Notas da disciplina MAT0264 - Anéis e Corpos

Prof. Vinicius Rodrigues

17 de junho de 2025
v0.3.5

Licença

Sumário

Agradecimentos

O autor agradece às seguintes pessoas que contribuíram com a elaboração deste material:

- **Gabriel Alves Andretta** – Aluno do Bacharelado em Matemática do IME-USP. Foi monitor da disciplina "Anéis e Corpos" em 2025 e avisou sobre erros de digitação no texto.
- **Matheus Engelberg Teixeira da Silva Ulian** – Aluno do Bacharelado em Matemática do IME-USP. Apontou diversos erros de digitação no texto.
- **Renan Ribeiro Marcelino** – Aluno do Bacharelado em Ciência da Computação IME-USP. Colaborou com algumas correções de erros de digitação no texto a partir do GitHub.
- **Ugo Bruzzo** – Professor do Departamento de Matemática do IME-USP. Lecionou o primeiro terço dessa disciplina em 2025, e indicou uma porção considerável dos exercícios aqui expostos.

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 construções de todos os outros anéis relevantes, porém alguns outros anéis importantes e conhecidos, como $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, com o qual se espera que o estudante já possua alguma familiaridade, serão utilizados em exemplos desde seu início, mesmo antes 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.

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 capítulo desenvolver formalmente os princípios da teoria dos conjuntos, mas apenas estabelecer convenções notacionais e fixar algumas definições que serão utilizadas ao longo do texto. Assume-se familiaridade do leitor com funções e com manipulação de conjuntos ao nível básico. Um curso de pré-cálculo ou um curso básico de álgebra linear apresentam conhecimentos mais do que suficientes para acompanhar a leitura deste texto.

1.1 Pares ordenados

Um par ordenado é um conjunto especial constituído a partir de dois outros conjuntos, a, b, e denotado por (a, b). Sua principal propriedade é que a, b são pares ordenados, vale que $(a, b) = (c, d)$ se, e somente se $a = c$ e $b = d$.

Formalmente, em Teoria dos Conjuntos, um par ordenado é definido como qualquer conjunto que possui esta propriedade. Um modo popular de o fazer é através do chamado par de Kuratowski, que define o par ordenado (a, b) como o conjunto $\{\{a\}, \{a, b\}\}$. Definindo-se o par ordenado dessa forma, fica a cargo do leitor interessado verificar que $(a, b) = (c, d)$ se, e somente se $a = c$ e $b = d$.

A definição de Kuratowski pode parecer estranha, ou anti-natural, mas satisfaz o que se espera de um par ordenado. Por isso mesmo, não é desejável que teoremas sobre Álgebra dependam dela. E não dependerão. Tudo que será utilizado ao longo de todo o texto é a propriedade mencionada no parágrafo anterior.

Se x é um par ordenado, existem únicos a, b tais que $x = (a, b)$. Tais a, b são chamados de *primeira coordenada* e {segunda coordenada}, respectivamente, e, em alguns contextos, será conveniente denotá-los por $\pi_1(x)$ e $\pi_2(x)$.

1.2 Famílias e produtos cartesianos

Funções são objetos matemáticos normalmente pensados como entes $f : X \to Y$ que recebem uma entrada x, em um conjunto de possíveis entradas $x \in X$ e devolvem uma saída $f(x) \in Y$. O conjunto X é chamado de *domínio* de f, e denotado por $\operatorname{dom} f$. O conjunto de todos os valores assumidos por f é a *imagem* de f, e denotado por $\operatorname{im}(f) = \{f(x) : x \in X\}$. Um conjunto que contém a imagem é chamado de um *contradomínio* de f. Na notação $f : X \to Y$, estamos

dizendo que Y é um contradomínio de f, de modo que $\mathrm{im}(f) \subseteq Y$. Note que o contradomínio de uma função não é único: por exemplo, considerando que o conjunto dos números complexos, $\mathbb{C}$, possui uma cópia do conjunto dos números reais, $\mathbb{R}$, dentro de si, a função $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2$ tem como contradomínios tanto $\mathbb{R}$ como $\mathbb{C}$ Formalmente, a função propriamente dita costuma ser definida como o conjunto dos pares ordenados $\{(x, f(x)) : x \in X\}$, mas tais detalhes serão de pouca relevância nesse texto.

Muitas vezes, em Matemática, pensamos no conceito de função com o intuito de representar um conjunto de valores indexados, em que a ideia de "dispositivo de entrada/saída" muito presente, por exemplo, em Cálculo Diferencial em integral perde importância. Uma dessas ocasiões é no tratamento de sequências. Formalmente, sequências são funções cujo domínio é o conjunto dos números naturais, mas, em muitos contextos, pensa-se em sequências como uma coleção de objetos enumerados, e não como um dispositivo de entrada/saída.

Nesses contextos, é muito usual trocar a terminologia usual utilizada para tratar funções por outra terminologia, em que a função, mesmo sendo o mesmo objeto matemático que no outro contexto, passa a ser chamada de *família*.

Uma família $a = (a_i : i \in I) = (a_i)_{i \in I}$ é uma função cujo domínio é I. Nessa notação, pensamos em i como sendo uma variável muda, como ocorre com o símbolo x nos parágrafos anteriores. I, que é o domínio da função, costuma ser chamado de conjuntos de índices. A notação não deixa explícito um contradomínio, como ocorre ao escrever $f : X \to Y$. Quando se torna relevante, costumamos escrever sentenças como "a família $(a_i)_{i \in I}$ assume valores em Y", ou, simplesmente, "$(a_i)_{i \in I}$ é uma família em Y". Já a_i é o elemento $a(i)$.

Nesse texto, consideraremos que $(a_i : i \in I)$ e $((i, a(i)) : i \in I)$ são o mesmo objeto matemático, não havendo qualquer distinção formal entre eles. A distinção é meramente notacional, e pode ser intercambiada a qualquer momento sem nenhuma perda de formalismo matemático.

No quadro abaixo, apresentamos uma comparação entre as duas notações. Enfatizamos novamente que, matematicamente, 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	$\mathrm{im}\, u$	$\{u_i : i \in I\}$
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 1.2.1 (Sequências)**.** Uma sequência é uma família cujo conjunto de índices é $\mathbb{N}$. Compare a intuição que passa as notações:

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

□

Exemplo 1.2.2 (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 1.2.3 (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 1.2.4 (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 1.2.5 (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:

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

1.3 Operações

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

Definição 1.3.1 (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

Grupos são estruturas matemáticas munidas de uma operação binária com algumas propriedades especiais. O principal objetivo deste texto é servir como texto para um estudo introdutório sobre anéis e corpos, que são estruturas matemáticas que possuem duas operações binárias com propriedades especiais. Conforme veremos no Capítulo 3, todo anel e todo corpo, com uma dessas operações, forma um grupo. Assim, é útil, para o estudo de anéis e corpos, o conhecimento de noções básicas sobre grupos.

Apesar das noções de anel e de corpo serem, ao nível de definição, noções mais complexas que a de grupo, a noção de grupo, em parte por ser menos restritiva, necessita o desenvolvimento de ferramentas específicas para seu estudo completo. A área do conhecimento matemático resultante do desenvolvimento dessa teoria é extremamente rica, e chamada de *Teoria dos Grupos*. Nosso objetivo, por outro lado, é focar no estudo inicial das teorias de anéis e corpos, e, portanto, não mergulharemos nesta importante área.

Assim, não é objetivo deste capítulo apresentar uma introdução ao estudo de grupos, mas sim apenas introduzir as noções e resultados básicos próprios de grupos que são estritamente necessários para os resultados envolvendo anéis e corpos descritos no restante do texto.

Definição 2.1.1. Um grupo é uma quádrupla $(G, \cdot, e)$, 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 comumente, *Abeliano*:

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

Caso valham apenas as propriedades associativas e do elemento neutro, dizemos que $(G, \cdot, e)$ é um *monoide*. Caso valha, adicionalmente, a propriedade comutativa, dizemos que $(G, \cdot, e)$ é um *monoide comutativo*. □

Alguns exemplos:

Exemplo 2.1.2. Abaixo, exemplificamos alguns grupos importantes.

a) Com a soma usual e 0, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ são grupos Abelianos.

b) 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.

c) 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.

d) Se X é um conjunto qualquer, o conjunto das bijeções de X em X é, com a composição usual de funções e a identidade, um grupo, cuja operação inversa é a inversão usual de funções. Tal grupo é denominado *grupo de permutações de* X.

   Caso X tenha ao menos 3 elementos, ele não é abeliano: sendo a, b, c três elementos distintos de X, sendo f a função que permuta a, b e fixa os demais elementos, g a que permuta b, c temos que $f \circ g(a) = f(a) = b$, mas $g \circ f(a) = g(b) = c$, logo, $f \circ g \neq g \circ f$.

□

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

- ao discursar sobre grupos e monoides, é comum omitir a operação e o elemento neutro, referindo-se apenas ao conjunto G, conforme fizemos acima ao mencionar que $\mathbb{Z}$ é um grupo. O mais formal, porém muito menos usual, feito principalmente em situações em há chance de confusão, é escrever que, por exemplo, $(\mathbb{Z}, +, 0)$ é um grupo.

- Como também ocorre com $\mathbb{Z}$, caso o grupo ou monoide 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 ou monoide em discurso não seja necessariamente 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.

  Porém, há grupos Abelianos cujas operações também são denotadas por $\cdot$, como no caso o grupo $\mathbb{T}$ mencionado acima.

Agora iniciaremos a provar algumas propriedades básicas sobre grupos.

Proposição 2.1.3 (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 2.1.4 (Unicidade dos inversos)**.** Seja $(G, \cdot, e)$ um grupo. Então todo $a \in G$ possui um único elemento inverso. 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, que $a \cdot b = b \cdot a = e$ e $a \cdot c = c \cdot a = e$. Segue que:

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

□

A unicidade 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 2.1.5 (Cancelamento)**.** Seja $(G, \cdot, e)$ um grupo e $a, b, c \in G$. Se $a \cdot b = a \cdot c$, 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 $ba = ca$. Segue que $(ba)a^{-1} = (ca)a^{-1}$.

Pela propriedade associativa, $b(aa^{-1}) = c(aa^{-1})$.

Pela definição de inverso, segue que $be = ce$.

Finalmente, pela neutralidade de e, segue que $b = c$. □

Corolário 2.1.6 (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, $b = e$. Para a segunda afirmação, note que $ba = ea$, logo, pela proposição anterior, $b = e$. □

Proposição 2.1.7 (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, não sendo nosso objetivo fornecer ao leitor um primeiro contato. Aqui apresentaremos a notação e as técnicas de "substituição de variáveis" que serão utilizadas.

Definição 2.2.1 (Soma de família finita)**.** Seja $G = (G, +, 0)$ um monoide comutativo. 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, 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 2.2.2. Qualquer que seja 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. Para o passo indutivo, 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:

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

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

□

A partir dessa generalidade, pode-se chegar na notação mais utilizada envolvendo somatórios: se $n \leq m$ e $I = \{n, \ldots, m\}$, escrevemos:

$$\sum_{i=n}^{m} a_i = \sum_{i\in I} a_i.$$

Como fazemos no cálculo de integrais, muitas vezes é desejável utilizar técnicas de substituição de variáveis para calcular ou simplificar somatórios. A proposição abaixo formaliza esta técnica.

Proposição 2.2.3 (Mudança de variável em somatório)**.** Seja G um monoide comutativo. 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:

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

□

Também podemos juntar, sempre que necessário, duas somas disjuntas sob um único sinal de somatório.

Proposição 2.2.4 (Concatenação de somatórios)**.** Seja I, J conjuntos disjuntos e G um monoide comutativo. Considere famílias $(a_i : i \in I)$ e $(a_i : i \in J)$, e a família $(a_i : i \in I \cup J)$. Vale a relação:

$$\sum_{i \in I} a_i + \sum_{i \in I} a_i = \sum_{i \in I \cup J} a_i$$

Demonstração. Provaremos por indução no tamanho de J. Se $J = \emptyset$, temos $I \cup J = J$ e $\sum_{i \in J} a_i = 0$, logo, segue a tese.

Se a proposição vale para todo J de tamanho n, suponha que $|J| = n+1$ e seja $J' = J \setminus \{j'\}$, onde $j' \in J$ é qualquer elemento arbitrário.

Então:

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

□

Antes de enunciar a próxima proposição, precisamos falar sobre notações de índices duplos. Se K é um conjunto que consiste apenas em pares ordenados (i, j), não é incomum encontrarmos na literatura a notação $\sum_{(i,j) \in K} a_{ij}$, bem como encontrar a notação $(a_{ij} : (i, j) \in K)$.

Tais notações são usadas no contexto no qual uma para todo i, j com $(i, j) \in K$, está definido um elemento a_{ij}. Para se encaixar no nosso formalismo, $(a_{ij} : i, j \in K)$ denota $(a_{\pi_1(k)\pi_2(k)} : k \in K)$, e $\sum_{(i,j) \in K} a_{ij}$ denota $\sum_{k \in K} a_{\pi_1(k)\pi_2(k)}$, onde π_1 e π_2 são as funções coordenadas de pares ordenados.

Proposição 2.2.5 (Concatenação de somatórios II)**.** Seja I um conjunto não vazio e, para cada $i \in F$, seja F_i um conjunto. Considere o conjunto finito $K = \bigcup_{i \in I} \{i\} \times F_i = \{(i, j) : i \in I, j \in F_i\}$.

Para cada $i \in I$, considere uma família de elementos de um monoide comutativo G, $(a_{ij} : j \in F_i)$. Considere também as famílias $(a_{ij} : (i, j) \in K) = (a_{ij} : i \in I, j \in F_i)$ e $(\sum_{j \in F_i} : i \in I)$. Vale a relação:

$$\sum_{i\in I}\left(\sum_{j\in F_i} a_{ij}\right) = \sum_{(i,j)\in K} a_{ij}$$

Demonstração. Provaremos por indução no tamanho de I. Se $I = \{i'\}$ é unitário, temos que $K = \{(i', j) : j \in F_{i'}\}$. Segue que $\phi : F_{i'} \to K$ dada por $\phi(j) = (i', j)$ é bijetora. Assim, pela proposição 2.2.3, temos que:

$$\sum_{i\in I}\left(\sum_{j\in F_i} a_{ij}\right) = \left(\sum_{j\in F_{i'}} a_{i'j}\right) = \sum_{(i,j)\in K} a_{ij}$$

Justificando melhor a última igualdade:

$$\sum_{j\in F_{i'}} a_{i'j} = \sum_{j\in F_{i'}} a_{\pi_1(\phi(j))\pi_2(\phi(j))} = \sum_{k\in K} a_{\pi_1(k)\pi_2(k)} = \sum_{(i,j)\in J} a_{ij}.$$

Agora provaremos o passo indutivo.

Suponha que $|I| = n + 1$ e que a hipótese vale para todo I de tamanho n. Fixe qualquer $i' \in I$ e considere $I' = I \setminus \{i'\}$.

Seja $K' = \{(i', j) : j \in F_{i'}\}$. e $\hat{K} = \{(i, j) : i \in I', j \in F_i\}$. Segue que K é a união disjunta de $\hat{K}$ e K'. Assim, pela Proposição 2.2.4, pelo caso base, e pelo passo indutivo, segue que:

$$\sum_{i\in I}\left(\sum_{j\in F_i} a_{ij}\right) = \left(\sum_{i\in I'}\sum_{j\in F_i} a_{ij}\right) + \left(\sum_{j\in F_{i'}} a_{i'j}\right) = \sum_{(i,j)\in \hat{K}} a_{ij} + \sum_{(i,j)\in K'} a_{ij} = \sum_{(i,j)\in K} a_{ij}$$

□

Agora provaremos a comutação de somatórios.

Proposição 2.2.6. Sejam I, J conjuntos não vazios e considere uma família $(a_{ij} : (i, j) \in I \times J) = (a_{ij} : i \in I, j \in J)$ em um monoide comutativo G.

Para cada $i \in I$, considere a família $(a_{ij} : j \in J)$, e, para cada $j \in J$, considere a família $(a_{ij} : i \in I)$.

Então:

$$\sum_{i\in I}\sum_{j\in J} a_{ij} = \sum_{j\in J}\sum_{i\in I} a_{ij}$$

Demonstração. Seja $K = I \times J$ e $K' = J \times I$. Temos que $\phi : I \times J \to J \times I$ dada por $\phi(i, j) = (j, i)$ é uma bijeção entre K e K'. Escrevendo de outra forma, $\phi(k) = (\pi_2(k), \pi_1(k))$. Note ainda que $\phi^2 = \mathrm{id}_K$.

Assim, pela Proposição 2.2.3 e Proposição 2.2.5, temos que:

$$\sum_{j\in J}\sum_{j\in J} a_{ij} = \sum_{(i,j)\in I\times J} a_{ij} = \sum_{k\in K} a_{\pi_1(\phi^2(k))\pi_2(\phi^2(k))}$$

$$= \sum_{k\in K'} a_{\pi_1(\phi(k))\pi_2(\phi(k))} = \sum_{k\in K'} a_{\pi_2(k)\pi_1(k)} = \sum_{(j,i)\in J\times I} a_{ij} = \sum_{j\in J}\sum_{i\in I} a_{ij}.$$

□

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 $a = 0$ ou $b = c$ (isto é, se $a \neq 0$, podemos cancelá-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. Grupos pode ser Abelianos ou não Abelianos, e, quando é Abeliano, lembra-nos da adição de inteiros.

Porém, estruturas como as dos números inteiros, racionais e reais parecem não ter sua estrutura algébrica completamente capturada pela noção de grupo Abeliano, pois possuem também outra operação binária – a multiplicação. Esta operação se relaciona com a soma através das propriedades distributivas. A noção de anel surge para capturar parte destas ideias, generalizando o estudo das estruturas mencionadas.

Definição 3.1.1 (Anel)**.** Um anel é uma 5-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 3.1.2 (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 3.1.3 (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 3.1.4 (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

Matrizes são objetos muito importantes na matemática, sendo amplamente utilizadas na Álgebra Linear.

Nesta seção, construiremos os anéis de matrizes com coeficientes em um anel arbitrário.

Definição 3.2.1. 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 cujas entradas são todas $0 \in A$, 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 3.2.2. 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. □

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

Proposição 3.2.3. 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. □

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 3.2.4 (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 e divisores de zero

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

Definição 3.3.1. 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 $2 \neq 0$.

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

Definição 3.3.2. 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 $ba = 0$. □

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

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

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 3.4.1 (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 3.4.2. 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 2.1.4, ficando como exercício.

Proposição 3.4.3. 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 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 3.5.1. Um anel ordenado é uma tupla $(A, +, \cdot, 0, 1, \leq)$ para a qual $(A, +, \cdot, 0, 1)$ 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 3.5.2 (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 que $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots, \}$.

3.6 Corpos e anéis de divisão

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

Definição 3.6.1 (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 3.6.2. 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 $\mathbb{Z}$.

3.7 O corpo dos números reais

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

Proposição 3.7.1. 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.

3.8 O corpo dos números complexos

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

A ideia é que se adiciona em $\mathbb{R}$ um novo elemento, i, para o qual vale $i^2 = -1$, e tal que 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 3.8.1 (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 $x \in \mathbb{H}$, existem 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 3.8.2. $\mathbb{C}$ é um corpo.

Demonstração.

Proposição 3.8.3. $\mathbb{H}$ 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 distinto 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:

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

□

□

3.9 O Anel dos Quatérnions

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 quatérnions $\mathbb{H}$, que descreveremos abaixo.

A ideia é que se adiciona 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 vemos que a nossa estrutura deverá ser não comutativa.

Definição 3.9.1 (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 $x \in \mathbb{H}$, existem 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 3.9.2. $\mathbb{H}$ 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 3.9.3. $\mathbb{H}$ é um anel de divisão.

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

3.10 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 3.10.1 (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 3.10.2 (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 3.10.3. $\mathbb{N}$ 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 3.10.4 (Subanel trivial)**.** Para todo A, temos que A é subanel de si. □

Exemplo 3.10.5. 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 3.10.6. Subanéis de anéis comutativos são comutativos.

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

3.11 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 3.11.1 (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 3.11.2. 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 $b \in A$, $(a-a')b = ab - a'b = ba - ba' = b(a - a')$. □

3.12 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 quatérnions $\mathbb{H}$, 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 quatérnions, 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.

Exercício 3.7. Seja A um anel e $Z = Z[A]$ seu centro. Seja $s \in A$ qualquer.

a) Mostre que $\left\{\sum_{i=0}^{n} a_i s^i : n \geq 0,\, a_0, \ldots, a_n \in Z\right\}$ é um subanel de A.

b) Mostre que tal subanel é comutativo.

Exercício 3.8. Prove que a interseção de qualquer coleção não vazia de subanéis de um dado anel é um subanel. Exiba um exemplo de dois subanéis de algum anel cuja união não seja um subanel.

Exercício 3.9. Seja A um anel e $\mathcal{S}$ uma coleção não vazia de subanéis de A tais que para todos $B, C \in \mathcal{S}$ existe $D \in \mathcal{S}$ tal que $B \cup C \subseteq D$. Mostre que $\bigcup_{B \in \mathcal{S}} B$ é um subanel de A.

Exercício 3.10. Seja A um anel e $\mathcal{S}$ uma coleção não vazia de subaneis de A que são também corpos, e tais que para todos $B, C \in \mathcal{S}$ existe $D \in \mathcal{S}$ tal que $B \cup C \subseteq D$. Mostre que $\bigcup_{B \in \mathcal{S}} B$ é um corpo.

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 4.1.1. Sejam A, R anéis. 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*. Finalmente, caso f seja bijetora, dizemos que f é um *isomorfismo*. □

A noção de isomorfismo é extremamente importante na Teoria de Anéis. Muitas vezes, temos dois anéis que "deveriam ser o mesmo", 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 4.1.2. Seja $A = \{0, 1\}$ e $R = \{Z, U\}$, onde Z, U são objetos diferentes, e diferentes de $0, 1$. Defina em A as operações $\cdot$ e $+$ dadas pelas seguintes tabelas:
Em A:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Em R:

+	Z	U
Z	Z	U
U	U	Z

·	Z	U
Z	Z	Z
U	Z	U

Intuitivamente, A e R correspondem a duas apresentações de uma mesma estrutura algébrica, porém, como $A \cap R = \emptyset$, estes dois anéis não são o mesmo anel. Como formalizar este fato? Ora, há uma relação biunívoca (uma bijeção) entre A e R que preserva suas operações, e ela é dada por $\phi(0) = Z$ e $\phi(1) = U$. Tal 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 4.1.3. 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.

Para ver que $f(0_A) = 0_R$, primeiro note que $f(0_A) = f(0_A+0_A) = f(0_A)+f(0_A)$. Cancelando $f(0_A)$, $f(0_A) = 0_R$.

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

A composição de homomorfismos é um homomorfismo.

Lema 4.2.1 (Composição de homomorfismos)**.** 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 4.2.2 (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, $\operatorname{im} f = \{f(a) : a \in A\}$, é um subanel de R. Se A é comutativo, $\operatorname{im} f$ 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 $a, b \in \operatorname{im} f$. 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, $a - b \in \operatorname{im} f$. Similarmente, $ab = f(x)f(y) = f(xy) \in \operatorname{im} f$, e $1_R = f(1_A) \in \operatorname{im} f$.

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

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

Proposição 4.2.3 (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) $\mathrm{id}_A : A \to A$ é um isomorfismo de anéis.

Demonstração. a) A composição de funções bijetoras é bijetora, e a composição de homomorfismos é homomorfismo (Proposição 4.2.1). 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 $a, b \in A$:

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

□

Agora introduziremos o núcleo de um homomorfismo.

Definição 4.2.4. 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 dada como se segue:

Proposição 4.2.5. 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 4.3.1. 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 4.3.2. 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 $x = x \cdot 1_R = x \cdot 0_R = 0_R$. □

Para uma recíproca, notemos que um homomorfismo acima existe para qualquer anel A:

Proposição 4.3.3. 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 4.3.4 (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 4.3.5. Seja $f : A \to R$ um homomorfismo de anéis. Então $\ker f$ é um ideal de A.

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

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

Proposição 4.3.6 (Ideal trivial)**.** Seja A um anel. Então $\{0\}$ e A são ideais de A. Estes ideais são chamados de *ideais principais*.

Demonstração. Exercício. □

Proposição 4.3.7 (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 4.3.8. $f : A \to R$ 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 4.3.9 (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 $I' \subseteq I$.

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 4.3.10. 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 4.3.11. 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 4.3.12. 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, $ax \in I + J$.

Concluímos 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 4.3.13. 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 4.4.1 (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 4.4.2 (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 4.4.3 (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 cujos ideais são todos triviais, 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 4.4.4 (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 4.4.5. 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 $x \in I_N$. Considerando que $x \in I_n$, 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 4.5.1. 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 4.5.2. 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 4.5.3. 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 $xb + yab = b$. Como $x \in I$, temos que $xb \in I$, e, como $ab \in I$, temos que $yab \in I$. Portanto, $b = xb + yab \in I$. □

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. Porém, vale que:

Proposição 4.5.4. Seja A um domínio de ideais principais e I um ideal primo não nulo de A. Então I é maximal.

Demonstração. Seja $I = \langle a \rangle$ para algum $a \in A$. Temos que $a \neq 0$, pois I é não nulo.

Seja J um ideal de A tal que $I \subseteq J$. Temos que $J = (b)$ para algum $b \in A$.

Como $a \in J$, temos que existe $c \in A$ tal que $a = bc \in I$, logo, $b \in I$ ou $c \in I$. Se $b \in I$, segue que $I = J$.

Se $c \in I$, segue que $c = ax$ para algum $x \in A$. Assim, $a = bac$. Como $a \neq 0$, segue que $a = bc$, logo, b é invertível e, portanto, $A = J$. □

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 4.6.1. 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 sub casos: $n + m \geq 0$ 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:

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

□

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

Definição 4.6.2. 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 4.6.3. 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 quádrupla $(V, +, 0, \cdot)$, 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 espaço 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, são normalmente 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 5.1.1. 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 5.1.2. 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 5.1.3 (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, $a + c \sim_I b + d$.
- Finalmente, 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 $a - b \sim 0$. □

Exemplo 5.1.4. 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 $k \in \mathbb{Z}$. □

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 5.2.1. 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 5.2.2. 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 5.2.3 (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 $A/I = \operatorname{im} q$ também é, pois q é homomorfismo de anéis. □

Em particular, temos:

Corolário 5.2.4. 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 5.3.1 (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 $q(a) = a + J$.

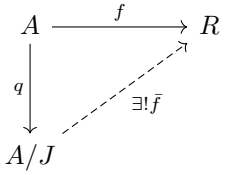


Figura 5.1: Teorema do homomorfismo.

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 5.3.2 (Primeiro Teorema do Isomorfismo)**.** Seja $f : A \to R$ um homomorfismo de anéis. Então, A/I é isomorfo a $\operatorname{im} f$. 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.

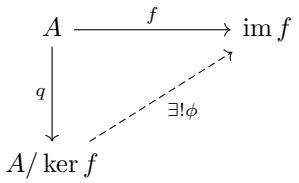


Figura 5.2: Primeiro Teorema do Isomorfismo.

Demonstração. Pelo Teorema do Homomorfismo, existe um único homomorfismo $\bar{\phi} : A/\ker f \to \operatorname{im} f$ 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 $b \in \operatorname{im} f$, existe $b \in A$ tal que $f(a) = b$. Logo, $b = f(a) = \bar{\phi}(q(a))$, assim, $b \in \operatorname{im} \phi$.

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 5.3.3. 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 $\operatorname{im} \phi$, 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 enunciá-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 5.3.4. 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 5.3.5 (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, $B/\ker f \cong \operatorname{im} f$. Veremos que $\operatorname{im} f = I + B/I$ e $\ker f = I \cap B$, o que completa a prova.

Temos que $\operatorname{im} f = \frac{I+B}{I}$ 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. □

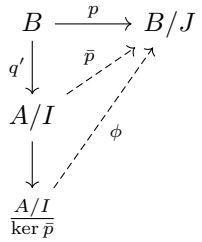
Finalmente, temos o Terceiro Teorema do Isomorfismo.

Teorema 5.3.6 (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 $\bar{f} \circ q' = f$.



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

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

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

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, $x \in \ker \bar{p}$.

Portanto, 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 5.3.7 (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 6.1.1. 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 6.1.2. 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) ⇒ (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 $c + ba = 1$. Assim, $q(1) = q(c) + q(ba) = 0 + q(b)q(a) = q(b)x$. Portanto, x é invertível. □

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

Proposição 6.1.3. 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 6.1.4. 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 6.2.1. 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 6.2.2. 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 6.2.3. 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 6.2.4. 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: $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad + bc}{bd}$, e,
- 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 6.2.5. 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 6.2.6. 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 disso, 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:

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

Temos que ambos os lados são iguais, pois:

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

□

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 6.2.7. 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 a 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 6.2.8 (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 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 7.1.1 (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 a 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 7.2.1 (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 a 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 7.2.2 (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 7.2.3 (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 7.2.4 (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.

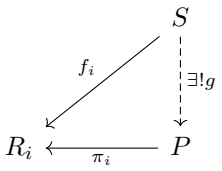
Demonstração. Sejam $a = (a_j : j \in I), b = (b_j : j \in I)$ em P. Então:

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

□

7.3 A propriedade universal do produto direto de anéis

Teorema 7.3.1 (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 $i \in I$.



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:

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

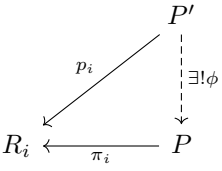
Vejamos que g é único. Se $\bar{g} : R \to S$ é um homomorfismo de anéis tal que $\pi_i \circ \bar{g} = f_i$, fixe $s \in S$. Devemos ver que $\bar{g}(s) = g(s)$. Como $\bar{g}(s) \in P$, escreva $\bar{g}(s) = (b_i)_{i\in I}$, onde $b_i \in R_i$ para cada $i \in I$. Temos, que, para cada $j \in I$:

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

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, $g = \bar{g}$.

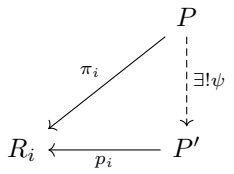
Agora suponha que P' e $(p_i : P' \to R_i)_{i\in I}$ são como no enunciado.

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 $i \in I$.

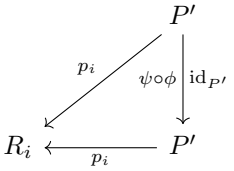


Nosso objetivo é mostrar que ϕ é isomorfismo. Construiremos uma inversa. Como ele é o único homomorfismo tal que $\pi_i \circ \phi = p_i$ para todo $i \in I$, e como todo isomorfismo é homomorfismo, isso conclui a prova.

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 $i \in I$.

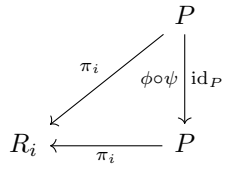


Tanto os mapas $\psi \circ \phi$ quanto a identidade $\mathrm{id}_{P'} : P' \to P'$ são homomorfismos de anéis que satisfazem o seguinte diagrama comutativo:



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:



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 $\pi_1 \circ g = h_1$ e $\pi_2 \circ g = h_2$.

Exercício 7.3. Decida quais dos seguintes conjuntos são subanéis 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

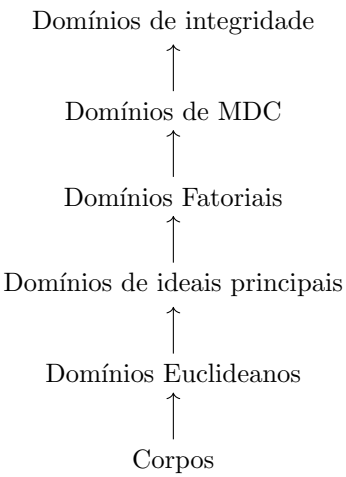
Divisibilidade em anéis

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, dando particular atenção aos domínios de integridade.

Neste capítulo, estudaremos diversos tipos de domínios de integridade que capturam boa parte das propriedades de divisibilidade dos números inteiros.

Uma esquematização encontra-se no diagrama abaixo:



8.1 Definição de divisibilidade

Definição 8.1.1. Seja R um anel comutativo. Definimos a relação de divisibilidade, $|$, em R, como se segue:

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

Algumas propriedades básicas:

Proposição 8.1.2. 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 $a \mid a$, pois $a = 1 \cdot a$.

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

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 $a \mid 0$ 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 $b \mid a$, então existe um *único* $c \in R$ tal que $a = bc$. Este elemento c é, muitas vezes, chamado de quociente de a por b.

Outra vantagem é a caracterização de $a \mid b$ e $b \mid a$ a seguir:

Proposição 8.1.3. Seja R um anel domínio de integridade. Se $a, b \in R$, são equivalentes:

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

Demonstração. Primeiro, suponha que $a \mid b$ e $b \mid a$. 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, $a \mid b$ e $b \mid a$. □

Com isso, definimos:

Definição 8.1.4. Seja R um anel comutativo. Dizemos que elementos $a, b \in R$ são associados se existe $u \in R$ invertível tal que $a = ub$. □

A relação de ser associado é uma relação de equivalência:

Lema 8.1.5. 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, 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 $uv \in R^*$.

□

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

Proposição 8.1.6. Seja R um anel comutativo e $a, b \in R$. São equivalentes:

a) $a \mid b$.

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

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

Demonstração. Primeiro, suponha que $a \mid b$. 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, $a \mid b$. □

8.2 Mínimo múltiplo comum e Máximo divisor comum

Nesta seção, definimos a noção de mínimo múltiplo comum e máximo divisor comum de dois elementos em um domínio de integridade.

Definição 8.2.1. Seja R um anel comutativo e $a_0, \ldots, a_n \in R$ não nulos.

Um mínimo múltiplo comum de $a_0, \ldots, a_n$ é, se existe, um elemento $m \in R$ tal que:

- $a_0 \mid m$, ..., $a_n \mid m$
- Se $c \in R$ é tal que $a_0 \mid c$, ..., $a_n \mid c$, então $m \mid c$.

Um máximo divisor comum de $a_0, \ldots, a_n$ é, se existe, um elemento $d \in R$ tal que:

- $d \mid a_0$, ..., $d \mid a_n$.
- Se $c \in R$ é tal que $c \mid a_0$, ..., $c \mid a_n$, então $c \mid d$.

O conjunto de todos os MMC's de a, b é $\mathrm{MMC}(a_0, \ldots, a_n)$. O conjunto de todos os MDC's de a, b é $\mathrm{MDC}(a_0, \ldots, a_n)$. □

Note que, pela simetria da definição, $\mathrm{MDC}(a, b) = \mathrm{MDC}(b, a)$ e $\mathrm{MMC}(a, b) = \mathrm{MMC}(b, a)$. É importante ressaltar que, no geral, $\mathrm{MMC}(a_0, \ldots, a_n)$ e $\mathrm{MDC}(a_0, \ldots, a_n)$ podem ser vazios, e, geralmente, quando não vazios, não são unitários. De fato:

Lema 8.2.2. Seja R um domínio de integridade e $a \in R$ não nulo.

Sejam $a_0, \ldots, a_n \in R$. Então todos os elementos de $\mathrm{MDC}(a_0, \ldots, a_n)$ são associados entre si. Analogamente, todos os elementos de $\mathrm{MMC}(a_0, \ldots, a_n)$ são associados entre si.

Reciprocamente, todo elemento de R associado a algum elemento de $\mathrm{MDC}(a_0, \ldots, a_n)$ é um MDC de $a_0, \ldots, a_n$, e todo elemento de R associado a algum elemento de $\mathrm{MMC}(a_0, \ldots, a_n)$ é um MMC de $a_0, \ldots, a_n$.

Demonstração. Sejam d, d' máximos divisores comuns de $a_0, \ldots, a_n$. Então, $d \mid a_0$, ..., $d \mid a_n$, $d' \mid a_0$, ..., $d' \mid a_n$. Logo, $d \mid d'$ e $d' \mid d$. Portanto, d e d' são associados entre si.

Similarmente, sejam m, m' mínimos múltiplos comuns de $a_0, \ldots, a_n$. Então, $m \mid a_0$, ..., $m \mid a_n$, $m' \mid a_0$, ..., $m' \mid a_n$. Logo, $m \mid m'$ e $m' \mid m$. Portanto, m e m' são associados entre si.

Para a recíproca, se d é MDC de $a_0, \ldots, a_n$ e d' é associado à d, então $d' \mid a_0$, ..., $d' \mid a_n$, pois $d \mid a_0$, ..., $d \mid a_n$ e $d' \mid d$. Se $x \in R$ é tal que $x \mid a_0$, ..., $x \mid a_n$, então $d' \mid d$ e $d \mid x$, logo $d' \mid x$.

Similarmente, se m é MMC de a, b e m' é associado à m, então m' é MMC de a, b. □

No geral, em domínios de integridade, podem existir pares de elementos sem MMC ou MDC. Porém:

Lema 8.2.3. Sejam $a, b \in R$ tais que $a \mid b$. Então $a \in \text{MDC}(a, b)$ e $b \in \text{MDC}(a, b)$.

Em particular, $0 \in \text{MDC}(a, 0)$ e $a \in \text{MMC}(a, 0)$. Além disso, se $a, b \neq 0$, temos $0 \notin \text{MMC}(a, b)$. e $0 \notin \text{MDC}(a, b)$.

Demonstração. Suponha que $a \mid b$. Temos que $a \mid b$ e $a \mid a$, logo, a é divisor comum de a, b. Se r é divisor comum de a, b, temos que $r \mid a$, logo, $a \in \text{MDC}(a, b)$.

Temos que $a \mid b$ e $b \mid b$, logo, b é múltiplo comum de a, b. Se r é múltiplo comum de a, b, temos que $b \mid r$, logo, $b \in \text{MMC}(a, b)$.

Para a última afirmação, se $a, b \neq 0$, temos que $0 \notin \text{MDC}(a, b)$, já que 0 divide apenas 0. Além disso, $0 \notin MMC(a, b)$, pois $ab \neq 0$ é múltiplo comum de a, b e não é múltiplo de 0. □

8.3 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 8.3.1 (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 $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Proposição 8.3.2 (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 8.3.3. 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 $p \mid ab$. Logo, $p \mid a$ ou $p \mid b$, 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 $p \mid ab$. 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, $p \mid a$ ou $p \mid b$. □

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

Proposição 8.3.4. 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 $p \mid ab$. Logo, $p \mid a$ ou $p \mid b$. Supondo $p \mid a$, 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 $p \mid b$ é análogo. □

A recíproca vale em domínios de ideais principais.

Proposição 8.3.5. 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 8.3.6. 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 $q = pu$.

Primeiro, note que q não é invertível, do contrário, teríamos que $p = qu^{-1} \in R^*$. Além disso, $q \neq 0$ já que $u, p \neq 0$.

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. □

Lema 8.3.7. Seja R um domínio de integridade e p um elemento primo.

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

Demonstração. Como na proposição anterior, temos que $q \notin R^*$ e $q \neq 0$.

Se $a, b \in R$ tão tais que $q \mid ab$, como $p \mid q$, segue que $p \mid ab$. Logo, $p \mid a$ ou $p \mid b$. Como $q \mid p$, segue que $q \mid a$ ou $a \mid b$. □

8.4 Domínios de MDC

Em $\mathbb{Z}$, sabemos que quaisquer dois elementos possuem um mdc (máximo divisor comum) e um mmc (mínimo múltiplo comum).

Nesta seção, estudaremos a classe de domínios de integridade que generaliza essa propriedade.

Definição 8.4.1. Um domínio de integridade R é um domínio de MDC se para todos $a, b \in R$ existe um mdc de a e b. □

Lema 8.4.2. Seja R um domínio de MDC. Então para todos $a_0, \ldots, a_n \in R$, $\mathrm{MDC}(a_0, \ldots, a_n) \neq \emptyset$.

Demonstração. Indução em n.

Para $n = 0$, temos que $a_0 \in \mathrm{MDC}(a_0)$.

Suponha que a tese vale para n. Veremos que vale para $n + 1$. Com efeito, sejam dados $a_0, \ldots, a_{n+1} \in R$. Fixe $m \in \mathrm{MDC}(a_0, \ldots, a_n)$. Tome $k \in \mathrm{MDC}(m, a_{n+1})$.

Temos que $k \mid m$, logo $k \mid a_0, \ldots, k \mid a_n$, e $k \mid a_{n+1}$.

Agora, se $x \in R$ é tal que $x \mid a_0, \ldots, x \mid a_{n+1}$, então $x \mid m$ e $x \mid a_{n+1}$, logo $x \mid k$. □

Como primeira propriedade, temos:

Proposição 8.4.3. Seja R um domínio de MDC e $a_0, \ldots, a_n \in R$. Então, para todo $x \in R$, temos $x\,\mathrm{MDC}(a_0, \ldots, a_n) = \mathrm{MDC}(xa_0, \ldots, xa_n)$.

Demonstração. Se $x = 0$, a igualdade nos diz que $\{0\} = \{0\}$. Assim, suponha que $x \neq 0$.

Seja $m \in \mathrm{MDC}(a_0, \ldots, a_n)$ e $\bar{m} \in \mathrm{MDC}(xa_0, \ldots xa_n)$. Veremos que xm e $\bar{m}$ são associados.

Como $m \in \mathrm{MDC}(a_0, \ldots, a_n)$, temos que $m \mid a_0, \ldots, m \mid a_n$. Logo, $xm \mid xa_0, \ldots, xm \mid xa_n$. Assim, $xm \mid \bar{m}$.

Para a recíproca, temos que $x \mid xa_0, \ldots, x \mid xa_n$. Segue que $x \mid \bar{m}$. Escreva $\bar{m} = xc$ para algum $c \in R$. Temos que $xc \mid xa_0, \ldots, xc \mid xa_n$. Cancelando, $c \mid a_0, \ldots, c \mid a_n$. Logo, $c \mid m$. Assim, $\bar{m} = xc \mid xm$. □

Poderíamos definir também a noção de domínio de MMC, mas isso não é necessário:

Proposição 8.4.4. Seja R um domínio de integridade. Então R é um domínio de MDC se, e somente se para todos $a, b \in R$, $\text{MMC}(a, b) \neq \emptyset$.

Além disso, nesses casos, se $a, b \neq 0$ e $m \in \text{MMC}(a, b)$, então o quociente de ab por m é um MDC de a e b.

Analogamente, se $a, b \neq 0$ e $d \in \text{MDC}(a, b)$, então o quociente de ab por d é um MMC de a e b.

Demonstração. Primeiro, suponha que R é um domínio de MDC. Fixe $a, b \in R$, veremos que existe um MMC de a, b. Se $a = 0$ ou $b = 0$, então $0 \in MMC(a, b)$. Assim, suponha que $a \neq 0 \neq b$. Segue que $0 \notin \text{MDC}(a, b)$.

Seja $d \in \text{MDC}(a, b)$. Escreva $a = da'$ e $b = db'$. Seja $m = da'b' = ab' = ba'$. Está claro que $a \mid m$ e $b \mid m$, e $ab = md$.

Suponha que $x \in R$ é tal que $a \mid x$ e $b \mid x$. Então $md = ab \mid xb$ e $md = ab \mid xa$. Como $xd \in \text{MDC}(ax, bx)$, temos que $xd \mid md$. Como $d \neq 0$, temos que $x \mid m$. Isso conclui que $m \in \text{MMC}(a, b)$.

Reciprocamente, suponha que para todos $a, b \in R$, $\text{MMC}(a, b) \neq \emptyset$. Veremos que para todos $a, b \in R$, $\text{MDC}(a, b) \neq \emptyset$. Se $a = 0$ ou $b = 0$, então $0 \in \text{MDC}(a, b)$. Assim, vamos supor $a, b \neq 0$.

Fixe $m \in \text{MMC}(a, b)$. Temos que $a \mid m$ e $b \mid m$, que $ab \mid am$ e $ab \mid bm$. Escreva $m = aa' = bb'$. Como ab é múltiplo de a e b, temos que $m \mid ab$. Escreva $ab = dm$. Afirmamos que $d \in \text{MDC}(a, b)$.

Com efeito, $ab = dm = daa' = dbb'$, logo, $b = da'$ e $b = db'$. Assim, $d \mid a$ e $d \mid b$. Agora seja $x \in R$ tal que $x \mid a$ e $x \mid b$. Temos que $x \mid ab$. Escreva $ab = xy$, $a = \bar{a}x$, $b = \bar{b}y$. Então $ab = \bar{a}xb = \bar{b}xa = xy$, assim, $\bar{a}b = \bar{b}a = y$. Logo, $b \mid y$ e $a \mid y$, e, assim, $m \mid y$.

Escreva $y = my'$. Segue que $ab = xy = xmy' = dm$. Cancelando m, segue que $xy' = d$, ou seja, $x \mid d$. □

Corolário 8.4.5. Seja R um domínio de MDC. Então para todos $a, b, x \in R$, temos que $x\,\text{MMC}(a, b) = \text{MMC}(xa, xb)$.

Demonstração. Seja $x = 0$ a igualdade é $\{0\} = \{0\}$. Se $a = 0$, temos que xb está em ambos os conjuntos. Se $b = 0$, temos que xa está em ambos os conjuntos.

Assim, suponha $a, b, x \neq 0$. Seja $d \in \text{MDC}(a, b)$. Escreva $md = ab$. Assim $(xm)(xd) = (xa)(xb)$ e $xd \in MDC(a, b)$. Logo, $(xm) \in \text{MMC}(xa, xb)$. □

Lema 8.4.6. Em um domínio de MDC, todo elemento irredutível é primo.

Demonstração. Seja $p \in R$ um elemento irredutível. Sejam $a, b \in R$ com $p \mid ab$. Veremos que $p \mid a$ ou $p \mid b$.

Seja $d \in \text{MDC}(p, a)$. Então $bd \in \text{MDC}(pb, ab)$. Como $p \mid pb$ e $p \mid ab$, segue que $p \mid bd$.

Como $d \mid p$, então d é invertível ou é associado à p.

Se d é associado à p, temos que $p \mid d$, e, portanto, $p \mid a$.

Se d é invertível, temos, de $p \mid bd$, que $p \mid b$. □

Finalmente, em um domínio de MMCs de quantidades finitas arbitrárias de elementos existem.

Proposição 8.4.7. Seja R um domínio de MDC e $a_0, \ldots, a_n \in R$. Então $\text{MMC}(a_0, \ldots, a_n) \neq \emptyset$ não são vazios.

Demonstração. Provaremos por indução em n. Para $n = 0$, note que $a \in \text{MMC}(a)$. Suponha que a proposição vale para n. Sejam $a_1, \ldots, a_{n+1} \in R$. Seja $m \in \text{MMC}(a_1, \ldots, a_n)$.

Seja $m' \in \text{MMC}(a_{n+1}, m)$. Afirmamos que $m' \in \text{MMC}(a_1, \ldots, a_{n+1})$.

m' é múltiplo comum de $a_1, \ldots, a_{n+1}$: temos que $a_{n+1} \mid m'$, $m \mid m'$, logo $a_1 \mid m'$, $\ldots$, $a_n \mid m'$.

Se x é múltiplo comum de $a_1, \ldots, a_{n+1}$, então $m \mid x$ e $a_{n+1} \mid x$, logo $m' \mid x$. □

8.5 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 8.5.1. Um Domínio de Fatoração Única (DFU) é um domínio de integridade R que satisfaz as condições abaixo.

1. Para todo $a \in R \setminus \{0\}$ não invertível, existe um inteiro $n \geq 1$, irredutíveis $p_1, \ldots, p_n$ tais que $a = p_1 \cdots p_n$.

2. Para todos $m, n \geq 1$ e irredutíveis $q_1, \ldots, q_m, p_1, \ldots, p_m$, se $q_1 \ldots q_m = p_1 \ldots p_m$, então $n = m$ e existe uma permutação $\sigma : \{1 \ldots, n\} \to \{1, \ldots, n\}$ tal que p_i é associado a $q_{\sigma(i)}$ para todo $i = 1, \ldots, n$.

□

Exemplo 8.5.2. Conforme argumentaremos mais a frente, $\mathbb{Z}$ é um domínio de fatoração única. Note que $2, 3, -2, -3$ são irredutíveis em $\mathbb{Z}$, e que $6 = 2 \cdot 3 = (-2) \cdot (-3)$. Perceba que 2 é associado à -2 e 3 é associado à -3. □

Lema 8.5.3. Seja R um DFU. Se $n, m \geq 1$ e $p_1, \ldots, p_n, q_1, \ldots, q_m$ são elementos irredutíveis e $(p_1 \ldots p_n) | (q_1 \ldots q_m)$, então existe $\sigma : \{1, \ldots, n\} \to \{1, \ldots, m\}$ injetora tal que p_i é associado a $q_{\sigma(i)}$ para todo $i \in \{1, \ldots, n\}$.

Demonstração. Seja x tal que $q_1 \ldots q_m = xp_1 \ldots, p_n$. Temos que $x \neq 0$, pois $q_1 \ldots q_n \neq 0$, uma vez que R é um domínio.

Se x é invertível, (xp_1) é associado à p_1, logo, xp_1 é irredutível. Como R é um DFU, $n = m$ e existe σ permutação de $\{1, \ldots, n\}$ tal que xp_1 é associado à $q_{\sigma(1)}$ e, para $2 \leq i \leq n$, p_i é associado à q_i. Como p_1 é associado à xp_1, segue a tese.

Se x não é invertível escreva $x = p_{n+1} \ldots p_{n+k}$, com $x_1, \ldots, x_k$ irredutíveis. Temos que $q_1 \ldots q_m = p_1 \ldots p_{n+k}$. Como R é um DFU, $k + n = m$ e existe σ permutação em $n + k = m$ tal que p_i é associado à $q_{\sigma(i)}$ para todo $i < k$. Restringindo-se σ à $\{1, \ldots, n\}$, segue a tese. □

Corolário 8.5.4. Em um DFU, todo elemento irredutível é primo. Assim, em um DFU, todo elemento não nulo e não invertível se escreve como um produto de primos.

Lema 8.5.5. Seja R um DFU e $a, b \in R \setminus \{0\}$. Se não existe $p \in R$ irredutível tal que $p \mid a$ e $p \mid b$, então $1 \in \text{MDC}(a, b)$.

Demonstração. De fato, temos que $1 \mid a$ e $1 \mid b$. Além disso, se $x \in R$ é tal que $x \mid a$ e $x \mid b$, então $x \neq 0$, pois $a, b \neq 0$. Se x é invertível, $x|1$, como queríamos. Por outro lado, se x não é invertível, escreva $x = p_1 \ldots p_n$ com $p_1, \ldots, p_n$ irredutíveis.

Segue que $p_1|a$ e $p_1|b$, o que é um absurdo. □

Para a próxima proposição, observe que se R é um domínio, $a, b, c, d \in R \setminus \{0\}$ e se a é associado à b e $a \neq 0$, então $c \mid d$ se, e somente se $ac \mid ad$.

Proposição 8.5.6. Todo DFU é um domínio de MDC.

Demonstração. Seja R um DFU. Se $a \mid b$ ou $b \mid a$, temos que o MDC$(a,b) \neq \emptyset$. Assim, vamos supor que $a \nmid b$ e $b \nmid a$. Em particular, $a, b \neq 0$ e $a, b \notin R^*$.

Escreva $a = p_1 \dots p_n$ e $b = q_1 \dots q_m$ com $p_1, \dots, p_n$ e $q_1, \dots, q_m$ irredutíveis.

Suponha que não existam i, j tais que p_i é associado à c_j, de modo que a sequência $c_1, \dots, c_k$ seja, na realidade, vazia. Então $1 \in$ MDC(a,b): de fato, temos que $a, b \neq 0$ e não existe $r \in R$ irredutível tal que $r \mid a$ e $r \mid b$, do contrário, existiriam i, j tais que r é associado a p_i e r é associado a q_j, de modo que q_i é associado a p_j, um absurdo.

Assim, suponha que existem i, j tais que p_i é associado a q_j.

Reordenando, podemos transformar $(p_1, \dots, p_n)$ nas sequências $(c_1, \dots, c_k)$ e $(c_{k+1}, \dots, c_{k+l})$, e $(q_1, \dots, q_m)$ nas sequências $(c'_1, \dots, c'_k)$ e $(c'_{k+1}, \dots, c'_{k+l'})$ de modo que:

$$a = \prod_{i=1}^{k+l} c_i,$$

$$b = \prod_{i=1}^{k+l'} c'_i.$$

Onde cada c_i é associado a c'_i para $1 \leq i \leq k$ e nenhum c_i é associado a nenhum c'_j para $k+1 \leq i \leq k+l$ e $k+1 \leq j \leq k+l'$. Note que $a \nmid b$ e $b \nmid a$, temos que as famílias $(c_{k+1}, \dots, c_{k+l})$ e $(c'_{k+1}, \dots, c'_{k+l'})$ são não vazias.

Afirmamos que $c = \prod_{i \in I} c_i$ é um MDC de a e b.

Está claro que $c \mid a$ e $c \mid b$. Suponha que $d \mid a$ e $d \mid b$. Devemos ver que $d \mid c$. Temos que $d \neq 0$, e se d é invertível, segue a tese.

Suponha por absurdo que $d \nmid c$.

Se d não é invertível, escreva $d = d_1 \dots d_t$ com d_i irredutíveis. Veremos, por indução, que para todo $s \in \{1, \dots, t\}$, que $d_1 \dots d_s | c$, o que concluirá a prova.

Para $s = 1$, temos que $d_1 | c_1 \dots c_{k+l}$ e $d_1 | c'_1 \dots c'_{k+l}$. Pelo lema anterior, existem i, j tais que d_1 é associado à c_i e d_1 é associado à c'_j. Se $i, j > k$ temos que c_i é associado à c'_j, o que é um absurdo. Assim, $i \leq k$ ou $j \leq k$, e, em qualquer caso, temos $d_1 | c$.

Suponha que a hipótese vale para $s < t$. Veremos que vale para $s+1$.

Temos que $d_1 \dots d_s | c$, logo, pelo lema anterior, existe $\sigma : \{1, \dots, s\} \to \{1, \dots, k\}$ injetora tal que cada d_i é associado à $c_{\sigma(i)}$, e, consequentemente, à $c'_{\sigma(i)}$. Como $d_1 \dots d_s d_{s+1} | c_1 \dots c_{k+l}$, cancelando os elementos associados por σ, temos que existe $\bar{i}$ fora da imagem de σ tal que d_{s+1} é associado à $c_{\bar{i}}$. Analogamente, existe $\bar{j}$ fora da imagem de σ tal que d_{s+1} é associado à $c'_{\bar{j}}$. Se $\bar{i}, \bar{j} > k$, temos um absurdo. Logo, sem perda de generalidade, $\bar{i} \leq k$ e $d_1 \dots d_{s+1} | c_{\sigma(1)} \dots c_{\sigma(s)} c_{\bar{j}}$ e $c_{\sigma(1)} \dots c_{\sigma(s)} c_{\bar{j}} | c$. □

A recíproca do Corolário 8.5.4 é verdadeira. Primeiro, precisamos:

Lema 8.5.7. Seja R um domínio de integridade, $p \in R$ um elemento primo e $q_1, \dots, q_n \in R$ irredutíveis. Se $p \mid q_1 \cdots q_n$, então existe i tal que p é associado à q_i.

Demonstração. Seguimos por indução em n. Para $n = 1$, se $p \mid q_1$, temos que $q_1 = pu$ para algum $u \in R$. Assim, $p \in R^*$ ou $u \in R^*$. Como $p \notin R^*$, segue que $u \in R^*$, logo, p é associado à q_1.

Para o passo indutivo, suponha que a tese é verdadeira para n e que $p \mid (q_1 \dots q_{n+1})$. Temos que $p \mid (q_1 \dots q_n)$ ou $p \mid q_{n+1}$. As hipóteses indutivas concluem a prova. □

Proposição 8.5.8. Suponha que R é um domínio em que todo elemento não nulo, não invertível se escreve como um produto de primos. Então R é um DFU.

Demonstração. Primeiro, verificaremos que todo irredutível é primo. Suponha que q é irredutível. Escreva $q = p_1 \cdots p_n$, com $p_1, \ldots, p_n$ primos. Temos que cada p_i divide q. Assim, pelo lema, existe i tal que p_i é associado a q. Em particular, q é primo.

Para provar a proposição, mostraremos, por indução em $k \geq 1$, que para todos n, m com $1 \leq n, m \leq k$ e $p_1, \ldots, p_n, q_1, \ldots, q_m$ irredutíveis, se $p_1 \ldots p_n$ é associado à $q_1 \ldots q_m$, então $n = m$ e existe uma permutação $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ tal que p_i é associado a $q_{\sigma(i)}$ para todo $i = 1, \ldots, n$.

No caso $k = 1$, temos que $n = m = 1$ e p_1 é associado à q_1.

Para o passo indutivo, suponha que a tese é verdadeira para k. Sejam $p_1, \ldots, p_n, q_1, \ldots, q_m$ irredutíveis (primos) com $1 \leq n, m \leq k+1$ tais que $p_1 \ldots p_n = q_1 \ldots q_m$. Se $m, n \leq k$, a hipótese indutiva conclui a prova. Sem perda de generalidade, vamos supor $n = k+1$. Assim, $(p_1 \cdots p_k)p_{k+1} = q_1 \cdots q_m$.

Como $p_{k+1} \mid q_1 \cdots q_m$, segue do lema anterior que existe i tal que p_{k+1} é associado a q_i.

Notemos que $m \geq 2$, caso contrário teremos que $p_1 \ldots p_k$ é invertível, o que implica que cada p_i é invertível.

Tome $\theta : \{1, \ldots, m\} \to \{1, \ldots, m\}$ de modo que $\theta(m) = i$. Escreva $p_{k+1} = wq_i$ com $w \in R^*$. Temos que $p_1 \cdots p_k w q_i = q_1 \cdots q_m = q_{\theta(1)} \cdots q_{\theta(m)}$. Cancelando, segue que $wp_1 \cdots p_k = q_{\theta(1)} \cdots q_{\theta(m-1)}$. Por hipótese indutiva, temos que $m - 1 = k$ e existe $\sigma : \{1, \ldots, k\} \to \{1, \ldots, k\}$ tal que wp_1 é associado à $q_{\theta(\sigma(1))}$, e, para $2 \leq j \leq k-1$, p_j é associado a $q_{\theta(\sigma(j))}$ para todo $j = 1, \ldots, k$.

Seja $\sigma' = \theta \circ \sigma \cup \{(k+1, i)\}$, o que conclui a prova. □

8.6 Domínios de Ideais Principais

Nessa seção, veremos que todo DIP é um DFU, bem como o conhecido Lema de Bézout.

Lema 8.6.1. Seja R um domínio de ideais principais. Então todo elemento não nulo, não invertível, possui um divisor irredutível.

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

a) $p_0 = a$.

b) $p_n \mid p$ 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 $p_0 \mid a$.

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 $p_n \mid a$. 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, nem associados à p_n. Seja $p_{n+1} = b$.

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

Como $p_{n+1} \mid p_n$, temos que $\langle p_n \rangle \subseteq \langle p_{n+1} \rangle$. Porém, a inclusão é própria, caso contrário, teríamos p_{n+1} e p_n são associados. □

Lema 8.6.2. 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, $a_{n+1} \mid a_n$, 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 8.6.3. Todo domínio de ideais principais é um domínio de fatoração única.

Proposição 8.6.4 (Lema de Bézout)**.** Seja R um domínio de ideais principais, $a_0, \ldots, a_n \in R$ e $d \in \mathrm{MDC}(a_0, \ldots, a_n)$ Então existem $x_0, \ldots, x_n \in R$ tais que $d = x_0 a_0 + \cdots + x_n a_n$ e d gera o ideal $\langle a_0, \ldots, a_n \rangle$.

Demonstração. Seja d' um gerador do ideal $\langle a_0, \ldots, a_n \rangle$.

Para cada $i \leq n$, $d | a_i$, logo, $a_i \in \langle d \rangle$, assim, segue que $\langle a_0, \ldots, a_n \rangle \subseteq \langle d \rangle$.

Seja d' um gerador do ideal $\langle a_0, \ldots, a_n \rangle$. Temos que, para cada $i \leq n$, $d' | a_i$, logo, $d' | d$. Assim, $\langle d \rangle \subseteq \langle d' \rangle \subseteq = \langle a_0, \ldots, a_n \rangle$.

Conclui-se que $\langle d \rangle = \langle a_0, \ldots, a_n \rangle$. Em particular, $d \in \langle a_0, \ldots, a_n \rangle$, o que nos dá a existência de $x_0, \ldots, x_n \in R$ tais que $d = x_0 a_0 + \cdots + x_n a_n$. □

8.7 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 8.7.1. Um domínio de integridade R é um domínio Euclideano se existe uma função $\nu : R \setminus \{0\} \to \mathbb{N} = \{0, 1, \ldots\}$ satisfazendo:

- para todos $a, b \in R$ com $b \neq 0$, existem $q, r \in R$ com $a = bq + r$ e $(r = 0$ ou $\nu(r) < \nu(b))$, e,
- 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 8.7.2. 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 8.7.3. 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 8.7.4. 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 8.7.5. 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.

Finalmente, 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 8.7.6. 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 8.7.7. 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, $a = bq \in \langle b \rangle$. □

8.8 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 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 $\nu(a) = m$.

Exercício 8.4. Determine todas as unidades de $\mathbb{Z}[i]$.

Exercício 8.5. Seja R um domínio e $a, b, c, d \in R$, com a, b não nulos e associados. Mostre que $c \mid d$ se, e somente se $ac \mid bd$.

Exercício 8.6. Seja R um domínio e $a, b, c, d \in R$, com a, b não nulos e associados. Mostre que ac é associado à bd se, e somente se c é associado à d.

Exercício 8.7. Seja R um domínio e $a, b \in R$ irredutíveis. Mostre que $a|b$ se, e somente se a e b são associados.

Exercício 8.8. Seja R um domínio e $a \in R$ irredutível. Mostre que para todo $x \in R$, $ax \notin R^*$.

Exercício 8.9. Seja R um domínio de fatoração única e $a_0, \ldots, a_n \in R$ não todos nulos. Mostre que $1 \in \text{MDC}(a_0, \ldots, a_n)$ se, e somente se, para todo $p \in R$ irredutível existe $i \in \{0, \ldots, n\}$ tal que $p \nmid a_i$.

Exercício 8.10. Considere $A = \mathbb{Z}[i\sqrt{3}] = \{a + bi\sqrt{3} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

a) Mostre que A é um domínio de integridade.

b) Mostre explicitamente quem são os elementos invertíveis de A.

c) Prove que 2 é irredutível em A.

d) Mostre que $\text{MDC}(4, 2(1 + i\sqrt{3})) = \emptyset$ em A.

e) Mostre que 2 não é primo em A.

Capítulo 9

Polinômios

Nesse capítulo, estudaremos os anéis de polinômios no contexto de anéis comutativos.

Apresentaremos uma construção do anel das séries formais, e a partir deste, extrairemos o anel de polinômios.

Após isso, veremos como se dá sua definição abstrata.

9.1 Séries Formais

Ao estudar Análise Real, Análise Funcional, Funções Analíticas ou mesmo Cálculo Diferencial e Integral, é comum se deparar com somas infinitas. Em tais assuntos, essas somas podem convergir ou divergir, e, mesmo quando convergem, não é sempre que podemos manipular essas somas infinitas como gostaríamos.

Para se falar em convergência de tais objetos, é necessária uma noção de convergência, o que pode ser feito por uma noção de métrica, ou, mais geralmente, por uma noção de topologia. Tal estudo foge do escopo deste texto.

Apesar disso, em anéis comutativos arbitrários, é possível estudar séries de potência como objetos formais, sem nunca de fato computar somar infinitas, ou falar em convergência. É o que faremos nesta seção.

Se R é um anel comutativo, intuitivamente uma série formal é um objeto que se escreve na forma:

$$a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{i=0}^{\infty} a_i x^i$$

onde $a_i \in R$.

Antes de definirmos o que, formalmente, é esse objetivo, vamos enunciar algumas propriedades que gostaríamos que esse objeto tivesse.

- **Igualdade:** é conveniente que, no aspecto formal, a igualdade entre séries formais seja determinada pelos seus coeficientes. Ou seja, que:

$$\sum_{i=0}^{\infty} a_i x^i = \sum_{i=0}^{\infty} b_i x^i \Leftrightarrow \forall i \in \mathbb{N}\, a_i = b_i.$$

- **Soma:** intuitivamente, se valem propriedades associativas, comutativas e distributivas, faz sentido que a soma satisfaça a propriedade a seguir, imaginando que as duas séries à

esquerda se juntam e se reordenam de modo a obter a da direita.

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) + \left(\sum_{i=0}^{\infty} b_i x^i\right) = \left(\sum_{i=0}^{\infty} (a_i + bi) x^i\right)$$

- **Produto:** intuitivamente, se, no lado esquerdo da igualdade, valerem propriedades distributivas "infinitas", como podemos definir produto? Ora, o coeficiente c_i da série produto resultante deveria ser obtido agrupando (por meio de uma soma) os coeficientes $a_j b_k$ com $j + k = i$. Isso é equivalente à igualdade abaixo:

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_j b_{i-j}\right) x^i$$

- Notação: $R[\![x]\!]$ é o conjunto de todas as séries formais em R.

Olhando apenas para as regras acima, parece que as letras x^i parecem não ter nenhum papel a não ser o de demarcar a "i-ésima posição." Com isso em mente, definimos:

Definição 9.1.1. Seja R um anel comutativo. Definiremos $R[\![x]\!]$ como o conjunto $R^{\mathbb{N}}$ munido das operações definidas abaixo. Nesse contexto, escrevemos, para $(a_i : i \in \mathbb{N}) \in R^{\mathbb{N}}$:

$$\sum_{i=0}^{\infty} a_i x^i = (a_i)_{i \in \mathbb{N}}.$$

Reforçamos que, neste contexto, não há nenhuma soma infinita ocorrendo, e o lado esquerdo é simplesmente definido como uma notação alternativa para o lado direito. Note ainda que, com essa definição, a propriedade da igualdade acima vale automaticamente.

Se $p \in \mathbb{R}[\![x]\!]$, escrevemos $p(x) = p$ para reforçar que estamos lidando com uma série formal, e escrevemos $p(x) = \sum_{i=0}^{\infty} p_i x^i$. Os elementos p_i são chamados de *coeficientes* de $p(x)$, e p_0 é chamado de *coeficiente constante*.

Operações: Se $p(x), q(x) \in R[\![x]\!]$, define-se:

$$p(x) + q(x) = \sum_{i=0}^{\infty} p_i x^i + \sum_{i=0}^{\infty} q_i x^i = \sum_{i=0}^{\infty} (p_i + q_i) x^i.$$

$$p(x) \cdot q(x) = \sum_{i=0}^{\infty} p_i x^i \cdot \sum_{i=0}^{\infty} q_i x^i = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} p_{i-j} q_j\right) x^i.$$

$$1_{R[\![x]\!]} = \sum_{i=0}^{\infty} \delta_{i0} x^i = (1, 0, 0, \dots).$$

$$0_{R[\![x]\!]} = \sum_{i=0}^{\infty} 0 x^i = (0, 0, 0, \dots).$$

□

Lema 9.1.2 (Séries formais formam anéis)**.** Se R é um anel comutativo, então $R[\![x]\!]$ é um anel comutativo.

Demonstração. A operação de soma de $\mathbb{R}[\![x]\!]$ é a mesma de $\mathbb{R}^{\mathbb{N}}$, que já verificamos satisfazer as propriedades de grupo Abeliano. Assim, $R[\![x]\!]$ é um grupo abeliano sob a soma.

Para as demais propriedades, fique $p(x), q(x), r(x) \in R[\![x]\!]$ e $i \in \mathbb{N}$.

- **Distributividade:** O i-ésimo coeficiente de $p(x) \cdot (q(x) + r(x))$ é:

$$\sum_{j=0}^{i} p_{i-j}(q_j + r_j) = \sum_{j=0}^{i} p_{i-j}q_j + \sum_{j=0}^{i} p_{i-j}r_j.$$

  O que coincide com o i-ésimo coeficiente de $p(x)q(x) + p(x)r(x)$.

- **Elemento Neutro:** Temos que:

$$p(x) \cdot 1 = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} p_{i-j}\delta_{0j} \right) x^i = \sum_{i=0}^{\infty} p_i x^i = p(x).$$

- **Comutatividade:** A i-ésima coordenada de $p(x) \cdot q(x)$ é $\sum_{j=0}^{i} p_{i-j}q_j = \sum(p_{i-j}q_j : j \in A_i)$, onde $A_i = \{0, \ldots, i\}$. A função $\phi : A_i \to A_i$ dada por $\phi(j) = i - j$ é bijetora, pois é injetora e A_i é finito. Assim:

$$\sum_{j=0}^{i} p_{i-j}q_j = \sum_{j=0}^{i} p_{i-\phi(j)}q_{\phi(j)} = \sum_{j=0}^{i} p_j q_{i-j} = \sum_{j=0}^{i} q_{i-j}p_j.$$

  E esta é a i-ésima coordenada de $q(x) \cdot p(x)$.

- **Associatividade:** Temos que a i-ésima coordenada de $(p(x) \cdot q(x)) \cdot r(x)$ é dada por:

$$\pi_i((p(x) \cdot q(x)) \cdot r(x)) = \sum_{j=0}^{i} \pi_{i-j}(p(x) \cdot q(x)) \cdot q_j = \sum_{j=0}^{i} \left(\sum_{k=0}^{i-j} p_{i-j-k}q_k \right) q_j$$

$$= \sum_{j=0}^{i} \sum_{k=0}^{i-j} p_{i-j-k}q_k q_j = \sum \left(p_{i-j-k}q_k r_j : (j,k) \in A \right).$$

  Onde $A = \{(j,k) : 0 \leq j \leq i, 0 \leq k \leq i - j\}$.

  Temos que a i-ésima coordenada de $p(x) \cdot (q(x) \cdot r(x))$ é dada por:

$$\pi_i(p(x) \cdot (q(x) \cdot r(x))) = \sum_{s=0}^{i} p_{i-s}\pi_s(q(x) \cdot r(x)) = \sum_{s=0}^{i} p_{i-s} \left(\sum_{t=0}^{s} q_{s-t}r_t \right)$$

$$= \sum_{s=0}^{i} \sum_{t=0}^{s} p_{i-s}q_{s-t}r_t = \sum \left(q_{i-s}q_{s-t}r_t : (s,t) \in B \right)$$

  onde $B = \{(s,t) : 0 \leq t \leq s \leq i\}$. A função $\phi : A \to B$ dada por $\phi(j,k) = (j + k, j)$ é bijetora: é em B, pois $0 \leq j \leq j+k \leq j+(i-j) = i$. É injetora, pois se $(j+k, j) = (j'+k', j')$ então $j = j'$ e, cancelando, $k = k'$. Finalmente, é sobrejetora, pois se $0 \leq t \leq s \leq i$, sendo $j = t$ e $k = s - t$, temos que $0 \leq j \leq i$, $0 \leq k = s - t \leq i - t = i - j$ e $j + k = s$. Assim, ϕ é bijetora. Portanto:

$$\sum (q_{i-s}q_{s-t}r_t : (s,t) \in B) = \sum \left(q_{i-(j+k)}q_{(j+k)-j}r_j : (j,k) \in A\right)$$
$$= \sum (q_{i-j-k}q_k r_j : (j,k) \in A).$$

□

Note que, ao menos por enquanto, a letra x é apenas parte da notação, e que não faz sentido, por enquanto, "substituir x" por algo.

9.2 Anéis de Polinômios

Na subseção anterior, introduzimos o anel das séries formais de um anel comutativo dado. Vimos que tal anel é um anel comutativo.

Deste anel, podemos extrair o anel de polinômios.

Definição 9.2.1. Seja R um anel comutativo e $p(x) \in R[\![x]\!]$.

Define-se o *suporte* de $p(x)$ por:

$$\operatorname{supp} p(x) = \{i \in I : p_i \neq 0\}.$$

Define-se o *grau* de $p(x)$ por:

$$\operatorname{gr}(p(x)) = \begin{cases} \infty & \text{se } \operatorname{supp} p(x) \text{ é infinito} \\ -\infty & \text{se } \operatorname{supp} p(x) = \emptyset \text{ (se } p(x) = 0) \\ \max \operatorname{supp} p(x) & \text{caso contrário.} \end{cases}$$

O *anel de polinômios com coeficientes em* R, denotado por $R[x]$, é o subconjunto de $R[\![x]\!]$ dado por:

$$R[x] = \{p \in R[\![x]\!] : \operatorname{gr}(p) < \infty\}.$$

Se $p(x) \in R[x]$ é não nulo, define-se o *coeficiente dominante* de $p(x)$ por $a_{\operatorname{gr}(p(x))}$. Ou seja, o coeficiente dominante de $p(x)$ é seu coeficiente não nulo de mais alta posição. □

Assim, formalmente, o conjunto dos polinômios foi construído como sendo o conjunto de sequências eventualmente nulas de elementos de R.

Lema 9.2.2. Seja R um anel comutativo. O anel de polinômios $R[x]$ é um subanel de $R[\![x]\!]$. Mais especificamente, dados $p(x), q(x) \in R[x]$:

a) $\operatorname{gr}(p(x)q(x)) \leq \operatorname{gr} p(x) + \operatorname{gr} q(x)$, e a igualdade vale se R for um domínio de integridade.

b) $\operatorname{gr}(p(x) + q(x)) \leq \max\{\operatorname{gr} p(x), \operatorname{gr}(q(x))\}$.

c) $\operatorname{gr} p(x) = \operatorname{gr}(-p(x))$.

Demonstração. Ambas as afirmações são óbvias se $p(x) = 0$ ou $q(x) = 0$, então suponhamos que $p(x)$ e $q(x)$ são ambos não nulos. Sejam n, m os graus de $p(x)$ e $q(x)$, respectivamente.

Calculemos o coeficiente $n + m$ de $p(x)q(x)$.

$$\pi_{n+m}(p(x)q(x)) = \sum_{j=0}^{n+m} p_{n+m-j}q_j.$$

Se $0 \leq j < m$ temos que $n + m - j > n$, e $p_{n+m-j} = 0$. Se $j > m$, temos que $q_j = 0$. Assim, o único termo possivelmente não nulo da soma é quando $j = m$, que é $p_n q_m$. Este é não nulo R for um domínio.

Por outro lado, se $l > n + m$ temos que:

$$\pi_l(p(x)q(x)) = \sum_{j=0}^{l} p_{l-j} q_j.$$

Se $0 \leq j \leq m$ temos que $l - j > m + n - m = n$, e $p_{l-j} = 0$. Se $j > m$, temos que $q_j = 0$. Assim, todos os coeficientes da soma são 0. Isso conclui que $\operatorname{gr}(p(x)q(x)) \leq n + m$, sendo $n + m$ se R for um domínio de integridade.

Para a segunda afirmação, se $l > \max\{\operatorname{gr} p(x), \operatorname{gr} q(x)\}$, temos que o l-ésimo coeficiente de $p(x) + q(x)$ é 0, pois este é $p_l + q_l = 0 + 0$.

A terceira afirmação é imediata.

Agora, para a afirmação principal, as afirmações itemizadas nos mostram que $R[x]$ é fechado pela soma, produto e diferença de $R[\![x]\!]$. Finalmente, note que o grau da série $1 = (1, 0, 0, \dots)$ é 0, logo, $1 \in R[x]$. □

Agora vamos trabalhar um pouco mais nossa notação.

Ao tratar de polinômios, intuitivamente, estamos tratando de expressões do tipo $a_0 + a_1 x + \cdots + a_n x^n$, onde $n \geq 0$ e $a_i \in R$ para cada $i \leq n$. De acordo com nosso formalismo até então, apesar de utilizarmos a notação de soma $\sum_{i=0}^{\infty} a_i x^i$ para tratar de séries formais e polinômios, os símbolos $\sum_{i=0}^{\infty}$ e x^i são apenas, por ora, parte da notação, e não têm outro significado além deste. Porém, ao pensar em um polinômio $a_0 + a_1 x + \cdots + a_n x^n$, pensamos que cada a_i tem um significado individual, bem como x. A seguir, expandiremos a nossa notação a fim de formalizar essa ideia.

Vamos definir o elemento $x \in R[x]$, bem como identificar uma cópia de R dentro de $R[x]$.

Definição 9.2.3. Seja R um anel comutativo. Em $R[x]$, seja $x = (0, 1, 0, 0, \dots)$ e, para cada $r \in R$, seja $\hat{r} = (r, 0, 0, \dots)$. □

Façamos uma pausa para discutir essa notação.

Ao pensar intuitivamente em polinômios, pensa-se em R como um subconjunto de $R[x]$. Porém, isso é, formalmente, falso: cada elemento de $R[x]$ é uma sequência de elementos de R, e, usualmente, uma sequência de elementos de R não é um elemento de R. Logo, no geral, $R \not\subseteq R[x]$.

Porém, conforme discutido acima, intuitivamente um polinômio é um objeto da forma $a_0 + a_1 x + \cdots + a_n x^n$ onde cada $a_i \in R$. Pondo $n = 0$ e $a_0 = r$, intuitivamente, $r \in R[x]$, o que sabemos, conforme discutido no parágrafo anterior, ser (provavelmente) falso. Apesar disso, há uma identificação natural de r em $R[x]$: o elemento $\hat{r}$, é o elemento de $R[x]$ que carrega o coeficiente r na posição correspondente à potência 0. Compare a definição formal de $\hat{r}$ com a ideia intuitiva de que r "deveria ser obtido" pondo $n = 0$ e $a_i = r$.

Já o elemento x é o elemento de $R[x]$ carrega o coeficiente 1 na posição correspondente à potência 1. Intuitivamente, x "deveria ser" ele é obtido colocando-se $n = 2$, $a_0 = 0$ e $a_1 = 1$ na expressão $a_0 + \cdots + a_n x^n$. Compare esse raciocínio intuitivo com a definição formal de x apresentada.

O lema abaixo mostra que os elementos $\hat{r}$ de fato agem como uma cópia de R dentro de $R[x]$. Devido a ele, mais a frente, apesar de não ser verdade, formalmente, que R é um subconjunto de $R[x]$, "identifica-se" $a \in R$ com $\hat{a}$, abandonando-se a notação $\hat{r}$ em favor de escrever simplesmente r, e considerando-se R como um subconjunto de $R[x]$, mesmo não tendo sido construído de modo que isso valha.

Um modo de melhor formalizar esse raciocínio é construir um novo anel $R[x]''$ isomorfo à $R[x]$ em que R é, de fato, um subconjunto de $R[x]$. Para isso, toma-se um conjunto disjunto de R que bijeta com $R[x] \setminus \{\hat{r} : r \in R\}$ e tranferimos a estrutura de $R[x]$ para $R \cup A$ preservando as operações de R, de modo a torná-los isomorfos. Não faremos esse trabalho aqui por envolver tecnicalidades que fogem do escopo deste texto e recomendamos ao leitor que, nesse momento, não se preocupe com tais tecnicalidades.

Lema 9.2.4. Na notação anterior, seja $\phi : R \to R[x]$ dada por $\phi(r) = \hat{r}$. Então h é um homomorfismo injetor.

Demonstração. Sejam $r, s \in R$. Então:

- $\phi(r+s) = (r+s, 0, 0, \dots) = \hat{r} + \hat{s} = \phi(r) + \phi(s)$.
- $\phi(rs) = (rs, 0, 0, \dots) = \hat{r} \cdot \hat{s} = \phi(r) \cdot \phi(s)$.
- $\phi(1_R) = \hat{1} = (1_R, 0, 0, \dots) = 1_{R[x]} = 1_{R[x]}$.

A injetividade é óbvia. □

Agora vejamos que o elemento x se comporta conforme esperado.

Lema 9.2.5. Na notação anterior, para todo $r \in R$ e $n, i \geq 0$:

$$\pi_i(\hat{r}x^n)(i) = \begin{cases} 0 & \text{se } i \neq n \\ r & \text{se } i = n. \end{cases}$$

Ou seja, $\hat{r}x^n = (0, 0, \dots, r, 0, \dots)$ onde o r está na posição n.

Demonstração. Fixe r Seguimos por indução. Para $n = 0$, temos que $\hat{r}x^0 = \hat{r} = (r, 0, 0, \dots)$ e para $n = 1$ temos que $\hat{r}x^1 = x = (0, r, 0, \dots)$.

Para o passo $n+1$, onde $n \geq 1$, temos que, sendo $i \geq 1$:

$$\pi_i(\hat{r}x^{n+1}) = \pi_i((\hat{r}x^n) \cdot x) = \sum_{j=0}^{i} \pi_{i-j}(\hat{r}x^n) \cdot \pi_j(x) = \pi_{i-1}(\hat{r}x^n).$$

Assim, se $i = n+1$, temos que a coordenada é r, e 0 caso contrário. Resta apenas verificar que a coordenada 0 é 0. Ora, a coordenada 0 se dá por $\pi_0(\hat{r}x^n)\pi_0(x) = 0$. □

Agora veremos que todo elemento de $R[x]$ se escreve como uma soma de elementos de R e potências de x, que é o esperado quando pensamos em polinômios.

Proposição 9.2.6. Na notação anterior, para todo $p(x) \in R[x]$ e $n \geq \operatorname{gr} p(x)$, existem únicos $r_0, r_1, \dots, r_n \in R$ tais que $p(x) = \sum_{i=0}^{n} \hat{r}_i x^i$, e estes são os coeficientes de $p(x)$.

Demonstração. Para a unicidade, note que se $p(x) = \sum_{i=0}^{n} \hat{r}_i x^i$, então para cada $i \leq n$, o i-ésimo coeficiente do lado direito é o i-ésimo coeficiente de $\hat{r}_i x^i$, que é r_i. Logo, r_i é o i-ésimo coeficiente de $p(x)$.

Para a existência, note que $p(x) = (p_0, p_1, \dots, p_n, 0, 0, \dots) = (p_0, 0, \dots) + (0, p_1, 0, \dots) + \cdots + (0, 0, \dots, p_n) = p_0x^0 + p_1x^1 + \cdots + p_nx^n = \sum_{i=0}^{n} \hat{p}_i x^i$. □

Note que, diferente do que ocorre na notação inicial sobre séries formais, a notação $\sum_{i=0}^{n} \hat{r}_i x^i$ expressa, de fato, uma soma (finita). Além disso, vale a comparação coeficiente-a-coeficiente.

Corolário 9.2.7. Na notação anterior, se $r_1, \dots, r_n$ e $s_1, \dots, s_n$ são elementos de R, então: $\sum_{i=0}^{n} \hat{r}_i x^i = \sum_{i=0}^{n} \hat{s}_i x^i$ se, e somente se, $r_i = s_i$ para todo $i \leq n$.

Notação: abandona-se $\hat{r}$ em favor de r, mesmo havendo ambiguidade de notação.

9.3 A propriedade universal do Anel de Polinômios

Se $p(x)$ é um polinômio, esperamos poder "substituir"x por um elemento r de R, a fim de obter um elemento de R.

A proposição abaixo formaliza e generaliza essa ideia.

Proposição 9.3.1 (Propriedade universal do anel de polinômios)**.** Seja R um anel comutativo. Então $R[x]$ é um anel comutativo que satisfaz a seguinte propriedade:

Para todo anel S, todo homomorfismo $f : R \to S$ e todo $s \in S$, existe um único homomorfismo $g : R[x] \to S$ tal que $g \circ \phi = f$ e $g(x) = s$.

Demonstração. Já vimos que $R[x]$ é um anel comutativo.

Defina $g : R[x] \to S$ por $g(p(x)) = \sum_{i=0}^{n} f(r_i)s^i$, onde $p(x) = \sum_{i=0}^{n} r_i x^i$. Note que g é bem definido, pois se $p(x) = \sum_{i=0}^{n} r_i x^i = \sum_{i=0}^{n} s_i x^i = q(x)$, então $r_i = s_i$ para todo $i \leq n$.

g é homomorfismo, pois, dados $p(x) = \sum_{i=0}^{n} r_i x^i$ e $q(x) = \sum_{i=0}^{m} s_i x^i$, escrevendo $a_i = 0$ para $i > n$ e $b_i = 0$ para $i > m$, temos que:

$$\begin{aligned} g(p(x) + q(x)) &= g\left(\sum_{i=0}^{\max\{n,m\}} (r_i + s_i)x^i\right) \\ &= \sum_{i=0}^{\max\{n,m\}} f(r_i + s_i)s^i \\ &= \sum_{i=0}^{n} f(r_i)s^i + \sum_{i=0}^{m} f(s_i)s^i \\ &= g(p(x)) + g(q(x)). \end{aligned}$$

$$\begin{aligned} g(p(x)q(x)) &= g\left(\sum_{i=0}^{n+m}\left(\sum_{j=0}^{i} r_{i-j}s_j\right)x^i\right) \\ &= \sum_{i=0}^{n+m}\left(\sum_{j=0}^{i} f(r_{i-j})f(s_j)\right)s^i \\ &= \sum_{i=0}^{n} f(r_i)s^i \cdot \sum_{j=0}^{m} f(s_j)s^j \\ &= g(p(x))g(q(x)). \end{aligned}$$

$$g(1_{R[x]}) = \sum_{i=0}^{0} f(1_R)s^i = 1_S.$$

A função g é única, pois se g' é outra tal função, temos que, dado $p(x) = \sum_{i=0}^{n} r_i x^i$, temos que $g'(p(x)) = \sum_{i=0}^{n} f(r_i)s^i = g(p(x))$. □

Exemplo 9.3.2. Seja R um anel comutativo e $R[x]$ o anel de polinômios sobre R. Para todo $s \in R$, existe um homomorfismo $\mathrm{av}_s : R[x] \to R$ tal que $\mathrm{av}_s(r) = r$ para todo $r \in R$ e $\mathrm{av}_s(x) = s$, de modo que para todo $p(x) = \sum_{i=0}^{n} r_i x^i \in R[x]$, $\mathrm{av}_s(p(x)) = \sum_{i=0}^{n} r_i s^i$.

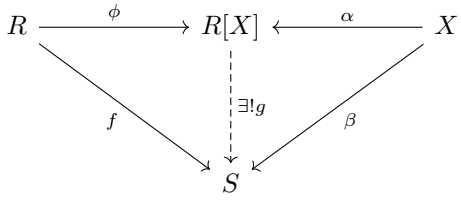
Esse homomorfismo é chamado de *avaliação em s*, e escrevemos $p(s) = \mathrm{av}_s(p(x))$. □

Uma forma de definir um anel de polinômios sem se referir a nenhuma peculiaridade de alguma construção particular é a partir de alguma propriedade que tem dentro da categoria dos anéis que apenas ele possui (a menos de isomorfismos).

Uma tal forma é a seguinte.

Definição 9.3.3. Seja R um anel comutativo e X um conjunto. Um anel de polinômios sobre R com variáveis em X é uma tripla $(R[X], \phi, \alpha)$, onde $R[X]$ é um anel comutativo e $\phi : R \to R[X]$ é um homomorfismo e $\alpha : X \to R[X]$ é uma função que satisfazem a seguinte propriedade:

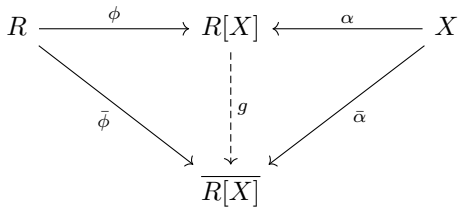
Para toda tripla (S, f, β) onde S é um anel comutativo, $f : R \to S$ é um homomorfismo e$\beta : X \to S$, existe um único homomorfismo $g : R[X] \to S$ tal que $g \circ \phi = f$ e $g \circ \alpha = \beta$.



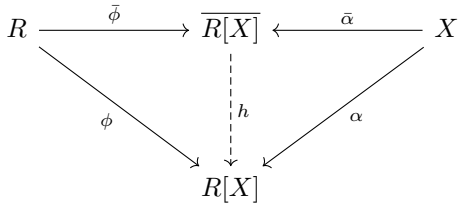
□

Proposição 9.3.4. Seja R um anel comutativo e X um conjunto. Se $(R[X], \phi, \alpha)$ e $(\overline{R[X]}, \bar{\phi}, \bar{\alpha})$ são anéis de polinômios sobre R com variáveis em X, então $R[X]$ e $\overline{R[X]}$ são isomorfos por um isomorfismo $g : R[X] \to \overline{R[X]}$ tal que $g \circ \alpha = \bar{\alpha}$ e $g \circ \phi = \bar{\phi}$.

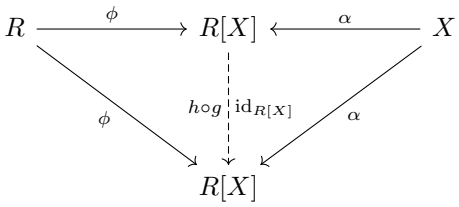
Demonstração. Aplicando a propriedade universal $R[X]$ para $(\overline{R[X]}, \overline{\phi}, \overline{\alpha})$, existe um homomorfismo $g : R[X] \to \overline{R[X]}$ tal que $g \circ \phi = \bar{\phi}$ e $g \circ \alpha = \bar{\alpha}$.



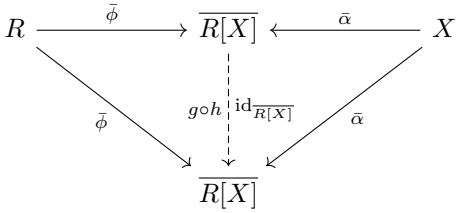
Aplicando a propriedade universal $\overline{R[X]}$ para $(R[X], \phi, \alpha)$, existe um homomorfismo $h : \overline{R[X]} \to R[X]$ tal que $h \circ \bar{\phi} = \phi$ e $h \circ \bar{\alpha} = \alpha$.



Aplicando a propriedade de $R[X]$ para a tripla $(R[X], \phi, \alpha)$, existe um único homomorfismo $u : R[X] \to R[X]$ tal que $u \circ \phi = \phi$ e $u \circ \alpha = \alpha$. É imediato que $\mathrm{id}_{R[X]}$ satisfaz essas propriedades. O mapa $h \circ g$ também satisfaz, pois $h \circ g \circ \phi = h \circ \bar{\phi} = \phi$ e $h \circ g \circ \alpha = h \circ \bar{\alpha} = \alpha$.



Aplicando a propriedade de $\overline{R[X]}$ para a tripla $(\overline{R[X]}, \bar{\phi}, \bar{\alpha})$, existe um único homomorfismo $v : \overline{R[X]} \to \overline{R[X]}$ tal que $v \circ \bar{\phi} = \bar{\phi}$ e $v \circ \bar{\alpha} = \bar{\alpha}$. É imediato que $\mathrm{id}_{\overline{R[X]}}$ satisfaz essas propriedades. O mapa $g \circ h$ também satisfaz, pois $g \circ h \circ \bar{\phi} = g \circ \phi = \bar{\phi}$ e $g \circ h \circ \bar{\alpha} = g \circ \bar{\alpha} = \bar{\alpha}$.



Assim, $g \circ h = \mathrm{id}_{\overline{R[X]}}$ e $h \circ g = \mathrm{id}_{R[X]}$. Portanto, g é um isomorfismo de anéis, e h é o inverso de g. □

Corolário 9.3.5. Seja R um anel comutativo e X, Y conjuntos de mesmas cardinalidades.

Se $(R[X], \phi, \alpha)$ e $(R[Y], \bar{\phi}, \bar{\alpha})$ são anéis de polinômios sobre R com variáveis em X e Y, respectivamente, então $R[X]$ e $R[Y]$ são isomorfos.

Demonstração. Seja $\theta : Y \to X$ uma bijeção. Basta ver que $(R[X], \phi, \alpha \circ \theta)$ é um anel de polinômios sobre R com variáveis em Y.

Seja S um anel comutativo e $f : R \to S$ um homomorfismo, e $\beta : Y \to S$ uma função. Temos que $\beta' = \beta \circ \theta^{-1} : X \to S$ é uma função. Então existe um único homomorfismo $g : R[X] \to S$ tal que $g \circ \phi = f$ e $g \circ \alpha = \beta'$. Desta última, $\alpha \circ \theta = \beta$.

Para ver que g é o único tal homomorfismo, se $h : R[Y] \to S$ é um homomorfismo tal que $h \circ \phi = f$ e $h \circ \alpha \circ \theta = \beta$, então $h \circ \alpha = \beta'$. Pela unicidade de g, segue que $g = h$. □

Proposição 9.3.6. Seja R um anel comutativo e X um conjunto. Então $R[x, y] \approx R[x][y]$.

Demonstração. Seja $X = \{x, y\}$, $\psi : R[x]$ a imersão canônica, $\psi' : R[x] \to R[x][y]$ a imersão, $\phi = \psi' \circ \psi$, $\alpha(x) = x \in R[x][y]$ e $\alpha(y) = y \in R[x][y]$. e $\alpha(x) = \psi'(x) \in R[x]$. Então, $(R[x][y], \phi, \alpha)$ é um anel de polinômios sobre R com variáveis em X.

Com efeito, seja S um anel comutativo, $f : R \to S$ um homomorfismo e $\beta : X \to S$ uma função. Então, existe um único homomorfismo $g : R[x] \to S$ tal que $g \circ \psi = f$ e $g(x) = \beta(x)$. Logo, existe um único homomorfismo $h : R[x][y] \to S$ tal que $h \circ \psi' = g$ e $h(y) = \beta(y)$. Assim, $h \circ \phi = h \circ (\psi' \circ \psi) = (h \circ \psi') \circ \psi = g \circ \psi = f$, $h(\alpha(y)) = h(y) = \beta(y)$ e $h(\alpha(x)) = h \circ \psi'(x) = g(x) = \beta(x)$.

Para ver a unicidade de h, se $\bar{h}$ é outra tal função, temos que $\bar{h} \circ \psi = (\bar{h} \circ \psi') \circ \psi = f$ e $\bar{h} \circ \alpha(x) = \bar{h} \circ \psi'(x) = \beta(x)$, logo, $\bar{h} \circ \psi' = g$. Além disso, $\bar{h} \circ \alpha = \beta$, logo, $\bar{h} = h$. □

Corolário 9.3.7. Sejam R, S anéis comutativos com unidade e $f : R \to S$ um isomorfismo. Então existe um único isomorfismo $\bar{f} : R[x] \to S[x]$ que satisfaz $\bar{f}(\sum_{i=0}^{n} r_i x^i) = \sum_{i=0}^{n} f(a_i) x^i$ para todos $n \geq 0$ e $r_0, \ldots, r_n \in R$.

Demonstração. Identificando $R \subseteq R[x]$ e $S \subseteq S[x]$, considere o único homomorfismo $\bar{f} : R[x] \to S[x]$ tal que $\bar{f}|_R = f$ e $f(x) = x \in S[x]$. Então $\bar{f}(\sum_{i=0}^n r_i x^i) = \sum_{i=0}^n f(a_i)x^i$.

Seja $g = f^{-1}$ e seja $\bar{g} : S[x] \to R[x]$ o homomorfismo tal que $\bar{g}|_S = g$ e $\bar{g}(x) = x \in R[x]$. Segue que $g \circ f|_R = \mathrm{id}_R$ $\bar{g} \circ \bar{f}(x) = x$, bem como $\mathrm{id}_{R[x]}$, logo, $\bar{g} \circ \bar{f} = \mathrm{id}_{R[x]}$. Analogamente, $f \circ g = \mathrm{id}_{S[x]}$. Logo, $\bar{f}$ é isomorfismo.

A unicidade de $\bar{f}$ vem do fato de que este é o único homomorfismo que satisfaz $\bar{f}|_R = f$ e $\bar{f}(x) = x$. □

Definição 9.3.8. Na notação acima, para $p \in R[x]$, $\bar{f}(p)$ é chamado de $f(p)$. □

9.4 Polinômios de várias variáveis

Nesta seção, daremos uma construção particular para $R[X]$, onde X é um conjunto arbitrário de indeterminadas e R é um anel comutativo.

Se $x, y, z \in X$, precisamos dar sentido às expressões como $x^2y^3z^4$ e $xy^2 + xz^3$. A definição abaixo cuida disso.

Definição 9.4.1. Seja X um conjunto qualquer. O conjunto $\mathbb{N}^{(X)}$ é o conjunto de funções $u : X \to \mathbb{N}$ tal que $\operatorname{supp} u = \{x \in X : f(x) \neq 0\}$ é finito.

Se $u, v \in \mathbb{N}^{(X)}$, define-se $u * v : X \to \mathbb{N}$ dada por $(u + v)(x) = u(x) + v(x)$. □

Lema 9.4.2. A operação $*$ definida acima é tal que $\operatorname{supp}(u * v) = \operatorname{supp} u \cup \operatorname{supp} v$, é associativa e comutativa. Além disso, dado $w \in \mathbb{N}^{(X)}$, temos que $\{(u, v) : u * v = w\}$ é finito.

Demonstração. A única afirmação não imediata é a última, que provaremos a seguir. Se $u*v = w$, temos que $\operatorname{supp} u, \operatorname{supp} v \subseteq \operatorname{supp} w$, que é finito. Assim, u, v são 0 fora de $\operatorname{supp} w$, e não podem ter valor maior do que $w(x)$ para $x \in \operatorname{supp} w$. Portanto, há no máximo $N = \prod_{x \in \operatorname{supp} w}(w(x)+1)$ escolhas para u, v, logo, no máximo N^2 escolhas para (u, v).

Observação: o número N^2 acima é uma cota superior para o número de pares (u, v) tal que $u * v = w$, mas, no geral, ele é substancialmente menor do que este. □

Agora definiremos o anel das séries formais de R com variáveis em X. A ideia é identificar cada elemento de $\mathbb{N}^{(X)}$ com um monômio. Por exemplo, se $X = \{x, y, z\}$ e $u(x) = 2$, $u(y) = 3$ e $u(z) = 4$, pensamos em u como $x^2y^3z^4 = y^3z^4x^2 = \ldots$. Assim, se temos ainda que $v(x) = 1$, $v(y) = 4$ e $v(z) = 0$, temos que $u * v = (x^2y^3z^4) * (xy^4z^0) = x^3y^7z^4$, como é esperado.

Desta forma, o que buscamos é, para se obter uma série formal com coeficientes em um anel comutativo R com variáveis em X, é associar a cada elemento de $\mathbb{N}^{(X)}$ (cada monômio), um elemento de R.

Definição 9.4.3. Seja R um anel comutativo e X um conjunto. O anel das séries formais de R com variáveis em X, denotado por $R[\![X]\!]$, é o conjunto de funções $f : \mathbb{N}^{(X)} \to R$. Um elemento $p = (p_u)_{u \in \mathbb{N}} \in R[\![X]\!]$ é denotado por:

$$p = \sum_{u \in \mathbb{N}^{(X)}} p_u u.$$

A série nula é dada pela família $0 = (0)_{u \in \mathbb{N}^{(X)}}$. O monômio 1 é a função nula $0 : X \to \mathbb{N}$. O elemento 1 de $R[\![X]\!]$ é a função $1 = (\delta_{1u})_{u \in \mathbb{N}^{(X)}}$, onde δ_{1u} é o delta de Kronecker, que vale 1 se $u = 1$ e 0 caso contrário.

A soma e produto de séries formais se dá por:

$$\sum_{u\in\mathbb{N}^{(X)}} p_u u + \sum_{u\in\mathbb{N}^{(X)}} q_u u = \sum_{u\in\mathbb{N}^{(X)}} (p_u + q_u)u$$

$$\sum_{u\in\mathbb{N}^{(X)}} p_u u \cdot \sum_{u\in\mathbb{N}^{(X)}} q_u u = \sum_{u\in\mathbb{N}^{(X)}} \sum_{v*w=u} (p_v q_w)u$$

□

Lema 9.4.4 (Séries formais formam anéis)**.** Se R é um anel comutativo e X um conjunto, então $R[\![X]\!]$ é um anel comutativo.

Demonstração. A operação de soma de $\mathbb{R}[\![x]\!]$ é a mesma de $\mathbb{R}^{\mathbb{N}^{(X)}}$, que já verificamos satisfazer as propriedades de grupo Abeliano. Assim, $R[\![x]\!]$ é um grupo abeliano sob a soma.

Para as demais propriedades, fique $p, q, r \in R[\![X]\!]$.

- **Distributividade:** Fixe $u \in \mathbb{N}^{(X)}$. O u-ésimo coeficiente de $p \cdot (q + r)$ é:

$$\sum_{v*w=u} p_v(q_w + r_w) = \sum_{v*w=u} p_v q_w + \sum_{v*w=u} p_v r_w$$

  O que coincide com o u-ésimo coeficiente de $pq + pr$.

- **Elemento Neutro:** Temos que:

$$p \cdot 1 = \sum_{u\in\mathbb{N}^{(X)}} \left(\sum_{v*w=u} p_v \delta_{1w} \right) u = \sum_{u\in\mathbb{N}^{(X)}} p_u u = p$$

- **Comutatividade:** A u-ésima coordenada de pq é $\sum_{v*w=u} p_v q_w = \sum(p_v q_w : (v, w) \in A)$, onde $A = \{(v, w) \in \mathbb{N}^{(X)} \times \mathbb{N}^{(X)} : v*w = u\}$. A função $\phi : A \to A$ dada por $\phi(v, w) = (w, v)$ é bijetora, pois é injetora e A é finito. Assim:

$$\sum(p_v q_w : (v, w) \in A) = \sum(p_w q_v : (v, w) \in A) = \sum(q_v p_w : (v, w) \in A) = \sum_{v*w=u} q_v p_w,$$

  que é a u-ésima coordenada de qp.

- **Associatividade:** Temos que a u-ésima coordenada de $((pq)r$ é dada por:

$$\sum_{v*w=u} \pi_v(pq) r_w u = \sum_{v*w=u} \sum_{s*t=v} p_s q_t r_w u = \sum(p_s q_t r_w : (s, t, v, w) \in A),$$

  onde $A = \{(s, t, v, w) : s * t = v, v * w = u\}$. Seja $B = \{(a, b, c) : a * b * c = u\}$. A função $\phi : B \to A$ dada por $\phi(a, b, c) = (a, b, a * b, c)$ é bijetora (verifique), logo:

$$\sum(p_s q_t r_w : (s, t, v, w) \in A) = \sum(p_a q_b r_c : (a, b, c) \in A) = \sum_{a*b*c=u} p_a q_b r_c.$$

  Analogamente, o u-ésimo coeficiente de $p(qr)$ é dado pela expressão acima.

□

Definição 9.4.5. Seja R um anel comutativo e X um conjunto. O anel de polinômios com coeficientes em R e variáveis em X, denotado por $R[X]$, é o subanel de $R[\![X]\!]$ formado pelos elementos $p \in R[\![X]\!]$ que têm suporte finito, onde $\operatorname{supp} p = \{u \in \mathbb{N}^{(X)} \in X : p_u \neq 0\}$. □

Lema 9.4.6. Se R é um anel comutativo e X um conjunto, então $R[X]$ é um subanel de $R[\![X]\!]$.

Demonstração. A soma e o produto de polinômios são polinômios, pois se $p = \sum_{u\in\mathbb{N}^{(X)}} p_u u$ e $q = \sum_{u\in\mathbb{N}^{(X)}} q_u u$, então $\operatorname{supp}(p+q) \subseteq \operatorname{supp} p \cup \operatorname{supp} q$ e $\operatorname{supp}(pq) = \{u \in \mathbb{N}^{(X)} : u = v * w, v \in \operatorname{supp} p, w \in \operatorname{supp} q\}$, que é finito. Além disso, as séries 0 e 1 são polinômios. □

9.5 Divisibilidade em anéis de polinômios

Proposição 9.5.1. Seja R é um anel comutativo E $p(x), d(x) \in R[x]$ com $d(x) \neq 0$ e o coeficiente dominante de d invertível. Então existem $q(x), r(x) \in R[x]$ tais que $p(x) = d(x)q(x) + r(x)$, onde $\deg(r(x)) < \deg(d(x))$.

Além disso, se R é domínio de integridade, então $q(x), r(x)$ são únicos.

Demonstração. Existência: fixe $d(x)$ e seja $\deg(d(x)) = k \geq 0$.

Se $p(x) = 0$, seja $q(x) = r(x) = 0$. Note que $\operatorname{gr}(0) = -\infty < \operatorname{gr}(d(x))$.

Se $p(x) \neq 0$, procedemos por indução em $m = \operatorname{gr}(p(x))$.

Para $m = 0$: se $0 < k$, seja $q(x) = 0$ e $r(x) = p(x)$. Então $p(x) = d(x)q(x) + r(x)$ e $\operatorname{gr}(r(x)) = 0 < k = \operatorname{gr}(d(x))$.

Se $0 = k$, então $p(x) = a \in K$, $d(x) = b \in K^*$. Seja $q(x) = ab^{-1}$ e $r(x) = 0$. Então $\operatorname{gr}(r(x)) = -\infty < 0 = \operatorname{gr}(d(x))$ e $0 < k$. Provaremos por indução em m que para todo $p(x) \in R[x]$ de grau m, existem $q(x), r(x) \in R[x]$ com $p(x) = q(x)d(x) + r(x)$ e $\operatorname{gr}(r(x)) < \operatorname{gr}(d(x))$.

Agora vamos supor que a hipótese vale para m. Provaremos que vale para $m+1$. Para $m + 1 < k$, seja $p(x) = r(x)$ e $q(x) = 0$. Então $q(x)d(x) + r(x) = r(x) = p(x)$ e $\operatorname{gr}(r(x)) = m + 1 < k = \operatorname{gr}(d(x))$.

Se $m + 1 \geq k$, seja a o coeficiente dominante de $p(x)$ e b o coeficiente dominante de $d(x)$. Temos que $p(x) - \frac{a}{b}d(x)x^{m+1-k}$ é um polinômio de grau $\leq n$, logo, pela hipótese indutiva, existem $q(x), r(x)$ tais que $p(x) - \frac{a}{b}d(x)x^{m+1-k} = d(x)q(x) + r(x)$, onde $\deg(r(x)) < k$. Segue que $p(x) = \left(\frac{a}{b}d(x)x^{m+1-k} + q(x)\right) d(x) + r(x)$, onde $\deg(r(x)) < k$.

Para a unicidade caso R seja domínio, se existem $q_1(x), r_1(x)$ e $q_2(x), r_2(x)$ tais que $p(x) = d(x)q_1(x) + r_1(x) = d(x)q_2(x) + r_2(x)$, temos que $d(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$. Se $q_1(x) - q_2(x) = 0$ segue a tese.

Caso contrário, temos $\operatorname{gr}(r_2(x) - r_1(x)) < \operatorname{gr}(d(x)) \leq \operatorname{gr}(d(x)(q_1(x) - q_2(x))) = \operatorname{gr}(r_2(x) - r_1(x))$, o que é uma contradição. □

Corolário 9.5.2. Seja K um corpo. Então $K[x]$ é um domínio Euclideano.

Demonstração. Já vimos que se K é um corpo, então $K[x]$ é um domínio de integridade.

Para completar a prova, note que para todos $p(x), q(x) \in K[x]\setminus\{0\}$, $\operatorname{gr}(p(x)q(x)) = \operatorname{gr}(p(x)) + \operatorname{gr}(q(x)) \geq \operatorname{gr}(p(x))$. □

Corolário 9.5.3. Se R é um anel comutativo, $a \in R$ e $p(x) \in R[x]$, então existe $q(x) \in R[x]$ tal que $p(x) = q(x)(x - a) + p(a)$.

Demonstração. Como $1 \in R[x]$, existem $q(x), r(x) \in R[x]$ tais que $p(x) = q(x)(x - a) + r(x)$ e $\deg(r(x)) \leq 0$. Assim, $r(x) = b$ para algum $b \in R$, logo, $p(x) = q(x)(x-a)+b$. Como a avaliação em a é homomorfismo, note que $p(a) = b$. Assim, $p(x) = q(x)(x - a) + p(a)$. □

Proposição 9.5.4. Seja R um anel comutativo e $p(x) \in R[x]$. Temos que $(x-a)|p(x)$ se, e somente se, $p(a) = 0$.

Demonstração. Se $p(a) = 0$, segue do corolário anterior que $(x-a)|p(x)$.

Reciprocamente, se $(x-a)|p(x)$, escreva $p(x) = q'(x)(x-a)$. Segue que $p(a) = q'(a)(a-a) = 0$. □

Corolário 9.5.5. Seja R um domínio de integridade e $a \in R$. Então $x - a \in R[x]$ é primo (e, portanto, irredutível).

Demonstração. Suponha que $(x-a)|p(x)q(x)$. Então $p(a)q(a) = 0$, logo, $p(a) = 0$ ou $q(a) = 0$. Assim, $(x-a)|p(x)$ ou $(x-a)|q(x)$. □

Proposição 9.5.6. Seja R um domínio de integridade. Os únicos elementos invertíveis de $R[x]$ são os elementos invertíveis de R.

Demonstração. Se $a \in R$ é invertível, então $aa^{-1} = 1$ também em $R[x]$. Se $a \in R[x]$ e existe b tal que $ab = 1$, temos que $\deg(a) + \deg(b) = 0$, logo, $\deg(a) = \deg b = 0$ e, assim, $a, b \in R$, e, portanto, $a, b \in R^*$. □

9.6 Raízes de polinômios

Definição 9.6.1. Seja R um domínio de integridade e $p(x) \in R[x]$ e $a \in R$. Dizemos que a é uma raiz de $p(x)$ se $p(a) = 0$. □

Proposição 9.6.2. Seja R um domínio de integridade e $p(x) \in R[x] \setminus \{0\}$. Seja $m = \mathrm{gr}(p(x))$. Então $R[x]$ tem no máximo m raízes.

Demonstração. Provaremos por indução em m. Caso $m = 0$, escreva $p(a) = b \neq 0$. Temos que para todo $a \in R$ $p(a) = b \neq 0$, logo, $p(x)$ tem 0 raízes.

Suponha que a afirmação vale para m. Provaremos que vale para $m+1$.

Seja $p(x)$ de grau $m+1$. Caso $p(x)$ não possua raízes, a prova está concluída. Caso contrário, seja a uma raiz de $p(x)$. Então $(x-a)|p(x)$, logo, existe $q(x) \in R[x]$ tal que $p(x) = q(x)(x-a)$

Como $\mathrm{gr}(p(x)) = \mathrm{gr}(q(x))+1$, temos por hipótese indutiva que $q(x)$ tem no máximo m raízes. Observe que se $b \neq a$ é raiz de $p(x)$, então $(b-a)q(b) = 0$, logo, b é raiz de $q(x)$. Assim, $p(x)$ tem no máximo $m+1$ raízes. □

Se R é um domínio de integridade e K é seu corpo de frações, podemos identificar R dentro de K como subanel. Assim, $R[x] \subseteq K[x]$.

Proposição 9.6.3. Seja R um domínio de fatoração única e F o corpo de frações de R. Seja $p(x) \in R[x] \subseteq K[x]$ não nulo e $u, v \in D$ com $v \neq 0$ e $1 \in \mathrm{MDC}(u, v)$.

Então, se $\frac{u}{v}$ é uma raiz de $p(x) = a_n x^n + \cdots + a_1 x + a_0$ onde $n = \mathrm{gr}\, p(x)$, temos que $u|a_0$ e $v|a_n$.

Demonstração. Temos que $0 = \sum_{i=0}^{n} a_i \frac{u^i}{v^i}$. Multiplicando por v^n, temos que $0 = \sum_{i=0}^{n} a_i u^i v^{n-i}$.

Como $p(x)$ tem raízes, $n > 0$, $-a_n u^n = \sum_{i=0}^{n-1} a_i u^i v^{n-i} = v \sum_{i=0}^{n-1} a_i u^i v^{n-i-1}$. Como $v|a_n u^n$ e $1 \in \mathrm{MDC}(v, u)$ e estamos em um domínio de fatoração única, temos que $v|a_n$.

Similarmente, $-a_0 v^n = \sum_{i=1}^{n} a_i u^i v^{n-i} = u \sum_{i=1}^{n} a_i u^{i-1} v^{n-i}$. Como $u|a_0 v^n$ e $1 \in \mathrm{MDC}(u, v)$ e estamos em um domínio de fatoração única, temos que $u|a_0$. □

Exemplo 9.6.4. Em $\mathbb{Q}[x]$, considere $p(x) = 2x^3 - x^2 - 4x + 2$. Caso $p(x) \in \mathbb{Z}[x]$ possua uma raiz racional, ela deve ser da forma $\frac{a}{b}$ com $a|2$ e $b|2$ com a, b primos entre si. As únicas opções de raízes são $\frac{1}{2}$,$-\frac{1}{2}$, 1, -1, 2, -2. □

9.7 Funções Polinomiais

Dado um anel comutativo R e $a_0, \ldots, a_n \in R$, é possível definir $f : R \to R$ dada por $f(x) = \sum_{i=0}^{n} a_i x^i$. Em muitos contextos, tais funções são chamadas de polinômios, ou funções polinomiais. Nesta seção, as chamaremos, para evitar confusão, de função polinomial, e estudaremos sua relação com polinômios.

Definição 9.7.1. Seja R um anel comutativo. Uma função polinomial é uma função $f : R \to R$ da forma $f(s) = \sum_{i=0}^{n} a_i s^i$ ($s \in R$), com $0 \leq i \leq n$ e $a_i \in R$. □

É possível que o leitor tenha indagado, desde o início do capítulo, sobre o motivo de polinômios não terem sido definidos como acima. O exemplo abaixo responde esta pergunta:

Exemplo 9.7.2. Considere $R = \mathbb{Z}^2$, $f, g : \mathbb{Z}^2 \to \mathbb{Z}^2$ dadas por $f(x) = x^3 + x^2$ e $g(x) = x^3 + x$. Então $f(0) = g(0) = 0$, e $f(1) = g(1) = 0$, logo, $f = g = 0$.

Apesar disso, f, g foram expressas com coeficientes distintos. Ou seja, não vale a propriedade de que dois polinômios de mesmo grau são iguais se, e somente se possuem a mesma sequência de coeficientes. □

Proposição 9.7.3. Seja R um anel comutativo. O conjunto das funções polinomiais de R forma um subanel do anel produto R^R. Se R é um domínio infinito, então tal anel é isomorfo à $R[x]$.

Demonstração. Seja $h : R \to R^R$ a função que associa $a \in R$ ao mapa constante $h(a) \in R^R$ dado por $h(a)(r) = a$ para todo $r \in R$. Está claro que $h(1)$ é o mapa constante $1 \in R^R$, que $h(a + b) = h(a) + h(b)$ e $h(ab) = h(a)h(b)$.

Pela propriedade universal do anel de polinômios, existe um homomorfismo $g : R[x] \to R^R$ tal que $g|_R = h$ e $g(x) = \mathrm{id}_R$.

Assim, sendo $p(x) = \sum_{i=0}^{n} a_i x^i$, temos que $g(p(x))(s) = \sum_{i=0}^{n} a_i s^i$.

Está claro que g é sobrejetora no conjunto das funções polinomiais, e, portanto, este forma um anel. Além disso, se R é um domínio infinito e $g(p(x)) = 0$, então $p(s) = 0$ para todo $s \in R$. Se $p(x) \neq 0$, o número de raízes de $p(x)$ seria finito. Como R é infinito, $p(x)$ tem infinitas raízes, assim, $p(x) = 0$. □

9.8 Mais divisibilidade em anéis de polinômios

Algumas vezes pode ser complicado decidir se certo polinômio é irredutível.

Sabemos que $x^2 - 2 \in \mathbb{Q}[x]$ é irredutível, pois, estudando-se os graus, caso tivesse um divisor não invertível, deveria ter um divisor de grau 1 – e, portanto, deveria ter uma raiz em $\mathbb{Q}$, o que sabemos não existir.

Da mesma forma, pode-se argumentar que $x^3 - 2 \in \mathbb{Q}[x]$ é irredutível. Porém, o mesmo argumento não se aplica a $x^4 - 2 \in \mathbb{Q}[x]$: sabemos que tal polinômio não possui uma raiz racional, porém, isso não implica que ele não possui, por exemplo, um divisor de grau 2. Conforme veremos adiante, tal polinômio é, de fato, irredutível sobre $\mathbb{Q}$, e mostraremos isso a partir de outro argumento.

Note ainda que $x^4+1 \in \mathbb{R}[x]$ não possui raiz real, porém, $x^4+1 = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$, logo, $x^4 + 1$ não é irredutível em $\mathbb{R}[x]$, embora não tenha raiz.

Para melhor estudar a reducibilidade em polinômios, definiremos a noção de conteúdo. Tal noção é motivada pelo seguinte lema:

Lema 9.8.1. Seja R um domínio de integridade, $p \in R[x] \setminus \{0\}$ e $a \in R \setminus \{0\}$. Escreva $p = \sum_{i=0}^{n} a_i x^i$. Então $a \mid p$ em $R[x]$ se, e somente se $a \mid a_i$ em R para todo $i \leq n$.

Demonstração. Suponha que $a \mid p$. Existe $q \in R[x]$ tal que $p = aq$. Como $\operatorname{gr} a = 0$, temos que $\operatorname{gr} p = \operatorname{gr} q$. Escreva $q = \sum_{i=0}^{n} b_i x^i$. Para todo $i \leq n$, $a_i = ab_i$, e, assim, $a|a_i$.

Reciprocamente, suponha que para todo $i \leq n$, $a \mid a_i$. Para cada $i \leq n$, existe $b_i \in R$ tal que $a_i = ab_i$. Logo, $p = a\sum_{i=0}^{n} b_i x^i$, e, portanto, $a \mid p$. □

Definição 9.8.2 (Conteúdo de um polinômio)**.** Seja R um domínio de MDC's e $p \in R[x] \setminus \{0\}$. Um *conteúdo* de p é um MDC de seus coeficientes. Explicitamente, se $p = \sum_{i=0}^{n} a_i x^i$ com $a_n \neq 0$, então um *conteúdo* de p é um elemento de $\operatorname{MDC}(a_0, \ldots, a_n)$.

O conjunto de todos os conteúdos de p é denotado por $C(p)$. Explicitamente, $C(p) = \operatorname{MDC}(a_0, \ldots, a_n)$.

Se $1 \in C(p)$, dizemos que p é *primitivo*. □

Façamos uma pausa para fazer algumas observações.

- Se escrevermos $p = \sum_{i=0}^{n} a_i x^i$ com $n > \operatorname{gr} p$ (de modo que $a_i = 0$ para $i \in \{\operatorname{gr} p+1, \ldots, n\}$), então $\operatorname{MDC}(a_0, \ldots, a_n) = C(p)$, pois para quaisquer $a_0, \ldots, a_k$, vale $\operatorname{MDC}(a_0, \ldots, a_k, 0) = \operatorname{MDC}(a_0, \ldots, a_k)$.
- Como $C(p)$ é um conjunto de MDCs, se $a, b \in C(p)$, então a, b são associados (em R), e, se $c \in R$ é associado à a, então $c \in C(p)$.
- Em particular, p é primitivo se, e somente se $C(p) = R^*$.

Em algum sentido, $C(p)$ é o conjunto dos MDCs de p com relação à R, conforme sintetiza o lema a seguir.

Lema 9.8.3. Seja R um domínio de MDC, $p \in R[x] \setminus \{0\}$ e $a \in R$. São equivalentes:

(a) $a \in C(p)$.

(b) $a \mid p$ em $R[x]$ e para todo $b \in R$, se $b \mid p$ então $b \mid a$.

Demonstração. $(a) \to (b)$: como a divide os coeficientes de p, temos que $a \mid p$. Se $b \mid p$, então b divide todos os coeficientes de p, e, portanto, a, que é o MDC destes.

$(b) \to (a)$: Como a divide p, a divide os coeficientes de p. Além disso, se $b \in R$ divide os coeficientes de p, então $b \mid p$, e, por hipótese, $b \mid a$. □

Lema 9.8.4. Seja R um domínio de MDC e $p \in R[x] \setminus \{0\}$. Se $a \in R$, então $C(ap) = aC(p)$.

Demonstração. Seja $p = \sum_{i=0}^{n} a_i x^i$. Então $ap = \sum_{i=0}^{n} aa_i x^i$. Dessa forma:

$$C(ap) = \operatorname{MDC}(aa_0, \ldots, aa_n) = a \operatorname{MDC}(a_0, \ldots, a_n) = aC(p).$$

□

Corolário 9.8.5. Seja R um domínio de MDC e $p \in R[x] \setminus \{0\}$. Se $a \in C(p)$, então $a \mid p$, e, se $p' \in R[x]$ é tal que $p = ap'$, então p' é primitivo.

Demonstração. Como já vimos $a \mid p$. Seja p' tal que $p = ap'$. Como $a \in aC(p')$, existe $b \in C(p')$ tal que $ab = a$. Cancelando $a \neq 0$, temos que $b = 1 \in C(p')$. □

Proposição 9.8.6 (Lema de Gauss)**.** Seja R um domínio de fatoração única e $p, q \in R[x] \setminus \{0\}$. Então $C(pq) = C(p)C(q)$[1]. Em particular, um produto de polinômios primitivos é primitivo.

[1] Nesta notação, $C(p)C(q) = \{ab : a \in C(p), b \in C(q)\}$.

Demonstração. Sejam $a \in C(p)$, $b \in C(q)$. Basta ver que $ab \in C(pq)$.

Escreva $p = \sum_{i=0}^{n} a_i x^i$, $q = \sum_{i=0}^{m} b_i x^i$. Então $pq = \sum_{i=0}^{n+m} \sum_{j=0}^{i} a_{i-j} b_j x^i$, onde $a_i = 0$ se $n < i \leq n+m$ e $b_i = 0$ se $m < i \leq n+m$.

Seja, para $i \leq n+m$, $c_i = \sum_{j=0}^{i} a_{i-j} b_j$. Devemos ver que $ab \in \mathrm{MDC}(c_0, \ldots, c_{n+m})$.

Dados i, j com $0 \leq i \leq n+m$ e $0 \leq j \leq i$, temos que $a | a_{i-j}$ e $b | b_j$, logo, $ab | a_{i-j} b_j$, logo, $ab \mid \left(\sum_{j=0}^{i} a_{i-j} b_j \right) = c_i$.

Para cada $i \leq m+n$, existem a'_i e b'_i tais que $a_i = a a'_i$ e $b_i = b b'_i$. Então, para cada $i \leq m+n$, $c_i = ab \sum_{i=0}^{n+m} a'_{i-j} b'_j$. Seja $c'_i = \sum_{i=0}^{n+m} a'_{i-j} b'_j$.

Segue que $\mathrm{MDC}(c_0, \ldots, c_{n+m}) = \mathrm{MDC}(abc'_0, \ldots, abc'_{n+m}) = ab\,\mathrm{MDC}(c'_0, \ldots, c'_{n+m})$. Assim, basta ver que $1 \in \mathrm{MDC}(c'_0, \ldots, c'_{n+m})$. Para tanto, basta ver que se $\alpha \in R$ é primo, então α não é divisor comum de $(c'_0, \ldots, c'_{n+m})$. Fixe α.

Do lema anterior, como $a \sum_{i=0}^{n} a'_i x^i = p$, segue que $1 \in \mathrm{MDC}(a_0, \ldots, a_n)$. Analogamente, $1 \in \mathrm{MDC}(b_0, \ldots, b_m)$. Seja $r \leq n$ o menor número que $\alpha \nmid a_i$ e $s \leq m$ o menor número que $\alpha \nmid b_j$.

Temos que se $p \nmid c'_{r+s}$: com efeito, $c'_{r+s} = \sum (a_{r+s-j} b_j : 0 \leq j \leq r+s, j \neq s) + a_r b_s$. Temos que $p | \sum (a_{r+s-j} b_j : 0 \leq j \leq r+s, j \neq s)$, pois divide cada somando, mas $p \nmid a_r b_s$, pois p é primo, deveríamos ter $p | a_r$ ou $p | a_s$. Assim, $p \nmid c'_{r+s}$. □

Proposição 9.8.7. Seja R um DFU, K seu corpo de frações, e $p, q \in R[x]$ com p primitivo. Então $p \mid q$ em $R[x]$ se, e somente se $p \mid q$ em $K[x]$.

Demonstração. É claro que se $p \mid q$ em $R[x]$, então $p \mid q$ em $K[x]$.

Agora suponha que $p \mid q$ em $K[x]$. Existe $r \in K[x]$ tal que $q = rp$. Existe $b \in R$ tal que $br \in R[x]$. Seja $a \in C(br)$ e $r' \in R[x]$ primitivo tal que $br = ar'$. Então $bq = brp = ar'p$.

Do Lema de Gauss, fixado $m \in C(q)$, temos $bm \in bC(q) = C(bq) = C(ar'p) = aC(r'p) \ni a$, logo, a é associado à bm em R. Assim, existe $u \in R^*$ tal que $a = ubm$, e, portanto, $aq = ubmq = umar'p$. Cancelando a, temos que $q = umr'p$, e, portanto, $p | q$ em $R[x]$. □

Corolário 9.8.8. Seja R um DFU, K seu corpo de frações e sejam $p, q \in R[x]$ primitivos. Então p, q são associados em $R[x]$ se, e somente se p, q são associados em $K[x]$.

Proposição 9.8.9. Seja R um DFU, K seu corpo de frações e seja $p \in R[x]$ primitivo de grau $k \geq 1$. Então p é irredutível em $R[x]$ se, e somente se p é irredutível em $K[x]$, e, nesse caso, p é primo em $K[x]$ e $R[x]$.

Demonstração. Primeiro, suponha que p é irredutível em $K[x]$. Como $K[x]$ é um domínio Euclidiano, temos que p é primo em $K[x]$. Afirmamos que p é primo em $R[x]$: se $p \mid ab$, com $a, b \in R[x]$, temos que $p \mid a$ ou $p \mid b$ em $K[x]$, e, portanto, em $R[x]$.

Reciprocamente, suponha que p é redutível em $K[x]$ e escreva $p = qt$, com $q, t \in K[x]$ de modo que $n = \mathrm{gr}\, q$ e $m = \mathrm{gr}\, t$ são ambos ≥ 1.

Existem $b, d \in R \setminus \{0\}$ com $bq, dt \in R[x]$. Tome $a \in C(bq)$ e $c \in C(dt)$, e q', t' primitivos com $bq = aq'$ e $dt = ct'$. Note que $\mathrm{gr}\, q' = \mathrm{gr}\, q = n$ e $\mathrm{gr}\, t' = \mathrm{gr}\, t = m$.

Segue que $bdp = bdqt = acq't'$. Pelo Lema de Gauss, bd e ac são associados, e, portanto, existe $u \in R^*$ tal que $bdu = ac$. Assim, $acp = bdup = acuq't'$. Cancelando ac, temos que $p = uq't'$, e, portanto, uq', t' são divisores não invertíveis de p. □

Lema 9.8.10. Seja R um DFU. Todo elemento primo de R é um elemento primo de $R[x]$.

Demonstração. Seja $\alpha \in R$ primo. Então α é não nulo e não invertível em $R[x]$.

Suponha que $\alpha \mid pq$. Se $p = 0$ ou $q = 0$, como $\alpha \mid 0$, segue a tese.

Então suponha que $p, q \neq 0$. Seja $m \in C(p)$, $m' \in C(q)$. Pelo Lema de Gauss, $mm' \in C(pq)$. Assim, $\alpha \mid mm'$, logo, $\alpha \mid m$ ou $\alpha \mid m'$, logo, $\alpha \mid p$ ou $\alpha \mid q$.

Portanto, α é primo. □

Observação: o lema acima também vale para domínios de integridade. Ver Exercício 9.13.

Proposição 9.8.11. Seja R um DFU. Então $R[x]$ é um DFU.

Demonstração. Basta ver que todo elemento não nulo, não invertível de $R[x]$ é um produto de fatores primos.

Dado $p \in R[x]$ não nulo e não invertível de grau 0 ele é um produto de primos de R. Se $\operatorname{gr} p > 0$, escreva $p = mp'$, onde $m \in C(p)$ e p' é primitivo. Temos que m é invertível ou um produto de fatores primos de R. Logo, basta ver que p' é um produto de fatores primos de $R[x]$.

Seja K o corpo de frações de R.

Em $K[x]$, escreva $p' = p_0 \dots p_k$, com $p_0, \dots, p_k$ primos de $K[x]$. Para cada $i \leq k$, existe b_i tal que $b_i p_i \in R[x]$. Fixe $a_i \in C(b_i p_i)$ e p_i' primitivo com $b_i p_i = a_i p_i'$. Temos que $b_0 \dots b_k p' = a_0 \dots a_k p_0' \dots p_k'$. Pelo Lema de Gauss, $b_0 \dots b_k$ e $a_0 \dots a_k$ são associados. Existe $u \in R^*$ tal que $u b_0 \dots b_k = a_0 \dots a_k$. Segue que $p' = u p_0' \dots p_k'$, que é um produto de primos de $R[x]$. □

Teorema 9.8.12. Seja R um DFU e K seu corpo de frações. Seja $p = \sum_{i=0}^{n} a_i x^i \in R[x]$. Se existe $\alpha \in R$ irredutível tal que $\alpha \nmid a_n$, $\alpha \mid a_i$ para $i < n$ e $\alpha^2 \nmid a_0$, então p é irredutível em $K[x]$.

Demonstração. Se tal α existe, então $\operatorname{gr} p > 0$. Escreva $p = p'm$, onde $m \in C(p)$ e p' primitivo. Basta ver que p' é irredutível em $R[x]$. Escreva $p' = \sum_{i=0}^{n} a_i' x^i$.

Temos que $a_i = m a_i'$ para todo $i \leq n$. Como $\alpha \nmid m$, temos que $\alpha \nmid a_n'$, $\alpha \mid a_i'$ para $i < n$ e $\alpha^2 \nmid a_0$.

Suponha por absurdo que p' é redutível em $R[x]$. Então $p' = qt$, onde $\operatorname{gr} q = m > 0$ e $\operatorname{gr} r = k > 0$ (pois p' é primitivo).

Escreva $q = \sum_{i=0}^{m} b_i x^i$ e $t = \sum_{i=0}^{k} c_i x^i$.

Temos que $a_0' = b_0 c_0$, logo, $\alpha \mid b_0$ ou $\alpha \mid c_0$. Sem perda de generalidade, vamos supor que $\alpha \mid b_0$. Como $\alpha \nmid {a_0'}^2$, temos que $\alpha \nmid c_0$.

Existe $i \leq n$ tal que $\alpha \nmid b_i$ (caso contrário teríamos que α divide todos os coeficientes de p'). Seja j o primeiro inteiro positivo tal que $\alpha \mid b_i$ para $i < j$.

Temos que $j \leq m < n$, então $\alpha \mid a_j = \sum_{i=0}^{j} c_{j-i} b_i$. Como $\alpha \mid \sum_{i=0}^{j-1} c_{j-i} b_i$, segue que $\alpha \mid c_0 b_j$.

Porém, $\alpha \nmid b_j$ e $\alpha \nmid c_0$, um absurdo. □

9.9 Exercícios

Exercício 9.1. Seja K um corpo. Demonstre, conforme o roteiro abaixo, que o ideal $\langle x - a \rangle$ é maximal no domínio $K[x]$.

a) Considere o homomorfismo avaliação de $K[x]$ em K que avalia $p(x)$ em a. Mostre que o núcleo desse homomorfismo é $\langle x - a \rangle$.

b) Demonstre que $K[x]/\langle x - a \rangle$ é isomorfo a K.

c) Conclua que $\langle x - a \rangle$ é maximal.

Exercício 9.2. Considere o anel de polinômios $K[x, y] = K[x][y]$ e $I = \langle y \rangle$.

- Mostre que I não é um ideal maximal exibindo um ideal próprio que o contém.

- Prove que I não é maximal estudando o quociente $K[x,y]/I$.

Exercício 9.3. Mostre que $\mathbb{R}[x]/\langle x^2+1\rangle$ é isomorfo à $\mathbb{C}$.

Exercício 9.4. Prove que $\mathbb{Z}[x]/\langle x^2+1\rangle$ é isomorfo à $\mathbb{Z}[i]$.

Exercício 9.5. Prove que se R é um domínio de integridade, então $R[\![x]\!]$ é um domínio de integridade.

Exercício 9.6. Considere $R = \mathbb{Z}_4^{\mathbb{N}}$ com a estrutura de anel produto. Seja $a \in R$ dado por $a(n) = 2$ para todo $n \in \mathbb{N}$. Mostre que o polinômio $ax \in R[x]$ possui infinitas raízes.

Exercício 9.7. Prove ou dê um contra-exemplo: os únicos polinômios invertíveis de $\mathbb{Z}_4[x]$ são os polinômios de grau 0 dados por 1 e 3.

Exercício 9.8. Seja K um corpo. Mostre que se $p(x) \in K[x]$ tem grau 2 ou 3, então $p(x)$ é irredutível se, e somente se, não possui raízes em K.

Exercício 9.9. Seja K um corpo. Mostre que $K[x]$ é K-espaço vetorial com a soma usual e o produto por escalar dado pela multiplicação usual de polinômios. Mostre que $(1, x, x^2, \dots)$ é uma base de $K[x]$.

Exercício 9.10. Seja R um anel comutativo. Dado $p = \sum_{i=0}^{n} a_i x^i \in R[x]$ com $n > 0$, define-se a *derivada formal* de p como $p' = \sum_{i=1}^{n} i a_i x^{i-1}$.

1. Mostre que a derivada formal está bem definida.
2. Mostre que $(p+q)' = p' + q'$ para todos $p, q \in R[x]$.
3. Mostre que $(cp)' = cp'$ para todo $c \in R$ e $p \in R[x]$.
4. Mostre que $(pq)' = p'q + pq'$ para todos $p, q \in R[x]$.

Exercício 9.11. Seja R um domínio de integridade. Na notação do exercício anterior, mostre que se $p \in R[x]$, $\alpha \in R$ e $p(\alpha) = 0$, então $(x-\alpha)^2 \mid p$ se, e somente se $p'(\alpha) = 0$.

Exercício 9.12. Seja K um corpo. Mostre que todo $p \in K[x]$ não nulo é primitivo.

Exercício 9.13. Seja R um domínio de integridade e $\alpha \in R$.

1. Mostre que se α é irredutível em R, então α é irredutível em $R[x]$.
2. Mostre que se α é primo em R, então α é primo em $R[x]$.

Exercício 9.14. Mostre que:

1. $x^2 + x + 1$ é irredutível em $\mathbb{Z}_2[x]$.
2. $x^2 + 1$ é irredutível em $\mathbb{Z}_3[x]$.
3. $x^3 - 9$ é irredutível em $\mathbb{Z}_{31}[x]$.
4. $x^3 - 9$ é redutível em $\mathbb{Z}_{11}[x]$.

Exercício 9.15. Mostre que:

1. $x^2 + x + 1$ é irredutível em $\mathbb{Z}_2[x]$.

2. $x^2 + 1$ é irredutível em $\mathbb{Z}_3[x]$.
3. $x^3 - 9$ é irredutível em $\mathbb{Z}_{31}[x]$.
4. $x^3 - 9$ é redutível em $\mathbb{Z}_{11}[x]$.

Exercício 9.16. Verifique se os polinômios abaixo são irredutíveis em $\mathbb{Q}[x]$:

1. $2x^4 - 8x^2 + 1$.
2. $x^4 + 3x + 5$.
3. $3x^4 + 2x^3 + 4x^2 + 5x + 1$.
4. $10x^{11} + 6x^3 + 6$.
5. $x^3 - 3n^2x + n^3$, onde $n \in \mathbb{Z}$.
6. $2x^4 + 4x^2 - 2$.
7. $x^3 - 15x^2 + 10x - 84$.
8. $x^4 + 4x^3 + 6x^2 + 2x + 1$.

Exercício 9.17. Mostre que para todo corpo F, o polinômio $f(x) = x4 + x3 + x + 1 \in F[x]$ não é irredutível em $F[x]$.

Capítulo 10

Extensão de corpos

Neste capítulo, estudaremos o básico da teoria de extensões de corpos, dando como aplicação a resolução de problemas clássicos envolvendo construtibilidade com régua e compasso.

10.1 Definições básicas

Definição 10.1.1. Dizemos que um corpo K estende um corpo L se $L \subseteq K$ e L é um subanel (subcorpo) de K. Escrevemos que K/L é uma extensão de corpos. □

Lembremos que, da álgebra linear, se K, L são corpos e K estende L então K é naturalmente um L-espaço vetorial. Explicitamente:

Proposição 10.1.2. Sejam K um corpo estendendo L. Então K é, com a multiplicação usual, um L-espaço vetorial.

Demonstração. $(K, +)$ é claramente um grupo abeliano. Além disso, se $u, v \in L$ e $a, b \in K$, temos que $u(a + b) = ua + ub$, que $(u + v)a = ua + uv$, que $1a = a$ e que $(uv)a = u(va)$. □

Definição 10.1.3. Na notação anterior, a dimensão de K como L-espaço vetorial é denotada por $[K : L]$. Tal dimensão é chamada de *grau de* F/E. □

Lema 10.1.4. Seja E, F, K corpos com K estendendo F e F estendendo K. Então $[K : E]$ é finito se, e somente se $[K : F]$ e $[F : E]$ são finitos, e, nesse caso, $[K : E] = [K : F][F : E]$.

Demonstração. Primeiro, suponha que $[K : F]$ e $[F : E]$ são finitos. Seja $\mathcal{B} = (b_i : 1 \leq i \leq n)$ uma base de K como F-espaço vetorial e $\mathcal{C} = (c_j : 1 \leq j \leq m)$ uma base de F como E-espaço vetorial.

Seja $\mathcal{D} = (b_i c_j : 1 \leq i \leq n, 1 \leq j \leq m)$. Afirmo que $\mathcal{D}$ é E-base de K.

$\mathcal{D}$ é L.I.: com efeito, sejam $x_{ij} \in E$ tais que $\sum (x_{ij} b_i c_j : 1 \leq i \leq n, 1 \leq j \leq m) = 0$. Então $\sum_{i=1}^{n} \left(\sum_{j=1}^{m} x_{ij} c_j \right) b_i = 0$. Como $\mathcal{B}$ é L.I., cada $\sum_{j=1}^{m} x_{ij} c_j = 0$. Como $\mathcal{C}$ é L.I., cada $x_{ij} = 0$. Portanto, $\mathcal{D}$ é L.I.

$\mathcal{D}$ é gerador: dado $k \in K$, existem $y_1, \ldots, y_n$ tais que $k = \sum_{i=1}^{n} y_i b_i$. Como $\mathcal{C}$ é gerador, existem $x_{ij} \in E$ tais que $y_i = \sum_{j=1}^{m} x_{ij} c_j$ para cada $1 \leq i \leq k$. Portanto, $k = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} x_{ij} c_j \right) b_i = \sum_{i=1}^{n} \sum_{j=1}^{m} x_{ij} c_j b_i$, o que mostra que $\mathcal{D}$ é gerador.

Note que $\mathcal{D}$ é uma família de tamanho $mn = [K : F][F : E]$.

Reciprocamente, suponha que $[K : E]$ é finito. Como F é um subespaço de K como E-espaço vetorial, temos que $[F : E] \leq [K : E]$. Ademais, uma base de K como E-espaço vetorial é um gerador de K como F-espaço vetorial, e, assim, esta contém uma base (finita). Logo, $[K : F] \leq [K : E]$. □

Definição 10.1.5. Seja F um corpo estendendo E e $a \in F$. Dizemos que $a \in F$ é um elemento algébrico sobre E se existe um polinômio não nulo $p \in E[x]$ tal que $p(a) = 0$. Caso contrário, a é dito transcendente sobre E. □

Exemplo 10.1.6. Todo elemento de $a \in E$ é algébrico sobre E, pois é raiz de $x - a$. □

Exemplo 10.1.7. Considere $\mathbb{Q} \subseteq \mathbb{C}$. Temos que i é algébrico sobre $\mathbb{Q}$, pois é raiz de $x^2 + 1$. □

Exemplo 10.1.8. Se K é um corpo, seja $K(x)$ o corpo de frações do domínio $K[x]$. Identificando $K \subseteq K[x] \subseteq K(x)$, temos que $x \in K(x)$ é transcendente sobre K. □

Definição 10.1.9. Seja F uma extensão de um corpo E e $A \subseteq F$.
Define-se $E[A]$ como sendo o menor subanel de F contendo E e A.
Define-se $E(A)$ como sendo o menor subcorpo de F contendo E e A.
Se $A = \{a_1, \ldots, a_n\}$, escrevemos $E[a_1, \ldots, a_n]$ e $E(a_1, \ldots, a_n)$, respectivamente. □

É claro que precisamos ver que $E[A]$ e $E(A)$ estão bem definidos.

Lema 10.1.10. Seja F uma extensão de um corpo E e $a \in F$. Então $E[A]$ e $E(A)$ estão bem definidos.

Demonstração. Lembremos que a interseção de subanéis é um subanel, e que a interseção de subcorpos é um subcorpo. Assim, sejam:

$$E[A] = \bigcap \{K \subseteq F : K \text{ é subanel de } E \text{ e } A \cup EK\}$$

$$E(A) = \bigcap \{K \subseteq F : K \text{ é subcorpo de } E \text{ e } A \cup EK\}$$

Segue que $E[A]$ e $E(A)$ são, respectivamente, um subanel e um subcorpo de F contendo E e a. É claro que se K é outro subanel (subcorpo) de F contendo E e a, então $K \subseteq E[A]$ (ou $K \subseteq E(A)$).

Se L é outro subanel mínimo dentre os subanéis que contém E e A, então $L \subseteq E[A]$ pela definição de $E[A]$, e $L \supseteq E[A]$ pela definição de L.

Analogamente, se L é outro subcorpo mínimo dentre os subcorpos que contém E e A, então $L \subseteq E(A)$ pela definição de $E(A)$, e $L \supseteq E(A)$ pela definição de L. □

Observação: na definição acima, $E[A]$ e $E(A)$ dependem também de F, apesar de tal fato não estar explícito na notação.

Lema 10.1.11. Seja F/E uma extensão de corpos e $A, B \subseteq F$. Então $E[A \cup B] = E[A][B]$ e $E(A \cup B) = E(A)(B)$

Demonstração. Temos que $E[A \cup B]$ é o menor subanel de F que contém E e $A \cup B$. Temos que $E[A][B]$ contém $E[A]$ e B, logo, contém E, A e B, assim, $E[A \cup B] \subseteq E[A][B]$.

Reciprocamente, $E[A][B]$ é o menor subanel de F que contém $E[A]$ e B. Temos que $E[A] \subseteq E[A \cup B]$, pois $E[A \cup B]$ contém E e A, e $E[A][B]$ contém B, logo, $E[A][B] \subseteq E[A \cup B]$.

Analogamente, $E(A \cup B) = E(A)(B)$. □

Lema 10.1.12. Seja F/E uma extensão de corpos e C um gerador de F/E. Então $F = \bigcup\{E(A) : A \in [C]^{<\infty}\}$. Analogamente, $E[C] = \bigcup\{E[A] : A \in [C]^{<\infty}\}$.

Demonstração. Se $A, B \subseteq C$ são finitos, então $E(A) \cup (B) \subseteq E(A \cup B)$. Logo, $K = \{E(A) : A \in [C]^{<\infty}\}$ é uma união dirigida de corpos, e, portanto, um corpo.

Como cada $E(A)$ com $A \in [C]^{<\infty}$ é tal que $E(A) \subseteq E(C)$, então $K \subseteq F = E(C)$. Por outro lado, para todo $c \in C$, temos que $c \in E(c) \subseteq E(C)$. Assim, $E(C) \subseteq K$.

A outra afirmação é similar. □

Lema 10.1.13. Seja F/E uma extensão de corpos e $a \in F$. Então $E[a] = \{p(a) : p \in E[x]\}$.

Demonstração. Temos que $\{p(a) : p \in E[x]\}$ é a imagem de $E[x]$ pela avaliação em a, e, portanto, é um subanel de F que claramente contém E e A. Pela definição de $p(a)$, é imediato que qualquer subanel de F que contém E e a também contém $\{p(a) : p \in E[x]\}$. □

Definição 10.1.14. Dizemos que uma extensão F/E é gerada por $A \subseteq F$ se $F = E(A)$.

Dizemos que F/E é finitamente gerada e existe $A \subseteq F$ finito tal que $F = E(A)$.

Finalmente, dizemos que F/E é de grau finito se $[F : E]$ é finito. □

10.2 Extensões algébricas

Nesta seção, discutiremos extensões e elementos algébricos, mencionando elementos transcendentes conforme necessário.

Definição 10.2.1. Seja E um corpo. Uma extensão algébrica de E é um corpo F contendo E tal que todo elemento de F é algébrico sobre E. □

Proposição 10.2.2. Seja F um corpo estendendo E e $a \in F$ um elemento algébrico de E. Então:

1. $\{p \in E[x] : p(a) = 0\}$ é um ideal maximal de $E[x]$.
2. $\{p \in E[x] : p(a) = 0\}$ possui um único gerador mônico q, e este é o único polinômio mônico irredutível que anula a.
3. $E[a] = E(a)$.
4. $E[a] \approx E[x]/(q)$.

Demonstração. Seja $I = \{p \in E[x] : p(a) = 0\}$. I é o núcleo da avaliação em a, e, portanto, é um ideal de $E[x]$. Pelo primeiro teorema do isomorfismo, $E[x]/I$ é isomorfo à $E[a]$, que é um subanel de um corpo, e, portanto, um domínio de integridade. Logo, I é primo. Como I é também não nulo, I é maximal. Logo, $E[x]$ é um corpo, e este é o menor subanel de F contendo E e a, logo, é também o menor subcorpo.

Seja q um gerador de I, que podemos supor ser mônico, pois I é um ideal. Ele é irredutível, pois $I = (q)$ é primo não nulo, e, portanto, q é primo. Se p é um polinômio irredutível que anula a, temos que $p = qx$ para algum $x \in E[x]$. Como p é irredutível, $q \in E$ ou $x \in E$. Como $q \notin E$, temos que $x \in E$, e, assim, o coeficiente dominante de p é o de qx, que é x, logo, $x = 1$. □

Corolário 10.2.3. Sejam F/E e F'/E extensões de corpos. Seja $p \in E[x]$ um polinômio irredutível para o qual $p(a) = 0$ e $p(b) = 0$, com $a \in F$ e $b \in F'$. Então $E[a]$ e $E[b]$ são isomorfos.

Demonstração. Seja q um polinômio mônico associado à p. Temos que $(p) = (q)$. Logo, $E[a] \approx E[x]/(p) \approx E[b]$. □

Proposição 10.2.4. Seja F uma extensão de um corpo E e $a \in F$ um elemento algébrico sobre E. Então $[E[a] : E]$ é o grau do único polinômio mônico irredutível que anula a, e uma base é $(1, a, \ldots, a^{n-1})$, onde $n = [E[a] : E]$.

Demonstração. Temos que $(1, a, \ldots, a^{n-1})$ é L.I., pois se $t_0, \ldots, t_{n-1} \in E$ tais que $t_0 + t_1 a + \cdots + t_{n-1}a^{n-1} = 0$, sendo $p(x) = t_0 + t_1 x + \cdots + t_{n-1}x^{n-1}$, temos que $p(a) = 0$. Como $\operatorname{gr} p < n$, o único modo de termos $p(a) = 0$ é com $p = 0$. Logo, $t_0 = t_1 = \cdots = t_{n-1} = 0$.

Agora seja $z \in E[a]$ um elemento arbitrário. Ele é da forma $z = p(a)$, com $p \in E[x]$. Seja q o único polinômio mônico irredutível que anula a. Então $p = qa + r$ para alguns $r, a \in E[x]$ com $\operatorname{gr} r < \operatorname{gr} q$

Logo, $z = p(a) = q(a)r(a) + r(a) = r(a)$. Sendo $r(x) = t_0 + t_1 x + \cdots + t_{n-1}x^{n-1}$, temos que $z = r(a) = t_0 + t_1 a + \cdots + t_{n-1}a^{n-1} \in \operatorname{span}(1, a, \ldots, a^{n-1})$.

□

Proposição 10.2.5. Seja F/E uma extensão de corpos de grau finito. Então F/E é algébrica e finitamente gerada.

Demonstração. Seja $n = [F : E]$ e $a \in F/E$. Então $(1, a, a^2, \ldots, a_n)$ é LD, logo existem $a_0, \ldots, a_n \in E$, não todos nulos, tais que $a_0 + a_1 a + \cdots + a_n a^n = 0$, sendo $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, temos que $p(a) = 0$. Assim, a é algébrico sobre E.

Seja $(b_1, \ldots, b_n)$ uma base de F como E-espaço vetorial. Então $F = E[b_1, \ldots, b_n]$, logo, F/E é finitamente gerada. □

Corolário 10.2.6. Seja F/E uma extensão e $a \in F$ um elemento algébrico sobre E. Então $E(a)/E$ é uma extensão algébrica.

Demonstração. Segue da proposição anterior, pois $E(a)/E$ tem grau finito. □

Uma recíproca parcial vale:

Proposição 10.2.7. Seja F/E uma extensão algébrica. São equivalentes:

(i) F/E é finitamente gerada.

(ii) F/E tem grau finito.

Demonstração. Já vimos que (ii) implica (i). Basta ver que (i) implica (ii).

Provaremos a proposição por indução no número de geradores de $F = E(a_1, \ldots, a_n)$.

Se $F = E(\emptyset)$, temos que $F = E$. Se $F = E(a)$, vimos que $[E(a) : E]$ é o grau do polinômio mônico irredutível que anula a. Logo, F/E é de grau finito.

Suponha que a tese vale para n geradores. Então vale para $n + 1$:

Temos que $F = E(a_1, \ldots, a_n, a_{n+1}) = E(a_1, \ldots, a_n)(a_{n+1})$. Por hipótese de indução, temos que $[E(a_1, \ldots, a_n) : E]$ é finito, e, como no caso $n = 1$, $[E(a_1, \ldots, a_n)(a_{n+1}) : E(a_1, \ldots, a_n)]$ é finito. Logo, $[F : E] = [E(a_1, \ldots, a_n) : E][E(a_1, \ldots, a_n)(a_{n+1}) : E(a_1, \ldots, a_n)]$ é finito. □

Proposição 10.2.8. Seja F/E uma extensão de corpos e $A \subseteq F$ uma coleção de elementos algébricos sobre E. Então $E[A] = E(A)$ e $E(A)/E$ é uma extensão algébrica.

Demonstração. Primeiro, provaremos a proposição para A finito por indução no número de elementos de A.

Temos que $E[\emptyset] = E(\emptyset) = E$ e E/E é uma extensão algébrica.

Para o passo indutivo, suponha que a tese vale para conjuntos A de n elementos. Mostraremos que valem para A de $n + 1$ elementos.

Seja $A \subseteq F$ com $n+1$ elementos e seja $B = A \setminus \{a\}$, onde $a \in A$ é arbitrário. Por hipótese de indução, $E[B] = E(B)$. Seja $L = E(B)$. Como a é algébrico sobre E, então a é algébrico sobre L. Assim, $E[A] = E[B][a] = L[a] = L(a) = E(B)(a) = E(A)$.

Além disso, $[E(B) : E]$ é finito por hipótese de indução, e $[E(A) : E(B)]$ é finito, logo $[E(A) : E]$ é finito.

Resta provar o teorema caso A seja infinito. Temos que $E(A) = \bigcup\{E(B) : B \in [A]^{<\infty}\} = \bigcup\{E[B] : B \in [A]^{<\infty}\} = E[A]$.

$E(A)$ é uma extensão algébrica, pois dado $b \in E(A)$, existe $B \in [A]^{<\infty}$ tal que $b \in E(B)$, e $E(b)$ é uma extensão algébrica. □

Proposição 10.2.9. Seja F/K e K/E extensões de corpos. Então F/E é uma extensão algébrica se, e somente se F/K e K/E são extensões algébricas.

Demonstração. Suponha que F/E é uma extensão algébrica. Então F/K é uma extensão algébrica, pois $E[x] \subseteq K[x]$, e K/F é uma extensão algébrica, pois $K \subseteq F$.

Reciprocamente, suponha que F/K e K/E são extensões algébricas. Fixe $a \in F$. Temos que existem $k_0, \ldots, k_n \in K$ tais que $k_0 + k_1 a + \cdots + k_n a^n = 0$. Como K/E é algébrica, sendo $A = \{k_0, \ldots, k_n\}$, temos que $E(A)$ é uma extensão algébrica e finitamente gerada de E, e, portanto, tem dimensão finita $[E(A) : E]$. Como $k_0, \ldots, k_n \in E(A)$, temos que a é algébrico sobre $E(A)$, e, portanto, $[E(A)(a) : E(A)]$ é finito. Logo, $[E(A)(a) : E]$ é finito, o que implica que a é algébrico sobre E. □

Proposição 10.2.10. Seja F/E uma extensão de corpos e K o conjunto dos elementos algébricos de F sobre E. Então K é um corpo e todo elemento de $F \setminus K$ é transcendente sobre K (em outras palavras, todo elemento algébrico sobre K está em K).

Demonstração. Temos que $1 \in K$. Se $a, b \in K$ e $b \neq 0$, então $E(a, b)$ é uma extensão algébrica de E, e $a - b, ab, b^{-1} \in E(a, b)$, logo, $a - b, ab, b^{-1} \in K$.

Assim, K é um subcorpo de F.

Se $a \in F$ é algébrico sobre K, então $a \in K$: temos que $K(a)/K$ é uma extensão algébrica, e K/F é uma extensão algébrica, logo, $K(a)/F$ é uma extensão algébrica. Como $a \in K(a)$, temos que a é algébrico sobre F, e, portanto, $a \in K$. □

10.3 Elementos transcendentes

Como uma interseção arbitrária de subcorpos é um subcorpo, $E(a)$ está bem definido e vale que $E[a] \subseteq E(a)$. Vimos que se a é algébrico sobre E, então $E(a) = E[a]$. Abaixo, caracterizaremos $E(a)$ quando a é transcendente sobre E.

Proposição 10.3.1. Seja F uma extensão de um corpo E e $a \in F$ um elemento transcendente sobre E. Então $E(a) = \{p(a)q(a)^{-1} : p, q \in E[x], q \neq 0\}$ é isomorfo à $\mathrm{Frac}(E[x])$.

Demonstração. Seja $h : E[x] \to E(a)$ a avaliação em a. Temos que h é um homomorfismo injetor, logo, existe um único homomorfismo injetor $g : \mathrm{Frac}(E(x)) \to E(a)$ tal que $g(p/1) = h(p) = p(a)$ para todo $p \in E[x]$.

Conforme estudado, $g(p/q) = h(p)h(q)^{-1}$ para todo $p, q \in E[x]$ com $q \neq 0$. Logo, a imagem de g é $\{p(a)q(a)^{-1} : p, q \in E[x], q \neq 0\}$, que é um subanel de $E(a)$ isomorfo a $\mathrm{Frac}(E[x])$, e, portanto, um subcorpo de $E(a) \subseteq F$. Como $E(a)$ é o menor subcorpo de F contendo E e a, temos que $E(a) = \{p(a)q(a)^{-1} : p, q \in E[x], q \neq 0\}$. □

10.4 Construtibilidade com Régua e Compasso

Definição 10.4.1. Se $p \in \mathbb{R}^2$ e $s > 0$, denotamos por $\text{circ}(p, s) = \{a \in \mathbb{R}^2 : \|p - a\| = s\}$.

Se $p, q \in \mathbb{R}^2$ com $p \neq q$, denotamos por $\text{reta}(p, q) = \{p + t(q - p) : t \in \mathbb{R}\}$ a única reta que passa por p e q.

Finalmente, se $C \subseteq \mathbb{R}^2$, define-se $\text{dist}(C) = \{\|a - b\| : a, b \in C, a \neq b\}$. □

A definição a seguir será utilizada apenas nesta seção.

Definição 10.4.2. Seja $\mathbb{P}_0 = \{(0, 0), (1, 0)\}$. Definido $\mathbb{P}_n$, definimos $\mathbb{P}_{n+1}$ como sendo o conjunto dos pontos $p \in \mathbb{R}^2$ que satisfazem uma das seguintes condições:

- $p \in \mathbb{P}_n$.
- $p \in \text{reta}(a, b) \cap \text{reta}(c, d)$, onde $\text{reta}(a, b) \neq \text{reta}(c, d)$ e $a, b, c, d \in \mathbb{P}_n$ com $a \neq b$ e $c \neq d$.
- $p \in \text{circ}(a, s) \cap \text{circ}(a', s')$, onde $a, a' \in \mathbb{P}_n$ com $a \neq a'$ e $s, s' \in \text{dist}\, \mathbb{P}_n$
- $p \in \text{circ}(a, s) \cap \text{reta}(b, c)$, onde $a, b, c \in \mathbb{P}_n$ com $b \neq c$ e $s \in \text{dist}\, \mathbb{P}_n$.

Seja $\mathbb{P} = \bigcup_{n \in \mathbb{N}} \mathbb{P}_n$. Seja $\mathbb{K} = \{x \in \mathbb{R} : (x, 0) \in \mathbb{P}\}$. □

Lema 10.4.3. $(0, 1), (1, 1) \in \mathbb{P}$.

Demonstração. Temos que $1 \in \text{dist}(\mathbb{P}_0)$, $\text{reta}((0, 0), (1, 0)) \cap \text{circ}((0, 0), 1) = \{(-1, 0), (1, 0)\}$ e $\text{reta}((0, 1), (1, 0)) \cap \text{circ}((1, 0), 1) = \{(0, 0), (2, 0)\}$. Logo, $(2, 0), (0, 1) \in \mathbb{P}_1$ e $2 \in \text{dist}(\mathbb{P}_1)$.

Temos que $(0, \sqrt{3}) \in \text{circ}((-1, 0), 2) \cap \text{circ}((1, 0), 2)$, logo, $(0, \sqrt{3}) \in \mathbb{P}_2$.

Agora note que $(0, 1) \in \text{circ}((0, 0), 1) \cap \text{reta}((0, 0), (0, \sqrt{3}))$ e que $(1, 1) \in \text{circ}((1, 0), 1) \cap \text{circ}((0, 1), 1)$. □

Lema 10.4.4. Se $(x, y) \in \mathbb{P}$, então $(y, x) \in \mathbb{P}$.

Demonstração. Suponha que $(x, y) \in \mathbb{P}$.

Tome n tal que $(x, y), (1, 1) \in \mathbb{P}_n$.

Primeiramente, suponha que $x + y \neq 0$. Seja $s = \|(x, y)\| \neq 0$. Note que $(x + y, x + y) \in \text{reta}((0, 0), (1, 1)) \cap \text{circ}((x, y), s)$ e que $(y, x) \in \text{circ}((x + y, x + y), s) \cap \text{circ}((0, 0), s)$.

Caso $x = -y \neq 0$, seja $s = \|(x, y)\| \neq 0$. Então $(y, x) \in \text{reta}((0, 0), (x, y)) \cap \text{reta}(0, 0, (x, y))$.

Caso $x = -y = 0$, é trivial. □

Lema 10.4.5. Se $(x, y) \in \mathbb{P}$, então $(x, 0), (0, y) \in \mathbb{P}$.

Demonstração. Sem perda de generalidade, podemos supor que $x, y \neq 0$. Seja $s = \|(x, y)\|$. Então $(2x, 0) \in \text{circ}((x, y), s) \cap \text{reta}((0, 0), (1, 0))$ e $(0, 2y) \in \text{circ}((x, y), s) \cap \text{reta}((0, 0), (0, 1))$. Daí, $(x, -y) \in \text{circ}((0, 0), s) \cap \text{circ}((2x, 0), s)$ e $(-x, y) \in \text{circ}((0, 0), s) \cap \text{circ}((0, 2y), s)$. Finalmente, $(x, 0) \in \text{reta}((x, -y), (x, y)) \cap \text{reta}((0, 0), (1, 0))$ e $(0, y) \in \text{reta}((-x, y), (0, y)) \cap \text{reta}((0, 0), (0, 1))$. □

Proposição 10.4.6. Sejam $x, y \in \mathbb{R}$. São equivalentes:

(i) $(x, y) \in \mathbb{P}$.

(ii) $x, y \in \mathbb{K}$.

(iii) $|x|, |y| \in \text{dist}\, \mathbb{P} \cup \{0\}$.

Demonstração. (i) $\Rightarrow$ (ii): seja $p = (x, y) \in \mathbb{P}$. Fixe n tal que $(x, y) \in \mathbb{P}_n$. É claro que $x \in \mathbb{K}$. Como $(y, x) \in \mathbb{P}$, segue que $y \in \mathbb{K}$.

Caso 1: $x = 0$. Nesse caso, $y = \|(0, 0) - (0, y)\| \in \text{dist}()\,\text{circ}((0, 0), (0, y))$

(ii) $\Rightarrow$ (i): existem u, v com $(x, v), (u, y) \in \mathbb{P}$. Logo, $(x, 0)$ e $(0, y)$ estão em $\mathbb{P}$. Se $x = 0$ ou $y = 0$, segue a tese. Caso contrário, $|x|, |y| \in \text{dist}(\mathbb{P})$. Finalmente, note que $(x, y) \in \text{circ}((x, 0), |y|) \cap \text{circ}((0, y), |x|)$.

(iii) $\Rightarrow$ (ii): Se $x, y \neq 0$, temos que $(x, 0) \in \circ((0, 0), |x|) \cap \text{reta}((0, 0), (1, 0))$ e $(0, y) \in \text{circ}((0, 0), |y|) \cap \text{reta}((0, 0), (0, 1))$.

(ii) $\Rightarrow$ (iii): Se $x = 0$, então $x \in \mathbb{K}$. Se $|x| \in \text{dist}\,\mathbb{P}$, então $(x, 0) \in \text{circ}((0, 0), |x|) \cap \text{reta}((0, 0), (1, 0))$, logo $x \in \mathbb{K}$. □

Proposição 10.4.7. $\mathbb{K}$ é um subcorpo de $\mathbb{R}$ fechado por raízes quadradas de números não negativos.

Demonstração. Temos que $1, 0 \in \mathbb{K}$.

Se $a, b \in \mathbb{K}$ e $a > b$, então $a-b, b-a \in \mathbb{K}$: temos que $(a, 0), (b, 0) \in \mathbb{P}$, então $b-a \in \text{dist}(\mathbb{P}) \subseteq \mathbb{K}$, e $(a - b, 0) \in \text{circ}((0, 0), b - a) \cap \text{reta}((0, 0), (1, 0))$.

Note que isso implica que se $a, b \in \mathbb{K}$, então $b - a \in \mathbb{K}$. Em particular, $-a \in \mathbb{K}$.

Se $a, b \in \mathbb{K}$ e $b \neq 0$, então $1 - b \in \mathbb{K}$, e, portanto, $(a, 1 - b) \in \mathbb{P}$. Note que $\text{reta}((0, 0), (1, 0)) \cap \text{reta}((0, 1), (a, 1 - b)) = \{(\frac{a}{b}, 0)\}$, logo, $\frac{a}{b} \in \mathbb{K}$.

Se $a, b \in \mathbb{K}$, então $ab \in \mathbb{K}$: se $b = 0$, $ab = 0 \in \mathbb{K}$. Se $b \neq 0$, temos que $\frac{1}{b} \in \mathbb{K}$, logo, $\frac{a}{\frac{1}{b}} = ab \in \mathbb{K}$.

Finalmente, se $a \geq 0 \in \mathbb{K}$, então sendo $l = \frac{c+1}{2}$, temos que $(1, \sqrt{c}) \in \text{circ}((l, 0), l) \cap \text{reta}((1, 0), (1, 1))$, pois $(1, 0) + \sqrt{c}((1, 1) - (1, 0)) = (1, \sqrt{c})$, e $(l - 1)^2 + (\sqrt{c})^2 = l^2 - 2l + 1 + c = l^2 - c - 1 + 1 + c = l^2$. Assim, $\sqrt{c} \in \mathbb{K}$. □

Proposição 10.4.8. $\mathbb{K}$ é o menor subcorpo de $\mathbb{R}$ fechado por raízes quadradas de números não negativos.

Demonstração. Devemos ver que se L é um subcorpo de $\mathbb{R}$ tal que para todo $c \in \mathbb{K}$, se $c \geq 0$ então $\sqrt{c} \in \mathbb{K}$, então $\mathbb{K} \subseteq \mathbb{L}$.

Devemos ver que para todo $(x, y) \in \mathbb{P}$, $x \in L$. Para tanto, mostraremos que para todo n e para todo $(x, y) \in \mathbb{P}_n$, $x \in L$.

Temos que $\mathbb{P}_0 = \{(0, 0), (1, 0)\}$. Como $0, 1 \in L$, a tese vale para a base $n = 0$.

Suponha que a tese vale para n. Veremos que vale para $n + 1$.

Seja $(x, y) \in \mathbb{P}_{n+1}$.

Caso 1: $(x, y) \in \mathbb{P}_n$. Nesse caso, $x \in L$ por hipótese de indução.

Caso 2: $(x, y) \in \text{reta}(a, b) \cap \text{reta}(c, d)$, onde $\text{reta}(a, b) \neq \text{reta}(c, d)$ e $a, b, c, d \in \mathbb{P}_n$ com $a \neq b$ e $c \neq d$. Por hipótese, as coordenadas de a, b, c, d estão em L.

Nesse caso, existem $s, t \in \mathbb{R}$ tal que $(x, y) = a + tb = c + sd$, e, portanto, $a + tb = c + sd$. Escrevendo $a = (a_1, a_2)$, $b = (b_1, b_2)$,$c = (c_1, c_2)$,$d = (d_1, d_2)$, temos o sistema linear em s, t:

$$\begin{pmatrix} d_1 & -b_1 \\ d_2 & -b_2 \end{pmatrix} \begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} a_1 - c_1 \\ a_2 - c_2 \end{pmatrix}$$

Como tal sistema tem solução, temos que s, t se escrevem como uma combinação de números racionais com $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2$, o que é um elemento de L. Logo, como $(x, y) = a + tb$, segue que $x, y \in L$.

Caso 3: $(x, y) \in \text{reta}(a, b) \cap \text{circ}(c, s)$, onde $a, b \in \mathbb{P}_n$ com $a \neq b$ e $c \in \mathbb{P}_n$ com $s \in \text{dist}(\mathbb{P}_n)$. Sejam $a = (a_1, a_2)$, $b = (b_1, b_2)$ e $c = (c_1, c_2)$.

Nesse caso, existe $t \in \mathbb{R}$ tal que $(x, y) = a + tb$ e $\|a + tb - c\| = s$. Isso ocorre se, e somente se $(a_1 + tb_1 - c_1)^2 + (a_2 + tb_2 - c_2)^2 = s^2$. Da fórmula quadrática, t, que existe, é uma combinação de somas, diferenças, produtos e raízes quadradas de $a_1, b_1, c_1, a_2, b_2, c_2, s^2$, que são todos, por hipótese de indução, elementos de L. Logo, $t \in L$. Assim, $x = a_1 + tb_1 \in L$.

Caso 4: $(x, y) \in \text{circ}(a, s) \cap \text{circ}(b, s')$, onde $a, b \in \mathbb{P}_n$ com $a \neq b$ e $s, s' \in \text{dist}(\mathbb{P}_n)$. Sejam $a = (a_1, a_2)$ e $b = (b_1, b_2)$. Nesse caso, $(x - a_1)^2 + (y - a_2)^2 = s^2$ e $(x - b_1)^2 + (y - b_2)^2 = s'^2$. Novamente, tais equações são resolvíveis pela fórmula quadrática, e com ela conclui-se que $x, y \in L$. □

Lema 10.4.9. $\mathbb{K} = \bigcup_{n\in\mathbb{N}} K_n$, onde $(K_n : n \in \mathbb{N})$ é a sequência de conjuntos definida recursivamente por $K_0 = \{1\}$ e $K_{n+1} = K_n \cup \{a - b, ab, a^{-1} : a, b \in K_n\} \cup \{b^{-1} : b \in K_n \setminus \{0\}\} \cup \{\sqrt{b} : b \geq 0, b \in \mathbb{K}_n\}$.

Demonstração. Por indução, em m, vemos que para todo m, n com $m \leq n$, $K_m \subseteq K_n$.

Também por indução, vemos que se L é um subcorpo de $\mathbb{R}$ fechado por raízes quadradas de números não negativos, então para todo $n \in \mathbb{N}$, $K_n \subseteq L$.

Resta ver que $K = \bigcup_{n\in\mathbb{N}} K_n$ é um subcorpo de $\mathbb{R}$. Para tanto, note que $1 \in K$. Se $b \in K \setminus \{0\}$, então existe $n \in K$ tal que $b \in K_n$. Logo, $b^{-1} \in K_{n+1}$. Similarmente, se- $b \geq 0$ e $b \in K$, então, $\sqrt{b} \in K$. Finalmente, se $a, b \in K$, existem n, m com $a \in K_n$ e $b \in K_m$. Sendo $k = \max(n, m)$, temos que $a - b, ab \in K_{k+1}$. □

Proposição 10.4.10. Todo elemento de $\mathbb{K}$ tem grau sobre $\mathbb{Q}$ igual a 2^i para algum $i \in \mathbb{N}$. Mais especificamente, se $a \in \mathbb{K}$, então existem $(a_0, \ldots, a_n) \in \mathbb{K}$ com $a = a_n$, com $[\mathbb{Q}(a_0) : \mathbb{Q}] \in \{1, 2\}$ e $[\mathbb{Q}(a_0, \ldots, a_i)(a_{i+1}) : \mathbb{Q}(a_0, \ldots, a_i)] \in \{0, 1\}$ para todo $i < n$.

Demonstração. Primeiro, note que a primeira parte da proposição é implicada pela segunda, já que dado $a \in \mathbb{K}$, se existem $a_0, \ldots, a_n \in \mathbb{K}$ com $a = a_n$, com $[\mathbb{Q}(a_0) : \mathbb{Q}] \in \{1, 2\}$ e $[\mathbb{Q}(a_0, \ldots, a_i)(a_{i+1}) : \mathbb{Q}(a_0, \ldots, a_i)] \in \{1, 2\}$ para todo $i < n$, então $[\mathbb{Q}(a_0, \ldots, a_n) : \mathbb{Q}]$ é uma potência de 2, e $[\mathbb{Q}(a) : \mathbb{Q}]$ divide esta potência, sendo também, portanto, uma potência de 2.

Para provar a segunda afirmação, procederemos por indução em n para mostrar que para todo $a \in K_n$, existem $a_0, \ldots, a_n \in K_n$ com $a = a_n$, com $[\mathbb{Q}(a_0) : \mathbb{Q}] \in \{1, 2\}$ e $[\mathbb{Q}(a_0, \ldots, a_i)(a_{i+1}) : \mathbb{Q}(a_0, \ldots, a_i)] \in \{1, 2\}$ para todo $i < n$.

Base: que $K_0 = \{1\}$, e $[\mathbb{Q}(1) : \mathbb{Q}] = 1$. Considere a sequência unitária (1).

Passo indutivo: suponha que a hipótese é válida para n. Mostraremos que ela é válida para $n + 1$.

Seja $c \in K_{n+1}$. Se $a \in K_n$, segue da hipótese indutiva.

Caso $c = a - b$ ou $c = ab$, com $a, b \in K_n$, por hipótese indutiva, existem $a_0, \ldots, a_n \in K_n$ com $a = a_n$, com $[\mathbb{Q}(a_0) : \mathbb{Q}] \in \{1, 2\}$ e $[\mathbb{Q}(a_0, \ldots, a_i)(a_{i+1}) : \mathbb{Q}(a_0, \ldots, a_i)] \in \{1, 2\}$ para todo $i < n$. Similarmente para b, existem $b_0, \ldots, b_m \in K_n$ com $b = b_m$, com $[\mathbb{Q}(b_0) : \mathbb{Q}] \in \{1, 2\}$ e $[\mathbb{Q}(b_0, \ldots, b_i)(b_{i+1}) : \mathbb{Q}(b_0, \ldots, b_i)] \in \{1, 2\}$ para todo $i < m$.

Considere $(a_0, \ldots, a_n, b_0, \ldots, b_m, c)$. Temos que $[\mathbb{Q}(a_0, \ldots, a_n)(b_0) : \mathbb{Q}(a_0, \ldots, a_n)]$ é o menor grau de um polinômio não nulo com coeficientes em $\mathbb{Q}(a_0, \ldots, a_n)$ que anula b_0. Ora, como $[\mathbb{Q}(b_0) : \mathbb{Q}]$ é 1 ou 2, segue que $[\mathbb{Q}(a_0, \ldots, a_n)(b_0) : \mathbb{Q}(a_0, \ldots, a_n)]$ também é 1 ou 2. Similarmente, $[\mathbb{Q}(a_0, \ldots, a_n, b_0, \ldots, b_{j+1}) : \mathbb{Q}(a_0, \ldots, a_n, b_0, \ldots, b_j)]$ é 1 ou 2. Finalmente, note que $[\mathbb{Q}(a_0, \ldots, a_n, b_0, \ldots, b_m)(c) : \mathbb{Q}(a_0, \ldots, a_n, b_0, \ldots, b_m)] = 1$, pois $c \in \mathbb{Q}(a_0, \ldots, a_n, b_0, \ldots, b_m)$.

Se $c = a^{-1}$ (ou $c = \sqrt{a}$), com $a \in K_n \setminus \{0\}$ (respectivamente, $\sqrt{a} = c$). Por hipótese indutiva, existem $a_0, \ldots, a_n \in K_n$ com $a = a_n$, com $[\mathbb{Q}(a_0) : \mathbb{Q}] \in \{1, 2\}$ e $[\mathbb{Q}(a_0, \ldots, a_i)(a_{i+1}) : \mathbb{Q}(a_0, \ldots, a_i)] \in \{1, 2\}$ para todo $i < n$. Considere $a_{n+1} = a^{-1}$. Então, caso $c = a^{-1}$ $[\mathbb{Q}(a_0, \ldots, a_n)(a_{n+1}) : \mathbb{Q}(a_0, \ldots, a_n)] = 1$, pois $a_{n+1} \in \mathbb{Q}(a_0, \ldots, a_n)$, e, caso $c = \sqrt{a}$, temos que $x^2 - a$ anula c, logo $[\mathbb{Q}(a_0, \ldots, a_n)(a_{n+1}) : \mathbb{Q}(a_0, \ldots, a_n)]$ é 1 ou 2. □

Definição 10.4.11. Dizemos que um ângulo α é construtível com régua e compasso se existem $a, b, c \in \mathbb{P}$ tais que a medida do ângulo $\angle abp$ é α. □

Da geometria analítica, temos o seguinte.

Proposição 10.4.12. Um ângulo α é construtível com régua e compasso se, e somente se o ponto $(\cos\alpha, \sin\alpha)$ é construtível.

Disso, segue a seguinte proposição.

Proposição 10.4.13. Um ângulo α é construtível com régua e compasso se, e somente se $\cos\alpha \in \mathbb{K}$.

Demonstração. Se $\cos\alpha \in \mathbb{K}$, temos que $\sin\alpha = \sqrt{1-(\cos\alpha)^2}$ ou $\sin\alpha = -\sqrt{1-(\cos\alpha)^2}$. Ambos esses números estão em $\mathbb{K}$. □

Proposição 10.4.14. É impossível trissectar, com régua e compasso, um ângulo de 60 graus $(\pi/3)$.

Demonstração. Da trigonometria, sabemos que para todo θ, θ', temos que:

$$\cos(\theta+\theta') = \cos(\theta)\cos(\theta') - \sin(\theta)\sin(\theta')$$
$$\sin(\theta+\theta') = \sin(\theta)\cos(\theta') + \cos(\theta)\sin(\theta').$$

Pondo $\theta' = 2\theta$ na primeira equação, segue que:

$$\begin{aligned}
\cos(3\theta) &= \cos(\theta)\cos(2\theta) - \sin(\theta)\sin(2\theta)\\
&= \cos(\theta)(\cos^2(\theta) - \sin^2(\theta)) - \sin(\theta)(2\sin(\theta)\cos(\theta))\\
&= \cos(\theta)(\cos^2(\theta) - \sin^2(\theta) - 2\sin^2(\theta))\\
&= \cos(\theta)(\cos^2(\theta) - 3\sin^2(\theta))\\
&= \cos(\theta)(\cos^2(\theta) - 3(1-\cos^2(\theta)))\\
&= \cos(\theta)(4\cos^2(\theta) - 3)\\
&= 4\cos^3(\theta) - 3\cos(\theta).
\end{aligned}$$

Pondo $\theta = \pi/9$, segue que $\cos(\pi/3) = \frac{1}{2} = 4\cos^3(\pi/9) - 3\cos(\pi/9)$. Assim, $p(x) = 8x^3 - 6x - 1$ anula $\cos(\pi/6)$, e, portanto, $\cos(\pi/9)$ é algébrico sobre $\mathbb{Q}$. $p(x)$ é irredutível sobre $\mathbb{Q}$: se não for, ele possui um divisor de grau 1 (pois seu grau é 3). Porém, se $a, b \in \mathbb{Z}$, $b \neq 0$ e $1 \in \mathrm{MDC}(a, b)$, então $a|1$ e $b|8$. Note que nenhum elemento de $\{1, -1, \frac{1}{2}, -\frac{1}{2}, \frac{1}{4}, -\frac{1}{4}, \frac{1}{8}, -\frac{1}{8}\}$ é raiz de $p(x)$, logo, $p(x)$ não possui raízes racionais.

Como $\cos(\pi/9)$ é algébrico sobre $\mathbb{Q}$ de grau 3 e 3 não é uma potência de 2, segue que $\cos(\pi/9)$ não está em $\mathbb{K}$. Logo, $\pi/9$ não é construtível com régua e compasso. □

Proposição 10.4.15. É impossível construir, com régua e compasso, um polígono regular de 18 lados.

Demonstração. Os ângulos internos de tal polígono tem 160 graus. Logo, o externo tem 20 graus. Como vimos, ângulos de 20 graus não são construtíveis com régua e compasso. □

Proposição 10.4.16. É impossível construir, com régua e compasso, um quadrado com a área de um círculo de raio 1.

Demonstração. Tal círculo tem área π. Um quadrado com área π tem lado $\sqrt{\pi}$. Porém, $\sqrt{\pi}$ não está em $\mathbb{K}$, caso contrário, teríamos $\pi \in \mathbb{K}$, mas π é transcendente sobre $\mathbb{Q}$. □

Proposição 10.4.17. É impossível construir, com régua e compasso, a base de um cubo de volume 2.

Demonstração. Para tanto, teríamos uma reta de comprimento $\sqrt[3]{2}$, número anulado por $x^3 - 2$, que é irredutível sobre $\mathbb{Q}$ (pois não possui raízes racionais). Logo, $\sqrt[3]{2}$ não está em $\mathbb{K}$, pois $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ e 3 não é uma potência de 2. □

10.5 Corpos de decomposição

Nesta seção, iniciaremos o estudo da decomposição de polinômios, caminhando para o estudo dos fechos algébricos dos corpos.

Definição 10.5.1. Seja E um corpo, $p \in E[x]$ um polinômio de grau $n \geq 1$ e F/E uma extensão de corpos.

- Dizemos que p *se fatora em* F, ou p *se decompõe em* F se existem $a_1, \ldots, a_n, u \in E$ tais que $p = u \prod_{i=1}^{n}(x - a_i)$ em $F[x]$.
- Se, adicionalmente, $F = E[a_1, \ldots, a_n]$, dizemos que F é um *corpo de decomposição de* F *sobre* E.

□

Vamos dar alguns exemplos.

Exemplo 10.5.2. $\mathbb{Q}[\sqrt{2}]$ é o corpo de decomposição de $x^2 - 2$ sobre $\mathbb{Q}$, pois $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ e $\mathbb{Q}\left[\sqrt{2}, -\sqrt{2}\right] = \mathbb{Q}\left[\sqrt{2}\right]$. □

Exemplo 10.5.3. $\mathbb{R}$ é o corpo de decomposição de $x^2 - 2$ sobre $\mathbb{R}$, pois $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ e $\mathbb{R} = \mathbb{R}\left[\sqrt{2}, -\sqrt{2}\right]$. □

Exemplo 10.5.4. $\mathbb{C}$ é o corpo de decomposição de $x^2 + 1$ sobre $\mathbb{R}$, pois $x^2 + 1 = (x - i)(x + i)$ e $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}[i, -i]$. □

Exemplo 10.5.5. O polinômio $x^2 - 2 \in \mathbb{Q}[x]$ se decompõe em $\mathbb{Q}[\sqrt[4]{2}]$, pois $\sqrt{2}, -\sqrt{2} \in \mathbb{Q}[\sqrt[4]{2}]$. Porém, $\mathbb{Q}[\sqrt[4]{2}]$ não é um corpo de decomposição de $x^2 - 2$ sobre $\mathbb{Q}$, uma vez que $\mathbb{Q}[\sqrt[4]{2}] \neq \mathbb{Q}[\sqrt{2}, -\sqrt{2}] = \mathbb{Q}[\sqrt{2}]$: o primeiro corpo é um $\mathbb{Q}$-espaço vetorial de dimensão 4, pois $\sqrt[4]{2}$ é raiz do polinômio $x^4 - 2$, que é irredutível sobre $\mathbb{Q}$, e $\sqrt{2}$ é raiz do polinômio $x^2 - 2$, que é irredutível sobre $\mathbb{Q}$. □

10.6 Exercícios

Exercício 10.1. Seja F um corpo estendendo E e $a \in F$ um elemento transcendente sobre E. Mostre que $E[a]$ é isomorfo ao anel de polinômios $E[x]$.

Exercício 10.2. Prove ou dê um contra-exemplo: se F/E é uma extensão algébrica e K é um corpo intermediário entre E e F, então F/K e K/E são extensões algébricas.

Exercício 10.3. Seja F/E uma extensão de corpos. Mostre que $[F : E] = 1$ se, e somente se $F = E$.

Exercício 10.4. Seja F/E uma extensão de corpos. Mostre que se $[F : E]$ é um número primo, então os únicos subcorpos de F contendo E são E e F.

Exercício 10.5. Dê um exemplo de uma extensão de corpos finitamente gerada que não possui grau finito. Justifique.

Exercício 10.6. Seja F/E uma extensão de corpos e $A \subseteq F$ um conjunto qualquer. Mostre que $E(A)$ é isomorfo ao corpo de frações de $E[A]$.

Exercício 10.7. Seja F/E uma extensão de corpos e $u \in F$. Mostre que se o grau de u sobre E é finito e ímpar, então $E(u) = E(u^2)$.

Exercício 10.8. Seja F/E uma extensão algébrica e D um subanel de F contendo E. Mostre que D é um corpo. Forneça um exemplo que mostre que a hipótese da algebricidade é necessária.

Exercício 10.9. Um número complexo é dito um *inteiro algébrico* se for a raiz de um polinômio mônico com coeficientes inteiros.

(a) Se $u \in \mathbb{C}$ é algébrico sobre $\mathbb{Q}$, mostre que existe $n \geq 1$ tal que nu é um inteiro algébrico.

(b) Mostre que se $u \in \mathbb{Q}$ é um inteiro algébrico, então $u \in \mathbb{Z}$.

Exercício 10.10. Seja F/E uma extensão de corpos e $u, v \in F$ elementos de grau $m, n < \infty$ sobre E, respectivamente. Mostre que $[E(u, v) : E] \leq mn$. Mostre ainda que se m, n são primos entre si, então $[E(u, v) : E] = mn$.

Exercício 10.11. Mostre que os subcorpos $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ de $\mathbb{C}$ são isomorfos como $\mathbb{Q}$-espaços vetoriais, mas não são isomorfos como corpos.

Exercício 10.12. Seja L um subcorpo de $\mathbb{R}$. Mostre que $a \in \mathbb{L}$ é algébrico sobre L se, e somente se $\sqrt{a}$ é algébrico sobre L.

Exercício 10.13. Seja F/E uma extensão de corpos e $p \in E[x]$ irredutível. Mostre que se $\alpha \in F$ é tal que $p(\alpha) = 0$, então $(x - \alpha)^2 \nmid p(x)$.

Exercício 10.14 (Relações de Girard)**.** Seja K um corpo.

1. Sejam $n \geq 1$ $\alpha_1, \ldots, \alpha_n \in K$. Então, em $K[x]$, $\prod_{i=1}^{n}(x - \alpha_i) = \sum_{i=0}^{n} s_i x^i$, onde $s_n = 1$ e $s_i = (-1)^{n+i} \sum_{1 \leq j_1 < \cdots < j_{n-i} \leq n} \alpha_{j_1} \ldots \alpha_{j_{n-i}}$ para $0 \leq i < n$. Em particular, $s_0 = (-1)^n \alpha_1 \ldots \alpha_n$ e $s_1 = -(\alpha_1 + \cdots + \alpha_n)$.
2. Seja L/K uma extensão de corpos e $\alpha_1, \ldots, \alpha_n \in L$. Sejam $s_0, \ldots, s_n$ como no item 1. Se cada s_i é um elemento de K, mostre que cada α_i é algébrico sobre K de grau $\leq n$.

Exercício 10.15. Seja $p \in \mathbb{Z}$ um primo positivo. Para quais inteiros $n \geq 1$ o número $\sqrt[n]{p}$ é construtível?

Exercício 10.16. Prove que um polígono regular de 9 lados não é construtível com régua e compasso.

Exercício 10.17. Calcule $[F : E]$ e encontre uma base de E como F-espaco vetorial, nos seguintes casos.

(a) $F = \mathbb{Q}(\sqrt[5]{2})$, $E = \mathbb{Q}$.

(b) $F = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18})$, $E = \mathbb{Q}$.

(c) $F = \mathbb{Q}(\sqrt{2}, \sqrt{3} + \sqrt{5})$, $E = \mathbb{Q}$.

(d) $F = \mathbb{Q}(\sqrt{2}, \sqrt{6})$, $E = \mathbb{Q}[\sqrt{3}]$.

Exercício 10.18. Considere a extensão de corpos $\mathbb{C}/\mathbb{Q}$. Tome $a \in \mathbb{C} \setminus \mathbb{Q}$ tal que $a^3 = 1$. Calcule $[\mathbb{Q}(a) : \mathbb{Q}]$.

Exercício 10.19. Mostre que se F é um corpo finito, então a cardinalidade de F é p^n para algum número primo p e algum $n \in \mathbb{N}$.

Exercício 10.20. Mostre que se E é um corpo e $p = \sum_{i=0}^{n} a_i x^i$ é um polinômio irredutível de $E[x]$, então existe um corpo F e um homomorfismo $f : E \to F$ tal que, sendo $E' = f[E]$, F/E' é uma extensão de corpos, existe α raiz de $\sum_{i=0}^{n} f(a_i)x^i \in E'[x]$ e $F = E'(\alpha)$.

Exercício 10.21. Mostre que existe um corpo de 8 elementos.

Dica: utilize o exercício anterior para estender $\mathbb{Z}_2$.

Apêndice A

O Teorema Fundamental da Álgebra

Neste apêndice, esboçaremos uma prova do Teorema Fundamental da Álgebra.

Abaixo, utilizaremos que se $a, b \in \mathbb{C}$, então $|a| - |b| \leq |a + b| \leq |a| + |b|$.

Pela fórmula de Euler, para todo $\theta \in \mathbb{R}$, $e^{i\theta} = \cos\theta + i \sin\theta$. Desta forma, $|e^{i\theta}| = 1$ para todo $\theta \in \mathbb{R}$. Vale ainda que para todo $z \in \mathbb{C}$, $z = |z|e^{i\theta}$. Intuitivamente, estamos escrevendo z em coordenadas polares.

Vale ainda que para todo $k \in \mathbb{Z}$, $(e^{i\theta})^k = e^{i\theta k}$. Em particular, $e^{-i\theta} = \frac{1}{e^{i\theta}}$.

A.1 A demonstração

Teorema A.1.1. Todo polinômio complexo não constante tem raiz em $\mathbb{C}$.

Demonstração. Seja $f(z) = \sum_{k=0}^{n} a_k z^k$ uma função polinomial em $\mathbb{C}$, com $n \geq 1$, $a_n \neq 0$ e $a_k \in \mathbb{C}$ para todo $k = 0, \ldots, n$. Basta ver que f possui uma raiz em $\mathbb{C}$. Podemos supor que $n > 1$.

Dividindo f por a_n, podemos assumir que $a_n = 1$.

Seja $R = \inf\{|f(z)| : z \in \mathbb{Z}\}$. Veremos que este ínfimo é 0 e que é atingido, ou seja, que existe $z \in \mathbb{C}$ tal que $|f(z)| = R$.

Se $z \neq 0$, temos que

$$|f(z)| = \left|\sum_{k=0}^{n} a_k z^k\right| \geq |z^n| - \left|\sum_{k=0}^{n-1} a_k z^k\right| \geq |z|^n - \sum_{k=0}^{n-1} |a_k||z|^k. \tag{A.1}$$

Seja $g : (0, \infty) \to \mathbb{R}$ dada por $g(\xi) = \xi^n - \sum_{k=0}^{n-1} |a_k|\xi^k = \xi^n(1 - \sum_{k=0}^{n-1} |a_k|\xi^k)$. Da teoria de limites de números reais, como $g(\xi) \to \infty$ quando $\xi \to \infty$, existe $M > 0$ tal que para todo $\xi > M$, temos $g(\xi) > R + 1$. Segue que se $z \in \mathbb{C}$ e $|z| > M$, então $|f(z)| > R + 1$.

Pela definição de R, existe $(z_n : n \geq 1)$ uma sequência de números complexos tal que $|f(z_n)| \leq R + \frac{1}{n}$. Pelo Teorema do Confronto, temos que $|f(z_n)| \to R$ quando $n \to \infty$. Assim, para n suficientemente grande, temos que $|f(z_n)| - R \leq 1$, e, portanto, que $|z| \leq M$.

O conjunto $D = \{z \in \mathbb{C} : |z| \leq M\}$ é fechado e limitado e $h : D \to R$ dada por $h(z) = |f(z)|$ é contínua, logo, pelo Teorema de Weierstrass, f atinge mínimo. Pelo argumento precedente, este mínimo é menor ou igual a $R + \frac{1}{n}$ para todo n suficientemente grande, assim, este mínimo

deve ser $\leq R$. Por outro lado, este mínimo deve ser $\geq R = \inf\{|f(z)| : z \in \mathbb{C}\}$, logo, este mínimo é exatamente R. Portanto, existe $z_0 \in D$ tal que $|f(z_0)| = R$.

Agora veremos que $R = 0$. Se $R \neq 0$, seja $q(z) = p(z + z_0)/p(z_0)$. Temos que q é uma função polinomial não constante de grau $\leq n$, $q(z) \geq 1$ para todo z e $q(0) = 1$. Escreva $q(z) = 1 \sum_{k=l}^{n} b_k z^k$ com $l \geq 1$ tal que $b_l \neq 0$.

Escrevendo em coordenadas polares, existe $\theta \in \mathbb{R}$ tal que $-b_l = |b_l|e^{i\theta}$. Seja $r \in \mathbb{R}$ tal que $0 < r < 1$ e tal que $r^l|b_l| < 1$. Então:

$$\begin{aligned}
|q(re^{-i\theta})| =& \left|1 + \sum_{k=l}^{n} r^k e^{-i\theta k} b_k\right| \\
\leq& |1 + r^l b_l e^{-i\theta l}| + \left|\sum_{k=l+1}^{n} r^k e^{-i\theta k} b_k\right| \\
=& |1 - r^l|b_l|| + \left|\sum_{k=l+1}^{n} r^k e^{-i\theta k} b_k\right| \\
=& 1 - r^l|b_l| + \sum_{k=l+1}^{n} r^k |b_k| \\
=& 1 - r^l \left(|b_l| - \sum_{k=l+1}^{n} r^{k-l}|b_k|\right)
\end{aligned}$$

Como $r^l \left(|b_l| - \sum_{k=l+1}^{n} r^{k-l}|b_k|\right)$ converge para 0 por valores positivos quando $r \to 0^+$, segue que, para r suficientemente pequeno, tal expressão é menor que 1, logo, $|q(re^{-i\theta})| < 1$, o que é absurdo.

Assim, $R = 0$ e $f(z_0) = 0$. □