Notas da disciplina MAT0264 - Anéis e Corpos

Prof. Vinicius Rodrigues

14 de abril de 2025, 10:45

Sumário

Prefácio

Estas notas começaram a ser escritas durante o primeiro semestre de 2025, enquanto lecionava 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. Ao longo do texto, apresentaremos as contruções de todos os outros anéis relevantes, porém alguns outros 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 seu início, mesmo antes de que construções formais sejam apresentadas.

Ao final de cada seção serão apresentados exercícios. Recomenda-se que o estudante resolva-os 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, matemáticamente, funções e famílias podem ser vistas como o mesmo objeto.

Conceito	**Função**	**Família**
Mapa	$u : I \to A$	$(u_i)_{i\in I} = (u_i : i \in I)$
Valor	$u(i)$	u_i
Imagem	$\operatorname{ran} u$	$\{u_i : i \in I\}$
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 $u = (\frac{1}{2^n}))_{n\in\mathbb{N}}\cdots$
- Considere a função $u : \mathbb{N} \to \mathbb{R}$ dada por $u(n) = \frac{1}{2^n}\cdots$

□

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

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

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. □

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 $b \in B$. □

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 $i \in I$, $a_i \in A_i$.

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

□

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, $A^I = \{f : I \to A\}$. Note que:

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

□

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

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

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 $f : X^n \to X$. □

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 $0 \in G$, 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 $\mathbb{Z}_n = \{0, \ldots, n-1\}$ 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, $h = he = e$. □

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 $g \in G$, é único. Isto é $\forall a \in G\ \exists!\, b \in G\ a \cdot b = b \cdot a = e$.

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:

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

□

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 $(\,)^{-1} : G \to G$ (ou $- : G \to G$). 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, $b = c$. □

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. □

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 $n \to n+1$: 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:

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

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

□

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 $\phi : J \to I$ 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 $\phi : J \to I$ como no enunciado. Fixe $k \in J$ qualquer e sejam $I' = I \setminus \{\phi(k)\}$, $J' = J \setminus \{k\}$ e $\phi' = \phi|_{J'} : J' \to I'$, 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:

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

□

2.3 Exercícios

Exercício 2.1. Suponha que a, b e c sejam elementos de um anel A, e que a não é divisor de 0.

Mostre que se $ab = ac$, então ou $a = 0$ ou $b = c$ (isto é, se $a \neq 0$, podemos cancela-lo).

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, estururas 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 desas 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 $0 = 0 \cdot a$. □

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, assuma 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. □

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

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

c) $(-1)a = -a$.

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 $(-1)a = -(1a) = -a$. □

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 $(a_{ij})_{i,j} = (a_{ij} : (i, j) \in \{1, \ldots, n\} \times \{1, \ldots, m\})$. Quando conveniente, representamos a tal matriz de qualquer uma das duas formas a seguir:

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

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:** para todos $(a_{ij})_{i,j}, (b_{ij})_{i,j}, (c_{ij})_{i,j} \in M_{n\times m}(A)$, temos:
$$\big((a_{ij}) + (b_{ij})\big) + (c_{ij}) = (a_{ij} + b_{ij}) + c_{ij} = a_{ij} + (b_{ij} + c_{ij}) = (a_{ij}) + \big((b_{ij}) + (c_{ij})\big).$$

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

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 $\big((a_{ij}) \cdot (b_{jk})\big) \cdot (c_{kl})$. 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 $(a_{ij}) \cdot \big((b_{jk}) \cdot (c_{kl})\big)$. 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 $(a_{ij}) \cdot \big((b_{jk}) + (c_{jk})\big)$ 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 δ_{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:

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

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 $\sum_{k=1}^{n} b_{1k}a_{kn} = 1$. □

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 $b = 0$. □

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 Abeliano, 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 das unidades de A é denotado por A^*. □

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. □

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 $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$. □

3.5 Divisores de zero

Divisores de zero são elementos não nulos que, multiplicados entre si, resultam em zero.

Definição 3.13. Sejam A um anel. Um divisor de zero de A é um elemento $a \in A$ não nulo para o qual exista $b \in A$ não nulo tal que $ab = 0$ ou $ba = 0$. □

Divisores de zero são patológicos ao estudar a teoria de divisibilidade em anéis, assim, muitas vezes, eles são excluídos de tal estudo.

Note que um domínio de integridade é um anel comutativo sem divisores de zero.

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

Definição 3.14. 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. □

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

Definição 3.15 (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. □

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

3.7 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 3.16 (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. □

Todo corpo é um domínio de integridade. De fato:

Proposição 3.17. 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, $b = 0$. □

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

3.8 O corpo dos números reais

Assim como fizemos com $\mathbb{Z}$, assumiremos a existência do corpo dos números reais.
O corpo dos números reais é um corpo ordenado que satisfaz a propriedade de ser Dedekind-completo.
Formalmente:

Proposição 3.18. O corpo dos números reais $\mathbb{R}$ é um corpo ordenado, e satisfaz a propriedade de ser Dedekind-completo. Ou seja, tal que para todo $A \subseteq \mathbb{R}$ não vazio, se A é limitado superiormente (ou seja, se existe $a \in \mathbb{R}$ tal que $\forall x \in A, x \leq a$), então A admite um supremo (um menor limitante superior, ou seja, existe $b \in \mathbb{R}$ tal que $\forall x \in A, x \leq b$ e $\forall c \in \mathbb{R}$, se $x \leq c$ para todo $x \in A$, então $b \leq c$).

O estudo das propriedades dos números reais é um assunto central de um curso básico de Análise Real.
Nesse texto, detalharemos tais propriedades somente de acordo com nossa necessidade.

3.9 O corpo dos números complexos

A história dos números complexos remete à representar uma solução para a equação $x^2+1=0$, que não possui solução real.

A ideia é que adiciona-se em $\mathbb{R}$ um novo elemento, i, para o qual vale $i^2=-1$ e para o qual as demais propriedades operacionais de números reais são preservadas. Nesse anel, todo elemento se escreverá de forma única como $a+bi$, onde $a, bin\mathbb{R}$.

Apresentaremos uma construção a seguir.

Definição 3.19 (Quaternions)**.** Definimos $\mathbb{C}=\mathbb{R}^2$.

Se $a \in \mathbb{R}$, identifique $a=(a,0)$ e $i=(0,1)$.

Segue que, utilizando a linguagem de produto por escalar oriunda da álgebra linear, que para todo $x \in \mathbb{H}$, exisem únicos $a, b \in \mathbb{R}$ tais que $x=a+bi$.

Em $\mathbb{C}$, definimos a soma coordenada-a-coordenada. Da Álgebra Linear, sabemos que isso nos dá um grupo Abeliano.

Define-se também a multiplicação, inspirada pela discussão acima, como se segue: para $a, b, c, d \in \mathbb{R}$:

$$(a,b)(u,v)=(au-bv, bu+av).$$

Ou, em outra notação:

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

□

Proposição 3.20. $\mathbb{C}$ é um corpo.

Demonstração.

Proposição 3.21. $\mathbb{H}$ é um domínio de integridade.

Demonstração. 1 é neutro multiplicativo: dado $a+bi=(a,b)\in\mathbb{C}$, pela definição, temos que $(1,0)(a,b)=(a,b)$, pois as demais parcelas zeram. Analogamente, $(a,b)(1,0)=(a,b)$.

A multiplicação é associativa: Para $x, y, z \in \mathbb{H}$, tome $a, b, u, v, p, q \in \mathbb{R}$ com e $x=(a,b)$, $y=(u,v)$ e $z=(p,q)$. Temos que:

$$\begin{aligned}(xy)z &= (au-bv, bu+av)(p,q)\\ &= ((au-bv)p-(bu+av)q, (bu+av)p+(au-bv)q)\\ &= (aup-bvp-buq+avq, bup+avp+auq-bvq)\end{aligned}$$

e $x(yz)$ é dado por:

$$\begin{aligned}x(yz) &= (a,b)(up-pv, uq+vp)\\ &= (a(up-bv)-b(uq+vp), b(up-bv)+a(uq+vp))\\ &= (aup-bvq-bup+avq, bup+avp+auq-bvq)\end{aligned}$$

Comparando, segue.

A multiplicação é comutativa: Para $x, y \in \mathbb{H}$, temos que $x = (a, b)$ e $y = (u, v)$. Temos que:

$$\begin{aligned} xy &= (a,b)(u,v) = (au - bv, bu + av) \\ &= (ua - vb, va + ub) \\ &= (u,v)(a,b) \\ &= yx. \end{aligned}$$

A propriedade distributiva também é válida:

Para $x, y, z \in \mathbb{H}$, temos que $x = (a, b)$, $y = (u, v)$ e $z = (p, q)$. Temos que:

$$\begin{aligned} x(y+z) &= (a,b)((u,v) + (p,q)) \\ &= (a,b)(u+p, v+q) \\ &= (a(u+p) - b(v+q), b(u+p) + a(v+q)) \\ &= (au - bv, bu + av) + (ap - bq, bp + aq) \\ &= xy + xz \end{aligned}$$

Finalmente, todo elemento distindo de $(0, 0)$ é invertível: seja $x = (a, b) \in \mathbb{C}$ tal que $x \neq 0$. Então, $a^2 + b^2 \neq 0$. Considere $y = (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$. Calculemos xy:

$$\begin{aligned} xy &= (a,b)(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}) \\ &= (\frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}, \frac{-ab}{a^2+b^2} + \frac{ab}{a^2+b^2}) \\ &= \left(\frac{a^2+b^2}{a^2+b^2}, 0\right) \\ &= 1. \end{aligned}$$

□

□

3.10 O Anel dos Quaternions

Discutimos as noções de corpo e de anel de divisão. Por definição, todo corpo é um anel de divisão. Um dos primeiros exemplos de um anel de divisão que não é um corpo é o anel dos quaternions $\mathbb{H}$, que descreveremos abaixo.

A ideia é que adiciona-se em $\mathbb{R}$ três elementos distintos: i, j, k, para os quais valem as propriedades de que $i^2 = j^2 = k^2 = -1$, e $ij = k$, $jk = i$ e $ki = j$, e para o qual as demais propriedades operacionais de números reais são preservadas. Nesse anel, todo elemento se escreverá de forma única como $a + bi + cj + dk$, onde $a, b, c, d \in \mathbb{R}$.

Apresentaremos uma construção a seguir. Antes disso, note que, como $k = ij$, multiplicando ambos os lados por i à esquerda, supondo que a propriedade associativa ainda valha, temos que $ik = -j$.

Multiplicando por j à direita, temos que $kj = -1$.

Além disso, multiplicando por $i = jk$ à esquerda por j, temos que $ji = -1$. Assim, temos que $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$ e $ik = -j$.

Assumindo que $-i \neq i$, $-j \neq j$ e $-k \neq k$, temos que i, j, k vêmos que a nossa estrutura deverá ser não comutativa.

Definição 3.22 (Quaternions)**.** Definimos $\mathbb{H} = \mathbb{R}^4$.

Se $a \in \mathbb{R}$, seja $a = (a, 0, 0, 0)$, $i = (0, 1, 0, 0)$, $j = (0, 0, 1, 0)$ e $k = (0, 0, 0, 1)$.

Segue que, utilizando a linguagem de produto por escalar oriunda da álgebra linear, que para todo $x \in \mathbb{H}$, exisem únicos $a, b, c, d \in \mathbb{R}$ tais que $x = a + bi + cj + dk$.

Em $\mathbb{H}$, definimos a soma coordenada-a-coordenada. Da Álgebra Linear, sabemos que isso nos dá um grupo Abeliano.

Define-se também a multiplicação, inspirada pela discussão acima, como se segue: para $a, b, c, d, u, v, z, w \in \mathbb{R}$:

$$(a, b, c, d)(u, v, z, w) = (au - bv - cz - dw, av + bu + cw - dz, az + bw - cu + dv, aw + bz + cv - du).$$

Ou, em outra notação:

$$\begin{aligned}(a + bi + cj + dk)(u + vi + zj + kw)& \\ &= (au - bv - cz - dw) + (av + bu + cw - dz)i \\ &+ (az + bw - cu + dv)j + (aw + bz + cv - du)k.\end{aligned}$$

□

Note que, com isso, temos $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$ e $ki = j$, além de $i \neq -i$, $j \neq -j$ e $k \neq -k$.

Porém, $\mathbb{H}$ é um anel de divisão. Primeiro, provaremos que:

Proposição 3.23. $\mathbb{H}$ é um domínio de integridade.

Demonstração. 1 é neutro multiplicativo: dado $a + bi + cj + dk = (a, b, c, d) \in \mathbb{H}$, pela definição, temos que $(1, 0, 0, 0)(a, b, c, d) = (a, b, c, d)$, pois as demais parcelas zeram. Analogamente, $(a, b, c, d)(1, 0, 0, 0) = (a, b, c, d)$.

A multiplicação é associativa: Para $x, y, z \in \mathbb{H}$, temos que $x = (a, b, c, d)$, $y = (u, v, z, w)$ e $z = (p, q, r, s)$. Temos que:

$$(xy)z = (au - bv - cz - dw, av + bu + cw - dz, az + bw - cu + dv, aw + bz + cv - du)(p, q, r, s)$$

e $x(yz)$ é dado por:

$$x(yz) = (a, b, c, d)(up - vq - zr - sw, uq + vp + zs - tw, ur + vq - pw + zt, us + vq + pw - qt)$$

Expandindo os últimos produtos e comparando-os, vê-se que são iguais. Os detalhes ficam a cargo do leitor.

De maneira igualmente trabalhosa, porém mecânica, verifica-se às duas propriedades distributivas. □

Mais interessante é demonstrar que $\mathbb{H}$ é um anel de divisão. Para isso, precisamos mostrar que todo elemento não nulo de $\mathbb{H}$ é invertível.

Proposição 3.24. $\mathbb{H}$ é um anel de divisão.

Demonstração. Fica a cargo do leitor. Para um guia, ver o Exercício 3.4 □

3.11 Subanéis

Em Matemática, é comum que as estruturas estudadas possuam uma noção de subestrutura. Em geral, uma subestrutura de uma estrutura data 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 3.25 (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 $+|_{B^2} : B^2 \to B$ e $\cdot|_{B^2} : B^2 \to B$ são as restrições das operações de A à B^2. □

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:

Proposição 3.26 (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 $B \in B$.

Demonstração. Primeiro, notemos suponhamos 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 $(B, +|_B^2, 0_A)$ 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. □

Exemplo 3.27. $\mathbb{N}$ não é um subanel de $\mathbb{Z}$, pois $-1 \notin \mathbb{Z}$. 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 $a + b$. □

Exemplo 3.28 (Subanel trivial)**.** Para todo A, temos que A é subanel de si mesmo. □

Exemplo 3.29. 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 $n \in \mathbb{B}$: 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 $B = \mathbb{Z}$. □

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

Proposição 3.30. Subanéis de aneis 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 $a \cdot b = b \cdot a$. □

3.12 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 3.31 (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, $Z(A) = \{a \in A : \forall b \in A, ab = ba\}$. □

O centro de um anel sempre é um subanel.

Proposição 3.32. 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 $b \in A$, $(a - a')b = ab - a'b = ba - ba' = b(a - a')$. □

3.13 Exercícios

Exercício 3.1. Seja R um anel com identidade e seja S um subanel de R que contém a identidade de R. Prove que se u é uma unidade em S, então u é uma unidade em R. Apresente um exemplo que demonstre que a recíproca é falsa.

Exercício 3.2. Seja A um anel. Mostre que um anel A é um anel de divisão se, e somente se $A^* = A \setminus \{0\}$.

Exercício 3.3. No anel dos quaternions $\mathbb{H}$, identifique $x \in \mathbb{R}$ com $(x, 0, 0, 0) = x + 0i + 0j + 0k$.

Mostre que $\mathbb{R} = Z(\mathbb{H})$.

(Dica: após mostrar que $\mathbb{R} \subseteq Z(\mathbb{H})$, tome um elemento arbitrário de $Z(\mathbb{H})$ e estude sua multiplicação por i, j e k.)

Exercício 3.4. No anel dos quaternions, dado $q \in \mathbb{H}$, seu conjugado é definido como $\bar{q} = a + bi + cj + dk$.

a) Calcule $q\bar{q}$ e $q\bar{q}$.

b) Prove que, se $q \neq 0$, $\bar{q}(q\bar{q})^{-1}$ é inverso multiplicativo de q. Conclua que $\mathbb{H}$ é anel de divisão.

Exercício 3.5. Seja A um anel. Prove que se $q \in Z(A)$ e q é uma unidade, então $q^{-1} \in Z(A)$. Utilize esse fato para provar que o centro de qualquer anel de divisão é um corpo.

Exercício 3.6. Seja $\mathbb{Z}[i] = \{m + in : m, n \in \mathbb{Z}\} \subseteq \mathbb{C}$ (o conjunto dos inteiros de Gauss). Mostre que $\mathbb{Z}[i]$ é um subanel de $\mathbb{C}$, e que é um domínio de integridade.

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 aneis. Uma função $f : A \to R$ 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

$\cdot$	0	1
0	0	0
1	0	1

Em R:

$+$	Z	U
Z	Z	U
U	U	Z

$\cdot$	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 ϕ é um isomorfismo. □

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 $f : A \to R$ 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. □

4.2 Propriedades elementares

Lema 4.4. Sejam $f : A \to R$ e $g : R \to S$ homomorfismos de anéis. Então a composição $g \circ f : A \to S$ 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. □

Proposição 4.5 (Propriedades de homomorfismos)**.** Seja $f : A \to R$ 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, $\operatorname{ran} f = \{f(a) : a \in A\}$, é um subanel de R. Se A é comutativo, $\operatorname{ran} f$ 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 $a, b \in \operatorname{ran} f$. 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, $a - b \in \operatorname{ran} f$. Similarmente, $ab = f(x)f(y) = f(xy) \in \operatorname{ran} f$, e $1_R = f(1_A) \in \operatorname{ran} f$.

Portanto, $\operatorname{ran} f$ é um subanel de R. Se A é comutativo, $\operatorname{ran}(f)$ também é comutativo, pois dados $a, b \in \operatorname{ran} f$, 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 $\operatorname{ran} f$. Assim, f é um isomorfismo entre A e $\operatorname{ran} f$, dado que é um homomorfismo. □

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 $f : A \to R$ e $g : R \to S$ isomorfismos de anéis. Então:

a) $g \circ f$ é um isomorfismo de anéis.

b) $f^{-1} : R \to A$ é um isomorfismo de anéis.

c) $\operatorname{id}_A : A \to A$ 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, $f^{-1} : R \to A$ 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 id_A é claramente bijetora, e é um homomorfismo, pois, para todos $a, b \in A$:

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

□

Agora introduziremos o núcleo de um homomorfismo.

Definição 4.7. Seja $f : A \to R$ 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 $f : A \to R$ um homomorfismo. Então $f : A \to R$ 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 $f : A \to R$ 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 $f : A \to R$ 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 $x = x \cdot 1_R = x \cdot 0_R = 0_R$. □

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 $f : A \to R$ 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, $\ker f = A$. □

Podemos ver $\ker f$, em algum sentido, como uma medida do quão longe um homomorfismo f está de ser injetor: temos que $\{0\} \ker f \subseteq A$. Como vimos, f ser injetor é equivalente à $f = \{0\}$. 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. □

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 $f : A \to R$ 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 abaixos, 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. □

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.

Ideais também são preservados por imagens inversas.

Proposição 4.16. $f : A \to R$ um homomorfismo de anéis e J um ideal de R. Então $f^{-1}[J] = \{a \in A : f(a) \in J\}$ é um ideal de A.

Demonstração. Seja $I = f^{-1}[J]$. Temos que $J \neq \emptyset$ já que $0 \in \ker f \subseteq I$.

Sejam $a, b \in I$. Então $f(a), f(b) \in J$, logo, $f(a+b) = f(a)+f(b) \in J$, o que implica $a+b \in I$.

Agora seja $a \in A$ e $b \in I$. Temos que $f(ab) = f(a)f(b) \in J$ e $f(ba) = f(b)f(a) \in J$, pois $f(b) \in J$. Assim, $ab, ba \in J$. □

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 $ba \in I$. □

Proposição 4.17 (Ideal gerado)**.** Seja A um anel e $B \subseteq A$ um conjunto não vazio. Então, o conjunto $I = \{a_1b_1c_1 + \cdots + a_nb_nc_n : n \geq 1, a_i, c_i \in A, b_i \in B\}$ 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 $I = \{a_1b_1 + \cdots + a_nb_n : n \geq 1, a_i \in A, b_i \in B\}$.

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 $n, m \geq 1$, $a_1, \ldots, a_n, c_1, \ldots, c_n \in A$, $b_1, \ldots, b_n \in B$, $a'_1, \ldots, a'_m, c'_1, \ldots, c'_m \in A$ e $b'_1, \ldots, b'_m \in B$ tais que $x = a_1b_1c_1 + \cdots + a_nb_nc_n$ e $y = a'_1b_1c'_1 + \cdots + a'_mb'_md'_m$. Assim, $x + y = (a_1b_1 + \cdots + a_nb_n) + (a'_1b_1c_1 + \cdots + c_md_m) = (a_1b_1c_1 + \cdots + a_nb_nc_n) + (a'_1b'_1c'_1 + \cdots + a'_mb'_md'_m) \in I$. Concatenando as sequências, vemos que $x + y \in I$.

Seja $x \in A$ e $b \in I$. Então existem $n \geq 1$, $a_1, \ldots, a_n, c_1, \ldots, c_n \in A$ e $b_1, \ldots, b_n \in B$ tais que $b = a_1b_1c_n + \cdots + a_nb_nc_n$. Assim, $xb = (xa_1)b_1c_1 + \cdots + (xa_n)b_nc_n \in I$. Analogamente, $bx \in I$.

Agora, seja J um ideal de A que contém B. Fixe $x \in I$. Existem $n \geq 1$, $a_1, \ldots, a_n, c_1, \ldots, c_n \in A$ e $b_1, \ldots, b_n \in B$ tais que $x = a_1b1c_1 + \cdots + a_nb_nc_n$. Como J é um ideal de A e $B \subseteq A$, para cada $i \in \{1, \ldots, n\}$ temos que $a_ib_ic_i \in J$. Somando, segue que $x \in J$.

Finalmente, provaremos a afirmação final para quando $B \subseteq Z(R)$. Seja $I' = \{a_1b_1 + \cdots + a_nb_n : n \geq 1, a_i \in A, b_i \in B\}$. Veremos que $I = I'$. Pondo $c_1 = \cdots = c_n = 1$, vemos que que $I' \subseteq I$.

Reciprocamente, se $x = a_1b_1c_1 + \cdots + a_nb_nc_n \in I$ com $n \geq 1$, $a_1, \ldots, a_n, c_1, \ldots, c_n \in A$ e $b_1, \ldots, b_n \in B \subseteq Z(A)$, temos que $x = (a_1c_1)b_1 + \cdots + (a_nc_n)b_n \in I'$. □

Definição 4.18. Na notação da proposição acima, I é chamado de *ideal gerado por B* e denotamos por $\langle B\rangle$.

Caso $B = \{x_1, \ldots, x_n\}$, denotamos o ideal gerado por B como $\langle x_1, \ldots, x_n\rangle$. 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. □

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

Vimos que a interseção de ideais é um ideal. Porém, a união de ideais não precisa ser um ideal.

Exemplo 4.19. Considere, em $\mathbb{Z}$, os ideais $2\mathbb{Z}$ e $3\mathbb{Z}$. Temos que $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, mas $5 = 2 + 3 \notin \mathbb{Z} \cup 3\mathbb{Z}$. □

Qual seria, então, o menor ideal que contém a união de dois ideais?

Proposição 4.20. Seja A um anel e I, J ideais de A. Então $\langle I \cup J\rangle = I + J = \{a + b : a \in I, b \in J\}$

Demonstração. Como $0 \in I \cap J$, temos que $I \subseteq I + J$, já que para todo $a \in I$, $a + 0 \in I + J$. Similarmente, $J \subseteq I + J$.

Temos que $I + J$ é um ideal: se $a, b \in I + J$, então existem $x, y \in I$ e $u, v \in J$ tais que $a = x + u$ e $b = y + v$. Segue que $a + b = (x + y) + (u + v) \in I + J$. Agora, dado $a \in I + J$ e $x \in A$, temos que $a = i + j$ com $i \in I$ e $j \in J$. Segue que $xa = xi + xj \in I + J$, já que $xi \in I$ e $xj \in J$. Similarmente, $ax \in I + J$.

Concluimos que $I + J$ é um ideal de A que contém I e J. Vejamos que ele é o menor.

Se K é um ideal que contém I e J, vejamos que $I + J \subseteq K$. Seja $a + b \in I + J$, com $a \in I$ e $b \in J$. Como K é um ideal, $a \in K$ e $b \in K$, segue que $a + b \in K$. Assim, $I + J \subseteq K$. □

Apesar disso, uma união de uma cadeia de ideais é um ideal.

Proposição 4.21. Seja A um anel e $\mathcal{F}$ uma coleção não vazia de ideais de A tal que para todos $I, J \in \mathcal{F}$, $I \subseteq J$ ou $J \subseteq I$.

Então $\bigcup \mathcal{F} = \bigcup_{I \in \mathcal{F}} I$ é um ideal de A.

Demonstração. Seja $J = \bigcup \mathcal{F} = \bigcup_{I \in \mathcal{F}} I$.

Temos que $0 \in J$, pois para qualquer $I \in \mathcal{F}$, temos $0 \in I$.

Se $a, b \in J$, temos que $a + b \in J$: existem $I_1, I_2 \in \mathcal{F}$ com $a \in I_1, b \in I_2$. Como $I_1 \subseteq I_2$ ou $I_2 \subseteq I_1$ temos que $a, b \in I_1$ ou $a, b \in I_2$, e, assim, $a + b \in I_1$ ou $a + b \in I_2$. Em qualquer caso, $a + b \in J$.

Finalmente, se $a \in J$ e $b \in R$, temos que existe $I \in \mathcal{F}$ tal que $a \in I$. Assim, $ab, ba \in I \subseteq J$. □

4.4 Ideais Principais

Definição 4.22 (Ideal principal)**.** Um *ideal principal é um ideal gerado por um único elemento.* □

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

Definição 4.23 (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. □

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 de integridade 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 4.24 (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. □

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

Proposição 4.25 (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. □

Proposição 4.26. Seja R um domínio de ideais principais. Então, não existe uma sequência infinita de ideais $(I_n)_{n\in\mathbb{N}}$ tal que para todo $n \in \mathbb{N}$, $I_n \subsetneq I_{n+1}$.

Demonstração. Suponha que exista uma tal cadeia e seja $J = \bigcup_{n\in\mathbb{N}} I_n$. Como R é um domínio de ideais principais, J é um ideal principal, ou seja, existe $x \in R$ tal que $J = \langle x \rangle$.

Como $x \in J \bigcup_{n\in\mathbb{N}} I_n$, existe $N \in \mathbb{N}$ tal que $x \in I_N$. Como $x \in I_n$, temos que $\langle x \rangle \subseteq I_N$. Assim, $J = \langle n \rangle \subseteq I_N \subseteq I_{N+1} \subseteq J$, o que implica que $I_N = I_{N+1}$, um absurdo. □

4.5 Ideais Primos e Maximais

Dois outros importantes tipos de ideais são os ideais primos e maximais.

Definição 4.27. Seja A um anel. Um ideal I de A é dito *próprio* se $I \neq A$.

Um ideal próprio de A é dito *maximal* se ele não está contido propriamente em nenhum ideal próprio de A. Em símbolos:

Um ideal I de A é dito maximal se for próprio e, para todo ideal próprio J de A, se $I \subseteq J$ então $I = J$. □

Por sua vez, os ideais primos se definem como a seguir:

Definição 4.28. Seja A um anel comutativo. Um ideal primo de A é um ideal próprio $I \subseteq A$ tal que, para todos $a, b \in A$, se $ab \in I$, então $a \in I$ ou $b \in I$. □

Ideais primos podem ser generalizados para anéis não comutativos, mas este estudo não será realizado neste texto.

Em anéis comutativos, todo ideal maximal é primo:

Proposição 4.29. Seja A um anel comutativo e I um ideal maximal. Então I é primo.

Demonstração. Suponha que $a, b \in A$ são tais que $ab \in I$ e que $a \notin I$. Veremos que $b \in I$.

Como I é maximal, o ideal $I + \langle a \rangle$, por conter I propriamente, não é um ideal próprio, ou seja, $I + \langle a \rangle = A$.

Assim, existem $x \in I$ e $y \in A$ tais que $x + ya = 1$. Multiplicando ambos os lados por b, temos que $xb + yab = b$. Commo $x \in I$, temos que $xb \in I$, e, como $ab \in I$, temos que $yab \in I$. Portanto, $b = xb + yab \in I$. $\square$

Porém, nem todo ideal primo é maximal. Por exemplo, $\{0\}$ é um ideal primo de $\mathbb{Z}$ que não é maximal, já que $2\mathbb{Z}$ é um ideal próprio de $\mathbb{Z}$ que o contém propriamente.

4.6 Característica de um anel

Todo anel possui o elemento 0 e o elemento 1. Então, intuitivamente, também deve possuir os elementos $2 = 1 + 1$, $3 = 2 + 1$, $4 = 3 + 1$, e assim por diante, bem como seus opostos. Também esperamos que tais elementos operem de forma análoga aos inteiros, de modo que sejam verdadeiras expressões como $7 = 3 + 4$ ou $22 = 25 - 3$. Porém, como temos anéis finitos, como $\mathbb{Z}_2$, é impossível que qualquer anel contenha cópias de $\mathbb{Z}$. Expressões como $2 = 0$ intuitivamente devem ser verdade em $\mathbb{Z}_2$.

Utilizando a noção de homomorfismo, tal intuição pode ser formalizada pela seguinte proposição:

Proposição 4.30. Seja R um anel. Então existe um único homomorfismo $f : \mathbb{Z} \to R$.

Demonstração. Começaremos provando a unicidade. Caso f, g sejam dois homomorfismos de $\mathbb{Z}$ em R, temos que $g(0) = 0 = f(0)$ e $g(1) = 1 = f(1)$.

Por indução, vemos que para todo $n \geq 1$, temos que $g(n) = n = g(n)$: a base $n = 1$ foi afirmada acima. Para o passo indutivo, note que se tal hipótese vale para $n \geq 1$, então também vale para $n + 1$: $g(n + 1) = g(n) + g(1) = f(n) + f(1) = f(n + 1)$.

Finalmente, se $n < 0$, temos que $-n > 0$, logo $f(n) = f(-(-n)) = -f(-n) = -g(-n) = g(n)$.

Isso completa a prova da unicidade. Assim, resta apenas provar a existência.

Primeiro, definiremos $f(n)$ recursivamente para $n \geq 0$ como se segue:

- $f(0) = 0$.
- Definido $f(n)$ para $n \geq 0$, define-se $f(n + 1) = f(n) + 1$.

Assim, f está definido para todo inteiro não negativo. Se $n < 0$, define-se $f(-n) = -f(n)$.

Note que, qualquer que seja $n \in \mathbb{Z}$, $f(-n) = f(n)$.

Verificaremos que f é homomorfismo de anéis.

Preservação de 1: Note que $f(1) = f(0) + 1 = 0 + 1 = 1$.

Preservação da soma: Mostraremos que se $m, n \in \mathbb{Z}$, $f(m + n) = f(m) + f(n)$.

Caso 1: $m, n \geq 0$.

Fixe $n \geq 0$. Verificaremos, indutivamente, que $f(n + m) = f(n) + f(m)$ para todo $m \geq 0$. Para $m = 0$, temos que $f(n + m) = f(n) = f(n) + 0 = f(n) + f(0)$.

Supondo que a afirmação vale para m, temos que vale para $m + 1$: $f(n + (m + 1)) = f((n + m) + 1) = f(n + m) + 1 = (f(n) + f(m)) + 1 = f(n) + (f(m) + 1) = f(n) + f(m + 1)$.

Caso 2: $m, n < 0$.

Temos que $-n, -m > 0$ e $-(n+m) < 0$. Assim, $f(n+m) = f(-(-n-m)) = -f((-n)+(-m)) = -f(-n) - f(-m) = f(n) + f(m)$.

Caso 3: $n \geq 0$, $m < 0$.

Teremos dois subcasos: $n + m \geq 0$ e $n + m < 0$.

Caso $n + m \geq 0$, temos que $f(n+m) + f(-m) = f((n+m) + (-m)) = f(n)$ pelo primeiro caso, portanto, $f(n+m) = f(n) + (-f(-m)) = f(n) + f(m)$.

Caso $n + m < 0$, temos pelo primeiro caso que $f(n) + f(-n-m) = f(-m)$. Logo, $f(n) + f(m) = f(n+m)$.

Caso 4: $n < 0$, $m \geq 0$. Temos, pelo caso anterior, que $f(m+n) = f(n+m) = f(n)+f(m) = f(m) + f(n)$.

Preservação do produto: Mostraremos que se $m, n \in \mathbb{Z}$, $f(mn) = f(m)f(n)$.

Caso 1: $m, n \geq 0$.

Fixe $n \geq 0$. Verificaremos, indutivamente, que $f(nm) = f(n)f(m)$ para todo $m \geq 0$. Para $m = 0$, temos que $f(nm) = f(0) = 0 = f(n)f(0)$.

Supondo que a afirmação vale para m, temos que vale para $m+1$: $f(n(m+1)) = f(nm+n) = f(mn) + f(n) = f(n)f(m) + f(n) = f(n)(f(m) + 1) = f(n)f(m+1)$.

Caso 2: $m, n < 0$.

Temos que $-n, -m > 0$. Assim:

$$f(nm) = f((-n)(-m)) = -f(-n)f(-m) = -(-(f(n)f(m))) = f(n)f(m).$$

Caso 3: $n \geq 0$, $m < 0$. Temos que $-m > 0$. Assim:

$$f(nm) = f(-n(-m)) = -f(n)f(-m) = f(n)f(m).$$

Caso 4: $n < 0$, $m \geq 0$. Temos que $-m > 0$. Assim:

$$f(nm) = f(-(-n)m) = -f(-n)f(-m) = f(n)f(m).$$

□

Assim, podemos formalizar a notação $n \in \mathbb{R}$, e definir a característica de um anel como a seguir:

Definição 4.31. Seja R um anel e $n \in \mathbb{Z}$.

Em R, definimos o elemento n como sendo $\phi(n)$, onde $\phi : \mathbb{Z} \to R$ é o único homomorfismo de anéis dado na proposição acima.

Caso exista, definimos a *característica* de R como o menor inteiro positivo n tal que $n = 0_R$. Caso não exista, dizemos que a característica de R é zero. □

A característica 0 é

Proposição 4.32. Seja R um anel. Então a característica de R é zero se, e somente se, R contém um subanel isomorfo à $\mathbb{Z}$.

Demonstração. Seja $\phi : \mathbb{Z} \to R$ o único homomorfismo de anéis entre $\mathbb{Z}$ e R.

Se a característica de $\mathbb{Z}$ é 0, então para todo $n > 0$, $\phi(n) \neq 0$ e $\phi(-n) = -\phi(n) \neq 0$. Assim, ϕ é um monomorfismo, e sua imagem é isomorfa à $\mathbb{Z}$.

Reciprocamente, se R contém uma cópia isomorfa de $\mathbb{Z}$, seja $\psi : \mathbb{Z} \to R$ um monomorfismo.

Como o único homomorfismo de $\mathbb{Z}$ em R é ϕ, segue que $\phi = \psi$ é injetora, e, portanto, $\ker \phi = \{0\}$. Assim, não existe $n > 0$ tal que $\phi(n) = 0$. □

4.7 Exercícios

Exercício 4.1. Lembremos que, da Álgebra Linear, um espaço vetorial V sobre um corpo K é uma quadrupla $(V, +, 0, \cdot)$, onde $(V, +, 0)$ é um grupo Abeliano e $\cdot : K \times V \to V$ é uma operação que satisfaz:

- Associatividade: para todos $\alpha, \beta \in K$ e para todo $v \in V$, $(\alpha\beta)v = \alpha(\beta v)$.
- Distributividade: para todo $x, y \in K$ e para todo $v \in V$, $(x + y)v = xv + yv$.
- Distributividade II: para todo $x \in K$ e para todo $u, v \in V$, $x(u + v) = xu + xv$.
- Identidade: $1v = v$ para todo $v \in V$.

Uma transformação linear $T : V \to W$ entre dois espaços vetoriais V e W sobre um mesmo corpo K é uma função que preserva a estrutura de espaço vetorial, ou seja, satisfaz:

- $T(v + u) = T(v) + T(u)$ para todo $v, u \in V$.
- $T(\alpha v) = \alpha T(v)$ para todo $\alpha \in K$ e para todo $v \in V$.

Dado um espaço vetorial V, o conjunto de todas as transformações lineares de V em V, também chamadas de endomorfismos de V, é denotado por $\mathrm{End}(V)$. A função identidade $\mathrm{id}_V : V \to V$ é um endomorfismo, bem como a função nula.

Assumindo todo o exposto acima, mostre que, com a soma usual de transformações lineares (que é efetuada ponto-a-ponto) e com operação de composição como produto, $\mathrm{End}(V)$ é um anel.

Mostre com um exemplo que $\mathrm{End}(V)$ pode não ser comutativo.

Exercício 4.2. Seja V um espaco vetorial sobre um corpo K. Defina $\rho : K \to V^V$ da seguinte forma:

Para cada $\alpha \in K$, o mapa $\rho(\alpha) : V \to V$ é dado por $\rho(\alpha)(v) = \alpha v$ para todo $v \in V$.

Mostre que ρ é um homomorfismo de anéis, onde V^V é o anel dos endomorfismos de V.

(Dica: não se esqueça de verificar que ρ possui o contradomínio correto.)

Exercício 4.3. Seja R um anel e I um ideal de R. Mostre que I contém uma unidade se, e somente se, $I = R$.

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 $ac \sim bd$. □

Todo homomorfismo induz naturalmente uma relação de congruência. Explicitamente:

Proposição 5.2. Seja $f : A \to R$ 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 $ac \sim_f bd$. □

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 $q(a) = [a]_{\sim_I}$. □

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: $(q(a) + q(b))q(c) = q(a+b)q(c) = q((a+b)c) = q(ac+bc) = q(ac) + q(bc) = q(a)q(c) + q(b)q(c)$.

□

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 $A/I = \operatorname{ran} q$ também é, pois q é homomorfismo de anéis. □

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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "q"'] & R \\ A/J \arrow[ur, dashed, "\exists! \bar{f}"'] & \end{tikzcd}$$

Figura 5.1: Teorema do homomorfismo.

Demonstração. Definimos $\bar{f} : A/J \to R$ por $\bar{f}(a + J) = f(a)$. Então, g 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 $g : A/J \to R$ 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, $g = \bar{f}$. □

Como consequência, temos o Primeiro Teorema do Isomorfismo:

Teorema 5.10 (Primeiro Teorema do Isomorfismo)**.** Seja $f : A \to R$ um homomorfismo de anéis. Então, A/I é isomorfo a $\operatorname{ran} f$. Mais especificamente, existe um único homomorfismo $\phi : A/\ker f \to R$ tal que $q \circ \phi = f$, onde q é o mapa quociente, e este homomorfismo é necessariamente um isomorfismo.

$$
\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "q"'] & \operatorname{ran} f \\
A/\ker f \arrow[ur, dashed, "\exists!\phi"'] &
\end{tikzcd}
$$

Figura 5.2: Primeiro Teorema do Isomorfismo.

Demonstração. Pelo Teorema do Homomorfismo, existe um único homomorfismo $\bar{\phi} : A/\ker f \to \operatorname{ran} f$ tal que $\phi \circ q = f$, onde $q : A \to A/\ker f$ é o mapa quociente canônico dado por $q(a) = a + \ker f$.

Temos que ϕ é sobrejetor: dado $b \in \operatorname{ran} f$, existe $b \in A$ tal que $f(a) = b$. Logo, $b = f(a) = \bar{\phi}(q(a))$, assim, $b \in \operatorname{ran} \phi$.

Agora vejamos que ϕ é injetor. Suponha que $y \in A/\ker f$ é tal que $\phi(y) = 0$. Como q é sobrejetor, tome $a \in A$ tal que $y = q(a)$. Assim, $0 = \phi(y) = \phi \circ q(a) = f(a)$, logo, $a \in \ker f$. Como $q : A \to A/\ker f$ é o mapa quociente e $a \in \ker f$, segue que $y = q(a) = 0_{A/\ker f}$. Logo, $\ker \phi = \{0\}$, ou seja, ϕ é injetor. □

Como aplicação, temos:

Proposição 5.11. Seja R um anel e $n > 0$. Então R possui um subanel isomorfo à $\mathbb{Z}_n$ se, e somente se a característica de R é n.

Demonstração. Seja ϕ o único homomorfismo de $\mathbb{Z}$ em $\mathbb{R}$.

Vimos que, em $\mathbb{Z}$, para todo ideal não nulo I, temos que $I = \langle n \rangle$, onde m é o menor elemento positivo de m.

Suponha que a característica de R é $n > 0$. Nesse caso, por definição, a característica de R é o menor inteiro positivo do ideal $I = \ker \phi$. Pelo Primeiro Teorema do Isomorfismo, temos que $\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$ é isomorfo a $\operatorname{ran} \phi$, que é um subanel de R.

Reciprocamente, suponha que R possui um subanel S isomorfo a $\mathbb{Z}_n$. Seja $\psi : S \to \mathbb{Z}_n$ isomorfismo.

Seja ϕ o único homomorfismo de $\mathbb{Z}$ em S. Este necessariamente é, também, o único homomorfismo de $\mathbb{Z}$ em R.

$\psi \circ \phi$ é o único homomorfismo de $\mathbb{Z}$ em $\mathbb{Z}_n$, logo, o seu primeiro zero positivo é a característica de $\mathbb{Z}_n$, que é n. Assim, $\psi \circ \phi(n) = \psi(\phi(n)) = 0$. Como ψ é isomorfismo, segue que $\phi(n) = 0$. Além disso, se $0 < m < n$ e $\phi(m) = 0$, teremos $\psi(\phi(m)) = 0$, o que é absurdo, já que n é o primeiro zero de $\psi \circ \phi$. Portanto, a característica de R é a característica de S, que é n. □

Do primeiro Teorema do Isomorfismo, decorre o segundo Teorema do Isomorfismo. Para enuncia-lo, lembremos que se B, C são subconjuntos de um grupo abeliano A, então $B + C = \{b + c : b \in B, c \in C\}$.

Lema 5.12. Se A é um anel, B um subanel de A e I um ideal de A contido em B, então para todo $b \in B$, a classe de equivalência $[b]_I$ é a mesma tomando como ambiente tanto o anel B como o anel A.

Assim, $B/I \subseteq A/I$.

Além disso, sendo $q : A \to A/I$ o mapa quociente e $q' : B \to B/I$ o mapa quociente, temos que $q' = q|B$.

Demonstração. Fixe b. Devemos ver que $\{a \in A : a - b \in I\} = \{a \in B : a - b \in I\}$.

Assim, basta ver que se $a \in A$ e $a - b \in I$, então $a \in B$. Ora, $a = (a - b) + b$. Como $a - b \in I \subseteq B$ e $b \in B$, temos que $a \in B$.

Note que o lado esquerdo da igualdade é $q(b)$ e o direito é $q'(b)$, assim, segue a tese. □

Teorema 5.13 (Segundo Teorema do Isomorfismo)**.** Sejam A um anel, B um subanel de A e I um ideal de A. Então:

a) $I \cap B$ é um ideal de B.

b) $I + B$ é um subanel de A.

c) $\dfrac{I + B}{I} \cong \dfrac{B}{I \cap B}$.

Demonstração. Primeiro, verifiquemos que $I + B$ é um subanel de A.

Temos que $1 = 0 + 1 \in I + B$.

Se $x, y \in I + B$, então $x = a_1 + b_1$ e $y = a_2 + b_2$, onde $a_1, a_2 \in I$ e $b_1, b_2 \in B$. Segue que $a_1 - a_2 \in I$ e $b_1 - b_2 \in B$, logo, $x - y = (a_1 - a_2) + (b_1 - b_2) \in I + B$.

Além disso, $xy = (a_1 + b_1)(a_2 + b_2) = a_1a_2 + a_1b_2 + b_1a_2 + b_1b_2$. Temos que $a_1a_2 \in I$, $a_1b_2 \in I$, $b_1a_2 \in I$ e $b_1b_2 \in B$, logo, $xy \in I + B$. Assim, $I + B$ é um subanel de A.

Agora considere o mapa $q : I + B \to \frac{I+B}{I}$ dado por $q(x) = x + I$. Seja $f = q|_B : B \to \frac{I+B}{I}$ o homomorfismo restrito de q em B.

Pelo primeiro Teorema do Isomorfismo, $B/\ker f \cong \operatorname{ran} f$. Veremos que $\operatorname{ran} f = I + B/I$ e $\ker f = I \cap B$, o que completa a prova.

Temos que $\operatorname{ran} f = \frac{I+B}{I}$ pelo lema anterior, pois $I \subseteq B \subseteq I + B$.

Calculemos $\ker f$. Ora, se $x \in B$, temos que $f(x) = 0$ se, e somente se, $q(x) = 0$ se, e somente se $x \in I$. Como $x \in B$, isso é equivalente à $x \in I \cap B$, o que completa a prova. □

Finalmente, temos o Terceiro Teorema do Isomorfismo.

Teorema 5.14 (Terceiro Teorema do Isomorfismo)**.** Sejam A um anel, B um subanel de A e $I \subseteq J \subseteq B$ ideais. Seja $q : A \to A/I$ a projeção natural. Então $J/I = \{q(a) : a \in J\}$ é um ideal de A/I, e:

$$(B/I)/(J/I) \cong B/J.$$

Demonstração. Seja $p : B \to B/J$ o mapa quociente dado por $p(b) = b + J$ para todo $b \in B$. Seja $q' = q|B : B \to B/I$ o mapa quociente para B/I.

Temos que $\ker p = B \cap J = J$ e $I \subseteq J$. Assim, pelo Teorema do Homomorfismo, existe $\bar{p} : B \to B/J$ homomorfismo tal que $\bar{f} \circ q' = f$.

$$\begin{tikzcd}
B \arrow[r, "p"] \arrow[d, "q'"'] & B/J \\
A/I \arrow[ur, dashed, "\bar{p}"] \arrow[d] & \\
\frac{A/I}{\ker \bar{p}} \arrow[uur, dashed, "\phi"'] &
\end{tikzcd}$$

Pelo Primeiro Teorema do Isomorfismo, $(B/J)/\ker \bar{f} \cong \operatorname{ran} \bar{f}$. Calcularemos $\operatorname{ran} \bar{f}$ e $\ker \bar{f}$, o que concluirá a prova.

Temos que, para $\bar{p} \circ q' = p$. Como q' e p são sobrejetoras, temos:

$$\operatorname{ran} \bar{p} = \{p(x) : x \in A/I\} = \{\bar{p}(q(b)) : b \in B\} = \{p(b) : b \in B\} = \operatorname{ran} p = B/J.$$

Agora calcularemos $\ker \bar{p}$. Fixe $x \in A/I$. Existe $b \in B$ tal que $x = q(b)$. Se $x \in \ker \bar{p}$, então $0 = \bar{p}(x) = \bar{p}(q(b)) = p(b) = b + J$, logo, $b \in J$, e, portanto, $x = q(b) \in J/I$. Reciprocamente, se $x \in J/I$, então $x = q(b)$ para algum $b \in J$, logo, $p(b) = 0$, e, portanto, $p(x) = \bar{p}(q'(b)) = p(b) = 0$. Assim, $x \in \ker \bar{p}$.

Assim, temos que $\ker \bar{p} = J/I$, e este último é um ideal, pois núcleos de homomorfismos são ideais. □

No terceiro teorema do isomorfismo, vimos que se $I \subseteq J \subseteq A$, então J/I é um ideal de A/I. Quem são os ideais de um quociente? O teorema a seguir mostra que todos são dessa forma.

Teorema 5.15 (Teorema da correspondência)**.** Seja A é um anel e I um ideal de A. Considere a função $\phi : \{J \subseteq A : I \subseteq J \text{ e } J \text{é ideal de } A\} \to \{K \subseteq A/I : K \text{é ideal de } A/I\}$ dada por:

$$\phi(J) = J/I.$$

Então ϕ é uma bijeção entre os ideais de A que contêm I e os ideais de A/I. Além disso, ϕ é um isomorfismo de ordem, ou seja, se J_1, J_2 são ideais e $I \subseteq J_1, I \subseteq J_2 \subseteq A$, então $\phi(J_1) \subseteq \phi(J_2)$ se, e somente se $J_1 \subseteq J_2$.

Demonstração. Pelo Terceiro Teorema do Isomorfismo, o contradomínio de ϕ está correto. Pela definição de J/I, é claro que ϕ é uma função crescente (se $J_1 \subseteq J_2$, então $J_1/I \subseteq J_2/I$).

Agora, seja $\psi : \{K \subseteq A/I : K \text{é ideal de } A/I\} \to \{J \subseteq A : I \subseteq J \text{ e } J \text{é ideal de } A\}$ dada por $\psi(K) = q^{-1}[K]$, onde $q : A \to A/I$ é o mapa quociente dado por $q(a) = a + I$.

Como q é um homomorfismo e ideais são preservados por imagens inversas de homomorfismos, segue que cada $\psi(K)$ é um ideal de A. Além disso, $\psi(K)$ contém I, já que $\ker q = q^{-1}(0) = I \subseteq \psi(K)$. Finalmente, pela definição de pré-imagem, ψ também preserva a ordem.

Agora veremos que ϕ, ψ são isomorfismos inversos, o que completará a prova.

Dado um ideal J de A que contém I, temos que $\psi(\phi(I)) = \psi(J/I) = \{a \in A : q(a) \in J/I\}$. Afirmamos que esse conjunto é J. Com efeito, se $a \in J$, temos que $a \in A$ e $q(a) \in J/I$. Reciprocamente, se $a \in A$ e $q(a) \in J/I$, existe $b \in J$ tal que $q(a) = q(b)$. Assim, $b \in J$ e $a - b \in I \subseteq J$, logo, $a = (a - b) + b \in J$.

Agora, fixe um ideal K de A/I.

Veremos que $\phi(\psi(K)) = K$.

Temos que $\phi(\psi(K)) = \phi(q^{-1}[K]) = \phi(\{a \in A : q(a) \in K\}) = \{q(a) : a \in A \text{ e } q(a) \in K\}$. É imediato que este último é K, o que completa a prova. □

5.4 Exercícios

Exercício 5.1. Liste todos os elementos de $\mathbb{Z}_{12} = \mathbb{Z}/12\mathbb{Z}$ que são divisores de zero.

Capítulo 6

Domínios de Integridade

Neste capítulo, exploraremos com mais detalhes os domínios de integridade e a teoria que nasce deles.

6.1 Relações entre corpos e domínios de integridade

Conforme visto, todo corpo é um domínio de integridade, e a recíproca não é verdadeira (sendo $\mathbb{Z}$ um contra-exemplo).

A seguir, apresentaremos algumas relações entre corpos e domínios de integridade.

Proposição 6.1. Todo domínio de integridade finito é um corpo.

Demonstração. Seja R um domínio de integridade finito. Fixe $a \in R \setminus \{0\}$. Veremos que a é invertível.

Considere $\phi : R \setminus \{0\} \to R \setminus \{0\}$ dado por $\phi(x) = ax$.

Como R é um domínio de integridade, para todo $x \in R \setminus \{0\}$, temos $ax \neq 0$, logo, ϕ está bem definida.

ϕ é uma função injetora: se $\phi(x) = \phi(y)$, então $ax = ay$. Logo, $a(x - y) = 0$. Como $a \neq 0$ e R é um domínio de integridade, segue que $x - y = 0$, ou seja, $x = y$.

Como $R \setminus \{0\}$ é finito e $\phi : R \setminus \{0\} \to R \setminus \{0\}$ é injetora, segue que ϕ é sobrejetora. Em particular, existe $x \in X$ tal que $ax = \phi(x) = 1$. Logo, a é invertível. □

Portanto, restrito aos anéis finitos, o estudo dos corpos e domínios de integridade colapsa em um único estudo.

Outra relação importante é a que segue:

Proposição 6.2. Seja R um anel comutativo e I um ideal próprio de R. São equivalentes:

(i) R/I é um corpo;

(ii) I é maximal.

Demonstração. Seja $q : R \to I$ o mapa quociente.

(i) $\Rightarrow$ (ii): Suponha que R/I é um corpo.

I é um ideal próprio, caso contrário, teríamos que R/I é o anel trivial, que não é um corpo.

Agora suponha que J é um ideal que contém I propriamente. Veremos que $J = R$. Seja $a \in J \setminus I$. Como $a \notin I$, temos que $q(a) \neq 0$. Como A/I é um corpo, existe $b \in R$ tal que

$q(a)q(b) = 1$. Isso implica que existe $x \in I$ tal que $ab + x = 1$. Como $a \in J$ e $x \in I \subseteq J$, segue que $1 = ab + x \in J$, e, portanto, $J = R$.

(ii) $\Rightarrow$ (i): Suponha que I é maximal. Vejamos que R/I é um corpo.

Seja $x \in R \setminus I$ não nulo. Tome $a \in R$ tal que $q(a) = x$. Temos que $a \notin I$. Como $I + \langle a \rangle$ é um ideal que contém I propriamente, segue que $I + \langle a \rangle = R$. Logo, existe $b \in R$ e $c \in I$ tais que $c + ba = 1$. Logo, $q(1) = q(c) + q(ba) = 0 + q(b)q(a) = q(b)x$. Portanto, x é invertível. □

Será que podemos caracterizar, de forma análoga, ser um domínio de integridade? A resposta é positiva.

Proposição 6.3. Seja R um anel comutativo e I um ideal próprio de R. São equivalentes:

(i) R/I é um domínio de integridade.

(ii) I é primo.

Demonstração. Seja $q : R \to I$ o mapa quociente.

(i) $\Rightarrow$ (ii): Suponha que R/I é um domínio de integridade.

I é um ideal próprio, caso contrário, teríamos que R/I é o anel trivial, que não é um domínio de integridade.

Suponha que $a, b \in R$ tais que $ab \in I$. Temos que $q(a)q(b) = q(ab) = 0$. Como R/I é um domínio de integridade, temos que $q(a) = 0$ ou $q(b) = 0$, ou seja, que $a \in I$ ou $B \in I$.

Logo, I é primo.

(ii) $\Rightarrow$ (i): Suponha que I é primo. Vejamos que R/I é um domínio de integridade.

Sejam $x, y \in R$ tais que $q(x)q(y) = 0$. Devemos ver que $q(x) = 0$ ou $q(y) = 0$. Como $q(xy) = q(x)q(y) = 0$, segue que $xy \in I$. Então, $x \in I$ ou $y \in I$, ou seja, $q(x) = 0$ ou $q(y) = 0$. □

Como consequência, temos:

Corolário 6.4. Seja R um anel comutativo finito e I um ideal de R. Então I é primo se, e somente se I é maximal.

Demonstração. Temos que R/I é finito, e, portanto, é um corpo se, e somente se for um domínio de integridade. Portanto:

$$I \text{ é primo} \Leftrightarrow R/I \text{ é um domínio de integridade} \Leftrightarrow R/I \text{ é um corpo} \Leftrightarrow I \text{ é maximal}$$

□

6.2 O corpo de frações de um domínio de integridade

Conforme vimos, nem todo domínio de integridade é um corpo, sendo $\mathbb{Z}$ é o contra-exemplo mais usual. Apesar disso, parece que, em algum sentido, $\mathbb{Q}$ é o "menor" corpo que contém $\mathbb{Z}$.

Uma das construções mais usuais do corpo $\mathbb{Q}$ utiliza classes de equivalências de pares de elementos de $\mathbb{Z}$. Nesta seção, estudaremos esta construção de modo generalizado.

Iniciaremos apresentando uma construção do corpo de frações.

Definição 6.5. Seja R um domínio de integridade.

Definamos, em $R \times \{0\}$, a relação de equivalência $\sim$ a seguir:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

□

Ao longo desta seção, a notação $\sim$ será fixada e utilizada exclusivamente para esse fim. A ideia é pensar em cada par (a, b) como uma fração $\frac{a}{b}$. A relação $\sim$ captura a ideia que duas frações $\frac{a}{b}$ e $\frac{c}{d}$ são equivalentes se, e somente se, $ad = bc$.

Lema 6.6. Na notação acima, a relação $\sim$ é uma relação de equivalência em $R \times \{0\}$.

Demonstração. Seja $(a, b), (c, d), (e, f) \in R \times \{0\}$.

- Temos que $(a, b) \sim (a, b)$ pois $ab = ba$.
- Simetria: se $(a, b) \sim (c, d)$, temos que $ad = bc$. Logo, $cb = da$, o que nos dá $(c, d) \sim (a, b)$.
- Transitividade: suponha que $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Temos que $ad = bc$ e $cf = de$. Multiplicando a primeira equação por f e a segunda por b, temos que $adf = bcf$ e $bcf = deb$. Logo, $adf = deb$. Como $d \neq 0$, cancelando, temos que $af = eb$, ou seja, que $(a, b) \sim (e, f)$.

□

Assim, podemos definir:

Definição 6.7. O conjunto das classes de equivalência $(R \times R \setminus \{0\})/\sim$ será denotado por $\mathrm{Frac}(R)$.

A classe de equivalência de um par (a, b) será denotada por $\frac{a}{b}$ □

Observe que agora, formalmente, $\frac{a}{b} = \frac{c}{d}$ se, e somente se, $ad = bc$.
Porém, a igualdade $a = \frac{a}{1}$ não faz sentido e será discutida mais adiante.
Agora, definiremos as operações em $\mathrm{Frac}(R)$.

Definição 6.8. Seja R um domínio de integridade. Define-se, em $\mathrm{Frac}(R)$, as operações a seguir. Para $a, b, c, d \in R$ tais que $b, d \neq 0$:

- Soma: $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad + bc}{bd}$.
- Produto: $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{ac}{bd}$.

□

Note que a expressão $\frac{ac}{bd}$ faz sentido já que $bd \neq 0$. O próximo passo é mostrar que tais operações estão bem definidas.

Lema 6.9. Na notação anterior, a soma e o produto de frações estão bem definidas.

Demonstração. Consideremos $a, b, a', b', c, d, c', d' \in R$ tais que $b, b', d, d' \neq 0$ e tais que $\frac{a}{b} = \frac{a'}{b'}$ e $\frac{c}{d} = \frac{c'}{d'}$. Assim, sabemos que $ab' = a'b$ e $cd' = c'd$.

Devemos ver que $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ e $\frac{ac}{bd} = \frac{a'c'}{b'd'}$.
Começaremos pela segunda afirmação.
Queremos provar que $acb'd' = a'c'bd$. Temos:

$$acb'd' = (ab')(cd') = (a'b)(c'd) = a'c'bd.$$

Agora, para a soma, temos que provar que $adb'd' + bcb'd' = a'd'bd + b'c'bd$. Multiplicando a equação $ab' = a'b$ por $d'd$, a equação $cd' = c'd$ por $b'b$, e somando, segue a tese. □

Agora veremos que $\mathrm{Frac}(R)$ é um corpo.

Teorema 6.10. Seja R um domínio de integridade.

Então $\mathrm{Frac}(R)$ é um corpo cujo zero é $\frac{0}{1}$, cuja identidade multiplicativa é $\frac{1}{1}$ e com opostos aditivos $-\frac{a}{b} = \frac{-a}{b}$.

Além do mais, se $\frac{a}{b}$ é não nulo, então $a \neq 0$ e $\frac{b}{a}$ é seu inverso multiplicativo.

Demonstração. Primeiro, veremos que $\mathrm{Frac}(R)$, com a soma, é um grupo abeliano.

Antes, note que para todo $b \in R \setminus \{0\}$, temos que $\frac{0}{b} = \frac{0}{1}$, já que $0 \cdot 1 = 0 = 0 \cdot b$.

- $+$ é associativo: sejam $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathrm{Frac}(R)$. Temos que:

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cd + ef}{df} = \frac{a(df) + b(cd + ef)}{bdf} = \frac{adf + bcd + bef}{bdf}.$$

  Por outro lado, temos que:

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{(ad + bc)f + bed}{bdf} = \frac{adf + bcd + bef}{bdf}.$$

  Logo, $+$ é associativa.

- $+$ é comutativa: sejam $\frac{a}{b}, \frac{c}{d} \in \mathrm{Frac}(R)$. Temos que:

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

- $\frac{0}{1}$ é neutro: seja $\frac{a}{b} \in \mathrm{Frac}(R)$. Temos que:

-

$$\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + 0 \cdot b}{b \cdot 1} = \frac{a}{b}.$$

- Opostos aditivos: seja $\frac{a}{b} \in \mathrm{Frac}(R)$. Temos que:

$$\frac{a}{b} + \frac{-a}{b} = \frac{a \cdot b + (-a) \cdot b}{b \cdot b} = \frac{0}{b} = \frac{0}{1}.$$

Agora, provaremos as propriedades da multiplicação.

- $\cdot$ é associativo: sejam $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathrm{Frac}(R)$. Temos que:

$$\frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{cd}{df} = \frac{a(cd)}{b(df)} = \frac{(ac)d}{(bd)f} = \frac{ac}{bd}\frac{d}{f} = \left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f}.$$

- $\cdot$ é comutativo: sejam $\frac{a}{b}, \frac{c}{d} \in \mathrm{Frac}(R)$. Temos que:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \cdot \frac{a}{b}.$$

- $\frac{1}{1}$ é neutro: seja $\frac{a}{b} \in \mathrm{Frac}(R)$. Temos que:

$$\frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b}.$$

- Inversos multiplicativos: seja $\frac{a}{b} \in \text{Frac}(R)$ não nulo. Como $\frac{a}{b}$ é não nulo, temos que $a \neq 0$, uma vez que $\frac{0}{b} = \frac{0}{1}$. Assim, a fração $\frac{b}{a}$ é bem definida, e:

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}.$$

- Distributividade: sejam $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \text{Frac}(R)$. Temos que:

$$\frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{cd + ef}{df} = \frac{a(cd + ef)}{b(df)} = \frac{acd + aef}{bdf}.$$

Por outro lado, temos que:

$$\frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{ac \cdot f + ae \cdot d}{bdf} = \frac{acdb + aebf}{b^2 df}.$$

Temos que ambos os lados são iguais, pois:

$$b^2 df(acd + aef) = bdf(acdb + aebf).$$

□

Assim, à semelhança da relação que o corpo $\mathbb{Q}$ tem com $\mathbb{Z}$, construímos um corpo $\text{Frac}(R)$ a partir de um domínio de integridade R.

Existe uma identificação natural de R em $\text{Frac}(R)$, como dada a seguir:

Proposição 6.11. A função $\phi : R \to \text{Frac}(R)$ dada por $\phi(a) = \frac{a}{1}$ é um monomorfismo de anéis. Tal ϕ é denominado *identificação natural de R em* $\text{Frac}(R)$.

Demonstração. Fixe $a, b \in R$.

Injetividade: se $\frac{a}{1} = \frac{b}{1}$, então $a.1 = 1.b$, logo, $a = b$.

Preservação da identidade: temos que $\phi(1) = \frac{1}{1}$, que é a identidade em $\text{Frac}(R)$.

Preservação das somas: Temos que $\phi(a) + \phi(b) = \frac{a}{1} + \frac{b}{1} = \frac{a \cdot 1 + b \cdot 1}{1^2} = \frac{a+b}{1} = \phi(a + b)$.

Preservação dos produtos: Temos que $\phi(a) \cdot \phi(b) = \frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1^2} = \phi(ab)$. □

Devido à isso, é natural identificar $a \in R$ com $\phi(a) = \frac{a}{1}$, de modo a dar sentido à igualdade $a = \frac{a}{1}$.

Notemos ainda que, se $a, b \in R$ e $b \neq 0$, então $\frac{a}{b} = \phi(a)\phi^{-1}(b)$. Desse modo, pode-se pensar que, em algum sentido, $\text{Frac}(R)$ é o menor corpo que contém R. A proposição abaixo não apenas formaliza essa ideia, mas define categoricamente o que é o corpo de frações de um domínio de integridade de modo independente de construções.

Teorema 6.12 (Propriedade universal do Corpo de Frações)**.** Seja R um domínio de integridade, $\text{Frac}(R)$ seu corpo de frações e ϕ a identificação natural de R em $\text{Frac}(R)$.

Então, para cada corpo K e cada monomorfismo $f : R \to K$, existe um único homomorfismo de anéis g tal que $g \circ \phi = f$.

Além disso, se (L, ψ) é um par tal que L é um corpo e $\psi : R \to L$ é um monomorfismo de anéis tal que para todo corpo K e todo monomorfismo $f : R \to K$ existe um homomorfismo de anéis g tal que $g \circ \psi = f$, então L é isomorfo a $\text{Frac}(R)$ – e existe um único isomorfismo de anéis $u : L \to K$ tal que $u \circ \phi = \psi$.

Demonstração. Começaremos mostrando que o par $(\frac{(}{R}), \phi)$ tem a propriedade desejada.

Seja K um corpo e $f : R \to K$ um homomorfismo de anéis. Definimos $g : \mathrm{Frac}(R) \to K$ para $a, b \in R$ com $b \neq 0$ como a seguir:

$$g\left(\frac{a}{b}\right) = f(a)f(b)^{-1}.$$

Se $a', b' \in R$ e $b' \neq 0$ são tais que $\frac{a}{b} = \frac{a'}{b'}$, então $ab' = a'b$. Logo, $f(a)f(b') = f(a')f(b)$, ou seja, $f(a)f(b)^{-1} = f(a')f(b')^{-1}$ e, portanto, a função está bem definida.

Vejamos que g é homomorfismo:

- Preservação da soma: sejam $\frac{a}{b}, \frac{c}{d} \in \mathrm{Frac}(R)$. Temos que:

$$g\left(\frac{a}{b} + \frac{c}{d}\right) = g\left(\frac{ad+bc}{bd}\right) = f(ad+bc)f(bd)^{-1}$$

$$= f(a)f(d)^{-1} + f(b)f(c)^{-1} = g\left(\frac{a}{b}\right) + g\left(\frac{c}{d}\right).$$

- Preservação do produto: sejam $\frac{a}{b}, \frac{c}{d} \in \mathrm{Frac}(R)$ com $b, d \neq 0$. Temos que:

$$g\left(\frac{a}{b} \cdot \frac{c}{d}\right) = g\left(\frac{ac}{bd}\right) = f(ac)f(bd)^{-1} = f(a)f(b)^{-1}f(c)f(d)^{-1} = g\left(\frac{a}{b}\right) \cdot g\left(\frac{c}{d}\right).$$

- Preservação da identidade: sejam $\frac{a}{b} \in \mathrm{Frac}(R)$ com $b \neq 0$. Temos que:

$$g\left(\frac{1}{1}\right) = f(1)f(1)^{-1} = 1_K.$$

Temos que $g \circ \phi(a) = g(\frac{a}{1}) = f(a)f(1)^{-1} = f(a)$, para todo $a \in R$, logo, $g \circ \phi = f$.

Assim, g satisfaz todos os requisitos necessários.

Vejamos que g é único. Se $\bar{g} : \mathrm{Frac}(R) \to K$ é um homomorfismo de anéis tal que $\bar{g} \circ \phi = f$, fixe $a, b \in R$ com $b \neq 0$. Veremos que $g\left(\frac{a}{b}\right) = \bar{g}\left(\frac{a}{b}\right)$. Ora:

$$\bar{g}\left(\frac{a}{b}\right) = \bar{g}\left(\frac{a}{1} \cdot \frac{1}{b}\right) = \bar{g}\left(\frac{a}{1}\right) \cdot \bar{g}\left(\frac{1}{b}\right)$$

$$= \bar{g} \circ \phi(a) \cdot \bar{g}(\phi(b)^{-1}) = f(a)\bar{g}(\phi(b))^{-1} = f(a)f(b)^{-1} = g\left(\frac{a}{b}\right).$$

Isso prova a primeira parte do teorema. Para a segunda parte, suponha que (L, ψ) é um par tal que L é um corpo e $\psi : R \to L$ é um homomorfismo de anéis tal que para todo corpo K e todo monomorfismo $f : R \to K$ existe um homomorfismo de anéis g tal que $g \circ \psi = f$.

Aplicando a propriedade de (L, ψ) para o corpo K e homomorfismo ϕ, existe um único homomorfismo de anéis $u : L \to K$ tal que $u \circ \psi = \phi$. Basta ver que u é isomorfismo.

Aplicando a propriedade de (K, ϕ) para o corpo L e homomorfismo ψ, existe um homomorfismo de anéis $v : K \to L$ tal que $v \circ \phi = \psi$. Veremos que $v = u^{-1}$.

Aplicando a propriedade de (L, ψ) para o corpo L e homomorfismo ψ, existe um único homomorfismo de anéis $w : L \to L$ tal que $w \circ \psi = \psi$. Porém, $\mathrm{id}_L \circ \psi = \psi$ e $(v \circ u) \circ \psi = v \circ \phi = \psi$, logo, $\mathrm{id}_L = w = v \circ u$.

Aplicando a propriedade de (K, ϕ) para o corpo L e homomorfismo ϕ, existe um único homomorfismo de anéis $\bar{w} : L \to K$ tal que $\bar{w} \circ \phi = \phi$. Porém, $\mathrm{id}_K \circ \phi = \phi$ e $(u \circ v) \circ \phi = v \circ \psi = \phi$, logo, $\mathrm{id}_K = \bar{w} = u \circ v$.

Logo, u e v são isomorfismos inversos, e segue a tese.

□

6.3 Exercícios

Exercício 6.1. Demonstre, com suas próprias palavras, de modo que considere satisfatório, a seguinte afirmação demonstrada no texto: Todo domínio de integridade finito é um corpo.

Exercício 6.2. Mostre que cada corpo de característica zero contém um subcorpo isomorfo à $\mathbb{Q}$.

Exercício 6.3. Prove que para todo domínio R, a característica de R é igual à de $\mathrm{Frac}(R)$.

Capítulo 7

Produtos de anéis

Neste capítulo, estudaremos o produto direto de anéis.

7.1 Produtos de dois anéis

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

Definição 7.1 (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:

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

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

Com as operações explicitadas, o produto de dois anéis é, de fato, um anel.

Deixaremos a prova deste fato como exercício (ver Exercício 7.1), já que na seção seguinte provaremos um resultado mais geral.

7.2 Produtos de uma família de anéis

Definição 7.2 (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 7.3 (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:** $(a + b) + c = (a_i +_i b_i)_{i \in I} + c = ((a_i +_i b_i) +_i c_i)_{i \in I} = (a_i +_i (b_i +_i c_i))_{i \in I} = a + (b + c)$
- **Associatividade do produto:** Análogo.
- **Comutatividade da soma:** $a + b = (a_i +_i b_i)_{i \in I} = (b_i +_i a_i)_{i \in I} = b + a$
- **Neutro da soma:** $a + 0 = (a_i +_i 0_i)_{i \in I} = (a_i)_{i \in I} = a$
- **Inverso da soma:** Dado $a = (a_i)_{i \in I}$, considere $-a = (-a_i)_{i \in I}$. Então $a + (-a) = (a_i +_i (-a_i))_{i \in I} = (0_i)_{i \in I} = 0$.
- **Distributividade:** $a \cdot (b + c) = (a_i \cdot_i (b_i + c_i))_{i \in I} = (a_i \cdot_i b_i + a_i \cdot_i c_i)_{i \in I} = a \cdot b + a \cdot c$.
- **Distributividade II:** $(a + b) \cdot c = ((a_i + b_i) \cdot_i c_i)_{i \in I} = (a_i \cdot_i c_i + b_i \cdot_i c_i)_{i \in I} = a \cdot c + b \cdot c$.
- **Neutro do produto:** $a \cdot 1 = (a_i \cdot_i 1_i)_{i \in I} = (a_i)_{i \in I} = a$ e $1 \cdot a = (1_i \cdot_i a_i)_{i \in I} = (a_i)_{i \in I} = a$.

□

Definição 7.4 (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 $\pi_i : R \to R_i$ é dado por $\pi_i(a) = a_i$.

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

Lema 7.5 (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 $\pi_i : R \to R_i$ é um homomorfismo de anéis.

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

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

□

7.3 A propriedade universal do produto direto de anéis

Teorema 7.6 (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 $f_i : R_i \to S$, existe um único homomorfismo de anéis $g : p \to S$ tal que $\pi_i \circ g = f_i$ para todo $i \in I$.

$$\begin{tikzcd} & S \arrow[dl, "f_i"'] \arrow[d, dashed, "\exists! g"] \\ R_i & P \arrow[l, "\pi_i"] \end{tikzcd}$$

Além disso, tal propriedade caracteriza o produto direto. Ou seja, para quaisquer que sejam um anel P' e uma família de homomorfismos $(p_i : P' \to R_i)_{i \in I}$, se para todo anel S e toda família de homomorfismos de anéis $f_i : R_i \to S$ existir um único homomorfismo de anéis $f : P' \to S$ tal que $p_i \circ f = f_i$ para todo $i \in I$, então existe um único isomorfismo de anéis $\phi : P' \to P$ 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 $f_i : S \to R_i$ um homomorfismo de anéis. Defina $g : S \to P$ 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, $\pi_i \circ f = f_i$. Vejamos que g é homomorfismo de anéis. Dados $s, t \in S$, temos:

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

Vejamos que g é único. Se $\bar{g} : R \to S$ 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 $(p_i : P' \to R_i)_{i \in I}$ são como no enunciado.

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

$$\begin{tikzcd} & P' \arrow[dl, "p_i"'] \arrow[d, dashed, "\exists! \phi"] \\ R_i & P \arrow[l, "\pi_i"] \end{tikzcd}$$

Nosso objetivo é mostrar que ϕ 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 $\psi : P' \to P$ tal que $p_i \circ \psi = p_i$ para todo $i \in I$.

$$\begin{tikzcd} & P \arrow[dl, "\pi_i"'] \arrow[d, dashed, "\exists!\psi"] \\ R_i & P' \arrow[l, "p_i"] \end{tikzcd}$$

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

$$\begin{tikzcd} & P' \arrow[dl, "p_i"'] \arrow[d, "\psi\circ\phi"', "\mathrm{id}_{P'}"] \\ R_i & P' \arrow[l, "p_i"] \end{tikzcd}$$

Pois para todo $i \in I$, $p_i \circ \mathrm{id}_{P'} = p_i$ 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 $\psi \circ \phi = \mathrm{id}_{P'}$.

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

$$\begin{tikzcd} & P \arrow[dl, "\pi_i"'] \arrow[d, "\phi\circ\psi"', "\mathrm{id}_{P}"] \\ R_i & P \arrow[l, "\pi_i"] \end{tikzcd}$$

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

Assim, ψ e ϕ são isomorfismos inversos. Em particular, ϕ é isomorfismo, o que completa a prova. □

7.4 Exercícios

Exercício 7.1. Sejam A, B anéis. Prove diretamente que o produto direto $A \times B$ é um anel. A seguir, prova que as projeções $\pi_1 : A \times B \to A$ e $\pi_2 : A \times B \to B$ dadas por $\pi_1(a, b) = a$ e $\pi_2(a, b) = b$ são homomorfismos de anéis.

Exercício 7.2. Na notação do exercício anterior, prove diretamente que $A \times S$, com as projeções (π_1, π_2) satisfazem a propriedade universal do produto direto, ou seja, mostre que:

Para cada anel S e cada par de homomorfismos de anéis $h_1 : S \to A$ e $h_2 : S \to B$, existe um único homomorfismo de anéis $g : S \to A \times B$ tal que $\pi_1 \circ g = f_1$ e $\pi_2 \circ g = f_2$.

Exercício 7.3. Decida quais dos seguintes conjuntos sao subaneis do anel produto $\mathbb{R}^{[0,1]}$, onde $[0, 1]$ é o intervalo fechado dos números reais entre 0 e 1.

a) O conjunto de todas as funções $f : [0, 1] \to \mathbb{R}$ tais que $f(q) = 0$ para todo $q \in [0, 1]$.

b) O conjunto de todas as funções polinomiais $f : [0, 1] \to \mathbb{R}$.

c) O conjunto de todas as funções $f : [0,1] \to \mathbb{R}$ que possuem apenas um número finito de zeros, juntamente com a função zero.

d) O conjunto de todas as funções $f : [0,1] \to \mathbb{R}$ que possuem um número infinito de zeros.

e) O conjunto de todas as funções $f : [0,1] \to \mathbb{R}$ tais que $\lim_{x\to 1} f(x) = 0$.

f) O conjunto de todas as combinações lineares racionais das funções $\sin(nx)$ e $\cos(mx)$, onde m, n são inteiros não negativos.

g) O conjunto de todas as funções $f : [0,1] \to \mathbb{R}$ tais que $f(q) = 0$ para todo $q \in [0,1]$ e $f(0) = 1$.

Exercício 7.4. Seja C o anel das funções de $\mathbb{R}$ em $\mathbb{R}$ com a estrutura de anel produto. Demonstre que C não é um domínio.

Exercício 7.5. Seja C o anel das funções $f : \mathbb{R} \to \mathbb{R}$ com a soma e multiplicação usuais de funções. Para cada $r \in \mathbb{R}$, seja $M(r)$ o subconjunto de C dado por:

$$M(r) = \{f \in C : f(r) = 0\}.$$

a) Demonstre que $M(r)$ é um ideal maximal.

b) Dê um exemplo de um ideal próprio e não nulo de C que não seja maximal.

Capítulo 8

Divisibilidade em anéis

Neste capítulo, estudaremos a noção de divisibilidade em anéis. Tal noção é uma generalização da noção de divisibilidade em $\mathbb{Z}$.

Trataremos de divisibilidade apenas em anéis comutativos.

8.1 Definição de divisibilidade

Definição 8.1. Seja R um anel comutativo. Definimos a relação de divisibilidade, $|$, em R, como se segue:

Para $a, b \in R$, dizemos que $a|b$ (a divide b) se existe $c \in R$ tal que $b = ac$. □

Algumas propriedades básicas:

Proposição 8.2. Seja R um anel comutativo. Então a relação de divisibilidade $|$ em R é uma pré-ordem, ou seja, é reflexiva e transitiva. Além disso, 1 é elemento mínimo, e 0, elemento máximo

Demonstração. Sejam $a, b, c \in R$. Temos que $a|a$, pois $a = 1 \cdot a$.

Se $a|b$ e $b|c$, existem $e, f \in R$ tais que $b = ae$ e $c = bf$. Logo, $c = bf = aef = a(ef)$, o que implica em que $a|c$.

Temos que 0 é elemento máximo, já que para todo $a \in R$, $0 = 0a$. Por outro lado, 1 é elemento mínimo, já que para todo $a \in R$, $a = 1a$. □

Note que $a|0$ não implica, pelas nossas definições, que a é divisor de zero, uma vez que necessitaríamos da existência de $b \in R$ não nulo tal que $ab = 0$. Divisores de zero geram diversas patologias na teoria da divisibilidade, e estas não serão objeto primário de nosso estudo.

Assim, nos restringiremos aos anéis comutativos que não possuem divisores de zero, ou seja, aos domínios de integridade. Note que, nesses domínios, se $b \neq 0$ e $b|a$, então existe um *único* $c \in R$ tal que $a = bc$. Este elemento c é, muitas vezes, chamado de quociente de a por b.

Proposição 8.3. Seja R um anel domínio de integridade. Se $a, b \in R$, são equivalentes:

1. $a|b$ e $b|a$.
2. Existe $u \in R$ invertível tal que $a = ub$.

Demonstração. Primeiro, suponha que $a|b$ e $b|a$. Temos que existem c, d com $a = cb$ e $b = da$. Substituindo, temos que $b = dcb$. Cancelando, $1 = dc$. Assim, c é invertível.

Reciprocamente, como u é invertível, $a = ub$ e $u^{-1}a = b$, logo, $a|b$ e $b|a$. □

Com isso, definimos:

Definição 8.4. Seja R um anel comutativo. Dizemos que elementos $a, b \in R$ são associados se existe $u \in R$ invertível tal que $a = ub$. $\square$

A relação de ser associado é uma relação de equivalência:

Lema 8.5. Seja R um anel comutativo. A relação de ser associado é uma relação de equivalência em R.

Demonstração. Seja $a, b, c \in R$.

- Reflexividade: a é associado a si mesmo, pois $a = 1 \cdot a$ e $1 \in R^*$.
- Simetria: Se a é associado a b, então existe u invertível tal que $a = ub$. Logo, $b = u^{-1}a$, e, portanto, b é associado a a.
- Transitividade: Se a é associado a b e b é associado a c, então existem u, v invertíveis tais que $a = ub$ e $b = vc$. Logo, temos que $a = uvc$, e, portanto, a é associado a c, já que $uv \in R^*$.

$\square$

A relação de divisibilidade tem ligações com propriedades de ideais. Enunciaremos a primeira delas a seguir:

Proposição 8.6. Seja R um anel comutativo e $a, b \in R$. São equivalentes:

a) $a|b$.

b) $b \in \langle a \rangle$.

c) $\langle b \rangle \subseteq \langle a \rangle$.

Demonstração. Primeiro, suponha que $a|b$. Então existe $c \in R$ tal que $b = ac$. Como $\langle a = \{ac : c \in R\}$, segue b).

Agora suponha que $b \in \langle a \rangle$. Como $\langle b \rangle$ é o menor ideal que contém b e $\langle a \rangle$ é um ideal que contém b, segue que $\langle b \rangle \subseteq \langle a \rangle$.

Agora suponha que $\langle b \rangle \subseteq \langle a \rangle$. Em particular, $b \in \langle a \rangle$. Pela definição de $\langle a \rangle$, existe $c \in R$ tal que $b = ac$, e, assim, $a|b$. $\square$

8.2 Elementos primos e irredutíveis

Os números inteiros possuem uma classe muito importante de números: a dos primos. As definições abaixo generalizam a noção de primo.

Proposição 8.7 (Elementos primos)**.** Seja R um anel comutativo Dizemos que $p \in R$ é um elemento primo se $p \notin R^*$, $P \neq 0$, e, para todos $a, b \in R$, se $p|ab$, então $p|a$ ou $p|b$.

Proposição 8.8 (Elementos irredutíveis)**.** Seja R um anel comutativo. Dizemos que $p \in R$ é um elemento irredutível se $p \notin R^*$, $p \neq 0$, e, para todos $a, b \in R$, se $p = ab$, então $a \in R^*$ ou $b \in R^*$.

Elementos primos se relacionam com ideais primos, como vemos a seguir:

Proposição 8.9. Seja R um anel comutativo e $p \neq 0$. Então, p é primo se, e somente se $\langle p \rangle$ é um ideal primo.

Demonstração. Primeiro, suponha que p é primo. Segue que $\langle p \rangle = \{ap : a \in R\}$ não é 0, pois $p \in R$, e não é R, pois $p \notin R^*$. Agora, seja $a, b \in R$ tais que $ab \in \langle p \rangle$. Então $p|ab$. Logo, $p|a$ ou $p|b$, o que implica que $a \in \langle p \rangle$ ou $b \in \langle p \rangle$.

Reciprocamente, suponha que $\langle p \rangle$ é um ideal primo. Veremos que p é primo. Temos que $p \neq 0$ e p não é invertível (pois $\langle p \rangle \neq R$). Agora, seja $a, b \in R$ tais que $p|ab$. Logo, $ab \in \langle p \rangle$. Como $\langle p \rangle$ é primo, temos que $a \in \langle p \rangle$ ou $b \in \langle p \rangle$. Logo, $p|a$ ou $p|b$. □

A seguinte proposição relaciona primos e irredutíveis em domínios de integridade.

Proposição 8.10. Seja R um domínio de integridade Então, se $p \in R$ é primo, então p é irredutível.

Demonstração. Seja $p \in R$ primo. Para ver que p é irredutível, fixe $a, b \in R$ e suponha que $p = ab$.

Como $ab = p$, temos que $p|ab$. Logo, $p|a$ ou $p|b$. Supondo $p|a$, temos que $a = pc$ para algum $c \in R$. Logo, $p = pcb$, e, portanto, $1 = cb$, o que mostra que $b \in R^*$.

O caso em que $p|b$ é análogo. □

A recíproca vale em domínios de ideais principais.

Proposição 8.11. Seja R um domínio de ideais principais Então, se $p \in R$ é irredutível, p é primo.

Demonstração. Seja $p \in R$ irredutível. Veremos que $\langle p \rangle$ é primo. Para tanto, basta ver que $\langle p \rangle$ é maximal. Sabemos que esse ideal não é R. Suponha que existe $a \in R$ é tal que $\langle p \rangle \subseteq \langle a \rangle$.

Então $p = ab$ para algum $b \in R$. Como p é irredutível, temos que $a \in R^*$ ou $b \in R^*$. Se $a \in R^*$, então $\langle a \rangle = R$. Se $b \in R^*$, então $a = p \cdot b^{-1} \in \langle p \rangle$, e, portanto, $\langle p \rangle = \langle a \rangle$. □

Lema 8.12. Seja R um domínio de integridade e p um elemento irredutível.

Se $q \in R$ é associado à p, então q é irredutível.

Demonstração. Seja u invertível tal que $q = pu$.

Se $a, b \in R$ tão tais que $q = ab$, então $pu = ab$. Então, $p = (u^{-1}a)b$. Assim, $u^{-1}a$ é invertível ou b é invertível. Se b é invertível, segue a tese. Se $u^{-1}a = v$ é invertível, então $a = uv$ também é, e segue a tese. □

8.3 Domínios Euclideanos

O anel dos números inteiros possui uma propriedade muito importante: dado $n \in \mathbb{Z}$ e $d > 0$, existem únicos n, r tais que $0 \leq r < d$ e $a = nd + r$.

A noção de domínio Euclideano generaliza os anéis que possuem essa propriedade.

Definição 8.13. Um domínio de integridade R é um domínio Euclideano se existe uma função $\nu : R \setminus \{0\} \to \mathbb{N} = \{0, 1, \dots\}$ satisfazendo:

- Para todos $a, b \in R$ com $b \neq 0$, existem $q, r \in R$ com $a = bq + r$ e ($r = 0$ ou $\nu(r) < \nu(b)$).
- Para todos $a, b \in R \setminus \{0\}$, $\nu(ab) \geq \nu(a)$.

Tal função ν é chamada de valoração, ou grau. □

Um primeiro resultado simples:

Definição 8.14. Seja R um domínio Euclideano e ν uma função de valoração. Então se $a, b \in R$ são associados, temos $\nu(a) = \nu(b)$. □

Demonstração. Se a e b são associados, existe $u \in R^*$ tal que $a = ub$. Logo, $\nu(a) = \nu(ub) \geq \nu(b)$ e $\nu(b) = \nu(u^{-1}a) \geq \nu(a)$. Assim, $\nu(a) = \nu(b)$. □

Exemplo 8.15. O anel dos inteiros $\mathbb{Z}$ é um domínio Euclideano, com $\nu(n) = |n|$ para $n \neq 0$. Primeiro, é claro que se $a, b \in \mathbb{Z}$ são não nulos, então $|ab| = |a||b| \geq |a|1 = |a|$.

Agora, sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Sabemos que existem $q, r \in \mathbb{Z}$ tais que $a = q|b| + r$ e $0 \leq r < |b|$. Se $b > 0$, isso conclui a prova. Se $b < 0$, então $a = (-q)b + r$, e isso conclui a prova. □

Exemplo 8.16. No geral, não podemos exigir a unicidade de q, r. De fato, em $\mathbb{Z}$, considere $a = 3$, $b = 2$. Então $3 = 1 \cdot 2 + 1$ com $|1| < |2|$, mas também $3 = 2 \cdot 2 + (-1)$ com $|-1| < |2|$. □

Porém, temos o resultado a seguir. Mais adiante, veremos que esse será o caso para anéis de polinômios sobre corpos munidos da função grau.

Proposição 8.17. Seja R um domínio Euclideano e ν uma função de valoração tal que para todos $a, b \in R$ com $a, b, a + b \neq 0$, temos $\nu(a + b) \leq \max(\nu(a), \nu(b))$.

Então para todos $a, b \in R$ com $b \neq 0$, existem únicos $q, r \in R$ tais que $a = bq + r$ e ($r = 0$ ou $\nu(r) < \nu(b)$).

Demonstração. A existência de q, r como acima vem da definição de domínios Euclideanos. Adicionalmente, sejam $q', r' \in R$ tais que $a = bq' + r'$ e $r' = 0$ ou $\nu(r') < \nu(b)$.

Temos que $q'b + r' = qb + r$. Se $r = r'$, segue que $q = q'$. Similarmente, se $q = q'$, segue que $r = r'$. Portanto, vamos supor por absurdo que $r \neq r'$ e $q \neq q'$. Assim, $r' - r = (q - q')b + (r - r')$.

Se $r = 0$, temos que $\nu(r') < \nu(b) \leq \nu((q - q')b) = \nu(r)$, o que é absurdo.

Se $r' = 0$, temos que $\nu(-r) = \nu(r) < \nu(b) \leq (\nu(q - q')b) = \nu(r)$, o que é absurdo.

Se $r, r' \neq 0$, temos que $\nu(r' - r) \leq \max(\nu(r), \nu(r')) < \nu(b) \leq (\nu(q - q')b) = \nu(r)$, o que é absurdo. □

Proposição 8.18. Todo corpo é um domínio Euclideano.

Demonstração. Seja K um corpo e considere $\nu : K \setminus \{0\} \to N$ dada por $\nu(x) = 1$ para todo $x \in K \setminus \{0\}$.

Então, para $a, b \in K \setminus \{0\}$, temos que $\nu(ab) = 1 = \nu(a)$, e, dados $a, b \in K$ com $b \neq 0$, temos que $a = (ab^{-1})b + 0$. □

O resultado abaixo generaliza o que também já sabemos sobre $\mathbb{Z}$.

Proposição 8.19. Todo domínio Euclideano é um domínio de ideais principais.

Demonstração. Seja R um domínio Euclideano com valoração ν e I um ideal em R.

Se $I = \{0\}$, então I é gerado por 0.

Se $I \neq \{0\}$, então existe $b \in I$ tal que $\nu(b)$ é mínimo. Afirmamos que $I = \langle b \rangle$. É claro que $\langle b \rangle \subseteq I$, restando verificar que $I \subseteq \langle b \rangle$. De fato, tome $a \in I$. Existem $q, r \in R$ tais que $a = bq + r$ e $r = 0$ ou $\nu(r) < \nu(b)$. Se $r \neq 0$, temos que $\nu(r) < \nu(b)$, o que nos dá um absurdo, uma vez que $r = a - bq \in I$ e b é o elemento de menor valoração em I. Assim, $r = 0$, e, portanto, $a = bq \in \langle b \rangle$. □

8.4 Domínios de Fatoração Única

Domínios de Fatoração Única, também conhecidos como Domínios Fatoriais, ou Anéis Fatoriais, são domínios de integridade que capturam outra propriedade dos números inteiros: a do Teorema Fundamental da Aritmética.

Definição 8.20. Um Domínio de Fatoração Única (DFU) é um domínio de integridade R tal que para todo $a \in R \setminus \{0\}$ não invertível, existem um inteiro $n \geq 1$, irredutíveis $p_1, \ldots, p_n$ e $u \in R^*$ tais que $a = up_1 \cdots p_n$ e que, além disso, para quaisquer inteiros $m \geq 1$ e irredutíveis $q_1, \ldots, q_m$ para os quais existam u' tal que $a = u'q_1 \cdots q_m$, segue que $n = m$ e que existe uma permutação $\sigma : \{1 \ldots, n\} \to \{1, \ldots, n\}$ tal que p_i é associado a $q_{\sigma(i)}$ para todo $i = 1, \ldots, n$.

□

Pelo Teorema Fundamental da Aritmética, sabemos que $\mathbb{Z}$ é um DFU.
Mais geralmente:

Teorema 8.21. Todo domínio de ideais principais é um DFU.

Para provar esse teorema, precisaremos de alguns lemas.
Primeiro, precisaremos:

Lema 8.22. Seja R um domínio de ideais principais e $a \in R \setminus \{0\}$ não invertível. Então existe um elemento irredutível $p \in R$ tal que $p|a$.

Demonstração. Fique $a \in R$ como no enunciado e suponha por absurdo que a tese é falsa. Recursivamente, construiremos uma sequência $(p_n : n \in \mathbb{N})$ de elementos de $\mathbb{R}$ satisfazendo:

a) $p_0 = a$.

b) $p_n|p$ para todo $n \in \mathbb{N}$

c) $\langle p_n \rangle \neq R$.

d) $\langle p_n \rangle \subsetneq \langle p_{n+1} \rangle$.

O que nos dará um absurdo, por d).

Para ver que tal sequência existe, seja $p_0 = a$. Como a não é invertível, $\langle p_n \rangle \neq R$, e $p_0|a$.

Para o passo sucessor da recursão, construído p_n, como $\langle p_n \rangle \neq R$, sabemos que p_n não é invertível. Além disso, $0 \neq p_n$ pois $p_n|a$. Pelo mesmo motivo, p_n não é irredutível. Logo, existem $b, c \in R$ tais que $p_n = bc$ e nem b, nem c são invertíveis. Seja $p_{n+1} = b$.

Como $p_{n+1}|p_n$ e $p_n|p$, segue que $p_{n+1}|p$, Como b não é invertível, $\langle p_{n+1} \rangle \neq R$.

Como $p_{n+1}|p_n$, temos que $\langle p_n \rangle \subseteq \langle p_{n+1} \rangle$. Porém, a inclusão é própria, caso contrário, teríamos $p_{n+1} \in \langle p_n \rangle$, o que nos dá $p_n|p_{n+1}$. Assim, existe d tal que $b = dp_n$. Logo, $p_n = bc = dp_nc$. Cancelando $p_n \neq 0$, temos que $1 = dc$, o que nos dá um absurdo, pois c não é invertível. □

Lema 8.23. Seja R um domínio de ideais principais e $a \in R \setminus \{0\}$ não invertível. Então existem $p_1, \ldots, p_n$ irredutíveis tais que $a = p_1 \cdots p_n$.

Demonstração. Suponha que não. Em particular, a não é irredutível. Recursivamente, tomamos $(p_n : n \in \mathbb{N})$ e $(a_n : n \in \mathbb{N})$, com $a_n \in R$ satisfazendo:

a) $a = (p_0 \cdots p_n)a_n$.

b) $a_n = a_{n+1}p_{n+1}$.

c) Cada p_n é irredutível.

Para ver que isso é possível, como a é não nulo, não invertível e não irredutível, existe um irredutível p_0 tal que $a = p_0 a_0$.

Para o passo indutivo, como $a \neq 0$ não é um produto de irredutíveis, a_n não é invertível (pois $p_n a_n$ seria também irredutível) e não nulo. Logo, existem p_{n+1} e a_{n+1} tais que $a_n = p_{n+1}a_{n+1}$ com p_{n+1} irredutível.

Isso completa a construção. Assim, $a_{n+1}|a_n$, mas $a_n \neq a_{n+1}$, ou teríamos que existe b tal que $a_{n+1} = ba_n$, e, substituindo, seguiria que $a_n = a_n b p_{n+1}$, o que nos dá p_{n+1} é invertível, um absurdo.

Portanto, segue que para todo n, $\langle a_n \rangle \subsetneq \langle a_{n+1} \rangle$, uma contradição. □

Corolário 8.24. Seja R um domínio de ideais principais e $a \in R \setminus \{0\}$ não invertível. Então existem $p_1, \ldots, p_n$ primos tais que $a = p_1 \cdots p_n$.

Proposição 8.25. Seja R um domínio de integridade. Então todo elemento irredutível é primo.

Demonstração. Seja $r \in R$ irredutível. Suponha que $r|ab$, onde $a, b \in R$. Logo, $ab = rc$ para algum $c \in R$.

Se $a = 0$ ou $b = 0$, segue que $r|a$ ou $r|b$, respectivamente.

Se a é invertível ou b é invertível, também segue, respectivamente, que $r|b$ ou $r|a$.

Caso contrário, temos $c \neq 0$. Escreva $a = a_1 \cdots a_n$ e $b = b_1 \cdots b_m$ ecom $a_1, \cdots, a_n$, $b_1, \cdots, b_m$ irredutíveis. Temos que $a_1 \cdots a_n b_1 \cdots b_m = rc$. Se c é invertível, temos da unicidade dos DFU's que r é associado a algum a_i ou b_j, e, portanto, $r|a$ ou $r|b$.

Se c não é invertível, escreva $c = c_1 \cdots c_k$ com $c_1, \ldots, c_k$ irredutíveis. Novamente, pela unicidade dos DFU's, temos que r é associado a algum a_i ou b_j, e, portanto, $r|a$ ou $r|b$. □

Lema 8.26. Seja R um domínio de integridade. Se $r \in R$ é irredutível e r se escreve como um produto de primos, então r é primo.

Demonstração. Suponha que $r = p_1 \cdots p_n$ com $p_1, \ldots, p_n$ primos. Procedemos por indução em n.

Para $n = 1$ é trivial. Para o passo indutivo, se $r = p_1 \cdots p_n p_{n+1}$, então $p_1 \cdots p_n$ é invertível ou p_{n+1} é invertível. Temos que p_{n+1} não é invertível, logo, $p_1 \cdots p_n$ é invertível, e, portanto, r é associado ao primo p_{n+1}, e, portanto, é primo. □

Proposição 8.27. Seja R um domínio de integridade. São equivalentes:

a) R é um domínio de domínio de fatoração única.

b) Para todo $a \in R \setminus \{0\}$ não invertível, existem $p_1, \ldots, p_n$ primos tais que $a = p_1 \cdots p_n$.

8.5 Mínimo múltiplo comum e Máximo divisor comum

Definição 8.28. Seja R um anel comutativo e $a, b \in R$ não nulos.

Um mínimo múltiplo comum de a e b é, se existe, um elemento $m \in R$ tal que:

- $a|m$ e $b|m$.
- Se $c \in R$ é tal que $a|c$ e $b|c$, então $m|c$.

Um máximo divisor comum de a e b é, se existe, um elemento $d \in R$ tal que:

- $d|a$ e $d|b$.
- Se $c \in R$ é tal que $c|a$ e $c|b$, então $c|d$.

□

Lema 8.29. Seja R um domínio de integridade e $a \in R$ não nulo.

Sejam $a, b \in R$. Então todos os mínimos múltiplos comuns de a e b são associados entre si, e todos os máximos divisores comuns de a e b são associados entre si (caso existam).

Demonstração. Sejam d, d' máximos divisores comuns de a e b. Então, $d|a$ e $d|b$, $d'|a$ e $d'|b$. Logo, $d|d'$ e $d'|d$. Logo, d e d' são associados entre si.

Similarmente, sejam m, m' mínimos múltiplos comuns de a e b. Então, $m|a$ e $m|b$, $m'|a$ e $m'|b$. Logo, $m|m'$ e $m'|m$. Logo, m e m' são associados entre si. □

8.6 Exercícios

Exercício 8.1. Prove, com suas próprias palavras e de modo que considere satisfatório, que a relação de ser associado, em um anel comutativo, é uma relação de equivalência.

Exercício 8.2. Seja D um domínio de integridade e $a, b \in R$ não nulos. Redija com suas palavras, de forma que considere satisfatória, uma demonstração para o fato de que quaisquer dois mínimos múltiplos comuns de a e b são associados entre si, e que quaisquer dois máximos divisores comuns de a e b são associados entre si, caso existam.

Exercício 8.3. Seja R um domínio Euclideano munido de função grau ν e $a \in R$ não nulo. Seja m o menor valor assumido por ν. Prove que a é invertível se, e somente se $\nu(a) = m$.