

# Notas da disciplina MAT0264 - Anéis e Corpos

Prof. Vinicius Rodrigues

11 de abril de 2025, 19:26



# Sumário

<b>Prefácio</b>	<b>v</b>
<b>1 Pré-Requisitos Conjuntistas</b>	<b>1</b>
1.1 Famílias e produtos cartesianos . . . . .	1
1.2 Operações . . . . .	2
<b>2 Noções de Grupos</b>	<b>3</b>
2.1 Definição e Propriedades Básicas . . . . .	3
2.2 Somatórios . . . . .	5
<b>3 Anéis e subanéis</b>	<b>7</b>
3.1 A definição de anel . . . . .	7
3.2 Anéis de Matrizes . . . . .	8
3.3 Domínios de Integridade . . . . .	11
3.4 Elementos invertíveis . . . . .	11
3.5 O anel dos números inteiros . . . . .	12
3.6 Corpos e anéis de divisão . . . . .	13
3.7 Subanéis . . . . .	13
3.8 O centro de um anel . . . . .	14
3.9 Exercícios . . . . .	15
<b>4 Homomorfismos e Ideais</b>	<b>17</b>
4.1 Definição de homomorfismo . . . . .	17
4.2 Propriedades elementares . . . . .	18
4.3 Ideais . . . . .	20
<b>5 Quocientes e Teoremas do Homomorfismo</b>	<b>25</b>
5.1 Relações de congruência . . . . .	25
5.2 Quocientes . . . . .	27
5.3 Teoremas do isomorfismo . . . . .	28
<b>6 Produtos de anéis</b>	<b>29</b>
6.1 Produtos de dois anéis . . . . .	29
6.2 Produtos de uma família de anéis . . . . .	29
6.3 A propriedade universal do produto direto de anéis . . . . .	30



# Prefácio

Estas notas começaram a ser escritas durante o primeiro semestre de 2025, enquanto lecionada a disciplina MAT0264 - Anéis e Corpos, no Instituto de Matemática e Estatística da Universidade de São Paulo (IME-USP). No presente estado, elas estão em um formato de rascunho, e não são um material completo, nem revisado. O objetivo é que, ao longo do semestre, as notas sejam revisadas e completadas, de modo a se tornarem um material didático mais completo e acessível aos alunos da disciplina.

É assumido que o estudante já tem algum traquejo ao lidar com números inteiros e aritmética modular, tendo já estudado, formalmente, divisibilidade de inteiros, congruência módulo  $n$  e os anéis  $\mathbb{Z}_n$ . Será assumida a existência do anel dos números inteiros, e, ao longo do texto, apresentaremos as construções de todos os outros anéis relevantes. Porém, alguns anéis importantes e conhecidos, como  $\mathbb{Q}$ ,  $\mathbb{R}$  e  $\mathbb{C}$ , com o qual espera-se que o estudante já possua alguma familiaridade, serão utilizados em exemplos desde o começo, mesmo antes de que construções formais sejam apresentadas.

Ao final de cada seção, serão apresentados exercícios, que o estudante deve resolver para fixar o conteúdo apresentado.

O autor deste texto agradece ao Professor Ugo Bruzzo, que lecionou o primeiro terço dessa disciplina, e formulou uma porção considerável dos exercícios aqui expostos.



# Capítulo 1

## Pré-Requisitos Conjuntistas

Durante o texto, precisamos de algumas definições e resultados envolvendo noções básicas sobre conjuntos e funções.

Não é objetivo deste texto desenvolver a parte inicial da Teoria dos Conjuntos. Também não é o objetivo desta seção explicar toda a notação de conjuntos utilizada. Assumimos familiaridade do leitor com funções e com manipulação de conjuntos a nível básico. Apenas apresentaremos algumas definições, notações e resultados básicos que utilizaremos ao longo do texto.

### 1.1 Famílias e produtos cartesianos

Famílias são funções com notação especial. Muitas vezes, ao pensar em funções, pensamos em um “dispositivo de entrada/saída”. Quando, ao invés disso, estamos pensando apenas em um “conjunto indexado de valores”, a notação de família pode ser mais conveniente.

No quadro abaixo, apresentamos uma comparação entre as duas notações. Enfatizamos que, matematicamente, funções e famílias podem ser vistas como o mesmo objeto.

Conceito	Função	Família
Mapa	$u : I \rightarrow A$	$(u_i)_{i \in I} = (u_i : i \in I)$
Valor	$u(i)$	$u_i$
Imagem	$\text{ran } u$	$\{u_i : i \in I\}$
Intuição	objeto dinâmico	objeto estático
Inputs	domínio $I$	conjunto de índices $I$

Tabela 1.1: Comparativo de família e função

Como exemplos, consideremos sequências infinitas e finitas:

**Exemplo 1.1** (Sequências). Uma sequência é uma família cujo conjunto de índices é  $\mathbb{N}$ . Compare a intuição que passa as notações:

- Considere a sequência  $u = (\frac{1}{2^n})_{n \in \mathbb{N} \dots}$
- Considere a função  $u : \mathbb{N} \rightarrow \mathbb{R}$  dada por  $u(n) = \frac{1}{2^n} \dots$

□

**Exemplo 1.2** (Sequências finitas). Se  $n \geq 1$ , identificamos  $n = \{0, 1, \dots, n-1\}$ . Assim:

- Uma família com  $n$  elementos é uma família  $(a_i)_{i < n} = (a_i)_{i \in n} = (a_0, \dots, a_{n-1})$ .

Essa notação é bastante funcional no sentido de que dá significado como conjunto aos números naturais, e corresponde à construção usual dos números naturais na Teoria dos Conjuntos. Como desvantagem, seus contadores se iniciam no 0, e não no 1, o que pode ser pouco intuitivo e não coincidir com a notação da maioria dos textos de matemática, apesar de ser muito adotada em textos mais próximos de Teoria dos Conjuntos.  $\square$

Agora vamos seguir para a definição de produto cartesiano. Primeiro, vamos lembrar a definição de produto cartesiano de dois conjuntos.

**Definição 1.3** (Produto cartesiano de dois conjuntos). Sejam  $A, B$  conjuntos. Então  $A \times B = \{(a, b) : a \in A, b \in B\}$  é o *produto cartesiano de  $A$  e  $B$* . Ou seja, o conjunto de todos os pares ordenados  $(a, b)$  tais que  $a \in A$  e  $b \in B$ .  $\square$

Pares ordenados são conjuntos especiais que carregam duas coordenadas de modo a permitem distinguir a ordem dos elementos. Sua propriedade principal é a de se  $a, b, c, d$  são conjuntos, então  $(a, b) = (c, d)$  se, e somente se  $a = c$  e  $b = d$ . Uma construção usual, chamada de par de Kuratowski, para a qual não é difícil provar que vale essa propriedade, é dada por  $(a, b) = \{\{a\}, \{a, b\}\}$ . Porém, isso não será importante neste texto.

**Definição 1.4** (Produto cartesiano de conjuntos). Seja  $(A_i)_{i \in I}$  uma família de conjuntos. O produto cartesiano de conjuntos é o conjunto  $\prod_{i \in I} A_i$  definido como o conjunto de todas as famílias  $(a_i : i \in I)$  tais que para cada  $i \in I$ ,  $a_i \in A_i$ .

$$\prod_{i \in I} A_i = \{(a_i)_{i \in I} : \forall i \in I, a_i \in A_i\}.$$

$\square$

**Definição 1.5** (Exponenciação de conjuntos). Sejam  $A, I$  conjuntos. O conjunto  $A^I$  é o conjunto de todas as funções de  $I$  em  $A$ . Ou seja,  $A^I = \{f : I \rightarrow A\}$ . Note que:

$$A^I = \prod_{i \in I} A = \{(a_i)_{i \in I} : \forall i \in I, a_i \in A\}.$$

$\square$

Na notação anterior, se  $n \geq 1$ , então:

$$A^n = \{(a_i)_{i < n} : \forall i < n, a_i \in A\} = \{(a_0, \dots, a_{n-1}) : a_0, \dots, a_{n-1} \in A\} \approx A \times \dots \times A \text{ (} n \text{ vezes)}.$$

## 1.2 Operações

Ao trabalharmos com estruturas algébricas necessitaremos da noção de operação, que se define como a seguir:

**Definição 1.6** (Operações  $n$ -árias). Se  $X$  é um conjunto e  $n \in \mathbb{N}$ , uma operação  $n$ -ária em  $X$  é uma função  $f : X^n \rightarrow X$ .  $\square$

Operações 2-árias e 1-árias são frequentemente chamadas de *binárias* e *unárias*, respectivamente.

Caso  $*$  seja uma operação binária, a notação  $x * y$  é frequentemente utilizada para denotar  $x * y$ .

Caso  $*$  seja uma operação unária, a notação  $*x$  é frequentemente utilizada para denotar  $*(x)$ .



## Capítulo 2

# Noções de Grupos

### 2.1 Definição e Propriedades Básicas

O principal objetivo deste texto é servir como texto para um estudo introdutório sobre anéis e corpos. A noção de grupo é mais simples do que ambas essas estruturas, porém, necessita de ferramentas especiais para seu tratamento completo que fogem do escopo deste texto. Assim, não é objetivo deste capítulo apresentar uma introdução ao estudo de grupos, mas sim apenas enunciar as principais definições e propriedades que utilizaremos ao longo do texto.

**Definição 2.1.** Um grupo é uma quadrupla  $(G, \cdot, e)$ , tal que  $G$  é um conjunto,  $\cdot$  é uma operação binária em  $G$  e  $e \in G$ , e satisfazem:

- (**Propriedade associativa**)  $\forall a, b, c \in G \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$ .
- (**Elemento neutro**)  $\forall a \in G \ e \cdot a = a \cdot e = a$ .
- (**Elemento inverso**)  $\forall a \in G \ \exists b \in G \ a \cdot b = b \cdot a = e$ .

Se, adicionalmente, a seguinte propriedade é satisfeita, o grupo é chamado de *comutativo*, ou, mais comunmente, *Abeliano*:

- (**Comutatividade**)  $\forall a, b \in G \ a \cdot b = b \cdot a$ .

□

Algumas observações importantes sobre a notação utilizada no estudo de grupos:

- Ao discursar sobre grupos, é comum omitir a operação e o elemento neutro, referindo-se apenas ao conjunto  $G$ .
- Caso o grupo seja Abeliano, é comum que sua operação binária seja denotada por  $+$  ou outro símbolo similar. Nesse contexto, o elemento neutro é frequentemente denotado por  $0$ .
- Caso o grupo não seja Abeliano, é comum que sua operação binária seja denotada por  $\cdot$  ou outro símbolo similar. Nesse contexto, o elemento neutro é frequentemente denotado por  $e$ , e a operação é frequentemente omitida, ou seja,  $a \cdot b$  é frequentemente escrito como  $ab$ .

Alguns exemplos:

- Com a soma usual,  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  são grupos Abelianos.
- Com a multiplicação usual, o círculo unitário complexo  $\mathbb{T} = \{x \in \mathbb{C} : |x| = 1\}$  é um grupo Abeliano com elemento neutro 1. De fato, o produto de complexos é comutativo, associativo e tem 1 como elemento neutro. Note que  $1 \in \mathbb{T}$  e  $0 \notin \mathbb{T}$ . Se  $x \in \mathbb{T}$ , o inverso multiplicativo de  $x$  é dado por  $\frac{\bar{x}}{|x|^2}$ , onde  $\bar{x}$  denota o conjugado de  $x$ . Como  $|\bar{x}| = |x| = 1$ , segue que  $\mathbb{T}$  tem todos os inversos de todos seus elementos.
- Os inteiros módulo  $n$  ( $n \geq 1$ ), dados por  $\mathbb{Z}_n = \{0, \dots, n-1\}$  com a soma dada pela aritmética módulo  $n$ , são grupos.

Agora iniciaremos a provar algumas propriedades básicas sobre grupos.

**Proposição 2.2** (Unicidade do elemento neutro). Seja  $(G, \cdot, e)$  um grupo. Então, o elemento neutro  $e$  é único. Isto é, se  $h \in G$  é tal que  $\forall a \in G \ h \cdot a = a \cdot h = a$ , então  $h = e$ .

*Demonstração.* Note que  $h = he$ , pois  $e$  é elemento neutro. Por outro lado,  $e = he$ , pois  $h$  é elemento neutro. Assim,  $h = he = e$ .  $\square$

**Proposição 2.3** (Unicidade dos inversos). Seja  $(G, \cdot, e)$  um grupo. Então todo  $a \in G$  possui um único elemento inverso, ou seja, para todo  $a \in G$ ,  $\exists!$   $b \in G$   $a \cdot b = b \cdot a = e$ .

*Demonstração.* A existência do inverso é garantida pela definição de grupo. Para provar a unicidade, suponha que  $b, c$  são inversos de  $a$ , ou seja,  $a \cdot b = b \cdot a = e$  e  $a \cdot c = c \cdot a = e$ . Então, temos:

$$b = be = b(ac) = (ba)c = ec = c.$$

$\square$

A unicidade do elemento neutro e dos inversos nos permite definir a notação  $a^{-1}$  para o inverso de  $a$  em um grupo  $(G, \cdot, e)$ . Caso  $(G, +, 0)$  seja um grupo Abeliano, a notação  $-a$  é frequentemente utilizada para denotar o inverso de  $a$ , e, nesse caso,  $-a$  é chamado de *oposto* de  $a$ .

Note que assim, ficam definidos operadores unários  $()^{-1} : G \rightarrow G$  (ou  $- : G \rightarrow G$ ). Para o segundo caso, define-se também que  $a - b = a + (-b)$ .

**Proposição 2.4** (Cancelamento). Seja  $(G, \cdot, e)$  um grupo. Então, se  $a, b, c \in G$  e  $a \cdot b = a \cdot c$ , então  $b = c$ . Analogamente, se  $b \cdot a = c \cdot a$ , então  $b = c$ .

*Demonstração.* Provaremos a primeira afirmação. A segunda é análoga e fica como exercício. Suponha que  $ba = ca$ . Então  $b = be = b(aa^{-1}) = (ba)a^{-1} = (ca)a^{-1} = c(aa^{-1}) = ce = c$ . Assim,  $b = c$ .  $\square$

**Corolário 2.5** (Cancelamento II). Seja  $(G, \cdot, e)$  um grupo. Para todos  $a, b \in G$ , se  $ab = a$ , então  $b = e$ . Analogamente, se  $ba = a$ , então  $b = e$ .

*Demonstração.* Para a primeira afirmação, note que  $ab = ae$ , logo, pela proposição anterior,  $b = e$ . A segunda afirmação é análoga.  $\square$

**Proposição 2.6** (Regras de sinal). Seja  $G$  um grupo e  $a, b \in G$ . Então:

- a)  $((a)^{-1})^{-1} = a$  [na notação aditiva,  $-(-a) = a$ ].

b)  $(ab)^{-1} = b^{-1}a^{-1}$  [na notação aditiva,  $-(a+b) = (-b) + (-a)$ ].

c)  $e^{-1} = e$  [na notação aditiva,  $-0 = 0$ ].

*Demonstração.* a): Temos que  $(a^{-1})^{-1}a^{-1} = e = aa^{-1}$ . Cancelando  $a^{-1}$ , segue.

b): Temos que  $(ab)^{-1}(ab) = e = (b^{-1}a^{-1})ab$ . Cancelando  $ab$ , segue que  $(ab)^{-1} = b^{-1}a^{-1}$ . Analogamente,  $(ba)^{-1} = a^{-1}b^{-1}$ .

c): Temos que  $(e^{-1})e = e = ee$ . Cancelando  $e$  à direita, segue.

□

## 2.2 Somatórios

Nessa seção, formalizaremos a noção de somatório. É desejável que o leitor já possua familiaridade com alguma notação de somatório, mas aqui apresentaremos a notação e as técnicas de “substituição de variáveis” que serão utilizadas.

**Definição 2.7** (Soma de sequência finita). Seja  $G$  um conjunto munido de uma operação  $+$  associativa, comutativa e com neutro  $0$ . Define-se, recursivamente para  $n \geq 0$ , o somatório de famílias  $(a_i : i \in F)$ , onde  $F$  é um conjunto de  $n$  índices e  $a_i \in G$  para todo  $i \in F$ , como se segue:

- **Notação:** se  $a = (a_i)_{i \in F}$  é uma sequência de elementos de  $G$ , então usamos as notações:

$$\sum a = \sum (a_i : i \in F) = \sum_{i \in F} a_i.$$

- Caso base  $n = 0$  (soma vazia): só existe uma família com 0 elementos, que é a família vazia  $a = () = \emptyset = (a_i : i \in \emptyset)$ . Definimos:

$$\sum a = \sum_{i \in \emptyset} a_i = 0$$

- Passo recursivo  $n \rightarrow n+1$ : considere uma família  $(a_i)_{i \in F}$ , onde  $|F| = n+1$ . Define-se:

$$\sum (a_i : i \in F) = \sum (a_i : i \in F \setminus \{j\}) + a_j,$$

onde  $j \in I$  é qualquer elemento.

□

É claro que, para mostrar que a definição acima é consistente, precisamos mostrar que a soma não depende da escolha de  $j$ .

**Lema 2.8.** Qualquer que seja o tamanho (finito) de  $F$ ,  $\sum (a_i)_{i \in F}$  está bem definido.

*Demonstração.* Seja  $F$  um conjunto finito. Se  $|F| = 0$ , então  $F = \emptyset$ , e a soma é 0. Se  $|F| = 1$ , então  $F = \{j\}$  – só há uma escolha para  $j$ , e a soma é  $a_j$ . Se  $|F| = n+1$  para  $n \geq 1$ , tome  $j, k \in F$ . Devemos ver que  $\left(\sum_{i \in F \setminus \{j\}} a_i\right) + a_j = \left(\sum_{i \in F \setminus \{k\}} a_i\right) + a_k$ . Com efeito:

$$\begin{aligned}
\left( \sum_{i \in F \setminus \{j\}} a_i \right) + a_j &= \left( \left( \sum_{i \in F \setminus \{j, k\}} a_i \right) + a_k \right) + a_j = \left( \sum_{i \in F \setminus \{j, k\}} a_i \right) + (a_k + a_j) \\
&= \left( \sum_{i \in F \setminus \{j, k\}} a_i \right) + (a_j + a_k) = \left( \left( \sum_{i \in F \setminus \{j, k\}} a_i \right) + a_j \right) + a_k = \left( \sum_{i \in F \setminus \{k\}} a_i \right) + a_k.
\end{aligned}$$

□

**Proposição 2.9.** Seja  $G$  um conjunto munido de uma operação  $+$  associativa, comutativa e com neutro  $0$ . Seja  $(a_i : i \in I)$  uma família finita em  $G$  e  $\phi : J \rightarrow I$  uma função bijetora. Então:

$$\sum_{i \in I} a_i = \sum_{j \in J} a_{\phi(j)}.$$

*Demonstração.* Novamente, procedemos por indução no tamanho de  $n = |I|$ . A base de tamanho  $0$  é trivial, já que ambos os lados da igualdade são  $0$ .

Para o passo indutivo em que  $|I| = |J| = n + 1$ , considere  $\phi : J \rightarrow I$  como no enunciado. Fixe  $k \in J$  qualquer e sejam  $I' = I \setminus \{\phi(k)\}$ ,  $J' = J \setminus \{k\}$  e  $\phi' = \phi|_{J'} : J' \rightarrow I'$ , que é bijetora. Como  $|J'| = |I'| = n$ , por hipótese indutiva temos que  $\sum_{j \in J'} a_{\phi(j)} = \sum_{i \in I'} a_i$ . Segue que:

$$\sum_{j \in J} a_{\phi(j)} = \left( \sum_{j \in J'} a_{\phi(j)} \right) + a_{\phi(k)} = \left( \sum_{i \in I'} a_i \right) + a_{\phi(k)} = \sum_{j \in I} a_j.$$

□

## Capítulo 3

# Anéis e subanéis

Nesta seção, iniciaremos o estudo dos anéis e de estruturas relacionadas. Apresentaremos as definições dessas estruturas e suas propriedades mais elementares.

### 3.1 A definição de anel

No Capítulo 2, conhecemos, por alto, a definição de grupo. Um grupo é um conjunto munido de uma operação binária que satisfaz algumas propriedades. Ele pode ser Abeliano ou não Abeliano, e, quando é Abeliano, lembra-nos da adição de inteiros. Porém, estruturas como inteiros, racionais e reais não são apenas grupos Abelianos, pois possuem também outra operação binária – a multiplicação. Esta operação se relaciona com a soma através das propriedades distributivas.

A noção de anel visa capturar parte dessas ideias, de modo a generalizar o estudo das estruturas citadas acima.

**Definição 3.1** (Anel). Um anel é uma 4-upla  $(A, +, \cdot, 0, 1)$  conjunto  $A$  com duas operações binárias, adição e multiplicação, denotadas por  $+$  e  $\cdot$ , tais que:

- $(A, +, 0)$  é um grupo abeliano.
- **(Associatividade)** Para todo  $a, b \in A$ , temos  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ .
- **(Elemento identidade)**  $\forall a \in A$   $1 \cdot a = a \cdot 1 = a$ .
- **(Propriedades distributivas)** Para todos  $a, b, c \in A$ , temos:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \text{ e} \\ (a + b) \cdot c = a \cdot c + b \cdot c$$

Se, adicionalmente, a seguinte propriedade é satisfeita, o anel é chamado de *comutativo*.

- **(Comutatividade)**  $\forall a, b \in A$   $a \cdot b = b \cdot a$ .

□

Algumas observações:

- Como em grupos, ao discursar sobre anéis é comum omitir as operações, referindo-se apenas ao conjunto  $A$ .

- Ao discursar sobre anéis, e a exemplo do que foi feito ao enunciar as propriedades distributivas, são utilizadas as convenções usuais sobre precedência de operações envolvidas por parênteses. Assim,  $a + b \cdot c$  é interpretado como  $a + (b \cdot c)$ .
- Há textos que definem anéis sem incluir o elemento identidade 1. Nestes textos, a definição acima dá nome ao que chamam de *anéis com identidade*, ou *anéis com 1*. Nesse curso, não usaremos essa convenção, de modo que **todos nossos anéis possuem identidade**. De modo similar, alguns textos definem anéis como sendo comutativos. Também não adotaremos essa convenção. **Os nossos anéis podem ser não comutativos**.
- A definição de anel não exige que  $0 = 1$ .
- 0 é chamado de elemento nulo, e 1 de elemento identidade.

**Proposição 3.2** (Propriedade multiplicativa do 0). Seja  $A$  um anel. Então  $\forall a \in A$   $0 \cdot a = a \cdot 0 = 0$ .

*Demonstração.* Provaremos a primeira afirmação. A segunda é análoga e fica como exercício.

Temos que  $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$ . Cancelando, segue que  $0 = 0 \cdot a$ .  $\square$

**Proposição 3.3** (Anel trivial). Seja  $A = x$  um conjunto qualquer. Defina  $x \cdot x = x = x + x = 0 = 1$ . Então  $(A, +, \cdot, 0, 1)$  é um anel. Um anel dessa forma é chamado de *anel trivial*.

Além disso, se  $A$  é um anel tal que  $0 = 1$ , então  $A$  é um anel trivial.

*Demonstração.* A primeira afirmação (de que  $A$  como acima é um anel) fica como exercício.

Para a segunda afirmação, assumamos que  $A$  é um anel tal que  $0 = 1$ . Fixe  $a \in A$  qualquer. Então  $a = a \cdot 1 = a \cdot 0 = 0$ , ou seja,  $a = 0$ . Assim,  $A$  é o conjunto unitário  $\{0\}$ , que é um anel trivial.  $\square$

Todo anel satisfaz as conhecidas regras de sinais referentes à multiplicação e adição, como:

**Proposição 3.4** (Regras de sinal II). Seja  $A$  um anel e  $a, b \in A$ . Então:

- $(-a)b = a(-b) = -(ab)$
- $(-a)(-b) = ab$ .
- $(-1)a = -a$ .

*Demonstração.* a): Temos que  $ab + (-a)b = (-a)b + ab = [-a + a]b = 0b = 0$ . Assim,  $(-a)b = -(ab)$ . Analogamente,  $a(-b) = -(ab)$ .

b): Temos que  $(-a)(-b) = -[a(-b)] = -[-(ab)] = ab$  pela regra anterior.

c): Temos que  $(-1)a = -(1a) = -a$ .  $\square$

## 3.2 Anéis de Matrizes

Dado qualquer anel  $A$  e  $n, m \in \mathbb{N}$ , podemos construir o conjunto das matrizes com coeficientes em  $A$ .

**Definição 3.5.** Seja  $A$  um anel e  $n, m$  inteiros positivos. O conjunto  $M_{n \times m}(A)$  é o conjunto de matrizes  $n \times m$  cujos coeficientes estão em  $A$ . Formalmente,  $M_{n \times m}$  é o conjunto de todas as famílias  $(a_{ij})_{i,j} = (a_{ij} : (i, j) \in \{1, \dots, n\} \times \{1, \dots, m\})$ . Quando conveniente, representamos a tal matriz de qualquer uma das duas formas a seguir:

$$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \quad \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix}$$

Se  $(a_{i,j})_{i,j}$  e  $(b_{i,j})_{i,j}$  são matrizes  $n \times m$  em  $M_{n \times m}(A)$ , definimos sua *soma* como  $(a_{i,j}) + (b_{i,j})_{i,j} = (a_{i,j} + b_{i,j})_{i,j}$ . Em outra notação:

$$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} + \begin{pmatrix} b_{11} & \cdots & b_{1m} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nm} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & \cdots & a_{1m} + b_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} + b_{n1} & \cdots & a_{nm} + b_{nm} \end{pmatrix}$$

Se  $(a_{ij})_{i,j} \in M_{n \times m}(A)$  e  $(b_{ij})_{i,j} \in M_{m \times p}(A)$ , definimos o produto de matrizes como  $(a_{ij})_{i,j} \cdot (b_{ij})_{i,j} = (c_{ij})_{i,j}$ , onde  $c_{ij} = \sum_{k=1}^m a_{ik}b_{kj}$ . Em outra notação:

$$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & \cdots & b_{1p} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mp} \end{pmatrix} = \begin{pmatrix} c_{11} & \cdots & c_{1p} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{np} \end{pmatrix}$$

A matriz nula de  $M_{n \times m}(A)$  é a matriz cuja todas as entradas são  $0 \in A$ , e é denotada por  $0_{n \times m}$ , ou, simplesmente,  $0$ .

Caso  $n = m$ , abreviamos  $M_{n \times n}(A)$  como  $M_n(A)$ . □

Sobre a aditividade, independente de  $m, n$ , sempre temos um grupo Abeliano:

**Proposição 3.6.** Seja  $A$  um anel e  $n, m \in \mathbb{N}$ . Então, o conjunto  $M_{n \times m}(A)$ , munido da operação de soma de matrizes, é um grupo abeliano.

*Demonstração.* Sejam  $(a_{ij})_{i,j}, (b_{ij})_{i,j}, (c_{ij})_{i,j} \in M_{n \times m}(A)$ . Mostraremos que  $(M_{n \times m}(A), +)$  satisfaz as propriedades de um grupo abeliano:

1. **Fechamento:** Para todos  $(a_{ij})_{i,j}, (b_{ij})_{i,j} \in M_{n \times m}(A)$ , temos que  $(a_{ij} + b_{ij})_{i,j} \in M_{n \times m}(A)$ , pois  $A$  é fechado sob adição.
2. **Associatividade:** A soma de matrizes é associativa, pois, para todos  $(a_{ij})_{i,j}, (b_{ij})_{i,j}, (c_{ij})_{i,j} \in M_{n \times m}(A)$ , temos:

$$((a_{ij}) + (b_{ij})) + (c_{ij}) = (a_{ij} + b_{ij}) + c_{ij} = a_{ij} + (b_{ij} + c_{ij}) = (a_{ij}) + ((b_{ij}) + (c_{ij})).$$

3. **Elemento neutro:** A matriz nula é o elemento neutro. Com efeito, dado  $(a_{ij})_{i,j} \in M_{n \times m}(A)$ , temos:

$$(a_{ij}) + 0_{m \times n} = (a_{ij} + 0) = (a_{ij}).$$

4. **Elemento inverso:** Para cada  $(a_{ij})_{i,j} \in M_{n \times m}(A)$ , a matriz  $(-a_{ij})_{i,j}$ , é oposto aditivo, pois:

$$(a_{ij}) + (-a_{ij}) = (a_{ij} + (-a_{ij})) = 0$$

5. **Comutatividade:** A soma de matrizes é comutativa, pois, para todos  $(a_{ij})_{i,j}, (b_{ij})_{i,j} \in M_{n \times m}(A)$ , temos:

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) = (b_{ij} + a_{ij}) = (b_{ij}) + (a_{ij}).$$

Portanto,  $(M_{n \times m}(A), +)$  é um grupo abeliano.  $\square$

A multiplicação de matrizes é associativa e distributiva sobre a soma. Formalmente:

**Proposição 3.7.** Seja  $A$  um anel e  $n, m, p, q \geq 1$ . Então:

a) **(Associatividade)** Para todos  $(a_{ij})_{i,j} \in M_{n \times m}(A)$ ,  $(b_{jk})_{j,k} \in M_{m \times p}(A)$  e  $(c_{kl})_{k,l} \in M_{p \times q}(A)$ , temos:

$$((a_{ij}) \cdot (b_{jk})) \cdot (c_{kl}) = (a_{ij}) \cdot ((b_{jk}) \cdot (c_{kl})).$$

b) **(Distributividade)** Para todos  $(a_{ij})_{i,j} \in M_{n \times m}(A)$ ,  $(b_{jk})_{j,k}, (c_{jk})_{j,k} \in M_{m \times p}(A)$ , temos:

$$(a_{ij}) \cdot ((b_{jk}) + (c_{jk})) = (a_{ij}) \cdot (b_{jk}) + (a_{ij}) \cdot (c_{jk}).$$

E, para todos  $(a_{ij})_{i,j}, (b_{ij})_{i,j} \in M_{n \times m}(A)$  e  $(c_{jk})_{j,k} \in M_{m \times p}(A)$ , temos:

$$((a_{ij}) + (b_{ij})) \cdot (c_{jk}) = (a_{ij}) \cdot (c_{jk}) + (b_{ij}) \cdot (c_{jk}).$$

*Demonstração.* **a)** Sejam  $(a_{ij})_{i,j} \in M_{n \times m}(A)$ ,  $(b_{jk})_{j,k} \in M_{m \times p}(A)$  e  $(c_{kl})_{k,l} \in M_{p \times q}(A)$ . Considere o elemento  $(i, l)$  da matriz resultante de  $((a_{ij}) \cdot (b_{jk})) \cdot (c_{kl})$ . Pela propriedade distributiva, temos:

$$\sum_{k=1}^p \left( \sum_{j=1}^m a_{ij} b_{jk} \right) c_{kl} = \sum_{k=1}^p \left( \sum_{j=1}^m a_{ij} b_{jk} c_{kl} \right).$$

Comutando os somatórios e novamente pela propriedade distributiva, isso é:

$$\sum_{j=1}^m \left( \sum_{k=1}^p a_{ij} b_{jk} c_{kl} \right) = \sum_{j=1}^m a_{ij} \left( \sum_{k=1}^p b_{jk} c_{kl} \right),$$

que é exatamente o elemento  $(i, l)$  da matriz  $(a_{ij}) \cdot ((b_{jk}) \cdot (c_{kl}))$ . Assim, a associatividade é satisfeita.

**b)** Para a distributividade, considere  $(a_{ij})_{i,j} \in M_{n \times m}(A)$ ,  $(b_{jk})_{j,k}, (c_{jk})_{j,k} \in M_{m \times p}(A)$ . O elemento  $(i, k)$  da matriz resultante de  $(a_{ij}) \cdot ((b_{jk}) + (c_{jk}))$  é dado por:

$$\sum_{j=1}^m a_{ij} (b_{jk} + c_{jk}) = \sum_{j=1}^m (a_{ij} b_{jk} + a_{ij} c_{jk}) = \sum_{j=1}^m a_{ij} b_{jk} + \sum_{j=1}^m a_{ij} c_{jk}$$

Isso corresponde ao elemento  $(i, k)$  da matriz  $(a_{ij}) \cdot (b_{jk}) + (a_{ij}) \cdot (c_{jk})$ . A outra distributividade é provada de forma análoga.  $\square$

Como o produto de uma matriz de  $M_{n \times m}(A)$  com uma matriz de  $M_{m \times p}(A)$  é uma matriz de  $M_{n \times p}(A)$ , em geral, não há uma propriedade de fechamento para o produto de matrizes.

Lembremos que a matriz identidade de  $M_{n \times n}(A)$  é a matriz cujos elementos da diagonal principal são 1 e os demais são 0. Utilizando a notação do delta de Kronecker, em que  $\delta_{ij}$  é 1 caso  $i = j$  e 0 caso contrário, a matriz identidade é a matriz  $I_n = (\delta_{ij})_{i,j} \in M_n(A)$ .

Porém, tal fato acontece para matrizes quadradas. De fato, temos:

**Proposição 3.8** (Anéis de matrizes). Seja  $A$  um anel e  $n \geq 1$ . Com as operações de soma e multiplicação definidas acima, e com a identidade  $I_n$  como a matriz identidade de  $M_n(A)$ , o conjunto  $M_n(A)$  é um anel, denominado *anel das matrizes  $n \times n$  de  $A$* .

Se  $n \geq 2$  e  $A$  é um anel não trivial,  $M_n(A)$  não é comutativo.



*Demonstração.* Para a verificação das propriedades de anel, resta apenas ver que a matriz identidade  $I_n$  é uma identidade multiplicativa. Com efeito, dado  $(a_{ij})_{i,j} \in M_n(A)$ , temos:

$$\begin{aligned} (a_{ij}) \cdot I_n &= \left( \sum_{k=1}^n a_{ik} \delta_{kj} \right)_{i,j} \\ &= (a_{ij})_{i,j}, \end{aligned}$$

e:

$$\begin{aligned} I_n \cdot (a_{ij}) &= \left( \sum_{k=1}^n \delta_{ik} a_{kj} \right)_{i,j} \\ &= (a_{ij})_{i,j}. \end{aligned}$$

Para a última afirmação, considere  $(a_{ij})_{i,j}, (b_{ij})_{i,j} \in M_n(A)$  definidos por:

$$a_{ij} = \begin{cases} 1 & \text{se } i = j = 1 \\ 0 & \text{caso contrário} \end{cases} \quad b_{ij} = \begin{cases} 1 & \text{se } i = 1, j = n \\ 0 & \text{caso contrário} \end{cases}$$

Temos que o elemento  $(1, n)$  da matriz  $(a_{ij})(b_{ij})$  é dado por  $\sum_{k=1}^n a_{1k} b_{kn} = 1$ , enquanto o elemento  $(1, n)$  da matriz  $(b_{ij})(a_{ij})$  é dado por  $\sum_{k=1}^n b_{1k} a_{kn} = 1$ .  $\square$

Assim, os anéis de matrizes nos dão uma ampla gama de anéis não comutativos.

### 3.3 Domínios de Integridade

O anel dos números inteiros, bem como o anel dos racionais reais, possuem a seguinte importante propriedade:

**Definição 3.9.** Seja  $A$  um anel comutativo. Dizemos que  $A$  é um *domínio de integridade* se, e somente se,  $\forall a, b \in A$ , se  $ab = 0$ , então  $a = 0$  ou  $b = 0$ .  $\square$

Nem todos os anéis comutativos são domínios de integridade. Por exemplo, no anel dos inteiros módulo 4,  $\mathbb{Z}_4$ , temos que  $2 \cdot 2 = 4 = 0$ , e  $2 \neq 0$ .

### 3.4 Elementos invertíveis

Um anel, com sua soma, é um grupo Abelian, e, portanto, possui opostos aditivos. Porém, não necessita possuir opostos multiplicativos. Os elementos de um anel que possuem inversos no anel são os chamados *elementos invertíveis* ou *unidades*.

**Definição 3.10** (Elemento invertível). Seja  $A$  um anel. Um elemento  $a \in A$  é dito *invertível*, ou uma *unidade* se  $\exists b \in A$  tal que  $a \cdot b = b \cdot a = 1$ .

O conjunto de todas as unidades de  $A$  é denotado por  $A^*$ .  $\square$

**Definição 3.11.** Seja  $A$  um anel. Então, se  $a \in A^*$ , existe um **único**  $b \in A$  tal que  $a \cdot b = b \cdot a = 1$ . Este elemento é denotado por  $a^{-1}$ , e é chamado de *inverso* de  $a$ .  $\square$

Observação: para que a definição acima faça sentido, é necessário mostrar que se  $a$  é unidade, existe um **único**  $b \in A$  tal que  $a \cdot b = b \cdot a = 1$ . A existência é garantida pela definição de unidade, e a demonstração da unicidade é análoga à da unicidade do inverso em grupos (Proposição 2.3), ficando como exercício.

**Proposição 3.12.** Seja  $A$  um anel. Para todos  $a, b \in A^*$ , temos:

- a)  $ab \in A^U$  e  $(ab)^{-1} = b^{-1}a^{-1}$ .
- b)  $a^{-1} \in A^U$  e  $(a^{-1})^{-1} = a$ .
- c)  $1^{-1} = 1$ .

Além disso,  $A^*$  é, com a restrição da operação de multiplicação do anel, um grupo com identidade 1. Caso  $A$  é um anel comutativo,  $A^*$  é um grupo abeliano.

*Demonstração.* a): Sejam  $a, b \in A^*$ . Pela associatividade,  $(ab)(b^{-1}a^{-1}) = 1 = (b^{-1}a^{-1})(ab)$ , logo, pela unicidade do inverso,  $(ab)^{-1} = b^{-1}a^{-1}$ .

b): Seja  $a \in A^*$ . Temos que  $a^{-1}a = 1 = a(a^{-1})$ , logo, pela unicidade do inverso,  $(a^{-1})^{-1} = a$ .

c): Note que  $1 \cdot 1 = 1 = 1 \cdot 1$ , logo, pela unicidade do inverso,  $1^{-1} = 1$ .

Se  $A$  é um anel comutativo, então  $A^*$  é um grupo abeliano, pois para todo  $a, b \in A^*$ , temos que  $ab = ba$ , logo  $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$ .  $\square$

### 3.5 O anel dos números inteiros

Espera-se que o estudante já possua traquejo com o anel dos números inteiros, incluindo contato com a noção formal de divisibilidade, o teorema fundamental da aritmética e a noção de congruência módulo  $n$ .

Primeiramente, reconhecamos que  $\mathbb{Z}$  possui, além da estrutura de domínio de integridade, uma estrutura de ordem.

**Definição 3.13.** Um anel ordenado é uma tupla  $(A, +, \cdot, 0, 1, \leq)$  tal que  $(A, +, \cdot, 0, 1)$  é um anel comutativo tal que  $\leq$  é uma relação de ordem total (também chamada de ordem linear) em  $A$ , ou seja, que satisfaça:

- (Propriedade reflexiva)  $\forall a \in A, a \leq a$ .
- (Propriedade antissimétrica)  $\forall a, b \in A$ , se  $a \leq b$  e  $b \leq a$ , então  $a = b$ .
- (Propriedade transitiva)  $\forall a, b, c \in A$ , se  $a \leq b$  e  $b \leq c$ , então  $a \leq c$ .
- (Linearidade)  $\forall a, b \in A, a \leq b$  ou  $b \leq a$ .

e tal que:

- (Compatibilidade da soma)  $\forall a, b, c \in A$ , se  $a \leq b$ , então  $a + c \leq b + c$  e  $ac \leq bc$ .
- (Compatibilidade da multiplicação)  $\forall a, b, c \in A$ , se  $a \leq b$  e  $0 \leq c$ , então  $ac \leq bc$ .

Nesse caso, dizemos que  $a < b$  se  $a \leq b$  e  $a \neq b$ .

Os elementos positivos de  $A$  são os elementos maiores do que 0.

Os negativos são os menores do que 0.  $\square$

Assumiremos, sem demonstração (por fugir do escopo do texto), que existe uma estrutura  $\mathbb{Z} = (\mathbb{Z}, +, \cdot, 0, 1, \leq)$  como abaixo:

**Definição 3.14** (Inteiros, anel ordenado).  $\mathbb{Z} = (\mathbb{Z}, +, \cdot, 0, 1, \leq)$  é um domínio de integridade ordenado cujos elementos positivos possuem a propriedade da boa ordenação:

Qualquer subconjunto não vazio de inteiros positivos possui elemento mínimo.  $\square$

Assumiremos todos os fatos elementares sobre  $\mathbb{Z}$  que não foram provados, inclusive o fato de que  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ .

### 3.6 Corpos e anéis de divisão

Abaixo, segue a definição de anel de divisão e corpo. A noção de corpo será uma das noções mais importantes deste texto.

**Definição 3.15** (Corpo e Anel de Divisão). Um *anel de divisão* é um anel não trivial para o qual todo elemento não nulo é invertível. Um *corpo* é um anel de divisão comutativo.  $\square$

Todo corpo é um domínio de integridade. De fato:

**Proposição 3.16.** Seja  $K$  um corpo. Então  $K$  é um domínio de integridade.

*Demonstração.* Sabemos que  $K$  é um anel comutativo não trivial. Sejam  $a, b \in K$  tais que  $ab = 0$ . Se  $a = 0$ , então segue a tese. Caso contrário, como  $K$  é um corpo,  $a^{-1}$  existe. Assim, temos que  $b = (a^{-1}a)b = a^{-1}(ab) = 0$ , logo,  $b = 0$ .  $\square$

Porém, nem todo domínio de integridade é um corpo: por exemplo,  $\mathbb{Z}$  é um domínio que não é um corpo, pois 2 não possui inverso multiplicativo em  $\mathbb{Z}$ .

### 3.7 Subanéis

Em Matemática, é comum que as estruturas estudadas possuam uma noção de subestrutura. Em geral, uma subestrutura de uma estrutura dada é um subconjunto desta que seja, de forma natural, uma estrutura da mesma natureza daquela.

Veremos que, quando tratamos de anéis, nem todo subconjunto pode ser visto como uma subestrutura.

**Definição 3.17** (Subanel). Seja  $A$  um anel e  $B \subseteq A$ . Dizemos que  $B$  é subanel de  $A$  se, e somente se  $(B, +|_{B^2}, \cdot|_{B^2}, 0_A, 1_A)$  é um anel, onde  $+|_{B^2} : B^2 \rightarrow B$  e  $\cdot|_{B^2} : B^2 \rightarrow B$  são as restrições das operações de  $A$  à  $B^2$ .  $\square$

Na definição acima, estamos pedindo que  $B$  seja um subconjunto de  $A$  que possua as mesmas operações que  $A$ , e que essas operações sejam restritas a  $B$  e satisfaçam todas as cláusulas da definição de anel. Aparentemente, na prática, provar que um dado subconjunto de  $A$  é um subanel pode parecer uma tarefa longa. Porém, a seguinte proposição encurta esta tarefa significativamente:

**Definição 3.18** (Subanel). Seja  $A$  um anel e  $B \subseteq A$ . Então  $B$  é um subanel de  $A$  se, e somente se:

- $1_A \in B$
- Para todos  $a, b \in B$ ,  $a - b \in B$ .

- Para todos  $a, b \in B$ ,  $ab \in B$

Além disso, caso  $B$  seja um subanel de  $A$ , os opostos aditivos de  $B$  são os mesmos que os de  $A$ , ou seja, que  $-b \in B$  para todo  $b \in B$ .  $\square$

*Demonstração.* Primeiro, notemos suponha que  $B$  seja um subanel de  $A$ . Então  $B$  é fechado por  $+$ ,  $\cdot$  e  $1_A \in B$ . Resta apenas ver que para todos  $a, b \in B$ ,  $a - b \in B$ . Como  $B$  é fechado por soma, basta provar a última afirmação: que para todo  $b \in B$ ,  $-b \in B$ . Fixe  $b \in B$ . Como  $(B, +|_B, 0_A)$  é um grupo abeliano, existe  $x \in B$  tal que  $b + x = 0_B$ . Então, em  $a$ , segue que  $b + x = x + b = 0_A$ . Pela unicidade dos opostos em  $A$ , segue que  $-b = x \in B$ .

Reciprocamente, provaremos que se  $B$  possui  $1_B$  como elemento e é fechado por diferença e por produto, então  $B$  é um subanel de  $A$ . Iniciaremos verificando que  $B$  é fechado por soma, por opostos e que tem  $0_A$  como elemento.

Como  $1_A$  é elemento de  $B$ , temos que  $0_A = 1_A - 1_A \in B$ . Assim,  $B$  possui  $0_A$  como elemento. Agora, dado  $b \in B$ ,  $0_A - b = -b \in B$ , o que mostra que  $B$  é fechado por opostos. Finalmente, dados  $a, b \in B$ ,  $a - (-b) = a + b \in B$ , o que mostra que  $B$  é fechado para soma.

As propriedades associativas, comutativas, distributivas e de identidade valem em  $B$ , pois valem em  $A$  e as operações de  $B$  são as mesmas de  $A$ , restritas. Para finalizar, basta observar que dado  $a \in B$ ,  $(-a) \in B$ , como já mostrado, e que  $a + (-a) = (-a) + a = 0_A$ , o que mostra que  $B$  possui opostos aditivos.  $\square$

**Exemplo 3.19.**  $\mathbb{N}$  não é um subanel de  $\mathbb{Z}$ , pois  $-1 \notin \mathbb{N}$ . Porém, note que  $\mathbb{N}$  tem 1 e é fechado por soma e produto, o que mostra que na proposição anterior, a expressão  $a - b$  não pode ser substituída por  $a + b$ .  $\square$

**Exemplo 3.20** (Subanel trivial). Para todo  $A$ , temos que  $A$  é subanel de si mesmo.  $\square$

**Exemplo 3.21.** O único subanel de  $\mathbb{Z}$  é  $\mathbb{Z}$ : se  $B$  é um subanel de  $\mathbb{Z}$ , então  $0, 1 \in B$ . Por indução, para todo  $n \geq 1$  temos que  $n \in B$ : com efeito,  $1 \in B$ , e, se  $n \in B$ ,  $n + 1 \in B$ , logo vale o passo indutivo. Finalmente,  $-n \in B$  para todo  $n \geq 1$ . Como  $\mathbb{Z} = \{0\} \cup \{n \in \mathbb{Z} : n \geq 1\} \cup \{-n \in \mathbb{Z} : n \geq 1\}$ , temos que  $B = \mathbb{Z}$ .  $\square$

Como as operações de um subanel são as mesmas de um anel, um subanel de um anel comutativo é comutativo.

**Proposição 3.22.** Subanéis de anéis comutativos são comutativos.

*Demonstração.* Seja  $A$  um anel comutativo e  $B$  um subanel de  $A$ . Para todos  $a, b \in B$ , temos que o produto  $a \cdot b$  em  $B$  é dado pelo produto (comutativo)  $a \cdot b$  em  $A$ , logo  $a \cdot b = b \cdot a$ .  $\square$

### 3.8 O centro de um anel

Apesar de nem todo anel ser comutativo, todos os anéis possuem elementos que comutam com qualquer outro elemento – ao menos o elemento 1.

O centro do anel é o conjunto de tais elementos.

**Definição 3.23** (Centro de um anel). Seja  $A$  um anel.

O *centro* de  $A$ , denotado por  $Z(A)$ , é o conjunto dos elementos de  $A$  que comutam com todos os outros elementos de  $A$ .

Formalmente,  $Z(A) = \{a \in A : \forall b \in A, ab = ba\}$ .  $\square$

O centro de um anel sempre é um subanel.

**Proposição 3.24.** Para todo anel  $A$ , o conjunto  $Z(A)$  é um subanel de  $A$ .

*Demonstração.* Temos que  $1 \in Z(A)$  pois para todo  $b \in A$ ,  $1a = a1 = a$ .

Se  $a, a' \in A$ , temos que  $aa' \in Z(A)$  pois para todo  $b \in A$ ,  $(aa')b = a(a'b) = a(ba') = (ab)a' = (ba)a' = b(a'a)$ .

Finalmente, se  $a, a' \in A$ , temos que  $a - a' \in Z(A)$ , pois para todo  $b \in A$ ,  $(a - a')b = ab - a'b = ba - ba' = b(a - a')$ .  $\square$

## 3.9 Exercícios

**Exercício 3.1.** Seja  $A$  um anel. Mostre que um anel  $A$  é um anel de divisão se, e somente se  $A^* = A \setminus \{0\}$ .



## Capítulo 4

# Homomorfismos e Ideais

Em matemática, boa parte das coleções de estruturas estudadas possui uma classe de funções que preservam, em algum sentido, suas propriedades. O estudo generalizado destas estruturas é o que chamamos de *teoria de categorias*, tema que não será tratado neste texto. Na classe dos anéis, estas funções são o que chamamos de *homomorfismos*.

### 4.1 Definição de homomorfismo

Homomorfismos são funções que preservam a estrutura de anéis. Formalmente:

**Definição 4.1.** Sejam  $A, R$  anéis. Uma função  $f : A \rightarrow R$  é um *homomorfismo* se:

- $f(a + b) = f(a) + f(b)$  para todo  $a, b \in A$ .
- $f(-a) = -f(a)$  para todo  $a \in A$ .
- $f(0_A) = 0_R$
- $f(ab) = f(a)f(b)$  para todo  $a, b \in A$ .
- $f(1_A) = 1_R$ .

Caso  $f$  seja injetora, dizemos que  $f$  é um *monomorfismo*. Caso  $f$  seja sobrejetora, dizemos que  $f$  é um *epimorfismo*. Caso  $f$  seja bijetora, dizemos que  $f$  é um *isomorfismo*.  $\square$

A noção de isomorfismo é extremamente importante na Teoria de Anéis. Muitas vezes, temos dois anéis que “deveriam ser a mesma coisa”, mas, como objetos matemáticos, não são iguais. A noção de isomorfismo entra em campo para dizer que, mesmo que dois anéis não sejam o mesmo objeto, eles possuem exatamente as mesmas propriedades algébricas e operacionais. Para darmos um exemplo concreto:

**Exemplo 4.2.** Seja  $A = \{0, 1\}$  e  $R = \{Z, U\}$ , onde  $Z, U$  são objetos diferentes, e diferentes de  $0, 1$ . Defina em  $A$  as operações  $\cdot$  e  $+$  dadas pelas seguintes tabelas:

Em  $A$ :

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Em  $R$ :

+	Z	U
Z	Z	U
U	U	Z

·	Z	U
Z	Z	Z
U	Z	U

Intuitivamente,  $A$  e  $R$  correspondem a duas apresentações de uma mesma estrutura algébrica, porém, como  $A \cap R = \emptyset$ , estes dois anéis não são o mesmo anel. Como formalizar este fato? Ora, há uma relação biunívoca (uma bijeção) entre  $A$  e  $R$  que preserva suas operações, e ela é dada por  $\phi(0) = Z$  e  $\phi(1) = U$ . Tal  $\phi$  é um isomorfismo.  $\square$

Para todos os fins que interessam à Álgebra, anéis isomorfos tem exatamente as mesmas propriedades, e, assim, são considerados como sendo, em algum sentido, a mesma estrutura.

A definição de homomorfismo, por possuir várias cláusulas, pode parecer de longa verificação. A proposição abaixo encurta esta verificação substancialmente.

**Proposição 4.3.** Sejam  $A, R$  anéis e  $f : A \rightarrow R$  uma função. Então  $f$  é um homomorfismo se, e somente se:

- $f(a + b) = f(a) + f(b)$  para todo  $a, b \in A$ .
- $f(ab) = f(a)f(b)$  para todo  $a, b \in A$ .
- $f(1_A) = 1_R$ .

*Demonstração.* Provaremos o lado que não é imediatamente trivial. Começaremos mostrando que  $f(0_A) = 0_R$ . Temos que  $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A)$ , logo, cancelando,  $f(0_A) = 0_R$ .

Agora, vejamos que  $f(-a) = -f(a)$  para todo  $a \in A$ . Temos que  $f(a) + f(-a) = f(a + (-a)) = f(0_A) = 0_R$ , logo,  $f(-a) = -f(a)$ .

Assim,  $f$  é um homomorfismo.  $\square$

## 4.2 Propriedades elementares

**Lema 4.4.** Sejam  $f : A \rightarrow R$  e  $g : R \rightarrow S$  homomorfismos de anéis. Então a composição  $g \circ f : A \rightarrow S$  é um homomorfismo de anéis.

*Demonstração.* Sejam  $a, b \in A$ . Então:

- $g \circ f(a + b) = g(f(a + b)) = g(f(a) + f(b)) = g(f(a)) + g(f(b)) = (g \circ f)(a) + (g \circ f)(b)$ .
- $g \circ f(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)(g \circ f)(b)$ .
- $g \circ f(1_A) = g(f(1_A)) = g(1_R) = 1_S$ .

Assim,  $g \circ f$  é um homomorfismo de anéis.  $\square$

**Proposição 4.5** (Propriedades de homomorfismos). Seja  $f : A \rightarrow R$  um homomorfismo de anéis. Então:

- a) Para todo  $a \in A^*$ , temos  $f(a) \in R^*$  e  $f(a^{-1}) = f(a)^{-1}$ .



b) A imagem de  $f$ ,  $\text{ran } f = \{f(a) : a \in A\}$ , é um subanel de  $R$ . Se  $A$  é comutativo,  $\text{ran } f$  também é.

c) Se  $f$  é injetora, a imagem de  $f$  é um subanel de  $R$  isomorfo a  $A$ .

*Demonstração.* a) Se  $a \in A^*$ , então  $f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) = 1_R$  e  $f(a^{-1})f(a) = f(aa^{-1}) = f(1_A) = 1_R$ . Assim,  $f(a^{-1}) = f(a)^{-1}$  e  $f(a) \in R^*$ .

b) Seja  $a, b \in \text{ran } f$ . Então existem  $x, y \in A$  tais que  $a = f(x)$  e  $b = f(y)$ . Assim,  $a - b = f(x) - f(y) = f(x - y)$ . Logo,  $a - b \in \text{ran } f$ . Similarmente,  $ab = f(x)f(y) = f(xy) \in \text{ran } f$ , e  $1_R = f(1_A) \in \text{ran } f$ .

Portanto,  $\text{ran } f$  é um subanel de  $R$ . Se  $A$  é comutativo,  $\text{ran}(f)$  também é comutativo, pois dados  $a, b \in \text{ran } f$ , existem  $x, y \in A$  tais que  $a = f(x)$  e  $b = f(y)$ . Assim,  $ab = f(x)f(y) = f(xy) = f(yx) = f(y)f(x) = ba$ .

c) Se  $f$  é injetora, então  $f$  é bijetora entre  $A$  e  $\text{ran } f$ . Assim,  $f$  é um isomorfismo entre  $A$  e  $\text{ran } f$ , dado que é um homomorfismo.  $\square$

A noção de isomorfismo é uma relação de equivalência na classe dos anéis.

**Proposição 4.6** (Propriedades de isomorfismo). Sejam  $A, R, S$  anéis e  $f : A \rightarrow R$  e  $g : R \rightarrow S$  isomorfismos de anéis. Então:

- a)  $g \circ f$  é um isomorfismo de anéis.
- b)  $f^{-1} : R \rightarrow A$  é um isomorfismo de anéis.
- c)  $\text{id}_A : A \rightarrow A$  é um isomorfismo de anéis.

*Demonstração.* a) A composição de funções bijetoras é bijetora, e a composição de homomorfismos é homomorfismo. Como um isomorfismo é um homomorfismo bijetor, segue que a composição de dois isomorfismos é um isomorfismo.

b) Como  $f$  é um isomorfismo,  $f$  é bijetora, assim,  $f^{-1} : R \rightarrow A$  está bem definida e é bijetora. Verificaremos que  $f^{-1}$  é um homomorfismo. Dados  $r, s \in R$ , sejam  $a, b \in A$  tais que  $f(a) = r$  e  $f(b) = s$ . Temos que:

- $f^{-1}(r + s) = f^{-1}(f(a) + f(b)) = f^{-1}(f(a + b)) = a + b = f^{-1}(r) + f^{-1}(s)$ .
- $f^{-1}(rs) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = a \cdot b = f^{-1}(r)f^{-1}(s)$ .
- $f^{-1}(1_R) = f^{-1}(f(1_A)) = 1_A$ .

c) A função identidade  $\text{id}_A$  é claramente bijetora, e é um homomorfismo, pois, para todos  $a, b \in A$ :

- $\text{id}_A(a + b) = a + b = \text{id}_A(a) + \text{id}_A(b)$ .
- $\text{id}_A(ab) = ab = \text{id}_A(a) \text{id}_A(b)$ .
- $\text{id}_A(1_A) = 1_A$ .

$\square$

Agora introduziremos o núcleo de um homomorfismo.

**Definição 4.7.** Seja  $f : A \rightarrow R$  um homomorfismo de anéis. Definimos o *núcleo* de  $f$ , também chamado de *kernel* de  $f$ , como sendo o conjunto dos zeros de  $f$ . Em símbolos:

$$\ker f = \{a \in A : f(a) = 0_R\}.$$

□

Uma importante relação entre o homomorfismo e seu núcleo é dado como se segue:

**Proposição 4.8.** Sejam  $A, R$  anéis e  $f : A \rightarrow R$  um homomorfismo. Então  $f : A \rightarrow R$  é injetor (um monomorfismo) se, e somente se  $\ker f = \{0_A\}$ .

*Demonstração.* Primeiro, suponha que  $f$  é um monomorfismo. Sabemos que  $f(0_A) = 0_R$ , pois  $f$  é homomorfismo, e, portanto,  $\{0_A\} \subseteq \ker f$ . Reciprocamente, seja  $a \in \ker f$ . Temos que  $f(a) = 0_R = f(0_A)$ . Pela injetividade de  $f$  segue que  $a = 0_A \in \{0_A\}$ .

Agora suponha que  $\ker f = \{0_A\}$ . Veremos que  $f$  é injetora. Para tanto, sejam  $a, b \in A$  e suponha que  $f(a) = f(b)$ . Temos que  $f(a - b) = f(a) - f(b) = 0_R$ , assim,  $a - b \in \ker f = \{0_A\}$ , o que implica em  $a - b = 0_A$ , e, portanto,  $a = b$ . □

### 4.3 Ideais

Ideais são as estruturas responsáveis pela noção de quociente em anéis, assunto que será estudado no próximo capítulo. Introduziremos a noção de ideal neste capítulo pois ela tem interações fundamentais com a noção de homomorfismo, porém, apenas no próximo capítulo ficará clara a sua enorme importância para esta teoria. Nesta seção, motivaremos, nesta seção, a noção de ideal, a partir do núcleo de homomorfismos.

Para começar, notemos algumas propriedades do núcleo.

**Proposição 4.9.** Seja  $f : A \rightarrow R$  um homomorfismo de anéis. Seja  $I = \ker f$ . Então:

- a)  $0_A \in I$ .
- b) Para todos  $a, b \in I$ ,  $a + b \in I$ .
- c) Para todos  $a \in I$  e  $x \in A$ ,  $ax \in I$ .
- d) Para todos  $a \in I$  e  $x \in A$ ,  $xa \in I$ .

*Demonstração.* a)  $0_A \in I$  pois  $f(0_A) = 0_R$ .

b) Se  $a, b \in I$ , então  $f(a) = 0_R$  e  $f(b) = 0_R$ . Assim,  $f(a + b) = f(a) + f(b) = 0_R + 0_R = 0_R$ , logo,  $a + b \in I$ .

c) Se  $a \in I$  e  $x \in A$ , então  $f(a) = 0_R$ . Assim,  $f(ax) = f(a)f(x) = 0_R f(x) = 0_R$ , logo,  $ax \in I$ .

d) Se  $a \in I$  e  $x \in A$ , então  $f(a) = 0_R$ . Assim,  $f(xa) = f(x)f(a) = f(x)0_R = 0_R$ , logo,  $xa \in I$ . □

É possível indagar se  $\ker f$  é um subanel de  $A$ . Observemos que as propriedades c) e d) são mais fortes do que a propriedade exigida para produto para ser um subanel. Além disso,  $\ker f$  é fechado por diferenças, pois se  $a, b \in \ker f$ , pela propriedade d),  $(-1)b = -b \in \ker f$ , e, portanto,  $a - b \in \ker f$ . Porém,  $1_A$  raramente está em  $\ker f$ , como vemos a seguir:

**Proposição 4.10.** Seja  $f : A \rightarrow R$  um homomorfismo de anéis. Se  $1_A \in \ker f$ , então  $R$  é o anel trivial, ou seja,  $R = \{0_R\}$ .

*Demonstração.* Se  $1_A \in \ker f$ , então  $f(1_A) = 0_R$ . Como  $f$  é um homomorfismo, temos que  $f(1_A) = f(1_A \cdot 1_A) = f(1_A)f(1_A) = 0_R \cdot 0_R = 0_R$ . Como  $1_R = 0_R$ , segue que  $R = \{0_R\}$ , pois dado  $x \in R$  temos  $x = x \cdot 1_R = x \cdot 0_R = 0_R$ .  $\square$

Como recíproca, notemos que um homomorfismo acima existe para qualquer anel  $A$ :

**Proposição 4.11.** Seja  $A$  um anel e  $R = \{0_R\}$  um anel trivial.

Então  $f : A \rightarrow R$  dado por  $f(x) = 0_R$  para todo  $x \in A$  é um homomorfismo de anéis, e  $\ker f = A$ .

*Demonstração.* Temos que  $f$  é um homomorfismo de anéis, já que dados  $a, b \in R$ , temos  $f(a+b) = 0_R = 0_R + 0_R = f(a) + f(b)$ ,  $f(ab) = 0_R = 0_R \cdot 0_R = f(a)f(b)$ ,  $f(1_A) = 0_R = 1_R$ . Como  $f$  é a função nula,  $\ker f = A$ .  $\square$

Podemos ver  $\ker f$ , em algum sentido, como uma medida do quão longe um homomorfismo  $f$  está de ser injetor: temos que  $\{0\} \subseteq \ker f \subseteq A$ . Como vimos,  $f$  ser injetor é equivalente a  $f = \{0\}$ . No outro extremo,  $f$  ser constante significa que  $\ker f = A$ .

Vimos ainda que  $\ker f$  não é um subanel, mas que possui propriedades especiais. Tais propriedades são a definição de ideal.

**Definição 4.12** (Ideal). Seja  $A$  um anel. Um subconjunto  $I \subseteq A$  é dito *ideal*, ou um *ideal bilateral* se:

- a)  $0_A \in I$ .
- b) Para todos  $a, b \in I$ ,  $a + b \in I$ .
- c) Para todos  $a \in I$  e  $x \in A$ ,  $ax \in I$ .
- d) Para todos  $a \in I$  e  $x \in A$ ,  $xa \in I$ .

Caso  $I$  satisfaça todas as propriedades menos d),  $I$  é dito um ideal à direita. De forma similar, caso  $I$  satisfaça todas as propriedades menos c),  $I$  é dito um ideal à esquerda.  $\square$

Note que se  $A$  é um anel comutativo, então  $I$  é um ideal à esquerda se, e somente se,  $I$  é um ideal à direita. Assim, em anéis comutativos, a noção de ideal é equivalente à de ideal à esquerda ou à de ideal à direita. Por simplicidade, neste texto, focaremos nosso estudo em ideais bilaterais. Porém, muitos resultados aqui expressados possuem versões para ideais à esquerda e à direita.

Da discussão anterior, temos:

**Corolário 4.13.** Seja  $f : A \rightarrow R$  um homomorfismo de anéis. Então  $\ker f$  é um ideal de  $A$ .

Então, todo núcleo é um ideal. No próximo capítulo, veremos que vale uma recíproca: todo ideal é um núcleo de algum homomorfismo.

Todo anel possui ao menos os ideais abaixo, chamados de ideais triviais:

**Proposição 4.14** (Ideal trivial). Seja  $A$  um anel. Então  $\{0\}$  e  $A$  são ideais de  $A$ . Estes ideais são chamados de *ideais principais*

*Demonstração.* Exercício.  $\square$

**Proposição 4.15** (Interseção de ideais). Seja  $A$  um anel e  $\mathcal{F}$  uma coleção não vazia de ideais de  $A$ . Então  $\bigcap_{I \in \mathcal{F}} I = \bigcap \mathcal{F}$  é um ideal de  $A$ .

*Demonstração.* Seja  $I = \bigcap \mathcal{F}$ .

Então  $0 \in I$ , pois  $0 \in I$  para todo  $I \in \mathcal{F}$ .

Sejam  $a, b \in I$ . Então, para todo  $I \in \mathcal{F}$ , temos que  $a, b \in I$ , logo,  $a + b \in I$ . Assim,  $a + b \in \bigcap \mathcal{F}$ .

Seja  $a \in A$  e  $b \in I$ . Então, para todo  $I \in \mathcal{F}$ , temos que  $b \in I$ , logo,  $ab \in I$ . Assim,  $ab \in \bigcap \mathcal{F}$ .

Analogamente, se  $a \in I$  e  $b \in A$ , então  $ba \in I$ .  $\square$

**Proposição 4.16** (Ideal gerado). Seja  $A$  um anel e  $B \subseteq A$  um conjunto não vazio. Então, o conjunto  $I = \{a_1 b_1 c_1 + \dots + a_n b_n c_n : n \geq 1, a_i, c_i \in A, b_i \in B\}$  é o menor ideal  $A$  que contém  $B$  (ou seja, além de ser um ideal contendo  $B$ , se  $J$  é qualquer ideal contendo  $B$ , então  $I \subseteq J$ ).

Além disso, se  $B \subseteq Z(R)$ , onde  $Z(R)$  denota o centro de  $R$ , então  $I = \{a_1 b_1 + \dots + a_n b_n : n \geq 1, a_i \in A, b_i \in B\}$ .

*Demonstração.* Primeiro, verificaremos que  $I$  é um ideal.

$0 \in I$ , pois  $0 = 0b0$  para todo  $b \in B$ .

Considere  $x, y \in I$ . Então existem  $n, m \geq 1$ ,  $a_1, \dots, a_n, c_1, \dots, c_n \in A$ ,  $b_1, \dots, b_n \in B$ ,  $a'_1, \dots, a'_m, c'_1, \dots, c'_m \in A$  e  $b'_1, \dots, b'_m \in B$  tais que  $x = a_1 b_1 c_1 + \dots + a_n b_n c_n$  e  $y = a'_1 b'_1 c'_1 + \dots + a'_m b'_m c'_m$ . Assim,  $x + y = (a_1 b_1 + \dots + a_n b_n) + (a'_1 b'_1 c'_1 + \dots + a'_m b'_m c'_m) = (a_1 b_1 c_1 + \dots + a_n b_n c_n) + (a'_1 b'_1 c'_1 + \dots + a'_m b'_m c'_m) \in I$ . Concatenando as sequências, vemos que  $x + y \in I$ .

Seja  $x \in A$  e  $b \in I$ . Então existem  $n \geq 1$ ,  $a_1, \dots, a_n, c_1, \dots, c_n \in A$  e  $b_1, \dots, b_n \in B$  tais que  $b = a_1 b_1 c_1 + \dots + a_n b_n c_n$ . Assim,  $xb = (xa_1) b_1 c_1 + \dots + (xa_n) b_n c_n \in I$ . Analogamente,  $bx \in I$ .

Agora, seja  $J$  um ideal de  $A$  que contém  $B$ . Fixe  $x \in I$ . Existem  $n \geq 1$ ,  $a_1, \dots, a_n, c_1, \dots, c_n \in A$  e  $b_1, \dots, b_n \in B$  tais que  $x = a_1 b_1 c_1 + \dots + a_n b_n c_n$ . Como  $J$  é um ideal de  $A$  e  $B \subseteq A$ , para cada  $i \in \{1, \dots, n\}$  temos que  $a_i b_i c_i \in J$ . Somando, segue que  $x \in J$ .

Finalmente, provaremos a afirmação final para quando  $B \subseteq Z(R)$ . Seja  $I' = \{a_1 b_1 + \dots + a_n b_n : n \geq 1, a_i \in A, b_i \in B\}$ . Veremos que  $I = I'$ . Pondo  $c_1 = \dots = c_n = 1$ , vemos que  $I' \subseteq I$ .

Reciprocamente, se  $x = a_1 b_1 c_1 + \dots + a_n b_n c_n \in I$  com  $n \geq 1$ ,  $a_1, \dots, a_n, c_1, \dots, c_n \in A$  e  $b_1, \dots, b_n \in B \subseteq Z(A)$ , temos que  $x = (a_1 c_1) b_1 + \dots + (a_n c_n) b_n \in I'$ .  $\square$

**Definição 4.17.** Na notação da proposição acima,  $I$  é chamado de *ideal gerado por  $B$*  e denotamos por  $\langle B \rangle$ .

Caso  $B = \{x_1, \dots, x_n\}$ , denotamos o ideal gerado por  $B$  como  $\langle x_1, \dots, x_n \rangle$ . Em particular, se  $B = \{x\}$ , denotamos o ideal gerado por  $B$  como  $\langle x \rangle$ .

Caso  $B$  seja a imagem de uma família  $(x_i : i \in Z)$ , denotamos o ideal gerado por  $B$  como  $\langle x_i : i \in Z \rangle$ .

Em qualquer um desses casos,  $B$  é dito um gerador do ideal.  $\square$

Observação: note que o menor ideal contendo  $B = \emptyset$  é o ideal nulo,  $\{0\}$ . Escrevemos  $\langle \emptyset \rangle = \{0\}$ .

**Definição 4.18** (Ideal principal). Um *ideal principal* é um ideal gerado por um único elemento.  $\square$

Notemos que ideais triviais são principais à esquerda e à direita, pois  $0A = \{0\} = A0$  e  $A1 = A = 1A$ .

**Definição 4.19** (Domínio de ideais principais). Um domínio de ideais principais (DIP), ou anel principal, é um domínio de integridade  $A$  tal que todo ideal de  $A$  é principal.  $\square$

Em um anel comutativo  $A$ , como um domínio de integridade, pelo exposto acima, para todo  $x \in A$ , o conjunto  $xA = \{xa : a \in A\}$  é o conjunto  $\langle x \rangle$ . Assim, um domínio de ideais principais é um domínio cujos ideais são exatamente os conjuntos da forma  $xA$  para algum  $x \in A$ . Note que os ideais principais são sempre triviais, pois  $\langle 0 \rangle = \{0\}$  e  $\langle 1 \rangle = A$ .

Quais são exemplos de DIPs? Para começar, qualquer corpo é um DIP. Mais especificamente:

**Proposição 4.20** (Ideais de um corpo são triviais). Os únicos ideais de qualquer corpo são os triviais. Em particular, todo corpo é um DIP. Reciprocamente, se  $A$  é um anel comutativo não trivial cujo todo ideal é trivial, então  $A$  é um corpo.

*Demonstração.* Seja  $K$  um corpo e  $I$  um ideal de  $K$ . Se  $I = \{0\}$ , então  $I$  é trivial. Se  $I \neq \{0\}$ , então existe  $a \in I$  tal que  $a \neq 0$ . Daí  $1 = a^{-1}a \in I$ . Logo, para todo  $k \in K$ ,  $k = 1k \in I$ .

Para a recíproca, seja  $A$  um anel comutativo não trivial tal que todo ideal de  $A$  é trivial, e fixe  $x \in A \setminus \{0\}$ . Como  $Ax$  é um ideal trivial e  $0 \neq x \in Ax$ , temos que  $Ax = A$ . Logo, existe  $a \in A$  tal que  $ax = 1$ . Assim,  $x$  é invertível. Portanto,  $A$  é um corpo.  $\square$

Porém, nem todo DIP é um corpo, como exemplificado pelo anel dos números inteiros.

**Proposição 4.21** (Um DIP que não é um corpo). O anel dos inteiros  $\mathbb{Z}$  é um domínio de ideais principais que não é um corpo.

*Demonstração.* Seja  $I$  um ideal de  $\mathbb{Z}$ . Veremos que  $I$  é um ideal principal. Se  $I = \{0\}$ , então  $I$  é principal. Caso contrário,  $I$  contém ao menos um elemento positivo, já que, sendo  $x \in I \setminus \{0\}$ , temos que  $-x \in I$  e um dos  $x, -x$  é positivo.

Seja  $n$  o menor inteiro positivo de  $I$ . Afirmamos que  $I = n\mathbb{Z}$ . De fato, se  $x \in I$ , então escreva  $x = qn + r$ , onde  $q, r \in \mathbb{Z}$  e  $0 \leq r < n$ . Como  $x \in I$ , temos que  $r = x - qn \in I$ . Assim,  $r = 0$ , ou violaríamos a minimalidade de  $n$ . Logo,  $x = qn \in n\mathbb{Z}$ . Portanto,  $I \subseteq n\mathbb{Z}$ . Como  $n\mathbb{Z} = \langle n \rangle$  e  $n \in I$ , temos que  $n\mathbb{Z} \subseteq I$ , o que completa a prova.  $\square$



## Capítulo 5

# Quocientes e Teoremas do Homomorfismo

Ao estudar o anel dos números inteiros, normalmente são estudadas as relações de congruência e, subsequentemente, os anéis quocientes  $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ .

Neste capítulo, estudaremos quocientes de anéis de forma generalizada, e suas relações com ideais, relações de congruência e homomorfismos de anéis.

### 5.1 Relações de congruência

As relações de congruência de anéis são relações que generalizam a noção de “congruência módulo  $n$ ” do anel dos inteiros.

**Definição 5.1.** Seja  $A$  um anel. Uma relação de congruência em  $A$  é uma relação de equivalência  $\sim$  em  $A$  que “preserva operações”. Explicitamente, tal que para todos  $a, b, c, d \in A$ , se  $a \sim b$  e  $c \sim d$ , então  $a + c \sim b + d$  e  $ac \sim bd$ .  $\square$

Todo homomorfismo induz naturalmente uma relação de congruência. Explicitamente:

**Proposição 5.2.** Seja  $f : A \rightarrow R$  um homomorfismo de anéis. Então  $\sim_f = \{(a, b) \in A^2 : f(a) = f(b)\}$  é uma relação de congruência em  $A$ . De outro modo, a relação  $\sim_f$  em  $A^2$  dada por  $a \sim_f b$  se, e somente se  $f(a) = f(b)$ , é uma relação de congruência em  $A$ .

*Demonstração.*  $\sim_f$  é uma relação reflexiva, pois para todo  $a \in A$ ,  $f(a) = f(a)$ , logo,  $a \sim_f a$ .

$\sim_f$  é simétrica, pois se  $a \sim_f b$ , então  $f(a) = f(b)$ , e, portanto,  $f(b) = f(a)$ , o que implica em  $b \sim_f a$ .

$\sim_f$  é transitiva, pois se  $a \sim_f b$  e  $b \sim_f c$ , então  $f(a) = f(b)$  e  $f(b) = f(c)$ , logo,  $f(a) = f(c)$ , o que implica em  $a \sim_f c$ .

$\sim_f$  preserva soma, pois se  $a \sim_f b$  e  $c \sim_f d$ , então  $f(a) = f(b)$  e  $f(c) = f(d)$ , logo,  $f(a + c) = f(a) + f(c) = f(b) + f(d) = f(b + d)$ , o que implica em  $a + c \sim_f b + d$ .

$\sim_f$  preserva produto, pois se  $a \sim_f b$  e  $c \sim_f d$ , então  $f(a) = f(b)$  e  $f(c) = f(d)$ , logo,  $f(ac) = f(a)f(c) = f(b)f(d) = f(bd)$ , o que implica em  $ac \sim_f bd$ .  $\square$

A proposição abaixo classifica todas as relações de congruência a partir dos ideais de um anel.

**Proposição 5.3** (Relações de congruência vs ideais). Seja  $A$  um anel,  $\mathcal{R}(A)$  o conjunto de todas as relações de congruência em  $A$  e  $\mathcal{I}(A)$  o conjunto de todos os ideais de  $A$ . Então, existe uma bijeção entre  $\mathcal{R}(A)$  e  $\mathcal{I}(A)$  dada por  $\sim \mapsto I_\sim = \{a \in A : a \sim 0\}$ , cuja inversa se dá por  $I \mapsto \sim_I = \{(a, b) \in A^2 : a - b \in I\}$ .

*Demonstração.* Primeiro, vejamos que se  $\sim$  é uma relação de congruência, então  $I_\sim$  é um ideal de  $A$ .

- $0 \in I_\sim$ , pois  $0 \sim 0$ .
- Se  $a, b \in I_\sim$ , então  $a \sim 0$  e  $b \sim 0$ , logo  $a + b \sim 0 + 0 = 0$ , portanto,  $a + b \in I_\sim$ .
- Se  $x \in A$  e  $a \in I_\sim$ , então  $a \sim 0$  e  $x \sim 0$ , logo  $ax \sim a0 = 0$  e  $xa = 0a = 0$ , portanto,  $ax, xa \in I_\sim$ .

Agora, vejamos que se  $I$  é um ideal, então  $\sim_I$  é uma relação de congruência. De fato, temos que, para todos  $a, b, c, d \in A$ :

- $a \sim_I a$  pois  $a - a = 0 \in I$ .
- Se  $a \sim_I b$ , então  $a - b \in I$ , logo  $(-1)(a - b) = b - a \in I$ , e, portanto,  $b \sim_I a$ .
- Se  $a \sim_I b$  e  $b \sim_I c$ , então  $a - b \in I$  e  $b - c \in I$ , logo,  $(a - b) + (b - c) = a - c \in I$ , portanto,  $a \sim_I c$ .
- Se  $a \sim_I b$  e  $c \sim_I d$ , então  $a - b \in I$  e  $c - d \in I$ , logo,  $(a - b) + (c - d) = (a + c) - (b + d) \in I$ , portanto,  $a + c \sim_I b + d$ .
- Se  $a \sim_I b$  e  $c \sim_I d$ , então  $a - b \in I$  e  $c - d \in I$ , logo,  $(a - b)c = ac - bc \in I$  e  $b(c - d) = bc - bd \in I$ , logo  $(ac - bc) + (bc - bd) = ac - bd \in I$ , portanto,  $ac \sim_I bd$ .

Se  $I$  é ideal,  $I_{\sim_I} = I$ , pois, para todo  $a \in A$ :

$$a \in I_{\sim_I} \Leftrightarrow a \sim_I 0 \Leftrightarrow a - 0 \in I \Leftrightarrow a \in I.$$

Finalmente, se  $\sim$  é relação de congruência,  $\sim_{I_\sim} = \sim$ , pois, para todos  $a, b \in A$ :

$$a \sim_{I_\sim} b \Leftrightarrow a - b \in I_\sim \Leftrightarrow a - b \sim 0 \Leftrightarrow a \sim b.$$

Justificando a última equivalência: se  $a - b \sim 0$ , como  $b \sim b$ , temos que  $a - b + b \sim b$ , ou seja, que  $a \sim b$ . Reciprocamente, se  $a \sim b$ , como  $(-b) \sim (-b)$ , segue que  $a + (-b) \sim b + (-b)$ , ou seja, que  $a - b \sim 0$ .  $\square$

**Exemplo 5.4.** Como vimos,  $\mathbb{Z}$  é um domínio de ideais principais. Assim, todo ideal de  $\mathbb{Z}$  é da forma  $n\mathbb{Z}$ . Como para todo  $n$ ,  $n\mathbb{Z} = (-n)\mathbb{Z}$ , temos que  $\{n\mathbb{Z} : n \geq 0\}$  é a coleção de todos os ideais de  $\mathbb{Z}$ .

Quais são todas as relações de congruência em  $\mathbb{Z}$ ? Denotemos por  $\sim_n$  a relação  $\sim_{n\mathbb{Z}}$ .

Temos que  $\sim_0$  corresponde à relação de igualdade, pois  $a \sim_0 b$  se, e somente se,  $a - b = 0$ , ou seja,  $a = b$ . Note que a relação de igualdade sempre é uma relação de congruência, em qualquer anel.

Se  $n \geq 1$ ,  $\sim_n$  corresponde à relação de congruência módulo  $n$ , pois  $a \sim_n b$  se, e somente se,  $a - b \in n\mathbb{Z}$ , ou seja,  $a - b = kn$  para algum  $k \in \mathbb{Z}$ .  $\square$



## 5.2 Quocientes

Como feito nos inteiros, podemos, ao invés de trabalhar com relações de congruência, encontrar anéis em que a congruência corresponda exatamente à igualdade.

**Definição 5.5.** Seja  $A$  um anel e  $\sim$  uma relação de congruência.

Lembremos que o conjunto das classes de equivalência de  $\sim$  é denotado por  $A/\sim$ , e este corresponde, portanto, à  $\{[a]_\sim : a \in A\}$ , onde  $[a]_\sim = \{b \in A : b \sim a\}$  é a classe de equivalência de  $a$  com relação a  $\sim$ .

Define-se que  $[a]_\sim + [b]_\sim = [a + b]_\sim$  e que  $[a]_\sim [b]_\sim = [ab]_\sim$ . Com essas operações,  $(A/\sim, +, \cdot, [0]_\sim, [1]_\sim)$  é chamado de *anel quociente* de  $A$  por  $\sim$ .

Se  $I$  é um ideal define-se  $A/I = A/\sim_I$ , e este é munido das operações anteriores. Com essas operações,  $A/I = A/\sim_I$  como descrito acima é chamado de *anel quociente* de  $A$  por  $I$ .

Define-se o *mapa quociente* de  $A$  em  $A/I$  se dá por  $q : A \longrightarrow A/I$  dada por  $q(a) = [a]_{\sim_I}$ .  $\square$

É claro que precisamos mostrar que as operações acima estão bem definidas e torna estes, de fato, anéis.

**Lema 5.6.** As operações dos anéis quocientes estão bem definidas e os tornam anéis. Além disso, o mapa quociente é um epimorfismo (homomorfismo sobrejetor).

*Demonstração.* Como as relações de congruência estão em bijeção com os ideais, podemos tratar de um quociente arbitrário da forma  $A/\sim$ .

Primeiro, vejamos que as operações estão bem definidas, ou seja, que se  $a \sim b$  e  $c \sim d$ , então  $[ac]_\sim = [bd]_\sim$  e  $[a + b]_\sim = [b + d]_\sim$ .

De fato, como  $\sim$  é uma relação de congruência e  $a \sim b$  e  $c \sim d$ , temos que  $ac \sim bc$  e  $a + c \sim b + d$ , logo,  $[ac]_\sim = [bc]_\sim$  e  $[a + c]_\sim = [b + d]_\sim$ . Note ainda que como  $[a]_\sim = q(a)$  e  $q(1_A) = [1_A]_\sim$ , assim, segue que, caso  $A/\sim$  seja anel,  $q$  é homomorfismo sobrejetor.

Agora devemos ver que  $A/\sim$  é um anel. Temos que:

- Comutatividade da soma:  $q(a) + q(b) = q(a + b) = q(b + a) = q(b) + q(a)$ .
- Associatividade da soma:  $(q(a) + q(b)) + q(c) = q(a + b) + q(c) = q((a + b) + c) = q(a + (b + c)) = q(a) + q(b + c) = q(a) + (q(b) + q(c))$ .
- Neutro da soma:  $q(0) + q(a) = q(0 + a) = q(a)$ .
- Opostos:  $q(a) + q(-a) = q(a + (-a)) = q(0) = 0$ .
- Associatividade do produto:  $(q(a)q(b))q(c) = q(ab)q(c) = q((ab)c) = q(a(bc)) = q(a)q(bc) = q(a)(q(b)q(c))$ .
- Neutro do produto:  $q(1)q(a) = q(1a) = q(a)$ , e  $q(a)q(1) = q(a1) = q(a)$ .
- Distributividade:  $q(a)(q(b) + q(c)) = q(a)q(b + c) = q(a(b + c)) = q(ab + ac) = q(ab) + q(ac) = q(a)q(b) + q(a)q(c)$ .
- Distributividade II:  $(q(a) + q(b))q(c) = q(a + b)q(c) = q((a + b)c) = q(ac + bc) = q(ac) + q(bc) = q(a)q(c) + q(b)q(c)$ .

$\square$

Algumas propriedades particulares do quociente:

**Lema 5.7** (Propriedades do quociente). Na notação acima:

- a)  $\ker q = I$ .
- b)  $q(a) = a + I = \{a + x : x \in I\}$  para todo  $a \in A$ .
- c) Se  $A$  é anel comutativo,  $A/I$  também é.

*Demonstração.* a) Temos que  $\ker q = \{a \in A : q(a) = q(0)\} = \{a \in A : a \sim_I 0\} = \{a \in A : a \in I\} = I$ .

b) Temos que  $q(a) = [a]_{\sim_I} = \{b \in A : b \sim_I a\} = \{b \in A : b - a \in I\} = \{a + x : x \in I\}$  pois se  $b - a \in I$  se, e somente se  $a - b = x$  para algum  $x \in I$ .

c) Se  $A$  é comutativo, então  $A/I = \text{ran } q$  também é, pois  $q$  é homomorfismo de anéis.  $\square$

Em particular, temos:

**Corolário 5.8.** Todo ideal é o núcleo de algum homomorfismo.

### 5.3 Teoremas do isomorfismo

Os teoremas do homomorfismo dizem que certos homomorfismos “fatoram” para quocientes.

**Teorema 5.9** (Teorema do homomorfismo). Seja  $f : A \rightarrow R$  um homomorfismo de anéis e  $J$  um ideal tal que  $J \subseteq \ker f$ . Então, existe um único homomorfismo de anéis  $\bar{f} : A/J \rightarrow R$  tal que  $\bar{f} \circ q = f$ , onde  $q : A \rightarrow A/J$  é o mapa quociente canônico dado por  $q(a) = a + J$ .

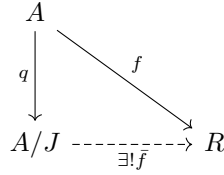


Figura 5.1: Teorema do homomorfismo.

*Demonstração.* Definimos  $\bar{f} : A/J \rightarrow R$  por  $\bar{f}(a + J) = f(a)$ . Então,  $\bar{f}$  é bem definido, pois se  $a + J = b + J$ , então  $a - b \in J \subseteq \ker f$ , logo,  $f(a - b) = 0_R$ , ou seja,  $f(a) = f(b)$ .

Agora, vejamos que  $\bar{f}$  é um homomorfismo de anéis. De fato, para todo  $a', b' \in A/J$ , sendo  $a' = a + J$  e  $b' = b + J$ , temos que:

- $\bar{f}(a' + b') = \bar{f}((a + J) + (b + J)) = \bar{f}((a + b) + J) = f(a + b) = f(a) + f(b) = \bar{f}(a + J) + \bar{f}(b + J)$ .
- $\bar{f}(a'b') = \bar{f}((a + J)(b + J)) = \bar{f}(ab + J) = f(ab) = f(a)f(b) = \bar{f}(a + J)\bar{f}(b + J)$ .
- $\bar{f}(1_{A/J}) = \bar{f}(1_A + J) = f(1_A) = 1_R$ .

Temos que  $\bar{f} \circ q = f$  por definição de  $\bar{f}$ . Para a unicidade, se  $g : A/J \rightarrow R$  é um homomorfismo tal que  $g \circ q = f$ , fixe  $a' \in A/J$ . Fixe  $a \in A$  tal que  $a' = q(a)$ . Então  $g(a') = g(q(a)) = f(a) = \bar{f}(q(a)) = \bar{f}(a')$ . Assim,  $g = \bar{f}$ .  $\square$

## Capítulo 6

# Produtos de anéis

Neste capítulo, estudaremos o produto direto de anéis.

### 6.1 Produtos de dois anéis

Dados anéis  $R$  e  $S$ , é possível dar à  $R \times S$  uma estrutura natural de anel.

**Definição 6.1** (Produto Direto de dois anéis). Sejam  $R, S$  anéis. O produto direto de  $R$  e  $S$  é o conjunto  $R \times S$  munido das operações “ponto à ponto”: dados  $a = (a_1, a_2) \in R \times S$  e  $b = (b_1, b_2) \in R \times S$ , temos:

$$a + b = (a_1 + b_1, a_2 + b_2)$$

$$a \cdot b = (a_1 \cdot b_1, a_2 \cdot b_2)$$

$$0 = (0_R, 0_S)$$

$$1 = (1_R, 1_S)$$

□

Exemplo: Seja  $R = \mathbb{Z}_3$  e  $S = \mathbb{Z}_4$ . Então  $(2, 2) \in R \times S$  e  $(1, 2) \in R \times S$ . Temos:

$$(2, 2) + (1, 2) = (2 + 1, 2 + 2) = (0, 0).$$

$$(2, 2) \cdot (2, 2) = (2 \cdot 2, 2 \cdot 2) = (1, 0).$$

**Exercício 6.1.** Prove que o produto direto de dois anéis é um anel.

### 6.2 Produtos de uma família de anéis

**Definição 6.2** (Produtos de anéis). Seja  $(R_i)_{i \in I}$  uma família de anéis, onde cada  $R_i$  tem as operações  $+_i, \cdot_i$  e constantes  $0_i, 1_i$ .

O produto (direto) de  $(R_i)_{i \in I}$  é o conjunto  $\prod_{i \in I} R_i$  munido das operações “ponto à ponto”: dados  $a = (a_i : i \in I), b = (b_i : i \in I)$  em  $\prod_{i \in I} R_i$ :

$$a + b = (a_i : i \in I) + (b_i : i \in I) = (a_i +_i b_i : i \in I) = (a_i +_i b_i)_{i \in I}$$

$$a \cdot b = (a_i : i \in I) \cdot (b_i : i \in I) = (a_i \cdot_i b_i : i \in I) = (a_i \cdot_i b_i)_{i \in I}$$

□

**Lema 6.3** (O produto de anéis está bem definido). Seja  $(R_i)_{i \in I}$  uma família de anéis. Então seu produto direto  $\prod_{i \in I} R_i$  é um anel com  $0 = (0_i : i \in I)$  e  $1 = (1_i : i \in I)$ .

*Demonstração.* Sejam  $a = (a_i : i \in I), b = (b_i : i \in I)$  e  $c = (c_i : i \in I)$  em  $\prod_{i \in I} R_i$ .

- **Associatividade da soma:**  $(a + b) + c = (a_i + b_i)_{i \in I} + c = ((a_i + b_i) + c_i)_{i \in I} = (a_i + (b_i + c_i))_{i \in I} = a + (b + c)$
- **Associatividade do produto:** Análogo.
- **Comutatividade da soma:**  $a + b = (a_i + b_i)_{i \in I} = (b_i + a_i)_{i \in I} = b + a$
- **Neutro da soma:**  $a + 0 = (a_i + 0_i)_{i \in I} = (a_i)_{i \in I} = a$
- **Inverso da soma:** Dado  $a = (a_i)_{i \in I}$ , considere  $-a = (-a_i)_{i \in I}$ . Então  $a + (-a) = (a_i + (-a_i))_{i \in I} = (0_i)_{i \in I} = 0$ .
- **Distributividade:**  $a \cdot (b + c) = (a_i \cdot (b_i + c_i))_{i \in I} = (a_i \cdot b_i + a_i \cdot c_i)_{i \in I} = a \cdot b + a \cdot c$ .
- **Distributividade II:**  $(a + b) \cdot c = ((a_i + b_i) \cdot c_i)_{i \in I} = (a_i \cdot c_i + b_i \cdot c_i)_{i \in I} = a \cdot c + b \cdot c$ .
- **Neutro do produto:**  $a \cdot 1 = (a_i \cdot 1_i)_{i \in I} = (a_i)_{i \in I} = a$  e  $1 \cdot a = (1_i \cdot a_i)_{i \in I} = (a_i)_{i \in I} = a$ .

□

**Definição 6.4** (Os mapas de projeção). Seja  $(R_i)_{i \in I}$  uma família de anéis e seja  $P = \prod_{i \in I} R_i$ . Para cada  $i \in I$ , o mapa de projeção  $\pi_i : P \rightarrow R_i$  é dado por  $\pi_i(a) = a_i$ .

Escrevendo de outra forma,  $\pi_i((a_j : j \in I)) = a_i$ .

□

**Lema 6.5** (Os mapas de projeção são homomorfismos). Seja  $(R_i)_{i \in I}$  uma família de anéis e seja  $P = \prod_{i \in I} R_i$ . Para cada  $i \in I$ , o mapa de projeção  $\pi_i : P \rightarrow R_i$  é um homomorfismo de anéis.

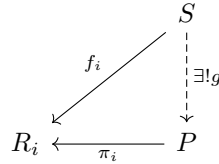
*Demonstração.* Sejam  $a = (a_j : j \in I), b = (b_j : j \in I)$  em  $P$ . Então:

- $\pi_i(a + b) = \pi_i((a_j + b_j)_{j \in I}) = a_i + b_i = \pi_i(a) + \pi_i(b)$
- $\pi_i(a \cdot b) = \pi_i((a_j \cdot b_j)_{j \in I}) = a_i \cdot b_i = \pi_i(a) \cdot \pi_i(b)$
- $\pi_i(1_P) = \pi_i((1_j)_{j \in I}) = 1_i$

□

### 6.3 A propriedade universal do produto direto de anéis

**Teorema 6.6** (Propriedade universal do produto direto de anéis). Seja  $(R_i)_{i \in I}$  uma família de anéis e seja  $P = \prod_{i \in I} R_i$  seu produto direto. Então, para cada anel  $S$  e cada família de homomorfismos de anéis  $f_i : R_i \rightarrow S$ , existe um único homomorfismo de anéis  $g : P \rightarrow S$  tal que  $\pi_i \circ g = f_i$  para todo  $i \in I$ .



Além disso, tal propriedade caracteriza o produto direto. Ou seja, para quaisquer que sejam um anel  $P'$  e uma família de homomorfismos  $(p_i : P' \rightarrow R_i)_{i \in I}$ , se para todo anel  $S$  e toda família de homomorfismos de anéis  $f_i : R_i \rightarrow S$  existir um único homomorfismo de anéis  $f : P' \rightarrow S$  tal que  $p_i \circ f = f_i$  para todo  $i \in I$ , então existe um único isomorfismo de anéis  $\phi : P' \rightarrow P$  tal que  $\pi_i \circ \phi = p_i$  para todo  $i \in I$ .

*Demonstração.* Seja  $P = \prod_{i \in I} R_i$  e seja  $S$  um anel comutativo. Para cada  $i \in I$ , considere  $f_i : S \rightarrow R_i$  um homomorfismo de anéis. Defina  $g : S \rightarrow P$  tal que, dado  $s \in S$ :

$$g(s) = (f_i(s))_{i \in I}.$$

Então, para cada  $i \in I$ ,  $\pi_i \circ g(s) = \pi_i(f_j(s) : j \in I) = f_i(s)$ , ou seja,  $\pi_i \circ g = f_i$ . Vejamos que  $g$  é homomorfismo de anéis. Dados  $s, t \in S$ , temos:

- $g(s + t) = (f_i(s + t))_{i \in I} = (f_i(s) + f_i(t))_{i \in I} = (f_i(s))_{i \in I} + (f_i(t))_{i \in I} = g(s) + g(t)$ .
- $g(s \cdot t) = (f_i(s \cdot t))_{i \in I} = (f_i(s) \cdot f_i(t))_{i \in I} = (f_i(s))_{i \in I} \cdot (f_i(t))_{i \in I} = g(s) \cdot g(t)$ .
- $g(1_S) = (f_i(1_S))_{i \in I} = (1_i)_{i \in I} = 1_P$ .

Vejamos que  $g$  é único. Se  $\bar{g} : S \rightarrow P$  é um homomorfismo de anéis tal que  $\pi_i \circ \bar{g} = f_i$ , fixe  $s \in S$ . Devemos ver que  $\bar{g}(s) = g(s)$ . Como  $\bar{g}(s) \in P$ , escreva  $\bar{g}(s) = (b_i)_{i \in I}$ , onde  $b_i \in R_i$  para cada  $i \in I$ . Temos, que, para cada  $j \in I$ :

$$b_j = \pi_j((b_i)_{i \in I}) = \pi_j \circ \bar{g}(s) = f_j(s).$$

Assim,  $f_j(s) = b_j$  para todo  $j \in I$ . Daí,  $\bar{g}(s) = (b_j)_{j \in I} = (f_j(s))_{j \in I} = g(s)$ . Portanto,  $g = \bar{g}$ .

Agora suponha que  $P'$  e  $(p_i : P' \rightarrow R_i)_{i \in I}$  são como no enunciado.

Aplicando a propriedade de  $P$  para  $(\pi_i : i \in I)$ , existe um homomorfismo de anéis  $\phi : P' \rightarrow P$  tal que  $\pi_i \circ \phi = p_i$  para todo  $i \in I$ .

$$\begin{array}{ccc} & P' & \\ & \swarrow p_i & \downarrow \exists! \phi \\ R_i & \xleftarrow{\pi_i} & P \end{array}$$

Nosso objetivo é mostrar que  $\phi$  é isomorfismo. Construiremos uma inversa. Como ele é o único homomorfismo tal que  $\pi_i \circ \phi = p_i$  para todo  $i \in I$ , e como todo isomorfismo é homomorfismo, isso conclui a prova.

Aplicando a propriedade de  $P'$  para  $(\pi_i : i \in I)$ , existe um homomorfismo de anéis  $\psi : P' \rightarrow P$  tal que  $p_i \circ \psi = \pi_i$  para todo  $i \in I$ .

$$\begin{array}{ccc} & P & \\ & \swarrow \pi_i & \downarrow \exists! \psi \\ R_i & \xleftarrow{p_i} & P' \end{array}$$

Tanto os mapas  $\psi \circ \phi$  quanto a identidade  $\text{id}_{P'} : P' \rightarrow P'$  são homomorfismos de anéis que satisfazem o seguinte diagrama comutativo:

$$\begin{array}{ccc}
 & P' & \\
 p_i \swarrow & \downarrow \psi \circ \phi & \downarrow \text{id}_{P'} \\
 R_i & \xleftarrow{p_i} & P'
 \end{array}$$

Pois para todo  $i \in I$ ,  $p_i \circ \text{id}_{P'} = p_i$  e  $p_i \circ \psi \circ \phi = \pi_i \circ \phi = p_i$ . Como a propriedade de  $P'$  diz que existe um *único* homomorfismo que satisfaz esse diagrama, segue que  $\psi \circ \phi = \text{id}_{P'}$ .

Analogamente, tanto os mapas  $\phi \circ \psi$  quanto a identidade  $\text{id}_P : P \rightarrow P$  são homomorfismos de anéis que satisfazem o seguinte diagrama:

$$\begin{array}{ccc}
 & P & \\
 \pi_i \swarrow & \downarrow \phi \circ \psi & \downarrow \text{id}_P \\
 R_i & \xleftarrow{\pi_i} & P
 \end{array}$$

Pois  $\pi_i \circ \text{id}_P = \pi_i$  e  $\pi_i \circ \phi \circ \psi = p_i \circ \psi = \pi_i$ . Como a propriedade de  $P$  diz que existe um *único* homomorfismo que satisfaz esse diagrama, segue que  $\phi \circ \psi = \text{id}_P$ .

Assim,  $\psi$  e  $\phi$  são isomorfismos inversos. Em particular,  $\phi$  é isomorfismo, o que completa a prova.  $\square$