2. Os grupos multiplicativos e abelianos dos exemplos anteriores foram definidos sem o número zero, pois em todos os casos, não existe um elemento inverso multiplicativo para zero.

Exemplo 3.1.9. O conjunto de matrizes de ordem $m \times n$ com entradas reais satisfaz as propriedades de grupo com a operação de soma. Ou seja, dadas as matrizes $A, B, C \in M_{m\times n}(\mathbb{R})$:

1. Associatividade:
   $(A+B)+C = A+(B+C)$.
2. Existência do elemento neutro:
   O elemento neutro desse conjunto é a matriz nula O, na qual suas entradas são todas nulas para que $A+O = A = O+A$.
3. Existência do elemento oposto:
   O elemento oposto de cada matriz A nesse conjunto é uma matriz $-A$ tal que as entradas de $-A$ são os elementos opostos das entradas da matriz A, então $A+(-A) = O = -A+A$.

Então, $(M_{m\times n}(\mathbb{R}), +)$ é grupo aditivo e também é abeliano pois quaisquer duas matrizes desse grupo comutam. A demonstração completa de que este conjunto é um grupo está disponível em [2], p. 148.

Exemplo 3.1.10. O conjunto de matrizes de ordem $n \times n$ com entradas reais cujo determinante é diferente de zero, satisfaz as propriedades de grupo com a operação de multiplicação usual. Ou seja, dadas as matrizes $A, B, C \in M_{n\times n}(\mathbb{R})$:

1. Associatividade:
   $(A \cdot B) \cdot C = A \cdot (B \cdot C)$.

2. Existência do elemento neutro:
   O elemento neutro desse conjunto é a matriz identidade
   $I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$ tal que $A \cdot I = A = I \cdot A$.

3. Existência do elemento inverso:
   O conjunto está definido apenas com matrizes invertíveis, pois uma matriz A possui $det(A) \neq 0$ se, e somente se A é invertível. Portanto para cada A, existe $A^{-1} \in M_{n\times n}(\mathbb{R})$ tal que $A \cdot A^{-1} = I = A^{-1} \cdot A$.

Deste modo, $M_{n\times n}(\mathbb{R})$ de matrizes invertíveis é grupo com a operação de multiplicação e é chamado de $GL(n, \mathbb{R})$, *Grupo Linear*. Portanto, $(GL(n, \mathbb{R}), \cdot)$ é grupo multiplicativo mas não é abeliano, pois há matrizes invertíveis que não comutam. A demonstração completa está em [2], p. 143.

Exemplo 3.1.11. Seja $F(\mathbb{R})$ o conjunto das funções reais bijetoras, tal que considera-se a composição como operação:

$$\begin{array}{rcl} \circ : \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ (f, g) & \longmapsto & f \circ g(x) = f(g(x)). \end{array}$$

Para $f, g, h \in F(\mathbb{R})$, este conjunto satisfaz as propriedades de grupo:

1. Associatividade:

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

2. Existência do elemento neutro:
Seja $i(x) = x$ a função identidade, então

$$f \circ i(x) = f(i(x)) = f(x) = i(f(x)) = i \circ f(x).$$

3. Existência do elemento inverso:
Seja $f^{-1}(x)$ a função inversa, então

$$f \circ f^{-1}(x) = f(f^{-1}(x)) = i(x) = f^{-1}(f(x)) = f^{-1} \circ f(x).$$

Pelos itens demonstrados acima, conclui-se que $(F(\mathbb{R}), \circ)$ é um grupo, porém não é abeliano pois duas funções bijetoras quaisquer podem não comutar. Por exemplo, dadas $f(x) = x^2$ e $g(x) = x+1$, tem-se

$$(f \circ g)(x) = (x+1)^2 \text{ e } (g \circ f)(x) = x^2 + 1.$$

3.2 PROPRIEDADES

Proposição 3.1. *Seja $(G, *)$ um grupo. Então:*

1. *Existe um único elemento neutro para $*$.*
2. *Para cada $g \in G$ existe um único elemento inverso $g^{-1} \in G$.*
3. *Vale a lei do cancelamento, ou seja, para $f, g, h \in G$ se $f * h = g * h$, então $f = g$.*
4. *Para todo $f, g \in G$ vale $(f * g)^{-1} = g^{-1} * f^{-1}$.*
5. *$\forall\ g \in G$ tem-se $(g^{-1})^{-1} = g$.*

Demonstração. Seja $(G, *)$ um grupo. Provar-se-á os itens da proposição:

1. Sejam e e e' elementos neutros em G. Portanto, para todo $g \in G$, tem-se que $g * e = g = e * g$ e $g * e' = g = e' * g$. Como $g = g$, então $g * e = g * e'$. Operando o inverso de g à esquerda em ambos os lados da igualdade:

$$\begin{aligned} g^{-1} * (g * e) &= g^{-1} * (g * e') \\ (g^{-1} * g) * e &= (g^{-1} * g) * e' \\ e * e &= e * e' \\ e &= e'. \end{aligned}$$

   Portanto, o elemento neutro de G é único.

2. Sejam $g \in G$ e $g^{-1}, g_o \in G$ os elementos inversos de g. Logo, para qualquer g, tem-se que $g * g^{-1} = e = g^{-1} * g$ e $g * g_o = e = g_o * g$. Como $e = e$, então $g * g^{-1} = g * g_o$. Operando algum elemento inverso de g à esquerda em ambos os lados da igualdade:

$$\begin{aligned} g_o * (g * g^{-1}) &= g_o * (g * g_o) \\ (g_o * g) * g^{-1} &= (g_o * g) * g_o \\ e * g^{-1} &= e * g_o \\ g^{-1} &= g_o. \end{aligned}$$

   Dessa forma, para cada elemento em G, o seu elemento inverso é único.

3. Por hipótese, $f, g, h \in G$ e $f * h = g * h$. Provar-se-á que $f = g$.
   Como G é grupo, sabe-se que existe o elemento inverso de $h \in G$, denotado por h^{-1} tal que $h * h^{-1} = e = h^{-1} * h$. Então, operando h^{-1} à direita de ambos os lados da igualdade, tem-se:

$$\begin{aligned} f * h &= g * h \\ (f * h) * h^{-1} &= (g * h) * h^{-1} \end{aligned}$$

e, pela associatividade em A, tem-se:

$$\begin{aligned} f*(h*h^{-1}) &= g*(h*h^{-1}) \\ f*e &= g*e. \end{aligned}$$

Como e é elemento neutro, conclui-se que $f = g$.

4. Pelo fato de G ser grupo, pode-se admitir que dados $f, g \in G$, $f*g \in G$ e existe $(f*g)^{-1} \in G$ tal que

$$(f*g)*(f*g)^{-1} = e = (f*g)^{-1}*(f*g).$$

Operando f^{-1} à esquerda em ambos os lados, tem-se:

$$f^{-1}*(f*g)*(f*g)^{-1} = f^{-1}*e.$$

Como a operação $*$ é associativa, tem-se que:

$$\begin{aligned} (f^{-1}*f)*g*(f*g)^{-1} &= f^{-1} \\ e*g*(f*g)^{-1} &= f^{-1} \end{aligned}$$

g * (f * g)$^{-1} = f^{-1}$.Operando g^{-1} à esquerda em ambos os lados:

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

Portanto, conclui-se que a igualdade é verdadeira.

5. G é grupo e $g \in G$, portanto $g^{-1} \in G$ e $g*g^{-1} = e = g^{-1}*g$. Como $g^{-1} \in G$ tem-se que $(g^{-1})^{-1} \in G$ e

$$g^{-1}*(g^{-1})^{-1} = e = (g^{-1})^{-1}*g^{-1}.$$

Operando g à esquerda tem-se:

$$\begin{aligned} g*\left[g^{-1}*(g^{-1})^{-1}\right] &= g*e \\ \left[g*g^{-1}\right]*(g^{-1})^{-1} &= g \\ e*(g^{-1})^{-1} &= g. \end{aligned}$$

Como e é elemento neutro, conclui-se que $(g^{-1})^{-1} = g$.

■

Observação 3. Generalizando o item 4 da proposição anterior, tem-se a seguinte igualdade:

$$(g_1 * g_2 * \cdots * g_n)^{-1} = g_n^{-1} * \cdots * g_2^{-1} * g_1^{-1}.$$

A demonstração dessa igualdade se dá pelo método de indução. Observe:
A igualdade vale para $n = 2$. Supõe-se que vale para $n = k$, então:

$$(g_1 * g_2 * \cdots * g_k)^{-1} = g_k^{-1} * \cdots * g_2^{-1} * g_1^{-1}.$$

Dessa forma pode-se provar que vale para $n = k + 1$, ou seja:

$$\begin{aligned}(g_1 * g_2 * \cdots * g_k * g_{k+1})^{-1} &= ((g_1 * g_2 * \cdots * g_k) * g_{k+1})^{-1} \\ &= g_{k+1}^{-1} * (g_1 * g_2 * \cdots * g_k)^{-1} \\ &= g_{k+1}^{-1} * g_k^{-1} * \cdots * g_2^{-1} * g_1^{-1}.\end{aligned}$$

Logo, vale para $n = k + 1$. Portanto, a igualdade é verdadeira.

Definição 3.5. Seja $(G, *)$ em grupo. A n-ésima potência de $g \in G$ é definida por $g^n = \underbrace{g * g * \cdots * g}_{n \text{ fatores } g}$, com $n \in \mathbb{N}^*$.

Definição 3.6. Seja $(G, *)$ um grupo e g um elemento qualquer de G. A ordem do elemento g é o menor inteiro m, se existir, para o qual $g^m = e$.

Definição 3.7. A ordem do grupo $(G, *)$ é a quantidade de elementos que o grupo contém, denotado por $o(G) = |G|$.

3.3 SUBGRUPO

Definição 3.8. Sejam $(G, *)$ um grupo com unidade e tal que $H \subseteq G$. Se H é um grupo com a operação $*$, então H é subgrupo de G e a notação é $H \leq G$.

Definição 3.9. H se define como:

1. **Subgrupo trivial:** se $H = \{e\}$ ou $H = G$;
2. **Subgrupo próprio:** se $H \neq G$.

Teorema 3.2. *Seja $(G, *)$ grupo, cujo elemento neutro é e. Suponha que $H \subseteq G$. H é um subgrupo de G, se e somente se,*

1. *H é fechado para $*$.*
2. *$e \in H$.*
3. *$\forall\ a \in H \Rightarrow a^{-1} \in H$.*

Demonstração. ($\Rightarrow$) Por hipótese, $H \leq G$, portanto H também é grupo, e:

1. Por definição H é um conjunto fechado para a operação $*$;
2. Seja e' o elemento neutro em H, então

$$e' * h = h = h * e' \ \forall h \in H.$$

   Como $H \subseteq G$, segue que $h \in G$ e sendo e o elemento neutro de G, segue que

$$e * h = h = h * e.$$

   Nota-se que $e' * h = h = e * h$. Utilizando a lei do cancelamento, tem-se

$$\begin{aligned} e' * h &= e * h \\ e' &= e. \end{aligned}$$

   Portanto, $e \in H$.

3. Por definição de grupo, todo elemento de H possui elemento inverso em H.

($\Leftarrow$) Por hipótese, $H \subseteq G$ sendo G um grupo. Para provar que H é subgrupo de G, basta mostrar que H também é grupo, portanto deve ser ser associativo, possuir elemento neutro e possuir elemento inverso para cada elemento de H. Por (1), H é fechado para a operação $*$ e, pelo fato de H ser subconjunto do grupo G, H é associativo. Tem-se que $e \in G$ também está em H, logo, H possui elemento neutro. Finalmente, para cada $h \in H$, há um elemento inverso $h^{-1} \in H$. Portanto, H é grupo e $H \leq G$. ■

Exemplo 3.3.1. $n\mathbb{Z}$ é subgrupo de $(\mathbb{Z}, +)$.
Observe que $n\mathbb{Z} = \{n \cdot a : n \in \mathbb{N} \text{ e } a \in \mathbb{Z}\}$ e que $n \cdot a \in \mathbb{Z}$ portanto $n\mathbb{Z} \subseteq \mathbb{Z}$.
Utilizando o teorema anterior, segue que:

(i) $n\mathbb{Z}$ é um conjunto fechado para a soma, pois $n \cdot a + n \cdot b = n(a + b)$ e $n \in \mathbb{N}$ e $a + b \in \mathbb{Z}$.

(ii) Seja $n0$ o elemento neutro de $n\mathbb{Z}$, pois $n0 + na = n(0 + a) = na = n(a + 0) = na + n0$.

(iii) Seja $-na = n \cdot (-a)$ o elemento oposto de na, pois $-na + na = n(-a) + na = n(-a + a) = n \cdot 0 = n(a - a) = na - na = na + (-na)$.

Pelos itens acima provados, conclui-se que $n\mathbb{Z}$ é subgrupo de $\mathbb{Z}$.

Definição 3.10. Seja G um grupo e $H \leq G$. Dado $g \in G$:

(i) $gH = \{g * h : h \in H\}$ é uma classe lateral à esquerda de H em G.

(ii) $Hg = \{h * g : h \in H\}$ é uma classe lateral à direita de H em G.

Definição 3.11. Seja G um grupo. H é dito subgrupo normal de G se as classes laterais à esquerda e à direita de H em G coincidem.
Notação: $H \trianglelefteq G$.

Proposição 3.3. *Todo grupo abeliano possui apenas subgrupos normais.*

Demonstração. Sejam H e G grupos tais que $H \leq G$, $h \in H$ e $g \in G$. Então:

$$\begin{aligned} gH &= \{g * h : h \in H\} \\ &= \{h * g : h \in H\} \\ &= Hg. \end{aligned}$$

Como $h \in H$, conclui-se que $H \trianglelefteq G$. ■

Definição 3.12. Sejam G um grupo e H um subgrupo normal de G. Define-se G/H como **grupo quociente**, o conjunto das classes laterais de H. Ou seja:

$$G/H = \{aH : a \in G\}.$$

Exemplo 3.3.2. Sejam o grupo $(\mathbb{Z}, +)$ e seu subgrupo $(2\mathbb{Z}, +)$. Como $\mathbb{Z}$ é abeliano, $2\mathbb{Z}$ é subgrupo normal.
Os elementos são da forma:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

$$2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}.$$

As classe laterais de $2\mathbb{Z}$ são:

$$\begin{aligned} 1 + 2\mathbb{Z} &= \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\} \\ 2 + 2\mathbb{Z} &= \{\ldots, -4, -2, 0, 2, 4, \ldots\}. \end{aligned}$$

Logo, o grupo quociente é

$$\mathbb{Z}/2\mathbb{Z} = \{1 + 2\mathbb{Z}, 2 + 2\mathbb{Z}\}.$$

3.4 ISOMORFISMOS DE GRUPOS

Definição 3.13. Sejam G e H grupos e a função $\lambda : G \to H$ tal que para todo $g, h \in G$:

$$\lambda(g * h) = \lambda(g) * \lambda(h).$$

Então λ é chamado de **homomorfismo**.

Exemplo 3.4.1. Sejam o grupo aditivo $\mathbb{Z}$ e a função

$$\begin{array}{rcl} \lambda : \mathbb{Z} & \to & \mathbb{Z} \\ x & \mapsto & 2x \end{array}$$

para todo $x \in \mathbb{Z}$. Provar-se-á que λ é um homomorfismo injetor. Sejam $x, y \in \mathbb{Z}$, então:

1. $\lambda(x+y) = 2 \cdot (x+y) = 2x + 2y = \lambda(x) + \lambda(y)$;
2. $\lambda(x) = \lambda(y) \Rightarrow 2x = 2y \Rightarrow x = y$.

Portanto, está provado que λ é um homomorfismo injetor.

Definição 3.14. Se λ é bijetora e também um homomorfismo, então λ é chamado de **isomorfismo**.

Definição 3.15. Sejam G um grupo e a função $\lambda : G \to G$:

- Se λ é homomorfismo, então λ é chamado de endorfismo;
- Se λ é isomorfismo, então λ é chamado de automorfismo.

4 ANÉIS DE GRUPO

4.1 ANÉIS DE GRUPO

Definição 4.1. Sejam G um grupo e A um anel tais que $g \in G$ e $a_g \in A$. Define-se o conjunto AG como

$$AG = \left\{ \sum_{g \in G} a_g \delta_g : a_g \in A \text{ e } a_g \neq 0 \text{ finitas vezes} \right\}.$$

Dois elementos $\sum_{g \in G} a_g \delta_g$ e $\sum_{h \in G} b_h \delta_h$ de AG são iguais quando $a_g = b_g$ para todo $g \in G$.
Nota-se que os elementos de AG são da forma:

$$\sum_{g \in G} a_g \delta_g = a_{g_1} \delta_{g_1} + a_{g_2} \delta_{g_2} + \ldots + a_{g_n} \delta_{g_n},$$

portanto, em alguns momentos deste capítulo, um elemento deste conjunto estará escrito como $\sum_{g \in G} a_g \delta_g$ ou como

$$a_{g_1} \delta_{g_1} + a_{g_2} \delta_{g_2} + \ldots + a_{g_n} \delta_{g_n}.$$

Proposição 4.1. *O conjunto AG é anel com as seguintes operações:*

$$+ : \quad \sum_{g \in G} a_g \delta_g + \sum_{h \in G} b_h \delta_h = \sum_{g \in G} (a_g + b_g) \delta_g$$

$$\cdot : \quad \left(\sum_{g \in G} a_g \delta_g \right) \cdot \left(\sum_{h \in G} b_h \delta_h \right) = \sum_{g,h \in G} (a_g \cdot b_h) \delta_{gh}.$$

Demonstração. Sejam $\sum_{g \in G} a_g \delta_g, \sum_{h \in G} b_h \delta_h, \sum_{i \in G} c_i \delta_i \in AG$. Para que AG seja anel, deve satisfazer as seguintes propriedades:

1. Associatividade da soma

$$\begin{aligned}\left(\sum_{g\in G} a_g\delta_g + \sum_{h\in G} b_h\delta_h\right) &+ \sum_{i\in G} c_i\delta_i \\ &= \sum_{g\in G}(a_g+b_g)\delta_g + \sum_{i\in G} c_i\delta_i \\ &= \sum_{g\in G}[(a_g+b_g)+c_g]\delta_g \\ &= \sum_{g\in G}[a_g+(b_g+c_g)]\delta_g \\ &= \sum_{g\in G} a_g\delta_g + \sum_{g\in G}(b_h+c_h)\delta_h \\ &= \sum_{g\in G} a_g\delta_g + \left(\sum_{g\in G} b_h\delta_h + \sum_{g\in G} c_i\delta_i\right)\end{aligned}$$

2. Comutatividade da soma

$$\begin{aligned}\sum_{g\in G} a_g\delta_g + \sum_{h\in G} b_h\delta_h &= \sum_{g\in G}(a_g+b_g)\delta_g \\ &= \sum_{g\in G}(b_g+a_g)\delta_g \\ &= \sum_{h\in G} b_h\delta_h + \sum_{g\in G} a_g\delta_g.\end{aligned}$$

3. Existência do elemento neutro
   Seja 0 o elemento neutro de A, então:

$$\sum_{g\in G} a_g\delta_g + \sum_{h\in G} 0\delta_h = \sum_{g\in G}(a_g+0)\delta_g = \sum_{g\in G} a_g\delta_g.$$

   Portanto, $\sum_{h\in G} 0\delta_h$ é o elemento neutro de AG. Pelo item 2 provado acima, AG possui comutatividade na soma, então

$$\sum_{g\in G} a_g\delta_g + \sum_{h\in G} 0\delta_h = \sum_{h\in G} 0\delta_h + \sum_{g\in G} a_g\delta_g = \sum_{g\in G} a_g\delta_g.$$

4. Existência do elemento oposto

   Seja $\sum_{g\in G} a_g\delta_g \in AG$, então $\sum_{g\in G}(-a_g)\delta_g \in AG$ é seu elemento oposto:

$$\sum_{g\in G} a_g\delta_g + \sum_{g\in G}(-a_g)\delta_g = \sum_{g\in G}[a_g + (-a_g)]\delta_g = \sum_{g\in G} 0\delta_g.$$

5. Associatividade do produto

$$\begin{aligned}
& \sum_{g\in G} a_g\delta_g \cdot \left(\sum_{h\in G} b_h\delta_h \cdot \sum_{i\in G} c_i\delta_i\right) \\
= & \sum_{g\in G} a_g\delta_g \cdot \sum_{h,i\in G} (b_h \cdot c_i)\delta_{hi} \\
= & \sum_{g,h,i\in G} [a_g \cdot (b_h \cdot c_i)]\delta_{g(hi)} \\
= & \sum_{g,h,i\in G} [(a_g \cdot b_h) \cdot c_i]\delta_{(gh)i} \\
= & \sum_{g,h\in G} (a_g \cdot b_h)\delta_{gh} \cdot \sum_{i\in G} c_i\delta_i \\
= & \left(\sum_{g\in G} a_g\delta_g \cdot \sum_{h\in G} b_h\delta_h\right) \cdot \sum_{i\in G} c_i\delta_i.
\end{aligned}$$

6. Propriedade distributiva

$$\begin{aligned}
& \sum_{g\in G} a_g\delta_g \cdot \left(\sum_{h\in G} b_h\delta_h + \sum_{i\in G} c_i\delta_i\right) \\
= & \sum_{g\in G} a_g\delta_g \cdot \sum_{h\in G} (b_h + c_h)\delta_h \\
= & \sum_{g,h\in G} [a_g \cdot (b_h + c_h)]\delta_{gh} \\
= & \sum_{g,h\in G} (a_g \cdot b_h + a_g \cdot c_h)\delta_{gh} \\
= & \sum_{g,h\in G} (a_g \cdot b_h)\delta_{gh} + \sum_{g,i\in G} (a_g \cdot c_i)\delta_{gi} \\
= & \sum_{g\in G} a_g\delta_g \cdot \sum_{h\in G} b_h\delta_h + \sum_{g\in G} a_g\delta_g \cdot \sum_{i\in G} c_i\delta_i.
\end{aligned}$$

Pelo fato de não ser necessariamente comutativo no produto, prova-se analogamente que

$$\left(\sum_{g\in G} a_g\delta_g + \sum_{h\in G} b_h\delta_h\right) \cdot \sum_{i\in G} c_i\delta_i =$$

$$\sum_{g\in G} a_g\delta_g \cdot \sum_{i\in G} c_i\delta_i + \sum_{h\in G} b_h\delta_h \cdot \sum_{i\in G} c_i\delta_i.$$

Assim, conclui-se que AG é anel. ■

Proposição 4.2. *Seja A um anel comutativo e G grupo abeliano então o anel de grupo AG é comutativo.*

Demonstração. Se $A = \{0\}$ então AG é anel comutativo. Suponha então que A tenha mais de um elemento.
Sejam os elementos de AG, $\sum_{g\in G} a_g\delta_g$ e $\sum_{h\in G} b_h\delta_h$. Então:

$$\left(\sum_{g\in G} a_g\delta_g\right) \cdot \left(\sum_{h\in G} b_h\delta_h\right) = \sum_{g,h\in G} (a_g \cdot b_h)\delta_{gh}.$$

Por definição, $a_g, b_h \in A$ e $g, h \in G$ e por hipótese, A é comutativo e G é abeliano, então segue que:

$$\sum_{g,h\in G}(a_g \cdot b_h)\delta_{gh} = \sum_{g,h\in G}(b_h \cdot a_g)\delta_{hg} = \left(\sum_{h\in G} b_h\delta_h\right)\cdot\left(\sum_{g\in G} a_g\delta_g\right).$$

Portanto, AG é anel comutativo. ■

A recíproca desta proposição, vale com uma condição sobre o anel A.

Proposição 4.3. *Seja A um anel com pelo menos, um elemento $p \neq 0$ tal que $p^2 \neq 0$. Se AG é comutativo então A é comutativo e G é abeliano.*

Demonstração. Se A possui apenas um elemento, obviamente é comutativo. Suponha então, que A possua mais de um elemento. Sejam $a, b \in A$ e $e \in G$ o elemento neutro de G.

(i) $(a\delta_e)\cdot(b\delta_e) = ab\delta_e$

(ii) $(b\delta_e)\cdot(a\delta_e) = ba\delta_e$.

Como AG é um anel comutativo, então

$$ab\delta_e = ba\delta_e,$$

ou seja, $ab = ba$. Portanto, A é anel comutativo.
Resta provar que G é grupo abeliano. Sejam g, h dois elementos de G e $0 \neq p \in A$ tal que $p^2 \neq 0$. Sejam $p\delta_g$ e $p\delta_h$ em AG. Então

(i) $(p\delta_g)\cdot(p\delta_h) = p^2\delta_{gh}$;

(ii) $(p\delta_h)\cdot(p\delta_g) = p^2\delta_{hg}$;

Por hipótese AG é comutativo, então $gh = hg$ e conclui-se que G é grupo abeliano. ■

Proposição 4.4. *Se A é anel com unidade então o anel de grupo AG possui unidade.*

Demonstração. Seja 1 a unidade em A. Então a unidade de AG é $1\delta_e$ pois

$$\begin{aligned}(1\delta_e)\cdot\sum_{h\in G}a_h\delta_h &= \sum_{h\in G}(1a_h)\delta_{eh}\\ &= \sum_{h\in G}a_h\delta_h\\ &= \sum_{h\in G}(a_h1)\delta_h\\ &= \sum_{h\in G}a_h\delta_h\cdot(1\delta_e).\end{aligned}$$

Logo, está provado que AG possui unidade. ■

Proposição 4.5. *Se AG possui unidade, então A também possui unidade.*

Demonstração. Seja $\sum_{h\in G}b_h\delta_h$ a unidade de AG. Provar-se-á que b_e é a unidade do anel A. Seja $a\in A$:

$$(i)\ a\delta_e=\left(\sum_{h\in G}b_h\delta_h\right)\cdot(a\delta_e)=\sum_{h\in G}(b_h\cdot a)\delta_h$$

$$\Rightarrow a\delta_e=\sum_{h\in G}(b_h\cdot a)\delta_h$$

$$\Rightarrow b_ha=0\ \forall\ h\in G\setminus\{e\}\text{ e }b_ea=a.$$

$$(ii)\ a\delta_e=(a\delta_e)\cdot\left(\sum_{h\in G}b_h\delta_h\right)=\sum_{h\in G}(a\cdot b_h)\delta_h$$

$$\Rightarrow a\delta_e=\sum_{h\in G}(a\cdot b_h)\delta_h$$

$$\Rightarrow ab_h=0\ \forall\ h\in G\setminus\{e\}\text{ e }ab_e=a.$$

Logo, A possui b_e como unidade. ■

Proposição 4.6. *Se o anel de grupo AG não possui divisores de zero, então A é anel sem divisores de zero.*

Demonstração. Sejam $a, b \in A$ tal que $a \cdot b = 0_A$. Para que A não possua divisores de zero, $a = 0_A$ ou $b = 0_A$.
Então:

$$(a\delta_e) \cdot (b\delta_e) = ab\delta_e = 0_A\delta_e = \sum_{g \in G} 0\delta_g.$$

Como AG não possui divisores de zero, segue que:

$$a\delta_e = 0_A\delta_e$$

ou

$$b\delta_e = 0_A\delta_e$$

então $a = 0_A$ ou $b = 0_A$. Portanto, A não possui divisores de zero. ■

Observação 4. Seja A anel com unidade 1 e G grupo com um elemento g de ordem finita $m > 1$. Então:

$$\begin{aligned}
& (1\delta_e + (-1)\delta_g) \cdot (1\delta_e + 1\delta_g + 1\delta_{g^2} + \ldots + 1\delta_{g^{m-1}}) \\
= \; & 1\delta_e + 1\delta_g + (-1)\delta_g + 1\delta_{g^2} + (-1)\delta_{g^2} + \ldots \\
& + 1\delta_{g^{m-1}} + (-1)\delta_{g^{m-1}} + (-1)\delta_{g^m} \\
= \; & 1\delta_e + (-1)\delta_e \\
= \; & (1-1)\delta_e \\
= \; & 0\delta_e.
\end{aligned}$$

De acordo com esse contra-exemplo, conclui-se que AG pode ter divisores de zero, mesmo que A não tenha.

Proposição 4.7. *Seja A um anel com unidade. Se AG tem elemento inverso multiplicativo então o anel A também possui elemento inverso.*

Demonstração. Seja $a \in A$ um elemento não nulo. Assim, $a\delta_e$ tem inverso $\sum_{h \in G} b_h\delta_h$. Logo, como $1_A\delta_e$ é unidade em AG,

$$1_A\delta_e = (a\delta_e) \cdot \left(\sum_{h \in G} b_h\delta_h \right) = \sum_{h \in G} ab_h\delta_h$$

$$\Rightarrow ab_e = 1.$$

Da mesma forma prova-se que $b_e a = 1$. Portanto, o elemento a possui inverso. ■

A recíproca da Proposição 4.7. nem sempre vale. Utilizando a Observação 4.1, tem-se que o anel de grupo AG possui divisores de zero, e pela Proposição 2.6. conclui-se que este anel possui elementos sem inverso, devido a sua contra-positiva.

4.2 SUBANÉIS DE ANÉIS DE GRUPO

Proposição 4.8. *Seja G um grupo com elemento neutro e. Sejam A, B anéis tais que $A \leq B$. Então, $AG \leq BG$.*

Demonstração. Para provar que $AG \leq BG$, será utilizada a Proposição 2.7:

(i) AG é não vazio, pois $0_A \delta_e \in AG$.

(ii) A soma com o oposto também está em AG:

$$\sum_{g \in G} a_g \delta_g - \sum_{h \in G} b_h \delta_h = \sum_{g \in G} (a_g - b_g)\delta_g \in AG$$

pois $a_g - b_g \in A, \forall\ g \in G$.

(iii) O produto está em AG:

$$\left(\sum_{g \in G} a_g \delta_g\right) \cdot \left(\sum_{h \in G} b_h \delta_h\right) = \sum_{g,h \in G} (a_g \cdot b_h)\delta_{gh}$$

pois $gh \in G$ e $a_g b_h \in A$.

Pelos itens acima demonstrados, conclui-se que $AG \leq BG$. ■

Proposição 4.9. *Sejam A um anel e G, H grupos tais que $G \leq H$. Então $AG \leq AH$.*

Demonstração. Para provar que $AG \leq AH$, será utilizada a Proposição 2.7. Sendo e o elemento neutro de G:

(i) AG é não vazio, pois $0_A\delta_e \in AG$.

(ii) A soma com o oposto também está em AG:

$$\sum_{g\in G} a_g\delta_g - \sum_{h\in G} b_h\delta_h = \sum_{g\in G}(a_g - b_g)\delta_g$$

pois $a_g - b_g \in A$ e $g \in G$.

(iii) O produto está em AG:

$$\left(\sum_{g\in G} a_g\delta_g\right)\cdot\left(\sum_{h\in G} b_h\delta_h\right) = \sum_{g,h\in G}(a_g \cdot b_h)\delta_{gh}$$

pois $gh \in G$ e $a_g b_h \in A$.

Pelos itens acima demonstrados, conclui-se que $AG \leq AH$. ■

4.3 ISOMORFISMOS DE ANÉIS DE GRUPO

Teorema 4.10. *Sejam A e B anéis e G e H grupos. Se A é isomorfo a B e G é isomorfo a H então AG e BH são isomorfos.*

Demonstração. Sejam $r : A \longrightarrow B$ e $s : G \longrightarrow H$ os respectivos isomorfismos. Ou seja, r e s são homomorfismos bijetores de modo que

- $r(a + b) = r(a) + r(b)$ e $r(a \cdot b) = r(a) \cdot r(b)$;
- $s(g * h) = s(g) * s(h)$,

para $a, b \in A$ e $g, h \in G$.
O objetivo dessa demonstração é provar que os anéis AG e BH

são isomorfos utilizando as hipóteses acima.
Seja $\sigma : AG \longrightarrow BH$ tal que

$$\sigma\left(\sum_{g\in G} a_g\delta_g\right) = \sum_{s(g)\in H} r(a_g)\delta_{s(g)}.$$

Primeiramente, será provado que σ é um homomorfismo. Sejam $\sum_{g\in G} a_g\delta_g, \sum_{h\in G} b_h\delta_h \in AG$, por definição,

$$\sum_{g\in G} a_g\delta_g + \sum_{h\in G} b_h\delta_h = \sum_{g\in G}(a_g + b_g)\delta_g$$

e nota-se que $s(G) = H$, pois S é sobrejetora. Além disto,

$$\left(\sum_{g\in G} a_g\delta_g\right)\cdot\left(\sum_{h\in G} b_h\delta_h\right) = \sum_{g,h\in G}(a_g \cdot b_h)\delta_{gh}.$$

(i) Para a soma do homomorfismo:

$$\begin{aligned}\sigma\left(\sum_{g\in G} a_g\delta_g + \sum_{h\in G} b_h\delta_h\right) &= \sigma\left(\sum_{g\in G}(a_g + b_g)\delta_g\right)\\ &= \sum_{s(g)\in H} r(a_g + b_g)\delta_{s(g)},\end{aligned}$$

como r é homomorfismo, segue que

$$\begin{aligned}\sum_{s(g)\in H} r(a_g + b_g)\delta_{s(g)} &= \sum_{s(g)\in H}\left(r(a_g) + r(b_g)\right)\delta_{s(g)}\\ &= \sum_{s(g)\in H} r(a_g)\delta_{s(g)} + \sum_{s(h)\in H} r(b_h)\delta_{s(h)}\\ &= \sigma\left(\sum_{g\in G} a_g\delta_g\right) + \sigma\left(\sum_{h\in G} b_h\delta_h\right).\end{aligned}$$

(ii) Para o produto do homomorfismo:

$$\begin{aligned}\sigma\left[\left(\sum_{g\in G} a_g\delta_g\right)\cdot\left(\sum_{h\in G} b_h\delta_h\right)\right] &= \sigma\left(\sum_{g,h\in G}(a_g \cdot b_h)\delta_{gh}\right)\\ &= \sum_{g,h\in G} r(a_g \cdot b_h)\delta_{s(gh)},\end{aligned}$$

como r e s são homomorfismos, segue que

$$\begin{aligned}\sum_{g,h\in G} r(a_g \cdot b_h)\delta_{s(gh)} &= \sum_{s(g),s(h)\in H} (r(a_g)\cdot r(b_h))\,\delta_{s(g)s(h)} \\ &= \sum_{s(g)\in H} r(a_g)\delta_{s(g)} \cdot \sum_{s(h)\in H} r(b_h)\delta_{s(h)} \\ &= \sigma\left(\sum_{g\in G} a_g\delta_g\right)\cdot\sigma\left(\sum_{h\in G} b_h\delta_h\right).\end{aligned}$$

Por (i) e (ii) está provado que σ é homomorfismo.
Agora, será provado que σ é bijetor, e para que seja bijetor, σ deve ser injetor e sobrejetor.

(i) Supõe-se que

$$\sigma\left(\sum_{g\in G} a_g\delta_g\right) = \sigma\left(\sum_{h\in G} b_h\delta_h\right).$$

ou seja,

$$\sum_{s(g)\in H} r(a_g)\delta_{s(g)} = \sum_{s(h)\in H} r(b_h)\delta_{s(h)},$$

dessa forma, sempre que $s(g) = s(h)$, deve-se ter $r(a_g) = r(b_h)$. Como r e s são funções injetoras, segue que

$$\begin{aligned} s(g) = s(h) &\Rightarrow g = h, \\ r(a_g) = r(b_h) &\Rightarrow a_g = b_h = b_g.\end{aligned}$$

Logo, $\sum_{g\in G} a_g\delta_g = \sum_{h\in G} b_h\delta_h$, assim conclui-se que σ é injetor.

(ii) Admite-se que

$$\sum_{j\in G} a_j\delta_j = \sigma\left(\sum_{s^{-1}(j)\in H} r^{-1}(a_j)\delta_{s^{-1}(j)}\right).$$

De fato:

$$\sigma\left(\sum_{s^{-1}(j)\in H} r^{-1}(a_j)\delta_{s^{-1}(j)}\right) = \sum_{s(s^{-1}(j))\in H} r\left(r^{-1}(a_j)\right)\delta_{s(s^{-1}(j))}$$
$$= \sum_{j\in G} a_j\delta_j$$

pois como r e s são bijetoras:

$$\exists \quad s^{-1}(j) \in G : s \circ s^{-1}(j) = j, \ \forall \ j \in H$$
$$\text{e} \quad \exists \quad r^{-1}(a_j) \in A : r \circ r^{-1}(a_j) = a_j, \ \forall \ a_j \in B.$$

Desse modo, conclui-se que σ é sobrejetor.
Por (i) e (ii) conclui-se que σ é bijetor. Portanto, como é homomorfismo bijetor, está provado que σ é isomorfismo.

■

Corolário 4.11. *Sejam A e B anéis e G um grupo. Se A é isomorfo a B então AG e BG são isomorfos.*

Demonstração. Nota-se que a identidade é isomorfismo entre G e G. Como consequência do teorema, AG e BG são isomorfos. ■

Corolário 4.12. *Sejam G e H grupos e A um anel. Se G e H são isomorfos, então AG é isomorfo a AH.*

Demonstração. Nota-se que a identidade é isomorfismo entre A e A. Portanto, AG e AH são isomorfos. ■

5 CONSIDERAÇÕES FINAIS

Como foco no objetivo em todo momento, o trabalho possibilitou um excelente estudo sobre anéis de grupos e possibilitará que outros estudantes brasileiros possam desfrutar do mesmo estudo em sua língua materna. Ao longo da pesquisa para produção deste trabalho, pude conhecer não somente as definições de anel de grupo como também sua história.

Ainda não se tem uma resposta completa sobre a recíproca do Teorema 4.3, do Capítulo 3, que trata sobre o isomorfismo entre dois anéis A e B e entre dois grupos G e H dado que os anéis de grupo AG e BH são isomorfos. Sua origem data em 1940, quando Graham Higman defendeu sua tese de pós-doutorado intitulada "The units of group-rings".

Já em 1947, esse questionamento se tornou oficialmente o problema do isomorfismo, problema que até hoje não foi demonstrado.

No entanto, observa-se que é um assunto recente e por este motivo, a quantidade de resultados é limitada. No Brasil, são famosos os nomes Polcino Milies e Jairo Gonçalves, ambos da Universidade de São Paulo.

Contudo, o objetivo geral deste trabalho foi alcançado, foi possível construir as demonstrações necessárias e fundamentais para um bom entendimento das suas definições e proposições. E desta forma, proporciona para o leitor uma visão abrangente sobre toda a teoria de anéis, grupos e anéis de grupos.

REFERÊNCIAS

[1] David S. Dummit & Richard M. Foote. *Abstract algebra*. 3ª ed. New Jersey: Jhon Wiley & Sons, 2004, p. 935.

[2] Hygino H. Domingues e Gelson Iezzi. *Álgebra Moderna*. 5ª ed. Saraiva Educação. São Paulo: Saraiva, 2018, p. 408.

[3] Adilson Gonçalves. *Introdução à álgebra*. 5ª ed. Projeto Euclides. Rio de Janeiro: IMPA, 2013, p. 194.

[4] Paulo A. Martin. *Grupos, corpos e teoria de Galois*. 1ª ed. Coleção textos universitários do IME-USP. São Paulo: Editora Livraria da Física, 2010, p. 430.

[5] César Polcino Milies e Sudarshan K. Sehgal. *An Introduction to Group Rings*. 1ª ed. Algebras and applications. Holanda: KLUWER ACADEMIC PUBLISHERS, 2002, p. 371.

[6] Arnaldo Garcia e Yves Lequain. *Elementos de álgebra*. 5ª ed. Projeto Euclides. Rio de Janeiro: IMPA, 2015, p. 326.