Universidade Estadual da Paraíba
Centro de Ciências e Tecnologia
Departamento de Matemática

Os Teoremas dos Ismorfismos para Anéis

José Maria de Queiroz Aires

Trabalho de Conclusão de Curso

Orientador: **Prof. Dr. Vandenberg Lopes Vieira**

Banca Examinadora:
Prof. Dr. Vandenberg Lopes Vieira - DM/UEPB
Prof. Dr. Juarez Dantas de Souza - DM/UEPB
Prof. Dra. Maria Isabelle Silva - DM/UEPB

Trabalho de Conclusão de Curso apresentado na Universidade Estadual da Paraíba, como parte dos requisitos exigidos para a obtenção do título de Licenciado em Matemática.

05 de Agosto 2013
Campina Grande - PB

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL – UEPB

A298t Aires, José Maria de Queiroz.

Os teoremas dos isomorfismos para anéis [manuscrito] / José Maria de Queiroz Aires. – 2013.

47 f.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Matemática) – Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2013.

"Orientação: Prof. Dr. Vandenberg Lopes Vieira, Departamento de Matemática".

1. Teoria dos Anéis. 2. Teoria dos Grupos. 3. Isomorfismo. I. Título.

21. ed. CDD 512.5

JOSÉ MARIA DE QUEIROZ AIRES

OS TEOREMAS DOS ISOMORFISMOS PARA ANÉIS

Monografia apresentada no Curso de Licenciatura Plena em Matemática da Universidade Estadual da Paraíba, em cumprimento às exigências para obtenção do Título de Licenciado em Matemática.

BANCA EXAMINADORA

Prof. Dr. Vandenberg Lopes Vieira
Departamento de Matemática – CCT/UEPB
Orientador

Maria Isabelle Silva

Profª. Drª. Maria Isabelle Silva
Departamento de Matemática – CCT/UEPB
Examinadora

Prof. Dr. Juarez Dantas de Souza
Departamento de Matemática – CCT/UEPB
Examinador

Campina Grande, 05 de Agosto de 2013

Aos meus pais, Mário e Maria.

DEDICO

Agradecimentos

A Deus e a todos que, além de saúde, paz e força me concede também a sabedoria necessária para alcançar mais esse objetivo em minha vida.

Aos meus pais José Aires e Maria Queiroz e aos meus irmãos Luciana Aires, Luciano Queiroz, Tarciano Aires e Juliana Queiroz, por terem me ensinado alguns princípios básicos na formação de um indivíduo (valores), nos quais foco pra ser uma pessoa, um filho, um aluno, um professor cada vez melhor.

Aos amigos e amigas, exclusivamente aos colegas Ana Flávia, Diego Sarmento, Francicleide Borges, Ikiara Farias, Manoel Luiz, que de uma forma ou de outra contribuíram apoiando, torcendo, lutando junto e sonhando em prol deste momento.

A todos os professores da alfabetização, do ensino fundamental, médio e superior, que além de conhecimento, me proporcionavam também a construção do gosto por esta profissão que pretendo seguir. Em particular, vale a lembrança aos mestres Aldo Trajano, Elizabeth Maracajá, Fernando Luiz, Francisco Sá, Marcelino Batista, Maria Batista e Onildo Freire, todos, professores de Matemática.

Ao meu orientador, Professor Vandenberg Lopes Vieira pelas suas sugestões, paciência e pelo incentivo dado durante toda a elaboração deste trabalho, bem como durante todo o tempo que passei cursando nesta instituição.

A todos aqueles que direta ou indiretamente contribuíram para a realização deste trabalho.

Meu muito obrigado!

Resumo

Neste trabalho, são apresentados resultados básicos sobre a Teoria dos Anéis, teoria essa que estuda as estruturas algébricas mais gerais com duas operações binárias. Tais resultados têm como foco principal os Teoremas de Isomorfismos para Anéis. Tais teoremas são uma forma de se estabelecer algumas identificações algébricas entre anéis, desde que um desses seja um anel quociente. Inicialmente, foram apresentados resultados importantes sobre a Teoria dos Grupos, os quais servem de suporte para àqueles apresentados sobre anéis.

Palavras-chave: Grupos, Anéis, Isomorfismo.

Sumário

Capítulo 1

Introdução

A Álgebra Moderna é o ambiente de estudo das estruturas algébricas[1], dentre as quais, se destacam de modo especial *grupo*, *anel* e *corpo*. Essas estruturas têm aplicações em vários ramos científicos, tais como a Matemática, a Química, a Informática, por exemplo. Dentre essas aplicações podemos citar a Criptografia na segurança da internet, que estuda os métodos para codificar uma mensagem, de maneira que apenas o legítimo destinatário consiga interpretá-la, a Teoria dos Códigos, que dedica-se ao estudo das formas organizadas de se acrescentar algum dado adicional a cada informação que se deseja transmitir ou armazenar, a Teoria das Simetrias, que é muito útil para a cristalografia e à física teórica que se baseia na álgebra de Lie. Vale ressaltar que nem todas essas aplicações são estudadas num curso de graduação, nem encontradas em livros introdutórios, pois precisam de um aprofundamento maior.

A Teoria dos Grupos surgiu a partir de diversos estudos a fim de provar se equações algébricas de qualquer grau são resolúveis por radicais. Já era sabido que as de grau um e dois possuíam um método denominado de fórmula de Bhaskara que gerava suas soluções. Quanto às de grau três, entre 1500 e 1515, o matemático italiano Scipione Del Ferro (1456-1526) descobriu um procedimento para resolver a equação cúbica

$$x^3 + px = q, \quad \text{com} \quad (p, q > 0)\,,$$

[1]Uma estrutura algébrica é um conjunto $\mathcal{A}$ não-vazio com uma ou mais operações.

ou nos tempos atuais

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} - \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}},$$

O que gerou vários estudos a fim de provar essa questão da resolubilidade citada acima.

Por volta de meados do século XVIII, o matemático Joseph-Louis Lagrange (1736-1813) começou a dar um norte a esse problema ao usar a teoria das permutações envolvendo as raízes da equação. Em 1824, o matemático norueguês Niels Henrik Abel (1802-1829) prova todas as conjecturas de Lagrange no que concerne a não haver nenhuma fórmula geral por radicais para resolver as equações de grau maior ou igual a 5. Mas, um questionamento ainda despertava interesse: por que as equações de grau maior ou igual a 5 não são, de modo geral, resolúveis por radicais, mais alguns tipos o são, como já se sabia bem antes de Abel? E o que caracterizava matematicamente essas ultimas? As respostas vêm com o matemático Francês Evariste Galois (1811-1832), que em sua obra aparece pela primeira vez o conceito de grupo, inclusive com essa nomenclatura. Resumidamente, o que Galois fez foi associar a cada equação um grupo formado por permutações de suas raízes e condicionar a resolubilidade por radicais a uma propriedade desse grupo. E como para toda equação de grau menor ou igual a 4 o grupo de permutações que lhe é associado goza dessa propriedade e para $n > 4$ sempre há equações cujo grupo não a satisfaz, a questão da resolubilidade por radicais estava por fim esclarecida.

O conceito algébrico de Ideais foi proposto primeiramente por Dedekind em 1876 na terceira edição do seu livro Vorlesungen über Zahlentheorie (Seminários em Teoria dos Números). Eles foram uma generalização para o conceito de número ideal desenvolvido por Ernst Kummer. Mais tarde o conceito foi expandido por David Hilbert e especialmente por Emmy Noether.

Contudo, novas estruturas algébricas ainda estavam por vir. Após várias tentativas de organização lógica, e de axiomatizar a álgebra, um delas feita pelo matemático Benjamin Peacock (1791-1858), publicada em 1830, vieram as ideias do irlandês R. Hamilton (1805-1865) que se engajou na tarefa de criar um sistema numérico que de-

sempenhasse no espaço tridimensional o mesmo papel, algebricamente falando, que o sistema dos números complexos desempenha no espaço bidimensional (o plano). Passando dez anos de estudos, ele descobriu que estes novos números tinha que ser do tipo

$$a + bi + cj + dk, \quad \text{com} \quad i^2 = j^2 = k^2 = -1$$

e que teria que abrir mão da comutatividade da multiplicação. A criação desses novos números, denominado de *quaternions*, mostrou que as leis clássicas da álgebra podem não ser aplicáveis em certos casos. Desse trabalho de Hamilton e de outras colaborações, já no século XIX, surgiram várias "novas estruturas algébricas".

Essas novas estruturas algébricas denominadas de anéis, receberam esse nome no final do XIX, através do trabalho introduzido pelo matemático D. Hilbert (1852-1943), diferentemente da definição abstrata de anel que só veio em 1914 dada pelo alemão A. Fraenkel (1891-1965). No entanto, foi Emmy Noether que, 30 anos mais tarde, construiu a teoria axiomática de anéis. Em 1921, nesta perspectiva abstrata, Noether conseguiu unificar anéis de polinómios e anéis de números – são conceitualmente semelhantes! Noether tem também os seus anéis: anéis Noetherianos. Seu principal teorema, o de que todo anel de divisão finito é comutativo e, portanto um corpo, foi provado por Wedderburn, em 1905.

Ao passo que foi axiomatizada toda essa teoria, surgiu também o conceito de Isomorfismo, que é estudado tanto na Teoria dos Grupos quanto na Teoria dos Anéis, com o intuito de ampliar conhecimentos a partir de um fenômeno para vários outros, ou seja, se dois objetos são isomorfos, então qualquer propriedade que é preservada via isomorfismo a um dos objetos, também é para o outro. Daí, se um isomorfismo é de uma parte relativamente desconhecida da matemática, para com outra mais conhecida, onde muitos teoremas já estão provados, fica fácil via isomorfismo resolver os problemas desse território desconhecido, com base nos muitos métodos conhecidos do outro objeto.

Dentro do conceito de isomorfismo, existe o teorema fundamental dos homomorfismos e dois corolários do mesmo, aos quais demos total ênfase no nosso estudo. Esses,

por sua vez, foram formulados e definidos em sua generalidade por Emmy Noether que publicou em 1927 todas as suas descobertas. Outra versão mais enxuta desses teoremas pode ser encontrada na obra de Richard Dedekind.

Três anos depois, B. L. Van der Waerden publicou um influente trabalho, o primeiro livro de álgebra abstrata, que já continha toda a tradicional abordagem sobre a Teoria dos Grupos e Teoria dos Anéis. Por exemplo, os três teoremas do isomorfismo de anéis aparecem explicitamente.

Este trabalho está organizado da seguinte forma: no Capítulo 2, são apresentados os resultados principais sobre grupos, destacando de forma especial os conceitos de subgrupos, classe de lateral e homomorfismo de grupos. No Capítulo 3, são considerados os resultados sobre anéis com conceitos inerentes tais como subanel, ideal, homomorfismo e, principalmente, os Teoremas dos Isomorfismos. No final, são apresentadas as conclusões.

Capítulo 2

Conceitos Preliminares

Neste capítulo, temos como objetivo introduzir os aspectos elementares das estruturas algébricas com uma única operação $\star$. Desse modo, será interessante, neste momento, estudar uma estrutura algébrica $(G, \star)$, para a qual, além de outras propriedades tem a de que toda equação linear da forma $a \star x = b$, com $a, b \in G$, tenha solução em G.

Vale ressaltar que alguns dos conceitos preliminares que serão apresentados podem ser encontrados em qualquer uma das referências [2], [4] e [5].

2.1 Definição e Exemplos de Grupos

Definição 2.1.1 *Um conjunto não vazio G munido de uma operação $\star$ é um* ***grupo*** *quando as propriedades seguintes são satisfeitas:*

$(\mathcal{G}_1)$ *A operação é associativa, isto é,*

$$a \star (b \star c) = (a \star b) \star c, \quad \forall\ a, b, c \in G.$$

$(\mathcal{G}_2)$ *Existe elemento neutro para $\star$, isto é,*

$$\exists\ e \in G \ \text{ tal que } \ a \star e = e \star a = a, \quad \forall\ a \in G.$$

$(\mathcal{G}_3)$ *Todo elemento em G é invertível em relação à operação $\star$, isto é,*

$$\forall\ a \in G, \quad \exists\ a' \in G \ \text{ tal que } \ a \star a' = a' \star a = e.$$

O grupo G assim definido será indicado por $(G, \star)$. Às vezes, para simplificar a notação, o indicaremos simplesmente por G. Isto naturalmente exige que não haja dúvida quanto à operação considerada sobre G.

Chama-se frequentemente a operação $\star$ de **produto**. Entretanto, isto não tem a princípio relação com os produtos que conhecemos sobre os conjuntos numéricos clássicos. Usa-se $a \cdot b$ ou ab (notação multiplicativa) ao invés de $a \star b$. Neste caso, diz-se que o grupo G é **multiplicativo**. Em geral, isso será considerado no desenvolvimento dos resultados sobre grupos, devendo-se apenas a uma questão de praticidade, pois tais resultados independem da notação usada para indicar a operação considerada em G. Especificamente, vamos considerar exemplos de grupos com operações indicadas por $+$, — os **grupos aditivos**.

Definição 2.1.2 *Um grupo* $(G, \star)$ *é* ***comutativo*** *ou* ***abeliano*** *quando*

$$a \star b = b \star a, \quad \forall\ a, b \in G,$$

ou seja, quando a operação em G *for comutativa.*

Exemplo 2.1.3 Com as operações usuais de adição, temos que

$$(\mathbb{Z}, +)\,, \quad (\mathbb{Q}, +)\,, \quad (\mathbb{R}, +) \quad \text{e} \quad (\mathbb{C}, +)$$

são exemplos clássicos de grupos abelianos. ♣

Exemplo 2.1.4 O conjunto $\mathbb{Z}_n = \left\{\overline{0},\ \overline{1},\ \overline{2}, \ldots, \overline{n-1}\right\}$ é um grupo abeliano sob a operação $\overline{a} + \overline{b} = \overline{a+b}, \quad \forall\ \overline{a}, \overline{b} \in \mathbb{Z}_n$.

Solução: Inicialmente, ressaltamos que, de acordo com os resultados sobre a relação de congruência módulo n, mostra-se que

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

define uma operação sobre $\mathbb{Z}_n$. Agora, dados $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, temos que,

$$\begin{aligned}
\overline{a} + \left(\overline{b} + \overline{c}\right) &= \overline{a} + \overline{b + c} \\
&= \overline{a + (b + c)} \\
&= \overline{(a + b) + c} \\
&= \overline{a + b} + \overline{c} \\
&= \left(\overline{a} + \overline{b}\right) + \overline{c}.
\end{aligned}$$

O elemento $\overline{0} \in \mathbb{Z}_n$ é tal que

$$\overline{a} + \overline{0} = \overline{a + 0} = \overline{a} = \overline{0 + a},$$

ou seja, $\overline{0}$ é o elemento neutro da operação. Por fim,

$$\overline{a} + \overline{n - a} = \overline{n} = \overline{0},$$

de modo que $\overline{n - a}$ é inverso aditivo de $\overline{a}$. Isso mostra que $(\mathbb{Z}_n, +)$ é um grupo, que é abeliano, pois

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

♣

Exemplo 2.1.5 Sejam o conjunto $G = \mathbb{R} - \{-1\}$ e a operação " $\star$ " em G definida por $a \star b = a + b + 3$. Mostrar que $(G, \star)$ é um grupo.

Solução: Dados $a, b, c \in G$,

$$a \star (b \star c) = a + b + c + 6 = (a \star b) \star c,$$

ou seja, a operação é associativa. Agora, o elemento $e = -3 \in G$ satisfaz

$$a \star e = a = e \star a,$$

de modo que $e = -3$ é um elemento neutro da operação. Por fim, $b = -6 - a \in G$ é tal que

$$a \star b = -3 = b \star a.$$

Logo, $b = -6 - a$ é inverso de a. Por conseguinte, $(G, \star)$ é um grupo, e como

$$a \star b = a + b + 3 = b \star a,$$

segue que G é abeliano. ♣

Exemplo 2.1.6 O conjunto $G = \mathcal{M}_{n\times m}(\mathbb{R})$ de todas as matrizes reais de ordem $n \times m$ é um grupo abeliano sob a adição usual. De fato,

a) $X + (Y + Z) = (X + Y) + Z, \quad \forall\ X, Y, Z \in G.$

b) $X + \mathbf{0} = \mathbf{0} + X, \quad \forall\ X \in G,$ em que

$$\mathbf{0} = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \dots & \vdots \\ 0 & \dots & 0 \end{pmatrix} \quad \text{(a matriz nula).}$$

c) Para

$$X = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} \in G,$$

a matriz

$$Y = \begin{pmatrix} -a_{11} & \dots & -a_{1m} \\ \vdots & \dots & \vdots \\ -a_{n1} & \dots & -a_{nm} \end{pmatrix} \in G$$

é tal que $X + Y = Y + X = \mathbf{0}$. Isso mostra que G é um grupo. A comutatividade da adição em G é imediata. ♣

Exemplo 2.1.7 Consideremos o conjunto $G = \mathcal{M}_n(\mathbb{R})$ de todas as matrizes reais de ordem n. Sabe-se que o produto usual de matrizes é associativo, ou seja, dadas as matrizes $X, Y, Z \in G$,

$$X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z.$$

Além disso, a matriz identidade de ordem n,

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

é o elemento neutro do produto, pois

$$X \cdot I_n = I_n \cdot X = X, \quad \forall\ X \in G.$$

Agora, como $\mathbf{0} \in G$ (a matriz nula de ordem n) e para tal não existe $Y \in G$, com $\mathbf{0} \cdot Y = I_n$, então $G = \mathcal{M}_n(\mathbb{R})$ não é um grupo. Aliás, dado $X \in G$, existe $Y \in G$ tal que $X \cdot Y = I_n$ se, e somente se, $\det X \neq 0$. ♣

Exemplo 2.1.8 No exemplo anterior, observamos que em $G = \mathcal{M}_n(\mathbb{R})$, pois a propriedade da existência de inverso não é satisfeita. No entanto, o conjunto

$$GL_n(\mathbb{R}) = \{X \in M_n(\mathbb{R}) : \det X \neq 0\} \subset G$$

é um grupo multiplicativo. De fato, pelo que foi exposto antes, é suficiente mostrar que $GL_n(\mathbb{R})$ é fechado sob o produto (já usando o fato que $I_n \in G$). Se $X, Y \in GL_n(\mathbb{R})$, então $\det X \neq 0$ e $\det Y \neq 0$; como o determinante do produto de duas matrizes é o produto de seus determinantes, então $\det(X \cdot Y) = \det X \cdot \det Y \neq 0$, ou seja, $X \cdot Y \in GL_n(\mathbb{R})$. Logo, $GL_n(\mathbb{R})$ é fechado sob o produto e, assim, é um grupo. Chama-se $GL_n(\mathbb{R})$ **grupo linear de grau** n **sobre** $\mathbb{R}$. Nota-se que, para $n > 1$, o grupo $GL_n(\mathbb{R})$ não é abeliano. Similarmente, tem-se os grupos lineares $GL_n(\mathbb{Q})$ e $GL_n(\mathbb{C})$. ♣

Exemplo 2.1.9 O conjunto $G = \mathbb{R}_+$ munido da operação $\star$ definida por $a \star b = \sqrt{a \cdot b}$ não é um grupo, pois a operação não é associativa. De fato, para $a = 2$, $b = 3$ e $c = 4$, temos

$$(2 \star 3) \star 4 = \sqrt{6} \star 4 = \sqrt{4\sqrt{6}}$$

e

$$2 \star (3 \star 4) = 2 \star \sqrt{12} = \sqrt{2\sqrt{12}},$$

isto é, $(2 \star 3) \star 4 \neq 2 \star (3 \star 4)$. ♣

Vamos destacar agora propriedades de um grupo G que seguem quase que imediatamente da definição. As duas primeiras referem-se às leis do cancelamento, e a outra à existência de solução de uma equação linear em G.

Proposição 2.1.10 *Seja $(G, \star)$ um grupo. Então, as leis do cancelamento à esquerda e à direita são válidas em G, isto é, dados $a, b, c \in G$,*

$$a \star b = a \star c \;\Rightarrow\; b = c \quad e \quad b \star a = c \star a \;\Rightarrow\; b = c.$$

Demonstração: Como existe $a_1 \in G$ tal que $a_1 \star a = e = a \star a_1$, temos

$$\begin{array}{rcl} a \star b = a \star c & \Rightarrow & a_1 \star (a \star b) = a_1 \star (a \star c) \qquad \text{(operando à esquerda com } a_1\text{)} \\ & \Rightarrow & (a_1 \star a) \star b = (a_1 \star a) \star c \qquad \text{(pois } \star \text{ é associativa)} \\ & \Rightarrow & e \star b = e \star c \qquad \text{(pois } a_1 \star a = e\text{)}, \end{array}$$

isto é, $b = c$. Da mesma forma, mostra-se que $b \star a = c \star a$ implica em $b = c$. ■

Proposição 2.1.11 *Seja $(G, \star)$ um grupo. Dados $a, b \in G$, as equações lineares $a \star x = b$ e $x \star a = b$ têm únicas soluções em G.*

Demonstração: Vamos mostrar a existência e unicidade de solução apenas para equação $a \star x = b$; o outro caso é tratado similarmente. Seja $a_1 \in G$, com $a_1 \star a = e$. Logo, o elemento $x_0 = a_1 \star b \in G$ é tal que

$$a \star (a_1 \star b) = (a \star a_1) \star b = e \star b = b,$$

isto é, x_0 é uma solução de $a \star x = b$. Suponhamos agora que $y_0 \in G$ seja outra solução. Por isso, $a \star x_0 = b$ e $a \star y_0 = b$, ou seja, $a \star x_0 = a \star y_0$. Logo, pela Proposição 2.1.10, temos $x_0 = y_0$, mostrando a unicidade de solução. ■

Proposição 2.1.12 *Seja $(G, \star)$ um grupo. Então,*

(1) *Existe único elemento $e \in G$ tal que*

$$e \star a = a \star e = a, \quad \forall\ a \in G.$$

(2) *Para cada $a \in G$, existe um único $a' \in G$ tal que*

$$a' \star a = a \star a' = e.$$

Por isso, em um grupo $(G, \star)$, o elemento neutro da operação e o inverso de cada elemento em G são únicos. Chama-se o elemento neutro de " $\star$ " a **identidade** de G. Quanto ao inverso a' de a, denotaremos de modo específico por a^{-1} ou $-a$, conforme a operação em G seja multiplicativa ou aditiva, respectivamente. Por exemplo, para o grupo $(\mathbb{Z}, +)$, o inverso de $a = 3$ é $-a = -3$ $(3 + (-3) = 0 = e)$; e para o grupo $(\mathbb{R}^*, \cdot)$, o inverso de $a = 3$ é $a^{-1} = 3^{-1} = \frac{1}{3}$ $(3 \cdot 3^{-1} = 1 = e)$.

Observação 2.1.13 No decorrer de todo texto, a identidade de um grupo G será indica por e. Além disso, se $\{G_i\}_{i\in\Lambda}$ é uma família de grupos, então e_i indicará a identidade do grupo G_i.

Observação 2.1.14 Em decorrência da Proposição 2.1.11, temos que um elemento $e \in G$ é a identidade do grupo $(G, \star)$ quando $e \star a = a$ para algum $a \in G$. Similarmente, para verificar que $a' \in G$ é o inverso de $a \in G$, basta mostrar que $a' \star a = e$ ou $a \star a' = e$.

Proposição 2.1.15 *Seja G um grupo abeliano e " $\cdot$ " uma operação em G. Então,*

(1) $(a^{-1})^{-1} = a, \quad \forall\ a \in G.$

(2) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}, \quad \forall\ a, b \in G.$

Demonstração: (1) Dado $a \in G$, um elemento $b \in G$ é, por definição, o inverso de a ou vice-versa, quando

$$a \cdot b = b \cdot a = e.$$

Como $a \cdot a^{-1} = a^{-1} \cdot a = e$, então $a = (a^{-1})^{-1}$.

(2) Vamos mostrar que

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = (b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e. \tag{2.1}$$

Usando a propriedade associativa da operação em G, pode-se omitir os parêntesis em (2.1), de modo que

$$\begin{aligned} (a \cdot b) \cdot (b^{-1} \cdot a^{-1}) &= a \cdot b \cdot b^{-1} \cdot a^{-1} = a \cdot e \cdot a^{-1} \\ &= e \end{aligned}$$

e

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

Por conseguinte, $(a\cdot b)^{-1} = b^{-1}\cdot a^{-1}$. ■

O resultado do item (2) da Proposição 2.1.15 pode ser generalizado da seguinte forma: para $a_1, a_2, \ldots, a_n \in G$,

$$(a_1\cdot a_2\cdots a_n)^{-1} = a_n^{-1}\cdot a_{n-1}^{-1}\cdots a_2^{-1}\cdot a_1^{-1}.$$

De fato, por indução, para $n = 2$ (o caso $n = 1$ é direto), temos $(a_1\cdot a_2)^{-1} = a_2^{-1}\cdot a_1^{-1}$. Supondo o resultado válido para $n \geq 2$, vamos verificar que vale para $n+1$, tal que

$$\begin{aligned}(a_1\cdot a_2\cdots a_n\cdot a_{n+1})^{-1} &= ((a_1\cdot a_2\cdots a_n)\cdot a_{n+1})^{-1}\\ &= a_{n+1}^{-1}\cdot(a_1\cdot a_2\cdots a_n)^{-1}\\ &= a_{n+1}^{-1}\cdot a_n^{-1}\cdot a_{n-1}^{-1}\cdots a_2^{-1}\cdot a_1^{-1}.\end{aligned}$$

2.2 Subgrupos

Dado um grupo G, faz-se necessário estudar algumas de suas propriedades através de seus subconjuntos, que também tenham estrutura de grupos. É o que faremos a seguir.

Definição 2.2.1 *Sejam $(G,\star)$ um grupo e $\mathcal{H}$ um subconjunto não vazio de G. Dizemos que $\mathcal{H}$ é subgrupo de G se, e somente se, $\mathcal{H}$ munido da operação induzida de G é também um grupo.*

Vale neste caso, fazer mais algumas ressalvas.

Observação 2.2.2 Um subgrupo $\mathcal{H}$ de um grupo G será sempre indicado em símbolos como sendo,

$$\mathcal{H} < G.$$

Observação 2.2.3 O elemento neutro de $\mathcal{H}$ será indicado por $e_{\mathcal{H}}$ e é o mesmo advindo do grupo G, ou seja,

$$e_{\mathcal{H}} = e.$$

Já o elemento inverso de $h \in \mathcal{H}$, é o mesmo tanto em $\mathcal{H}$ quanto em G.

Exemplo 2.2.4 Se e é o elemento neutro de G, então obviamente $\{e\}$ é um subgrupo de G. É imediato, também, que o próprio G é um subgrupo de si mesmo Estes subgrupos, ou seja, $\{e\}$ e G, são chamados de subgrupos triviais de G. ♣

Exemplo 2.2.5 Com a operação de soma usual temos a cadeia de subgrupos

$$\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C},$$

já com a multiplicação usual temos

$$\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*.$$

♣

Há casos, porém, em que para se determinar que um subconjunto $\mathcal{H}$ de G é realmente um subgrupo precisa-se de um critério, o qual será citado na proposição seguinte.

Proposição 2.2.6 *Sejam $(G, \cdot)$ um grupo e $\mathcal{H}$ um subconjunto não vazio de G. Então, $\mathcal{H}$ é subgrupo de G se, e somente se, uma das seguintes condições é verdadeira:*

(1) $h_1 \cdot h_2 \in \mathcal{H} \quad e \quad h_1^{-1} \in \mathcal{H}, \quad \forall\ h_1, h_2 \in \mathcal{H}.$

(2) $h_1 \cdot h_2^{-1} \in \mathcal{H}, \quad \forall\ h_1, h_2 \in \mathcal{H}.$

Exemplo 2.2.7 O subconjunto

$$\mathcal{H} = \left\{ \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in \mathcal{M}_2(\mathbb{R}) \right\}$$

é subgrupo do grupo aditivo $G = \mathcal{M}_2(\mathbb{R})$. De fato, consideremos $A, B \in \mathcal{H}$, digamos

$$A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} r & s \\ t & -r \end{pmatrix}.$$

Assim,

$$A + B = \begin{pmatrix} a+r & b+s \\ c+t & -(a+r) \end{pmatrix} \in \mathcal{H}$$

e

$$-A = \begin{pmatrix} -a & -b \\ -c & +a \end{pmatrix} \in \mathcal{H}.$$

Por isso, $\mathcal{H}$ é subgrupo de G. ♣

Exemplo 2.2.8 O subconjunto $\mathcal{H} = \{A \in GL(n, \mathbb{R}) : \det A = 2\}$ não é subgrupo de $(GL(n, \mathbb{R}), \cdot)$. De fato, para $A, B \in \mathcal{H}$, tal que

$$\det A = 2 \quad \text{e} \quad \det B = 2,$$

temos

$$\det(AB) = \det A \cdot \det B = 2 \cdot 2 = 4$$

isto é, $\mathcal{H}$ não é subgrupo de $(GL(n, \mathbb{R}), \cdot)$, pois $\det(AB) \notin \mathcal{H}$. ♣

2.3 Homomorfismos de Grupos

As funções que transformam uma soma (produto) de elementos do domínio, na soma (produto) de suas imagens, ou seja, que preservam as operações entre duas estruturas algébricas do mesmo tipo, são chamadas de homomorfismos e será o objeto de estudo neste momento.

Definição 2.3.1 *Consideremos dois grupos $(G, \star)$ e $(\mathcal{J}, \cdot)$. Uma função $f : G \longrightarrow \mathcal{J}$ é dita homomorfismo quando*

$$f(a \star b) = f(a) \cdot f(b), \quad \forall a, b \in G.$$

Pelo método de indução finita, podemos mostrar que dados $x_1, x_2, \ldots, x_n \in G$,

$$f(x_1 \star x_2 \star \cdots \star x_n) = f(x_1) \cdot f(x_2) \cdots f(x_n).$$

Exemplo 2.3.2 Sejam G_1 e G_2 dois grupos quaisquer. A função $f : G_1 \longrightarrow G_2$ dada por $f(x) = e_2, \forall\ x \in G_1$ é um homomorfismo − ***homomorfismo trivial.*** ♣

Exemplo 2.3.3 Seja G um grupo qualquer. A aplicação $Id_G(x) = x$, $\forall\ x \in G$ é um homomorfismo − ***homomorfismo identidade.*** ♣

Exemplo 2.3.4 Dados os grupos $G_1 = (\mathbb{R}_+, \cdot)$ e $G_2 = (\mathbb{R}, +)$, com as operações usuais. Mostremos que a aplicação

$$\begin{array}{rccc} h: & \mathbb{R}_+ & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \log x \end{array}$$

é um homomorfismo.

Solução: Tomemos $x, y \in \mathbb{R}_+$. Assim

$$h(x \cdot y) = \log x \cdot y = \log x + \log y = h(x) + h(y),$$

provando que h é um homomorfismo. ♣

Exemplo 2.3.5 Considere os grupos $G_1 = (\mathbb{Z}, +)$ e $G_2 = (\mathbb{R}, +)$. A aplicação $f : \mathbb{Z} \longrightarrow \mathbb{R}$ dada por $f(x) = x + 2$ não é um homomorfismo. De fato, para $x, y \in \mathbb{Z}$, temos

$$f(x + y) = x + y + 2,$$

e

$$f(x) + f(y) = x + y + 4,$$

ou seja,

$$f(x + y) \neq f(x) + f(y).$$

♣

Proposição 2.3.6 *Sejam G_1 e G_2 grupos multiplicativos e $f : G_1 \longrightarrow G_2$ um homomorfismo de grupos. Assim, considerando e_1 o elemento neutro de G_1 e e_2 o de G_2, vale que:*

(1) $f(e_1) = e_2$.

(2) $f(x^{-1}) = f(x)^{-1}, \quad \forall x \in G_1$.

Demonstração: (1) Como $e_1 \in G_1$ é tal que $e_1 \cdot e_1 = e_1$,temos

$$\begin{array}{rcl} e_1 = e_1 \cdot e_1 & \Rightarrow & f(e_1) = f(e_1 \cdot e_1) \quad \text{(usando a definição de homomorfismo)} \\ & \Rightarrow & f(e_1) = f(e_1) \cdot f(e_1) \quad \text{(operando à esquerda com } f(e_1)^{-1}\text{)} \\ & \Rightarrow & f(e_1) = e_2 \end{array}$$

(2) Pelo item (1), temos que:

$$f(e_1) = e_2.$$

Assim, dado $x \in G_1$,

$$\begin{array}{rcl} x \cdot x^{-1} = e_1 & \Rightarrow & f(x \cdot x^{-1}) = f(e_1) \quad \text{(usando (1))} \\ & \Rightarrow & f(x \cdot x^{-1}) = e_2 \quad \text{(usando a definição de homomorfismo)} \\ & \Rightarrow & f(x) \cdot f(x^{-1}) = e_2 \quad \text{(operando à esquerda com } f(x_1)^{-1}\text{)} \\ & \Rightarrow & f(x^{-1}) = f(x)^{-1} \end{array}$$

■

2.3.1 Núcleo e Imagem de um Homomorfismo

Apresentaremos a seguir os conceitos de núcleo e imagem de um homomorfismo $f : G \longrightarrow \mathcal{J}$, os quais desempenham um importante papel na teoria dos grupos. No que concerne à imagem, veremos pelo item (2) da Proposição 2.3.11 que $\mathrm{Im}(f)$ é subgrupo de $\mathcal{J}$. Veremos também do item (1) dessa mesma proposição que o núcleo de f além de ser um subgrupo de G, tem por (3) uma estrutura muito mais interessante.

Definição 2.3.7 *Seja $f : G \longrightarrow \mathcal{J}$ um homomorfismo de grupos. O núcleo desse homomorfismo, denotado por $\mathcal{N}(f)$ ou $\ker(f)$, é o seguinte conjunto,*

$$\mathcal{N}(f) = \{x \in G;\ f(x) = e_2\}.$$

Vale ressaltar que como $f(e_1) = e_2$ (cf. Proposição 2.3.6), então $e_1 \in \mathcal{N}(f)$. Portanto, ao menos o elemento neutro de G pertence ao núcleo de f, isto é, o núcleo é diferente do vazio.

Definição 2.3.8 *Seja $f : G \longrightarrow \mathcal{J}$ um homomorfismo de grupos. A imagem desse homomorfismo, denotada por $\mathrm{Im}(f)$, é o seguinte conjunto*

$$\mathrm{Im}(f) = \{f(x) \in \mathcal{J}; x \in G\}.$$

Mais adiante, veremos na (proposição 2.3.11) que o núcleo de f está contido em G e a imagem de f em $\mathcal{J}$, e mais, que são subgrupos dos respectivos grupos G e $\mathcal{J}$.

Exemplo 2.3.9 Determinar o núcleo e a imagem do homomorfismo $f : \mathbb{R}_+ \longrightarrow \mathbb{R}$ definido por $f(x) = \log x$. (cf. exemplo 2.3.4).

Solução: Dado x em $\mathbb{R}_+$, temos

$$x \in \mathcal{N}(f) \Leftrightarrow f(x) = e_2 \Leftrightarrow \log x = 0 \Leftrightarrow x = 1.$$

Portanto,

$$\mathcal{N}(f) = \{x \in G; f(x) = e_2\} = \{1\} = \{e_1\}.$$

Além disso, consideremos $y \in \mathbb{R}$ de modo a verificar se existe para ele, $x \in \mathbb{R}_+$ tal que

$$f(x) = y.$$

Sendo++,

$$f(x) = y \Leftrightarrow \log x = y \Leftrightarrow x = 10^y \in \mathbb{R}_+.$$

Logo,

$$f(10^y) = y, \quad \forall y \in \mathbb{R},$$

implicando que

$$\mathrm{Im}(f) = \{f(x) : x \in \mathbb{R}_+\} = \mathbb{R}.$$

♣

Exemplo 2.3.10 Considere os grupos $G = (\mathbb{R}^2, +)$ e $\mathcal{J} = (\mathbb{R}, +)$. Mostrar que a função

$$\begin{array}{rccc} g: & \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ & (x,y) & \longmapsto & x \end{array}$$

é um homomorfismo, determinando em seguida seu núcleo e imagem.

Solução: Sejam $\alpha_1 = (x_1, y_1)$ e $\alpha_2 = (x_2, y_2)$ pontos em $\mathbb{R}^2$. Assim,

$$\begin{aligned} \alpha_1 + \alpha_2 &= (x_1, y_1) + (x_2, y_2) \\ &= (x_1 + x_2, y_1 + y_2). \end{aligned}$$

Por conseguinte,

$$\begin{aligned} g(\alpha_1 + \alpha_2) &= g(x_1 + x_2, y_1 + y_2) \\ &= x_1 + x_2 \\ &= g(x_1, y_1) + g(x_2, y_2) \\ &= g(\alpha_1) + g(\alpha_2) \end{aligned}$$

Logo, a aplicação é um homomorfismo. Encontremos seu núcleo e imagem respectivamente.

Dado $\alpha = (x, y) \in \mathbb{R}^2$. Ora,

$$\alpha \in \mathcal{N}(g) \Leftrightarrow g(\alpha) = e_2 \Leftrightarrow g(x, y) = 0 \Leftrightarrow x = 0.$$

Portanto,

$$\mathcal{N}(g) = \left\{\alpha \in \mathbb{R}^2; x = 0\right\} = \left\{(0, y) \in \mathbb{R}^2; y \in \mathbb{R}\right\}.$$

Por outro lado, é fácil notar que segundo a função dada

$$g(a, y) = a \quad \forall\ y \in \mathbb{R},$$

o que implica

$$\mathrm{Im}(g) = \mathbb{R}.$$

♣

Proposição 2.3.11 *Seja $f : G_1 \longrightarrow G_2$ um homomorfismo de grupos. Então são válidas as seguintes afirmativas:*

(1) $\mathcal{N}(f) < G_1$ *(o núcleo de f é subgrupo de G_1).*

(2) $\mathrm{Im}(f) < \mathcal{J}$ *(a imagem de f é subgrupo de G_2).*

(3) *f é injetora* $\Leftrightarrow \mathcal{N}(f) = \{e_1\}$.

Demonstração: (1) Pela Proposição 2.3.6, sabemos que

$$f(e_1) = e_2.$$

Também,

$$e_1 \in \mathcal{N}(f) \Rightarrow \mathcal{N}(f) \neq \varnothing.$$

Sejam agora, $a, b \in N(f)$. Assim,

$$f(a) = e_2 \quad \text{e} \quad f(b) = e_2. \tag{2.2}$$

Em seguida, analisemos a seguinte situação:

$$\begin{aligned} f(a \cdot b^{-1}) &= f(a) \cdot f(b^{-1}) && \text{(usando a definição de homomorfismo)} \\ &= f(a) \cdot (f(b))^{-1} && \text{(Pela proposição 2.3.6)} \\ &= e_2 \cdot (e_2)^{-1} && \text{(usando (2.2))} \\ &= e_2. \end{aligned}$$

Portanto,

$$a \cdot b^{-1} \in \mathcal{N}(f),$$

acarretando que,

$$\mathcal{N}(f) < G.$$

(2) Consideremos $y_1, y_2 \in \operatorname{Im}(f)$, digamos

$$y_1 = f(a) \quad \text{e} \quad y_2 = f(b), \text{ com } a, b \in G_1. \tag{2.3}$$

Assim,

$$\begin{aligned} f(a \cdot b^{-1}) &= f(a) \cdot f(b^{-1}) && \text{(usando a definição de homomorfismo)} \\ &= f(a) \cdot f(b)^{-1} && \text{(usando (2.3))} \\ &= y_1 \cdot y_2^{-1} \end{aligned}$$

Portanto,

$$y_1 \cdot y_2^{-1} \in \operatorname{Im}(f),$$

em outras palavras,

$$\operatorname{Im}(f) < G_2.$$

(3) Suponhamos que f seja injetora. Assim, dado $x \in G_1$,

$$\begin{aligned} x \in \mathcal{N}(f) \Leftrightarrow f(x) &= e_2 && \text{(definição de núcleo de um homomorfismo)} \\ &= f(e_1) && \text{(pela proposição 2.3.6)} \end{aligned}$$

o que implica $f(x) = f(e_1)$. Por hipótese, como f é injetora, podemos concluir que $x = e_1$, isto é,

$$\mathcal{N}(f) = \{e_1\}.$$

Reciprocamente, suponhamos que $\mathcal{N}(f) = \{e_1\}$ e sejam $x_1, x_2 \in G_1$ de modo que $f(x_1) = f(x_2)$. Assim,

$$f(x_1) = f(x_2) \Rightarrow f(x_1) \cdot f(x_2)^{-1} = e_2 \Rightarrow f\left(x_1 \cdot x_2^{-1}\right) = e_2.$$

Por isso,

$$x_1 \cdot x_2^{-1} \in \mathcal{N}(f) \Rightarrow x_1 \cdot x_2^{-1} = e_1 \Rightarrow x_1 = x_2.$$

Logo, f é injetora. ■

Capítulo 3

Introdução à Teoria dos Anéis

Vimos até o momento o estudo de estruturas algébricas munidas apenas de uma operação. A partir de agora, tomando por base tudo que foi visto, estudaremos estruturas algébricas mais específicas. Trabalharemos num conjunto $\mathcal{A}$ munido de duas operações que satisfazem algumas condições naturais, condições estas que nos leva a definição seguinte:

3.1 Definição e Exemplos de Anéis

Definição 3.1.1 *Dado um conjunto não vazio $\mathcal{A}$ provido de duas operações uma de soma e outra de multiplicação denotadas respectivamente por " $+$ " e por " $\cdot$ ". Dizemos que a terna $(\mathcal{A}, +, \cdot)$ é um anel quando as seguintes propriedades com respeito às operações em questão são verídicas:*

($\mathcal{G}_1$) *A operação é associativa, isto é,*

$$a + (b + c) = (a + b) + c, \quad \forall\ a, b, c \in G.$$

($\mathcal{G}_2$) *Existe elemento neutro para $\star$, isto é,*

$$\exists\ e \in G \ \ tal\ que \ \ a + e = e + a = a, \quad \forall\ a \in G.$$

($\mathcal{G}_3$) *Todo elemento em G é invertível em relação à operação $+$, isto é,*

$$\forall\ a \in G, \quad \exists\ a' \in G \ \ tal\ que \ \ a + a' = a' + a = e.$$

($\mathcal{G}_4$) *A adição é comutativa, isto é,*

$$a + b = b + a, \quad \forall\ a, b \in G.$$

($\mathcal{P}_5$) *A multiplicação é associativa, isto é,*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c), \quad \forall a, b, c \in \mathcal{A}.$$

($\mathcal{P}_6$) *A multiplicação é distributiva com respeito à adição, isto é,*

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad e \quad (a + b) \cdot c = a \cdot c + b \cdot c, \quad \forall a, b, c \in \mathcal{A}.$$

Definição 3.1.2 *O anel $(\mathcal{A}, +, \cdot)$ é chamado de comutativo quando permite a comutatividade de seus elementos com respeito à multiplicação, isto é,*

$$a \cdot b = b \cdot a, \quad \forall a, b \in \mathcal{A}.$$

Quando não houver ambiguidade nem confusão de sentido, podemos omitir as respectivas operações e representar um anel $(\mathcal{A}, +, \cdot)$ apenas por $\mathcal{A}$.

Também no anel $\mathcal{A}$, a notação multiplicativa $a \cdot b$ pode ser escrita como sendo ab e a soma $a + (-b)$ por $a - b$, quaisquer que sejam $a, b \in \mathcal{A}$.

O elemento neutro da adição descrito no item ($\mathcal{G}_2$) da definição 2.1.1, será denotado por $0_{\mathcal{A}}$ ou apenas 0. Assim,

$$a + (-a) = 0_{\mathcal{A}} = 0, \quad \forall a, \in \mathcal{A}.$$

Definição 3.1.3 *Diz-se que um anel $\mathcal{A}$ possui unidade quando sua multiplicação admite um elemento neutro e de modo que*

$$ae = a = ea, \quad \forall a \in \mathcal{A}.$$

A unidade de um anel $\mathcal{A}$ é o elemento neutro da multiplicação e será denotado por $1_{\mathcal{A}}$ ou 1, não tendo nada a ver com o elemento inteiro 1.

Exemplo 3.1.4 Com as operações usuais de soma e multiplicação usuais, temos que

$$(\mathbb{Z}, +, \cdot), \quad (\mathbb{Q}, +, \cdot), \quad (\mathbb{R}, +, \cdot) \ \text{ e } \ (\mathbb{C}, +, \cdot)$$

são exemplos clássicos de anéis numéricos com unidade 1. ♣

Exemplo 3.1.5 A estrutura algébrica $\mathcal{A} = \{0_A\}$ definida pelas operações

$$0_A + 0_A = 0_A \quad \text{e} \quad 1_A + 1_A = 1_A$$

é um anel comutativo com unidade 0_A que recebe o nome de anel trivial. Desse modo, este caso é o único em que $1_A = 0_A$. ♣

O anel $\mathcal{A} = \{0_A\}$ não desperta muito interesse. Assim, vamos sempre supor que a unidade de um anel, caso exista, seja $1_A \neq 0_A$.

Exemplo 3.1.6 O conjunto $\mathbb{Z}_n = \left\{\overline{0},\ \overline{1}, \ldots, \overline{n-1}\right\}$, munido das operações $\overline{a} + \overline{b} = \overline{a+b}$ e $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.é o anel das classes de resto módulo m com unidade $\overline{1}$. ♣

Exemplo 3.1.7 Consideremos o conjunto $\mathbb{Z}\left[\sqrt{2}\right]$ como sendo

$$\mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2}; a, b \in \mathbb{Z}\right\}.$$

Sejam $x, y \in \mathbb{Z}\left[\sqrt{2}\right]$ tais que $x = a_1 + b_1\sqrt{2}$ e $y = a_2 + b_2\sqrt{2}$, com $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Vamos definir as operações " + " e " $\cdot$" em $\mathbb{Z}\left[\sqrt{2}\right]$ da seguinte forma:

$$x + y = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$

e

$$x \cdot y = (a_1 + a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}.$$

Munido destas operações, $\mathbb{Z}\left[\sqrt{2}\right]$ é um anel comutativo com unidade, onde $0_{\mathcal{A}} = 0+0\sqrt{2}$ corresponde ao número inteiro 0 e $1_{\mathcal{A}} = 1+0\sqrt{2}$ ao inteiro 1. Numa abrangência geral, para cada inteiro d,

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

com as operações vistas acima é também um anel comutativo com unidade. Em particular, para $d = -1$ obtemos o anel

$$\mathbb{Z}[\sqrt{-1}] = \{a + bi : a, b \in \mathbb{Z}\},$$

o qual recebe o nome de ***anel dos inteiros de Gauss***. ♣

De maneira análoga e considerando as mesmas operações usadas no anel $\mathbb{Z}\left[\sqrt{d}\right]$, para cada inteiro d

$$\mathbb{Q}[\sqrt{d}] = \left\{a + b\sqrt{d}; a, b \in \mathbb{Q}\right\}$$

também é um anel comutativo com unidade (a unidade sendo o inteiro 1).

Exemplo 3.1.8 Como vimos no exemplo 2.1.6 do capítulo anterior, o conjunto das matrizes reais de ordem n denotado por $\mathcal{A} = \mathcal{M}_n(\mathbb{R})$ é um grupo abeliano com a operação de soma usual. Além disso, sob a operação de multiplicação usual de matrizes, sabe-se que

$$X \cdot I_n = X = I_n \cdot X, \quad \forall\ X, \in \mathcal{A}.$$

Por outro lado, para quaisquer $X, Y \in \mathcal{A}$ temos em geral

$$X \cdot Y \neq Y \cdot X.$$

Logo, A é um anel comutativo não-abeliano.

Outro fato importante a expor aqui é que esses respectivos resultados podem ser ampliados tanto aos inteiros e racionais quanto aos complexos e a elementos de qualquer natureza, desde que a matriz possuia ordem n. Portanto, com as operações de adição e multiplicação são anéis das matrizes também $\mathcal{M}_n(\mathbb{Z})$, $\mathcal{M}_n(\mathbb{Q})$, $\mathcal{M}_n(\mathbb{C})$, $\mathcal{M}_n(\mathcal{B})$.

Nestes casos citados acima, nota-se que para $n = 0$ a unidade do anel será

$$0_{\mathcal{A}} = \begin{pmatrix} 0_{\mathcal{B}} & \dots & 0_{\mathcal{B}} \\ \vdots & \ddots & \vdots \\ 0_{\mathcal{B}} & \dots & 0_{\mathcal{B}} \end{pmatrix}_{nxn}.$$

Por sua vez, se $n > 1$ a unidade em $\mathcal{B}$ será dada pela matriz

$$1_{\mathcal{A}} = \begin{pmatrix} 1_{\mathcal{A}} & \dots & 0_{\mathcal{A}} \\ \vdots & \ddots & \vdots \\ 0_{\mathcal{A}} & \dots & 1_{\mathcal{A}} \end{pmatrix}_{nxn}.$$

3.2 Propriedades de um Anel

Destacaremos algumas propriedades inerentes a um anel $\mathcal{A}$. Estas por sua vez, são consequências imediatas das propriedades de suas operações. Quanto à adição, por exemplo, já foram vistas algumas propriedades elementares na proposição 2.1.10, na proposição 2.1.11, e na proposição 2.1.12 do capítulo anterior. Portanto, destacaremos agora algumas propriedades sob a multiplicação.

Teorema 3.2.1 *Seja $\mathcal{A}$ um anel. Então para quaisquer $a, b \in \mathcal{A}$,*

(1) $0_{\mathcal{A}} \cdot a = a \cdot 0_{\mathcal{A}} = 0_{\mathcal{A}}$.

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

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

Demonstração: (1) Sabemos que $0_{\mathcal{A}} + 0_{\mathcal{A}} = 0_{\mathcal{A}}$. Desse modo, pela propriedade distributiva da multiplicação sobre a adição de $\mathcal{A}$, temos

$$a \cdot 0_{\mathcal{A}} = a \cdot (0_{\mathcal{A}} + 0_{\mathcal{A}}) = a \cdot 0_{\mathcal{A}} + a \cdot 0_{\mathcal{A}}. \tag{3.1}$$

$(\mathcal{A}, +)$ é um grupo. Assim, para $(a \cdot 0_{\mathcal{A}}) \in \mathcal{A}$ existe $-(a \cdot 0_{\mathcal{A}}) \in \mathcal{A}$, tal que $-(a \cdot 0_{\mathcal{A}}) + (a \cdot 0_{\mathcal{A}}) = 0_{\mathcal{A}}$. Portanto, adicionando $-(a \cdot 0_{\mathcal{A}})$ aos membros de (3.1), obtemos

$$\begin{aligned} -(a \cdot 0_{\mathcal{A}}) + (a \cdot 0_{\mathcal{A}}) &= -(a \cdot 0_{\mathcal{A}}) + (a \cdot 0_{\mathcal{A}}) + (a \cdot 0_{\mathcal{A}}) \Rightarrow \\ 0_{\mathcal{A}} &= 0_{\mathcal{A}} + (a \cdot 0_{\mathcal{A}}) \\ &= (a \cdot 0_{\mathcal{A}}). \end{aligned}$$

De maneira análoga, prova-se que $0_{\mathcal{A}} \cdot a = 0_{\mathcal{A}}$.

(2) Pela propriedade anterior,

$$(-a) \cdot b + ab = (-a + a) \cdot b = 0_{\mathcal{A}} \cdot b = 0_{\mathcal{A}},$$

ou seja,

$$(-a) \cdot b = -(ab). \tag{3.2}$$

Por outro lado,

$$a \cdot (-b) + a \cdot b = a \cdot (-b + b) = a \cdot 0_{\mathcal{A}} = 0_{\mathcal{A}},$$

isto é,

$$a \cdot (-b) = -(a \cdot b). \tag{3.3}$$

De (3.2) e (3.3), as igualdades $a \cdot (-b) = (-a) \cdot b = -(ab)$, tornam-se verdadeiras.

(3) Da propriedade (2), vimos que

$$\begin{aligned} (-a) \cdot (-b) + (-(a \cdot b)) &= (-a) \cdot (-b) + ((-a) \cdot b) \\ &= (-a) \cdot (-b + b) \\ &= (-a) \cdot 0_{\mathcal{A}} \\ &= 0_{\mathcal{A}}. \end{aligned}$$

Logo,

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

■

Proposição 3.2.2 *Seja $\mathcal{A}$ um anel qualquer. Como $\mathcal{A}$ munido da operação soma é um grupo abeliano, vale para $m, n \in \mathbb{Z}$ as seguintes propriedades:*

(1) $m \cdot a + n \cdot a = (m + n) \cdot a, \quad \forall\ a \in \mathcal{A}.$

(2) $m \cdot (n \cdot a) = (m \cdot n) \cdot a, \quad \forall\ a \in \mathcal{A}.$

(3) $(m \cdot a) \cdot (n \cdot b) = (m \cdot n) \cdot (a \cdot b) \quad \forall\ a, b \in \mathcal{A}.$

(4) $(-m) \cdot a = m \cdot (-a) = -(m \cdot a), \quad \forall\ a \in \mathcal{A}.$

Demonstremos apenas as igualdades vistas em (2) e (3).

Demonstração: (2) Para algum $a \in \mathcal{A}$ e usando o fato de $\mathcal{A}$ ser um anel, temos

$$\begin{aligned} m \cdot (n \cdot a) &= m \cdot \underbrace{(a + \cdots + a)}_{n \text{ parcelas}} \\ &= \underbrace{(a + \cdots + a) + \cdots + (a + a + \cdots + a)}_{m \text{ parcelas}} \\ &= \underbrace{(a + a + \cdots + a) + a + \cdots + (a + a + \cdots + a) + a}_{m \text{ parcelas}} \\ &= m\left[(a + a + \cdots + a) + a\right] \\ &= m\underbrace{(a + a + \cdots + a + a)}_{n \text{ parcelas}}. \\ &= (m \cdot n) \cdot a. \end{aligned}$$

(3) Dados $a, b \in \mathcal{A}$ tais que

$$\begin{aligned} (m \cdot a) \cdot (n \cdot b) &= \underbrace{(a + \cdots + a)}_{m \text{ parcelas}} \cdot \underbrace{(b + \cdots + b)}_{n \text{ parcelas}} \\ &= \underbrace{a \cdot (b + \cdots + b) + \cdots + a \cdot (b + \cdots + b)}_{m \text{ parcelas}} \\ &= m\left(a \cdot (b + \cdots + b)\right) \\ &= m\left(\underbrace{a \cdot b + \cdots + a \cdot b}_{n \text{ parcelas}}\right) \\ &= (m \cdot n) \cdot (a \cdot b)\,. \end{aligned}$$

■

3.3 Subanéis

Nesta seção, estudaremos algumas propriedades de um anel $\mathcal{A}$ através de seus subconjuntos. Esses também com estrutura de anel.

Definição 3.3.1 *Sejam $\mathcal{A}$ um anel e $\mathcal{B}$ um subconjunto não-vazio de $\mathcal{A}$. Dizemos que $\mathcal{B}$ é um subanel de $\mathcal{A}$, se $\mathcal{B}$ munido das operações de adição e multiplicação induzidas de $\mathcal{A}$, é também um anel.*

Observação 3.3.2 Um subanel $\mathcal{B}$ de um anel $\mathcal{A}$ será sempre indicado em símbolos como sendo,

$$\mathcal{B} \subset \mathcal{A}.$$

Exemplo 3.3.3 Seja $\mathcal{A}$ um anel qualquer. Então, os subconjuntos $\mathcal{B}_1 = \{0_\mathcal{A}\}$ e $\mathcal{B}_2 = \mathcal{A}$ são subanéis de $\mathcal{A}-$ ***subanéis triviais***. ♣

Exemplo 3.3.4 Com as operações usuais, são subanéis os conjuntos numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Desse modo, temos a seguinte cadeia de subanéis

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

♣

Exemplo 3.3.5 Se $n \in \mathbb{N}$, então temos a seguinte cadeia de subanéis

$$\mathcal{M}_n(\mathbb{Z}) \subset \mathcal{M}_n(\mathbb{Q}) \subset \mathcal{M}_n(\mathbb{R}) \subset \mathcal{M}_n(\mathbb{C}).$$

♣

Exemplo 3.3.6 Para cada inteiro d, $\mathbb{Z}[\sqrt{d}]$ é um subanel de $\mathbb{Q}[\sqrt{d}]$. ♣

Vimos até o momento exemplos clássicos de subanéis. Agora, apresentaremos uma ferramenta bastante proveitosa para verificar quando um subconjunto não-vazio $\mathcal{B}$ é um subanel de um anel $\mathcal{A}$.

Teorema 3.3.7 *Sejam $\mathcal{A}$ um anel e $\mathcal{B}$ um subconjunto não-vazio de $\mathcal{A}$. Dizemos que $\mathcal{B}$ é um subanel de $\mathcal{A}$ se, e somente se, para quaisquer $a, b \in \mathcal{B}$*

$$ab \in \mathcal{B} \quad e \quad a - b \in \mathcal{B}.$$

Demonstração: Suponhamos que $\mathcal{B}$ seja um subanél de $\mathcal{A}$. Assim, $(\mathcal{B}, +)$ é um grupo abeliano e,como consequência disto,

$$a - b \in \mathcal{B}, \quad \forall\ a, b \in \mathcal{B}.$$

Por hipótese também, $ab \in \mathcal{B}$, para quaisquer $a, b \in \mathcal{B}$. Por outro lado, se $ab \in \mathcal{B}$ e $a - b \in \mathcal{B}$ para quaisquer $a, b \in \mathcal{B}$, então $(\mathcal{B}, +)$ é um grupo abeliano. Também, como $ab \in \mathcal{B}$ e $\mathcal{B} \subset \mathcal{A}$, as propriedades comutativa e distributiva da multiplicação sobre a adição em $\mathcal{A}$, são válidas em $\mathcal{B}$. Logo, $(\mathcal{B}, +, \cdot)$ é um anel e, consequentemente é um subanél de $\mathcal{A}$. ■

Exemplo 3.3.8 O subconjunto $\mathcal{H} = \mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2}; a, b \in \mathbb{Z}\right\}$ é um subanel de $\mathbb{R}$.De fato, sejam $x, y \in \mathcal{H}$ tais que $x = a_1 + b_1\sqrt{2}$ e $y = a_2 + b_2\sqrt{2}$. Desse modo,

$$\begin{aligned} x \cdot y &= \left(a_1 + b_1\sqrt{2}\right)\left(a_2 + b_2\sqrt{2}\right) \\ &= (a_1 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in \mathcal{H}, \end{aligned}$$

e

$$\begin{aligned} x - y &= \left(m_1 + n_1\sqrt{2}\right) - \left(m_2 + n_2\sqrt{2}\right) \\ &= (m_1 - m_2) + (n_1 + n_2)\sqrt{2} \in \mathcal{H}. \end{aligned}$$

Portanto, $\mathcal{H}$ é subanel de $\mathbb{R}$. ♣

Exemplo 3.3.9 Sejam $\mathcal{A} = \mathcal{M}_2(\mathbb{Q})$ e $\mathcal{B}$ um subconjunto de $\mathcal{A}$ tal que

$$\mathcal{B} = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Q} \right\}.$$

Claramente, $\mathcal{B} \neq \emptyset$. Também, Se $x, y \in \mathcal{A}$ tais que

$$x = \begin{pmatrix} 0 & a_1 \\ 0 & b_1 \end{pmatrix} \quad \text{e} \quad y = \begin{pmatrix} 0 & a_2 \\ 0 & b_2 \end{pmatrix},$$

com $a_1, a_2, b_1, b_2 \in \mathbb{Q}$. Então,

$$x \cdot y = \begin{pmatrix} 0 & a_1b_2 \\ 0 & b_1b_2 \end{pmatrix} \in \mathcal{B},$$

e

$$x - y = \begin{pmatrix} 0 & a_1 - a_2 \\ 0 & b_1 - b_2 \end{pmatrix} \in \mathcal{B}.$$

Logo, $\mathcal{B}$ é subanel de $\mathcal{A}$. ♣

3.4 Homomorfismos de Anéis

Estudaremos homomorfismos de anéis com o mesmo objetivo com o qual estudamos homomorfismos de grupos. Desse modo, destacaremos a seguir, algumas aplicações $f : \mathcal{A} \longrightarrow \mathcal{B}$ que preservam as respectivas operações entre os anéis $\mathcal{A}$ e $\mathcal{B}$, da seguinte forma:

Definição 3.4.1 *Sejam $(\mathcal{A}, +, \cdot)$ e $(\mathcal{B}, +, \cdot)$ dois anéis. Uma função $f : \mathcal{A} \longrightarrow \mathcal{B}$ é dita **homomorfismo** de $\mathcal{A}$ em $\mathcal{B}$ quando as seguintes condições são satisfeitas:*

(a) $f(x+y) = f(x) + f(y), \quad \forall\ x, y \in \mathcal{A}.$

(b) $f(x \cdot y) = f(x) \cdot f(y), \quad \forall\ x, y \in \mathcal{A}.$

Tanto em (a) quanto em (b) da definição acima, as operações de adição e multiplicação do lado esquerdo da igualdade refere-se ao anel $\mathcal{A}$ enquanto as do lado direito ao anel $\mathcal{B}$.

Notemos também que a condição (a) implica que f é um homomorfismo do grupo $(\mathcal{A}, +)$ no grupo $(\mathcal{B}, +)$. Portanto, podemos recorrer a alguns resultados sobre homomorfismos de grupos, para com isso definirmos que

$$f(0_{\mathcal{A}}) = 0_{\mathcal{B}} \quad \text{e} \quad f(-a) = -f(a), \quad \forall\ a \in \mathcal{A},$$

e

$$f(x-y) = f(x) - f(y), \quad \forall\ a \in \mathcal{A}.$$

Exemplo 3.4.2 Dados $\mathcal{A}$ e $\mathcal{B}$ dois anéis quaisquer. A função $f : \mathcal{A} \longrightarrow \mathcal{B}$ definida por

$$f(x) = 0_{\mathcal{B}}, \quad \forall\ x \in \mathcal{A}$$

é um homomorfismo $-$ ***o homomorfismo trivial.*** ♣

Exemplo 3.4.3 Para um anel $\mathcal{A}$ qualquer, a aplicação $f : \mathcal{A} \longrightarrow \mathcal{A}$ dada por

$$Id_{\mathcal{A}}(x) = x, \quad \forall\ x \in \mathcal{A}$$

é um homomorfismo $-$ ***o homomorfismo identidade.*** ♣

Exemplo 3.4.4 Para cada $n > 1$, a função $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ definida por

$$f(m) = \overline{m}, \quad \forall m \in \mathbb{Z}$$

é um homomorfismo de anéis. De fato, para $x, y \in \mathbb{Z}$, temos

$$f(x+y) = \overline{x+y} = \overline{x} + \overline{y} = f(x) + f(y)$$

e

$$f(x \cdot y) = \overline{x \cdot y} = \overline{x} \cdot \overline{y} = f(x) \cdot f(y).$$

Logo, f é um homomorfismo. ♣

Exemplo 3.4.5 Consideremos a função $g : \mathbb{Z} \longrightarrow 2\mathbb{Z}$ dada por $g(x) = 2x$, $\forall\ x \in \mathbb{Z}$. Mostrar que não ocorre um homomorfismo de anéis.

Solução: Sejam $x, y \in \mathbb{Z}$ tais que

$$g(x+y) = 2(x+y) = 2x + 2y = g(x) + g(y),$$

ou seja, g é um homomorfismo entre os grupos $(\mathbb{Z}, +)$ e $(2\mathbb{Z}, +)$. Por outro lado,

$$g(x \cdot y) = 2xy$$

e

$$g(x) \cdot g(y) = 4xy.$$

Portanto, a não ser para o caso em que $x = 0$ e $y = 0$, g não é um homomorfismo entre os anéis $(\mathbb{Z}, +, \cdot)$ e $(2\mathbb{Z}, +.\cdot)$, desde que $g(x \cdot y) \neq g(x) \cdot g(y)$. ♣

Proposição 3.4.6 *Seja $f : \mathcal{A} \longrightarrow \mathcal{B}$ um homomorfismo de anéis. Então a imagem* $\mathrm{Im}(f)$ *é subanel de $\mathcal{B}$.*

Demonstração: Dados $y_1, y_2 \in \mathrm{Im}(f)$, digamos

$$y_1 = f(a) \quad \text{e} \quad y_2 = f(b), \text{ com } a, b \in G. \tag{3.4}$$

Assim,

$$\begin{aligned} f(a \cdot b) &= f(a) \cdot f(b) && \text{(usando a definição de homomorfismo)} \\ &= y_1 \cdot y_2. && \text{(pela equação (3.4))} \end{aligned}$$

Portanto,

$$y_1 \cdot y_2 \in \mathrm{Im}(f).$$

Por outro lado,

$$\begin{aligned} f(a - b) &= f(a) - f(b) && \text{(usando a definição de homomorfismo)} \\ &= y_1 - y_2, && \text{(pela equação (3.4))} \end{aligned}$$

assim

$$y_1 - y_2 \in \mathrm{Im}(f).$$

Logo,

$$\mathrm{Im}\,(f) \subset \mathcal{B}.$$

■

3.5 Núcleo de um Homomorfismo

Definimos na teoria dos grupos os conceitos de núcleo e imagem de um homomorfismo, os quais podem ser estendidos também a teoria dos anéis. No que concerne a imagem de um homomorfismo $f : \mathcal{A} \longrightarrow \mathcal{B}$ de anéis, já sabemos da proposição 3.4.6 que $\mathrm{Im}(f)$ é subanel de $\mathcal{B}$. Já para núcleo, veremos (cf. exemplo 3.7.4) que este tem uma estrutura muito mais interessante que a de apenas um subanel.

Definição 3.5.1 *Sejam $\mathcal{A}$ e $\mathcal{B}$ anéis e $f : \mathcal{A} \longrightarrow \mathcal{B}$ um homomorfismo entre eles. Definimos como sendo o* ***núcleo*** *de f, denotado por $\mathcal{N}(f)$ ou $Ker(f)$, o seguinte subconjunto de $\mathcal{A}$ dado por*

$$\mathcal{N}\,(f) = \{x \in \mathcal{A} : f\,(x) = 0_{\mathcal{B}}\}\,.$$

Exemplo 3.5.2 O núcleo do homomorfismo $f : \mathcal{A} \longrightarrow \mathcal{B}$ visto no exemplo 3.4.2, é o proprio anel $\mathcal{A}$. ♣

Exemplo 3.5.3 O núcleo do homomorfismo identidade visto no exemplo 3.4.3 é trivial, isto é,

$$\mathcal{N}\,(f) = \{0_{\mathcal{A}}\}\,.$$

♣

Exemplo 3.5.4 Determinar o núcleo do homomorfismo $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ definido por $f\,(m) = \overline{m}$. (cf. Exemplo 3.4.4).

Solução: Seja $m \in \mathbb{Z}$. Assim,

$$\begin{aligned} m \in \mathcal{N}\,(f) &\Leftrightarrow f\,(m) = 0_{\mathcal{B}} \\ &\Leftrightarrow \overline{m} = \overline{0} \\ &\Leftrightarrow m \in n \cdot \mathbb{Z}. \end{aligned}$$

Logo,

$$\mathcal{N}(f) = n \cdot \mathbb{Z}.$$

♣

Exemplo 3.5.5 Seja $\mathcal{A} = \mathbb{Z}\left[\sqrt{2}\right] = \left\{m + n\sqrt{2}; m, n \in \mathbb{Z}\right\}$ e consideremos $f : \mathcal{A} \longrightarrow \mathcal{A}$ assim definida: $f\left(m + n\sqrt{2}\right) = m - n\sqrt{2}$. f é um homomorfismo de anéis pois segundo as operações definidas no exemplo 3.1.7, se $a, b \in \mathcal{A}$ tais que $a = m + n\sqrt{2}$ e $b = r + s\sqrt{2}$, então

$$\begin{aligned} f(a+b) &= f\left(\left(m + n\sqrt{2}\right) + \left(r + s\sqrt{2}\right)\right) \\ &= f\left((m+r) + (n+s)\sqrt{2}\right) \\ &= (m+r) - (n+s)\sqrt{2} \\ &= f(a) + f(b) \end{aligned}$$

e

$$\begin{aligned} f(a \cdot b) &= f\left(\left(m + n\sqrt{2}\right) \cdot \left(r + s\sqrt{2}\right)\right) \\ &= f\left((mr + 2ns) + (ms + nr)\sqrt{2}\right) \\ &= (mr + 2ns) - (ms + nr)\sqrt{2} \\ &= f(a) \cdot f(b). \end{aligned}$$

Portanto, f é de fato um homomorfismo de anéis.Vamos determinar agora $\mathcal{N}(f)$. Dado $a \in \mathcal{A}$ tal que $a = m + n\sqrt{2}$, assim,

$$\begin{aligned} a \in \mathcal{N}(f) &\Leftrightarrow f\left(m + n\sqrt{2}\right) = 0 \\ &\Leftrightarrow m - n\sqrt{2} = 0 - 0\sqrt{2} \\ &\Leftrightarrow m = n = 0. \end{aligned}$$

Logo,

$$\mathcal{N}(f) = \{0\}.$$

♣

Exemplo 3.5.6 Sejam os anéis $\mathcal{A} = \mathbb{C}$ e $\mathcal{B} = \mathcal{M}_2(\mathbb{R})$ e a função $f : \mathcal{A} \longrightarrow \mathcal{B}$ dada por

$$f(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \quad \forall a + bi \in \mathbb{C}.$$

f é um homomorfismo. De fato, dados $x, y \in \mathbb{C}$ tais que $x = a + bi$ e $y = c + di$, definiremos

$$x + y = (a + c) + (b + d)\, i$$

e

$$x \cdot y = (ac - bd) + (ad - bc)\, i.$$

Desse modo,

$$\begin{aligned} f(x+y) &= \begin{pmatrix} a+c & -(b+d) \\ b+d & a+c \end{pmatrix} \\ &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \\ &= f(x) + f(y) \end{aligned}$$

e

$$\begin{aligned} f(x \cdot y) &= \begin{pmatrix} ac-bd & -(ad-bc) \\ ad-bc & ac-bd \end{pmatrix} \\ &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \\ &= f(x) \cdot f(y). \end{aligned}$$

Portanto, f é um homomorfismo. Seja agora $x = a + bi \in \mathbb{C}$. Temos que

$$\begin{aligned} x \in \mathcal{N}(f) &\Leftrightarrow f(a+bi) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ &\Leftrightarrow \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ &\Leftrightarrow a = b = 0, \end{aligned}$$

de onde segue que $x = 0$. Logo,

$$\mathcal{N}(f) = \{0\}.$$

♣

Há algo de especial no que se refere aos núcleos encontrados no exemplo 3.5.5 e no exemplo 3.5.6. Através deles, podemos definir na teoria dos anéis o conceito de homomorfismo injetor. Vejamos a seguir.

Proposição 3.5.7 *Seja $f : \mathcal{A} \longrightarrow \mathcal{B}$ um homomorfismo de anéis. Dizemos que f é injetivo se, e somente se, $\mathcal{N}(f) = \{0_{\mathcal{A}}\}$.*

Demonstração: Suponhamos que f seja um homomorfismo injetivo e tomemos $x \in \mathcal{N}(f)$. Assim, $f(x) = 0_{\mathcal{B}}$. Já vimos que $f(0_{\mathcal{A}}) = 0_{\mathcal{B}}$. Logo, segue por hipótese que

$$f(x) = f(0_{\mathcal{A}}) \Rightarrow x = 0_{\mathcal{A}}.$$

Portanto,

$$\mathcal{N}(f) = \{0_{\mathcal{A}}\}.$$

Por outro lado, tomemos como hipótese que $\mathcal{N}(f) = \{0_{\mathcal{A}}\}$. Desse modo, dados $x_1, x_2 \in \mathcal{A}$ tais que

$$f(x_1) = f(x_2) \Rightarrow f(x_1) - f(x_2) = 0_{\mathcal{B}} \Rightarrow f(x_1 - x_2) = 0_{\mathcal{B}}.$$

Por isso,

$$x_1 - x_2 \in \mathcal{N}(f) \Rightarrow x_1 - x_2 = 0_{\mathcal{A}} \Rightarrow x_1 = x_2.$$

Logo, f é injetivo. ■

3.6 Isomorfismo de Anéis

Existem anéis $\mathcal{A}$ e $\mathcal{B}$ que são os mesmos do ponto de vista algébrico. Em outras palavras, existe uma função homomorfismo f de $\mathcal{A}$ em $\mathcal{B}$, que preserva todas as propriedades entre estes anéis. Formalmente, estas funções levam a definição de isomorfismo.

Definição 3.6.1 *Sejam $\mathcal{A}$ e $\mathcal{B}$ dois anéis. Um homomorfismo $f : \mathcal{A} \longrightarrow \mathcal{B}$ bijetivo chama-se* ***isomorfismo****.*

Vale ressaltar que como um isomorfismo é um tipo especial de homomorfismo, então todas as propriedades inerentes aos homomorfismos vistas ate o momento se aplicam também aos isomorfismos.

Proposição 3.6.2 *Se $f : \mathcal{A} \longrightarrow \mathcal{B}$ é um isomorfismo de anéis, então $f^{-1} : \mathcal{B} \longrightarrow \mathcal{A}$ também é isomorfismo de anéis.*

Demonstração: O fato de f ser uma bijeção garante que f^{-1} também é uma aplicação bijetora, só que obviamente de $\mathcal{B}$ em $\mathcal{A}$. A demonstração deste fato será deixado a cargo do leitor. Seguindo, vemos que se f um isomorfismo do grupo aditivo $\mathcal{A}$ no grupo aditivo $\mathcal{B}$, então f^{-1} é um isomorfismo do grupo aditivo $\mathcal{B}$ no grupo aditivo $\mathcal{A}$, pois f^{-1} conserva as operações. De fato, tomemos $y_1, y_2 \in \mathcal{B}$. Como f é sobrejetora, $y_1 = f(x_1)$ e $y_2 = f(x_2)$, para convenientes elementos $x_1, x_2 \in \mathcal{A}$. Dai,

$$f^{-1}(y_1) = f^{-1}(f(x_1)) = x_1 \quad \text{e} \quad f^{-1}(y_2) = x_2.$$

Então:

$$\begin{aligned} f^{-1}(y_1 + y_2) &= f^{-1}(f(x_1) + f(x_2)) \\ &= f^{-1}(f(x_1 + x_2)) \\ &= x_1 + x_2 \\ &= f^{-1}(y_1) + f^{-1}(y_2). \end{aligned}$$

Por outro lado, resta-nos provar que f^{-1} preserva as multiplicações. Sejam $c, d \in \mathcal{B}$. Como f é sobrejetora, $c = f(a)$ e $d = f(b)$, para elementos $a, b \in \mathcal{A}$. Vale observar que

$$a = f^{-1}(c) \quad \text{e} \quad b = f^{-1}(d).$$

Posto que,

$$\begin{aligned} f^{-1}(cd) &= f^{-1}(f(a) \cdot f(b)) \\ &= f^{-1}(f(a \cdot b)) \\ &= a \cdot b \\ &= f^{-1}(c) \cdot f^{-1}(d), \end{aligned}$$

concluindo a demonstração. ■

Devido a esta demonstração que acabamos de fazer, podemos dizer que dois anéis $\mathcal{A}$ e $\mathcal{B}$ são **isomorfos** quando ocorre um isomorfismo entre eles. Simbolicamente, escrevemos

$$\mathcal{A} \simeq \mathcal{B}.$$

O isomorfismo $f : \mathcal{A} \longrightarrow \mathcal{B}$ preserva todas as propriedades do anel $\mathcal{A}$, fato que não ocorria quando tínhamos apenas um homomorfismo. Por isso, os anéis $\mathcal{A}$ e $\mathcal{B}$ são

considerados os mesmos. Assim, o elemento $a \in \mathcal{A}$ é identificado, via o isomorfismo f, com o elemento $f(a) \in \mathcal{B}$, ou seja, o elemento a é tido como se fosse igual ao elemento $f(a)$, já que possuem as mesmas propriedades algébricas. Denotamos essa correspondência por

$$a \longleftrightarrow f(a).$$

Exemplo 3.6.3 Se $\mathcal{A}$ é um anel então a aplicação $Id_{\mathcal{A}} : \mathcal{A} \longrightarrow \mathcal{A}$ tal que $Id_{\mathcal{A}}(x) = x, \forall$ $x \in \mathcal{A}$ é um isomorfismo de anéis, pois além de ser bijetora, é também um homomorfismo, uma vez que

$$Id_{\mathcal{A}}(x+y) = x+y = Id_{\mathcal{A}}(x) + Id_{\mathcal{A}}(y)$$

e

$$Id_{\mathcal{A}}(x \cdot y) = x \cdot y = Id_{\mathcal{A}}(x) \cdot Id_{\mathcal{A}}(x).$$

♣

Exemplo 3.6.4 A aplicação $f : \mathbb{Z}\left[\sqrt{2}\right] \longrightarrow \mathbb{Z}\left[\sqrt{2}\right]$ é um isomorfismo de anéis, pois segundo o exemplo *3.5.5* f é um homomorfismo. Além disso, $\mathcal{N}(f) = \{0\}$. Desse modo, pela proposição 3.5.7, f é injetivo. Por outro lado, a aplicação também é sobrejetora. De fato, dado $y = m+n\sqrt{2} \in \mathbb{Z}\left[\sqrt{2}\right]$, basta tomar $x = m-n\sqrt{2} \in \mathbb{Z}\left[\sqrt{2}\right]$ de modo que

$$f(x) = f\left(m - n\sqrt{2}\right) = m + n\sqrt{2} = y.$$

Portanto, f é um homomorfismo bijetivo, ou seja, é um isomorfismo de anéis. ♣

Exemplo 3.6.5 De acordo com o exemplo 3.5.6, a função $f : \mathbb{C} \longrightarrow \mathcal{M}_2(\mathbb{R})$ definida por

$$f(a+bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \forall a+bi \in \mathbb{C},$$

é um homomorfismo. Além disso, como $\mathcal{N}(f) = \{0\}$, pela proposição 3.5.7, f é injetivo. Por fim, como $\mathrm{Im}(f) = \mathcal{M}_2(\mathbb{R})$, temos que f é bijetivo e, assim, é um isomorfismo. ♣

Exemplo 3.6.6 De acordo com o exemplo 3.4.4, a aplicação $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ é um homomorfismo cujo núcleo segundo o exemplo 3.5.4 é

$$\mathcal{N}(f) = \{0, \ \pm m, \ \pm 2m, \ldots\}.$$

Como $\mathcal{N}(f) \neq 0_{\mathcal{A}}$, pela proposição 3.5.7, f não é injetivo. Portanto, f não é bijetivo e, assim, não se verifica um isomorfismo entre os anéis. ♣

Para enunciar o teorema fundamental dos homomorfismos para anéis e seus corolários, precisamos antes definir um dos instrumentos mais poderosos para o desenvolvimento da teoria dos anéis. É o que será feito a seguir.

3.7 Ideais em um Anel Comutativo

O conceito de ideal pode ser aplicado a toda qualidade de anel, no entanto nos restringiremos a usá-lo apenas em anéis comutativos, devido a sua importância nestes casos, bem como as limitações que os objetivos deste trabalho estabelecem.

Definição 3.7.1 *Seja $\mathcal{A}$ um anel comutativo. Um subconjunto $\mathcal{I} \subset \mathcal{A}$, $\mathcal{I} \neq \varnothing$ será chamado de* ***ideal*** *em $\mathcal{A}$ se, para quaisquer $x, y \in \mathcal{I}$ e $a \in \mathcal{A}$, verificam-se as relações seguintes:*

(1) $x - y \in \mathcal{I}$.

(2) $a \cdot x \in \mathcal{I}$.

Exemplo 3.7.2 Se $\mathcal{A}$ é um anel comutativo, então $\{0_{\mathcal{A}}\}$ e o próprio $\mathcal{A}$ são ideais em $\mathcal{A}$ – ***ideais triviais***. ♣

Exemplo 3.7.3 No anel $\mathbb{Z}$, os subconjuntos $n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}$, são ideais em $\mathbb{Z}$, qualquer que seja o inteiro n, pois se $b, c \in n\mathbb{Z}$, tais que $b = r \cdot n$ e $c = s \cdot n$ para quaisquer inteiros r e s, então

$$\begin{aligned} b - c &= r \cdot n - s \cdot n \\ &= n(r - s), \end{aligned}$$

com $r - s \in \mathbb{Z}$. Por outro lado, seja $a \in \mathbb{Z}$ e $x \in n\mathbb{Z}$, então, $x = nq$, com $q \in \mathbb{Z}$. Daí,

$$ax = a\,(nq) = (aq)\,n = n\,(aq)\,, \quad \text{com } aq \in \mathbb{Z}.$$

Portanto, $ax \in n\mathbb{Z}$. Logo, $n\mathbb{Z}$ é um ideal em $\mathbb{Z}$. ♣

Exemplo 3.7.4 O núcleo de um homomorfismo de anéis $f : \mathcal{A} \longrightarrow \mathcal{B}$ é um ideal em $\mathcal{A}$.

Solução: Como $f\,(0_{\mathcal{A}}) = 0_{\mathcal{B}}$, então $0_{\mathcal{A}} \in \mathcal{A}$ e, portanto, $\mathcal{N}\,(f) \neq \emptyset$. Sejam agora $x, y \in \mathcal{N}\,(f)$. Então $f\,(x) = f\,(y) = 0_{\mathcal{B}}$. Logo,

$$\begin{aligned} f\,(x-y) &= f\,(x) - f\,(y) \\ &= 0_{\mathcal{B}} - 0_{\mathcal{B}} \\ &= 0_{\mathcal{B}}, \end{aligned}$$

e portanto, $x - y \in \mathcal{N}\,(f)$. Por fim, dado $x \in \mathcal{N}\,(f)$, então $f\,(x) = 0_{\mathcal{B}}$ e, portanto, qualquer que seja $a \in \mathcal{A}$

$$\begin{aligned} f\,(a \cdot x) &= f\,(a) \cdot f\,(x) \\ &= f\,(a) \cdot 0_{\mathcal{B}} \\ &= 0_{\mathcal{B}}, \end{aligned}$$

o que mostra que $a \cdot x \in \mathcal{N}\,(f)$. Portanto, $\mathcal{N}\,(f)$ é um ideal em $\mathcal{A}$. ♣

3.8 O Teorema Fundamental dos Homomorfismos para Anéis

Vamos considerar, o principal teorema que versa sobre homomorfismos de anéis e seus respectivos corolários. Para tal, notemos primeiramente que, se $f : \mathcal{A} \longrightarrow \mathcal{B}$ é um homomorfismo de anéis, então $\mathcal{N}\,(f)$ é um ideal de $\mathcal{A}$ (cf. exemplo 3.7.4). Por isso, $\frac{\mathcal{A}}{\mathcal{N}(f)}$ é um anel.

Teorema 3.8.1 (*1º* ***Teorema do Isomorfismo***) *Seja $f : \mathcal{A} \longrightarrow \mathcal{B}$ um homomorfismo de anéis. Então,*

$$\frac{\mathcal{A}}{\mathcal{N}\,(f)} \simeq \mathrm{Im}\,(f)\,.$$

Demonstração: Definamos

$$\begin{array}{rccl} \Phi: & \frac{\mathcal{A}}{\mathcal{N}(f)} & \longrightarrow & \mathrm{Im}\,(f) \\ & x+\mathcal{N}(f) & \longmapsto & f(x). \end{array}$$

A função Φ está bem definida. De fato, se $\overline{x},\overline{y}\in\frac{\mathcal{A}}{\mathcal{N}(f)}$ tais que $\overline{x}=\overline{y}$, então

$$x\equiv y\,(\mathrm{mod}\,\mathcal{N}(f)),$$

isto é,$x=y+a$, com $a\in\mathcal{N}(f)$.Ora, se $a\in\mathcal{N}(f)$ pela definição de núcleo de um homomorfismo de anéis $f(a)=0_{\mathcal{B}}$. Daí,

$$\begin{array}{rcccl} \Phi(\overline{x}) & = & f(x) & = & f(y+a) \\ & & & = & f(y)+f(a) \\ & & & = & f(y) \\ & & & = & \Phi(\overline{y}). \end{array}$$

Portanto, Φ está bem definida. Sejam agora $\overline{x},\overline{y}\in\frac{\mathcal{A}}{\mathcal{N}(f)}$. Logo,

$$\begin{array}{rcl} \Phi(\overline{x}+\overline{y}) & = & \Phi(\overline{x+y}) \\ & = & f(x+y) \\ & = & f(x)+f(y) \\ & = & \Phi(\overline{x})+\Phi(\overline{y}) \end{array}$$

e

$$\begin{array}{rcl} \Phi(\overline{x}\cdot\overline{y}) & = & \Phi(\overline{x\cdot y}) \\ & = & f(x\cdot y) \\ & = & f(x)\cdot f(y) \\ & = & \Phi(\overline{x})\cdot\Phi(\overline{y}). \end{array}$$

Portanto, Φ é um homomorfismo. Além disso,

$$\Phi(\overline{x})=\Phi(\overline{y}) \quad\Rightarrow\quad f(x)=f(y) \quad\Rightarrow\quad f(x-y)=0_{\mathcal{B}}.$$

Desse modo, $x-y\in\mathcal{N}(f)$, isto é, $x=y+a$, para algum $a\in\mathcal{N}(f)$. Com isso,

$$\overline{x}=\overline{y}+\overline{a}=\overline{y},$$

Pois $\overline{a} = \overline{0}$. Assim, Φ é injetora. Por outro lado, Φ é claramente sobrejetora. Logo, Φ é um isomorfismo, ou seja, $\frac{\mathcal{A}}{\mathcal{N}(f)} \simeq \mathrm{Im}\,(f)$. ■

Exemplo 3.8.2 Usando o primeiro teorema do isomorfismo, mostrar que os anéis $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ e $\mathbb{Z}_n$ são isomorfos, para cada $n \in \mathbb{Z}$.

Solução: Usando a definição de isomorfismo, consideremos a função

$$\begin{aligned} \Phi : \quad \frac{\mathbb{Z}}{n\mathbb{Z}} &\longrightarrow \mathbb{Z}_n \\ x + n\mathbb{Z} &\longmapsto \overline{x}. \end{aligned}$$

Não é difícil mostrar que Φ está bem definida. Já sabemos do exemplo 3.4.4, que a função $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ definida por $f(m) = \overline{m}$, para todo $m \in \mathbb{Z}$ é claramente um homomorfismo sobrejetor de anéis. Sabemos também do exemplo 3.5.4, que dado $m \in \mathbb{Z}$, temos que $\mathcal{N}(f) = n\mathbb{Z}$. Desse modo, concluímos pelo primeiro teorema do isomorfismo que

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mathbb{Z}_n.$$

♣

Este exemplo pode ser mostrado também usando a própria definição de isomorfismo, fato que será deixado a cargo do leitor.

Exemplo 3.8.3 Consideremos o anel

$$\mathcal{A} = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R} \right\} \subset \mathcal{M}_2(\mathbb{R})$$

e seja $\mathcal{I}$ o seguinte ideal de $\mathcal{A}$

$$\mathcal{I} = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{R} \right\}.$$

Mostrar que $\dfrac{\mathcal{A}}{\mathcal{I}}$ é isomorfo ao corpo dos números reais $\mathbb{R}$.

Solução: Facilmente, verifica-se que $\mathcal{A}$ é subanél de $\mathcal{M}_2(\mathbb{R})$. Tomando agora

$$z = \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \in \mathcal{A}, \quad \text{com} \quad c, d \in \mathbb{R}$$

e sendo $x, y \in \mathcal{I}$ tais que

$$x = \begin{pmatrix} 0 & b_1 \\ 0 & 0 \end{pmatrix} \quad \text{e} \quad y = \begin{pmatrix} 0 & b_2 \\ 0 & 0 \end{pmatrix}, \quad \text{com} \quad b_1, b_2, c, d \in \mathbb{R},$$

implica que

$$\begin{aligned} x - y &= \begin{pmatrix} 0 & b_1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & b_2 \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & b_1 - b_2 \\ 0 & 0 \end{pmatrix} \in \mathcal{I}, \end{aligned}$$

e

$$\begin{aligned} z \cdot x &= \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & b_1 \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & cb_1 \\ 0 & 0 \end{pmatrix} \in \mathcal{I}. \end{aligned}$$

Portanto, $\mathcal{I}$ é um ideal de $\mathcal{A}$. Seguindo, vamos descrever os elementos do anel $\dfrac{\mathcal{A}}{\mathcal{I}}$. Dado

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \mathcal{A},$$

temos que

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

Ora, como

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in \mathcal{I},$$

então

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \mathcal{I} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \mathcal{I}.$$

Além disso, para $a, b \in \mathbb{R}$,

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \mathcal{I} = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} + \mathcal{I}$$

se, e somente se,

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} - \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a-b & 0 \\ 0 & a-b \end{pmatrix} \in \mathcal{I},$$

ou seja, se, e somente se, $a - b = 0$, de modo que $a = b$. Logo,

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

Agora, verifica-se que a função $f : \mathcal{A} \to \mathbb{R}$ dada, para qualquer

$$x = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \mathcal{A}$$

por

$$f(x) = a,$$

é um homomorfismo, pois dados $x_{1,}x_2 \in \mathcal{A}$ tais que

$$x_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \quad \text{e} \quad x_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix},$$

então

$$\begin{aligned} f(x_1 + x_2) &= f\left(\begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ 0 & a_1 + a_2 \end{pmatrix}\right) \\ &= a_1 + a_2 \\ &= f(x_1) + f(x_2) \end{aligned}$$

e

$$\begin{aligned} f(x_1 \cdot x_2) &= f\left(\begin{pmatrix} a_1 \cdot a_2 & b_1 \cdot b_2 \\ 0 & a_1 \cdot a_2 \end{pmatrix}\right) \\ &= a_1 \cdot a_2 \\ &= f(x_1) \cdot f(x_2). \end{aligned}$$

Portanto, f é um homomorfismo que claramente é sobrejetor. Para finalizar, dado

$$x = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \mathcal{A},$$

então

$$x \in \mathcal{N}(f) \quad \Leftrightarrow \quad f(x) = 0 \quad \Leftrightarrow \quad a = 0.$$

Portanto,

$$\begin{aligned} \mathcal{N}(f) &= \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in \mathcal{A} : b \in \mathbb{R} \right\} \\ &= \mathcal{I}. \end{aligned}$$

Assim, concluímos do primeiro teorema para homomorfismos que

$$\frac{\mathcal{A}}{\mathcal{I}} \simeq \mathbb{R}.$$

♣

Finalizaremos esta seção dando ênfase a dois corolários do Teorema 3.8.1.

Corolário 3.8.4 (*2º* ***Teorema do Isomorfismo***) *Sejam $\mathcal{B}$ um subanel de um anel $\mathcal{A}$ e $\mathcal{I}$ um ideal de $\mathcal{A}$. Então*

$$\frac{\mathcal{B}}{\mathcal{B}\cap\mathcal{I}} \simeq \frac{\mathcal{B}+\mathcal{I}}{\mathcal{I}}.$$

Demonstração: Notemos primeiramente que dados $b_1 + i_1$, $b_2 + i_2 \in \mathcal{B} + \mathcal{I}$, com b_1,$b_2 \in \mathcal{B}$ e i_1,$i_2 \in \mathcal{I}$ temos que

$$(b_1 + i_1)(b_2 + i_2) = \underbrace{b_1 b_2}_{\in\mathcal{B}} + \underbrace{b_1 i_2 + i_1 b_2 + i_1 i_2}_{\in\mathcal{I}} \in \mathcal{B} + \mathcal{I}$$

e

$$(b_1 + i_1) - (b_2 + i_2) = \underbrace{b_1 - b_2}_{\in\mathcal{B}} + \underbrace{i_1 - i_2}_{\in\mathcal{I}} \in \mathcal{B} + \mathcal{I}.$$

Desse modo, $\mathcal{B} + \mathcal{I}$ é um subanel de $\mathcal{A}$. Por outro lado, como $\mathcal{B}$ é um subanel de $\mathcal{A}$ e $\mathcal{I}$ um ideal de $\mathcal{A}$, se x,$y \in \mathcal{I}$ e $b + i \in \mathcal{B} + \mathcal{I}$, onde $b \in \mathcal{B}$, $i \in \mathcal{I}$, então

$$x - y \in \mathcal{I}$$

e

$$(b + i)\, x = \underbrace{bx}_{\in\mathcal{I}} + \underbrace{ix}_{\in\mathcal{I}} \in \mathcal{I}.$$

Portanto, $\mathcal{I}$ é um ideal de $\mathcal{B} + \mathcal{I}$. Agora, se x,$y \in \mathcal{B} \cap \mathcal{I}$, então tanto x,y pertence ao subanél $\mathcal{B}$ do anel $\mathcal{A}$ e dai resulta que $x - y \in \mathcal{B}$, quanto x,y pertence ao ideal $\mathcal{I}$, donde segue que $x - y \in \mathcal{I}$. Ora, como $x - y$ pertence a $\mathcal{B}$ e também a $\mathcal{I}$,

$$x - y \in \mathcal{B} \cap \mathcal{I}.$$

Sejam $a \in \mathcal{B}$ e $x \in \mathcal{B} \cap \mathcal{I}$. dai, $x \in \mathcal{B}$ e $x \in \mathcal{I}$ o que implica $ax \in \mathcal{B}$, e $ax \in \mathcal{I}$, já que $\mathcal{I}$ é um ideal por hipótese. Por consequinte,

$$ax \in \mathcal{B} \cap \mathcal{I}.$$

Portanto, $\mathcal{B} \cap \mathcal{I}$ é um ideal de $\mathcal{B}$. Consideremos agora, a função

$$\begin{array}{rccc} f: & \mathcal{B} & \longrightarrow & \frac{\mathcal{B}+\mathcal{I}}{\mathcal{I}} \\ & x & \longmapsto & x + I = \overline{x}. \end{array}$$

Dados x,$y \in \mathcal{B}+\mathcal{I}$, teremos

$$f(x+y) \;=\; \overline{x+y} \;=\; \overline{x}+\overline{y} \;=\; f(x)+f(y)$$

e

$$f(x\cdot y) \;=\; \overline{x\cdot y} \;=\; \overline{x}\cdot\overline{y} \;=\; f(x)\cdot f(y).$$

Desse modo, f é um homomorfismo. Observem também que se $\overline{x} \in \frac{\mathcal{B}+\mathcal{I}}{\mathcal{I}}$, então $\overline{x} = x+\mathcal{I}$, com $x = b+a$, em que $b \in \mathcal{B}$, $a \in \mathcal{I}$. Logo,

$$\begin{aligned} \overline{x} &= (b+a)+\mathcal{I} \\ &= (b+\mathcal{I})+(a+\mathcal{I}) \\ &= b+\mathcal{I}, \end{aligned}$$

pois $a+\mathcal{I} = \mathcal{I}$. Portanto, $f(b) = b+\mathcal{I} = \overline{x}$ e assim, f é sobrejetiva. Por fim, dado $x \in \mathcal{B}$ e sendo $\mathcal{I}$ o zero do anel quociente $\frac{\mathcal{B}+\mathcal{I}}{\mathcal{I}}$, temos

$$x \in \mathcal{N}(f) \;\Leftrightarrow\; f(x) = \mathcal{I} \;\Leftrightarrow\; x+\mathcal{I} = \mathcal{I},$$

isto é,

$$x \in \mathcal{N}(f) \;\Leftrightarrow\; x \in \mathcal{I} \quad \text{e} \quad x \in \mathcal{B} \;\Leftrightarrow\; x \in \mathcal{B}\cap\mathcal{I}.$$

Portanto, $\mathcal{N}(f) = \mathcal{B}\cap\mathcal{I}$, o que torna válido

$$\frac{\mathcal{B}}{\mathcal{B}\cap\mathcal{I}} \simeq \frac{\mathcal{B}+\mathcal{I}}{\mathcal{I}}.$$

■

Para encerrar, apresentaremos o terceiro teorema do isomorfismo, cuja demonstração não será apresentada.

Corolário 3.8.5 (*3º* ***Teorema do Isomorfismo***) *Sejam $\mathcal{J}$ e $\mathcal{I}$ ideais de um anel $\mathcal{A}$ tal que $\mathcal{J} \subset \mathcal{I}$. Então,*

$$\frac{\mathcal{A}/\mathcal{J}}{\mathcal{I}/\mathcal{J}} \simeq \mathcal{A}/\mathcal{I}.$$

3.9 Conclusão

Neste trabalho foram apresentados alguns resultados básicos sobre a Teoria dos Anéis, mais especificamente, tendo como foco principal os resultados sobre isomorfosmos de anéis. Tal objetivo foi o de explorar conceitos que, em geral, não são vistos em um curso de Licenciatura.

Tais resultados nos possibilita adentrar de forma mais eficaz num estudo de estruturas algébricas com duas operações binárias o que, de certa forma, generaliza os resultados obtidos sobre grupos.

Bibliografia

[1] Coutinho, S.C. Números Inteiros e Criptografia RSA. Rio de Janeiro: IMPA, 2011.

[2] Domingues, H.H. Iezzi, G. Álgebra Moderna. 4 ed. São Paulo: Atual, 2003.

[3] Garcia, A. Lequain, Y. Elementos de Álgebra. 6 ed. Rio de Janeiro: IMPA, 2012.

[4] Gonçalves, A. Introdução à Álgebra. 5 ed. Rio de Janeiro: IMPA, 2012.

[5] Hefez, A. Curso de Álgebra. 4 ed. Rio de Janeiro: IMPA, 2010.

[6] http://pt.wikipedia.org/wiki/%C3%81lgebra_abstrata, página consultada em 20 de maio de 2013.

[7] http://www.mat.unb.br/~maierr/anotas.pdf, página consultada em 22 de maio de 2013.