Álgebra I

Notas de aula

Prof. Dr. Victor do Nascimento Martins

Universidade Federal do Espírito Santo
Campus de Alegre

PREFÁCIO

O propósito dessas notas de aula é fornecer um material de apoio sucinto e objetivo para a disciplina de *Álgebra I* que compõe a grade de disciplinas obrigatórias do curso de licenciatura em matemática da Universidade Federal do Espírito Santo, campus de Alegre. Sendo assim, o principal foco é cobrir todo conteúdo de tal disciplina.

Ressaltamos que para uma melhor compreensão do conteúdo e um aprofundamento maior dos tópicos aqui apresentados, o aluno deverá, sempre que possível, consultar as referências bibliográficas indicadas.

Essas notas foram iniciadas após a primeira experiência do autor ministrando, no segundo semestre de 2019, a disciplina de Álgebra II da grade antiga do curso cujo conteúdo continha os tópicos da teoria de anéis presentes na disciplina de Álgebra I. A necessidade mais imediata dessas notas se deu devido a aprovação de um semestre emergencial de ensino remoto na UFES a partir de setembro de 2020 em função da pandemia causada pelo corona vírus e que impossibilitou a continuidade do ensino presencial.

É importante ressaltar ainda que este material está em construção, sendo apenas uma primeira divulgação emergencial, dado o momento atual de ensino remoto. Portanto, quaisquer correções, sugestões e comentários serão bem recebidos.

Alegre, outubro de 2020.

Victor Martins

CONTEÚDO PROGRAMÁTICO

Números inteiros: divisibilidade e congruências. Anéis: subanéis, ideais, anéis quocientes, homomorfismo. Anéis de polinômios: o algoritmo da divisão, polinômios irredutíveis e ideais maximais, fatorização única e critério de Eisenstein.

Horas/aula	**Tópicos**
	PARTE I
30	**Números inteiros:** Conjunto dos número inteiros. Indução e princípio do menor inteiro. Divisibilidade: critérios de divisibilidade. Divisibilidade: *mdc* e *mmc*. Números primos. Teorema Fundamental da Aritmética. Congruências. Os inteiros módulo n. Pequeno Teorema de Fermat. Equações com congruências. Sistemas de congruências: Teorema Chinês do Resto.
	PARTE II
30	**Anéis:** Primeiras definições. Subanéis. Ideais. Anel quociente. Homomorfismos de anéis. O corpo de frações de um domínio. Polinômios. Polinômios com coeficientes em anéis. Algoritmo da divisão. Ideais principais e máximo divisor comum. Polinômios irredutíveis. Fatoração única. Critério de Eisenstein.

SUMÁRIO

INTRODUÇÃO

0.1 Sistemas de numeração

CAPÍTULO 1

NÚMEROS NATURAIS

1.1 Os axiomas de Peano

1.2 O princípio da boa ordenação e o axioma de indução

1.3 Exercícios

(1) Mostre que não existe nenhum número natural n tal que $1 < n < 2$.

(2) Mostre que, dado um número natural n qualquer, não existe nenhum número natural m tal que $n < m < n + 1$.

(3) Mostre, por indução, que:

(a) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots + n(n+1) = \dfrac{n(n+1)(n+2)}{3}$, para todo $n \in \mathbb{N}$;

(b) $1 + n \leq 2^n$, para todo $n \in \mathbb{N}$;

(c) $2^n < n!$, para todo $n \geq 4$, $n \in \mathbb{N}$.

(4) Mostre, usando o Princípio da Boa Ordenação (PBO), que:

(a) $1 + 2 + 3 + \ldots + n = \dfrac{n(n+1)}{2}$, para todo $n \in \mathbb{N}$;

(b) $1 + n \leq 2^n$, para todo $n \in \mathbb{N}$.

CAPÍTULO 2

NÚMEROS INTEIROS

2.1 Princípio do menor inteiro e indução

2.1.1 Princípio do menor inteiro

2.1.2 Primeiro princípio de indução

2.1.3 Segundo princípio de indução

2.1.4 Exercícios

(1) Encontre cotas inferiores, cotas superiores, o elemento mínimo e o elemento máximo, caso existam, para cada um dos conjuntos a seguir.

(a) $A = \{-4, -7, 2, 6, 0, 1, -1\}$

(b) $B = \{x \in \mathbb{Z} : \ x \geq 11\}$

(c) $C = \{x \in \mathbb{Z} : \ x < 5\}$

(d) $D = \{x \in \mathbb{Z} : \ x \geq -8\}$

(e) $E = \{x \in \mathbb{Z}_+^* : \ 3 \quad \text{é divisor de} \quad x^2\}$

(f) $F = \{x \in \mathbb{Z}_+^* : \ 5 \quad \text{é divisor de} \quad x^3\}$

(g) $G = \{x \in \mathbb{Z} : \ x \quad \text{é múltiplo positivo de} \quad 4\}$

(h) $H = \{x \in \mathbb{Z} : \ x \quad \text{é múltiplo negativo de} \quad 6\}$

(2) Mostre que

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

para todo $n \geq 1$.

(3) Verifique se as seguintes fórmulas são válidas para $n \geq 1$.

(a) $5 + 9 + 13 + \cdots + (4n + 1) = n(2n + 3)$;

(b) $1 + 4 + 9 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$;

(c) $1 + 2^3 + 3^3 + \cdots + n^3 = \left(\dfrac{n(n+1)}{2}\right)^2$.

(4) Uma **progressão aritmética** de razão r e termo inicial a_1 é uma sequência

$$a_1, a_2, \ldots, a_n, \ldots$$

em que a diferença de dois termos consecutivos é sempre igual a r, isto é

$$a_n - a_{n-1} = r, \ \forall \ n \geq 2.$$

Considere uma progressão aritmética de razão r e termo inicial a_1. Mostre que:

(a) $a_n = a_1 + (n-1)r$;

(b) a soma S_n dos n primeiros termos dessa progressão é dada por

$$S_n = \frac{n(a_1 + a_n)}{2}.$$

(5) Uma **progressão geométrica** de razão $q \neq 1$ e termo inicial a_1 é uma sequência

$$a_1, a_2, \ldots, a_n, \ldots$$

em que o quociente de dois termos consecutivos é sempre igual a q, isto é

$$\frac{a_n}{a_{n-1}} = q, \ \forall \ n \geq 2.$$

Considere uma progressão geométrica de razão $q \neq 1$ e termo inicial a_1. Mostre que:

(a) $a_n = a_1 q^{n-1}$;

(b) a soma S_n dos n primeiros termos dessa progressão é dada por

$$S_n = a_1 \frac{1 - q^n}{1 - q}.$$

(6) Conjecture uma fórmula para as expressões a seguir e, em seguida, demonstre-a.

(a) $1+\frac{1}{2}=2-\frac{1}{2}, \qquad 1+\frac{1}{2}+\frac{1}{4}=2-\frac{1}{4}, \qquad 1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}=2-\frac{1}{8}$

(b) $1=1, \quad 1-4=-(1+2), \quad 1-4+9=1+2+3, \quad 1-4+9-16=-(1+2+3+4).$

(7) (a) Seja $A=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Calcule A^2 e A^3 para determinar uma possível fórmula para A^n, $n \in \mathbb{N}$.

(b) Demonstre a fórmula encontrada no item anterior por indução.

(8) Se $0 \leq k \leq n$, define-se o "coeficiente binomial" $\begin{pmatrix} n \\ k \end{pmatrix}$ por $\begin{pmatrix} n \\ k \end{pmatrix} = \frac{n!}{k!(n-k)!}$. Mostre que

(a) $\begin{pmatrix} n \\ k-1 \end{pmatrix} + \begin{pmatrix} n \\ k \end{pmatrix} = \begin{pmatrix} n+1 \\ k \end{pmatrix}, \quad k \neq 0, n$ (Relação de Stifel)

(b) $\begin{pmatrix} n \\ k \end{pmatrix}$ é sempre um número natural.

(9) Faça uma conjectura a respeito da soma

$$S_n = \begin{pmatrix} n \\ 0 \end{pmatrix} + \begin{pmatrix} n \\ 1 \end{pmatrix} + \begin{pmatrix} n \\ 2 \end{pmatrix} + \ldots + \begin{pmatrix} n \\ n \end{pmatrix}, \, n \in \mathbb{N}.$$

Prove sua conjectura.

(10) Seja F_i o i-ésimo termo da sequência de Fibonacci. Mostre que:

(a) $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$;

(b) $F_1 + F_3 + \cdots + +F_{2n-3} + F_{2n-1} = F_{2n}$;

(c) $F_2 + F_4 + \cdots + F_{2n-2} + F_{2n} = F_{2n-1} - 1$.

(11) (Fuvest 1981) P é uma propriedade relativa aos números naturais. Sabe-se que:

(i) P é verdadeira para o natural $n = 10$.

(ii) Se P é verdadeira para n, então P é verdadeira para $2n$.

(iii) Se P é verdadeira para n, $n \geq 2$, então P é verdadeira para $n-2$.

Pode-se concluir que:

(a) P é verdadeira para todo natural n.

(b) P é verdadeira somente para os números naturais n, $n \geq 10$.

(c) P é verdadeira para todos os números naturais pares.

(d) P é verdadeira somente para as potências de 2.

(e) P não é verdadeira para os números ímpares.

(12) (Cespe - Abin 2010, Oficial Técnico de Inteligência, adaptado) Considere uma função proposicional $P(n)$ relativa aos números inteiros não negativos que satisfaça as seguintes propriedades:

(i) $P(3)$ é verdadeira;

(ii) se, para um número inteiro não negativo n, $P(n)$ for verdadeira, então $P(n^2)$ também será verdadeira;

(iii) se, para um número inteiro não negativo $n \geq 2$, $P(n)$ for verdadeira, então $P(n-1)$ também será verdadeira.

Julgue os itens que se seguem, acerca de $P(n)$ e suas propriedades.

(a) A função proposicional "a raiz quadrada de n é um número inteiro" não pode ser usada como exemplo para $P(n)$.

(b) $P(n)$ é verdadeira para todo inteiro não negativo.

(13) Mostre que a função proposicional

$$P(n) : 1 + 3 + 5 + \cdots + (2n - 1) = n^2 + 3$$

satisfaz a segunda propriedade do Primeiro Princípio de Indução, mas não satisfaz a primeira propriedade, qualquer que seja $a \in \mathbb{N}$ escolhido.

2.2 Divisão euclidiana

2.2.1 Exercícios

(1) Sejam a e b inteiros quaisquer. Mostre que:

(a) se $a|b$, então $a|(-b)$;

(b) se $a|b$ e $a|(b + c)$, então $a|c$;

(c) se $a|b$ então $a|rb$ para qualquer inteiro r;

(d) se $a|b$ e $a \neq 0$, então $|a| \leq |b|$.

(2) Mostre que, se $a|(2x - 3y)$ e $a|(4x - 5y)$, então $a|y$.

(3) Na divisão euclidiana do inteiro $a = 427$ por um inteiro positivo b, o quociente é 12 e o resto é r. Encontre os valores de b e r.

(4) Dê uma definição de número inteiro **par** e de número inteiro **ímpar** utilizando o algoritmo da divisão.

(5) Utilizando o algoritmo da divisão, mostre as afirmações a seguir:

   (a) A soma de dois inteiros pares é um inteiro par.

   (b) A soma de dois inteiros ímpares é um inteiro par.

   (c) A soma entre um inteiro par e um inteiro ímpar é um inteiro ímpar.

(6) Utilizando indução, mostre que $24|n(n^2-1)(3n+2)$ para todo n natural.

(7) Mostre que, para todo $n \in \mathbb{N}_0$ temos:

   (a) $7|(2^{3n}-1)$

   (b) $2|(3^n-1)$

(8) Mostre que o quadrado de qualquer número inteiro ímpar é da forma $8k+1$, com k inteiro.

(9) Mostre que, se m e n são inteiros ímpares, então $8|(m^2+n^2-2)$.

(10) Seja a inteiro. Mostre que, na divisão de a^2 por 8, os restos possíveis são $0, 1$ ou 4.

(11) Determine os inteiros positivos que divididos por 17 deixam um resto igual ao quadrado do quociente.

(12) Se m e n forem inteiros ímpares, mostre que m^2-n^2 é divisível por 8.

(13) Mostre que, para todo natural j, 10^j pode ser escrito na forma $9b_j+1$, para algum b_j natural.

(14) Mostre que, para todo natural j, 10^j pode ser escrito na forma $11c_j+(-1)^j$, para algum c_j natural.

(15) Mostre que um número natural $a = a_n a_{n-1} \dots a_1 a_0$ é divisível por 11 se, e somente se, a soma alternada dos seus algarismos

$$a_0 - a_1 + a_2 - \cdots + (-1)^n a_n$$

for divisível por 11.

(16) Enuncie e prove um critério de divisibilidade por 3.

(17) Enuncie e prove um critério de divisibilidade por 5.

(18) Enuncie e prove um critério de divisibilidade por 4.

(19) Mostre que todo inteiro ímpar pode ser escrito como diferença de dois quadrados.

(20) Mostre que, dados três inteiros consecutivos, um deles é múltiplo de 3.

(21) Sejam a e b inteiros com $b > 0$. Mostre que, dentre os números $a, a+1, a+2, \ldots, a+b-1$, um e apenas um deles é múltiplo de b. Em outras palavras, um conjunto de b inteiros consecutivos contém exatamente um múltiplo de b.

(22) Sejam a, b e m inteiros com $m \neq 0$. Mostre que, se $m|(b-a)$, então a e b deixam o mesmo resto quando divididos por m.

(23) Mostre que todo número com três algarismos, todos eles iguais, é divisível por 37.

2.3 Números primos, MDC e MMC

2.3.1 Teorema fundamental da Aritmética

2.3.2 A procura de números primos

2.3.3 Máximo divisor comum

2.3.4 Mínimo múltiplo comum

2.3.5 Exercícios

(1) Determine todos os números primos p tais que $3p + 1$ seja um quadrado perfeito.

(2) Encontre todos os pares de primos p e q tais que $p - q = 3$.

(3) Calcule o menor número natural n para o qual $n, n+1, n+2, n+3, n+4$ e $n+5$ são todos compostos.

(4) Mostre que 7 é o único número primo da forma $n^3 - 1$.

(5) Mostre que todo número primo que deixa resto 1 quando dividido por 3 também deixa resto 1 quando dividido por 6.

(6) Sejam $a_1, \ldots, a_n$ números inteiros com $n \geq 2$, e p um número primo. Mostre que se $p|a_1 a_2 \cdots a_n$, então $p|a_i$ para algum i.

(7) Mostre que $\sqrt{2}$ é irracional.

(8) Mostre que se p for um número primo, então $\sqrt{p}$ é irracional.

(9) Seja a um número natural, tal que $a \geq 2$. Considere a decomposição em fatores primos

$$a = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n},$$

em que $n \geq 1$, $r_i \geq 1$ para todo $i = 1, \ldots, n$ e os fatores primos p_i são todos distintos.

(a) Mostre que todos os divisores b de a são da forma

$$b = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n},$$

em que $0 \leq s_i \leq r_i$, para todo $i = 1, \ldots n$.

(b) Conclua que o número de divisores positivos de a (incluindo 1 e a) é dado pelo produto

$$(r_1 + 1)(r_2 + 1) \cdots (r_n + 1).$$

(10) (a) Mostre que todo número natural ímpar é da forma $4k + 1$ ou $4k - 1$, em que k é um inteiro positivo.

(b) Mostre que todo número da forma $4k - 1$ tem pelo menos um fator primo da mesma forma.

(c) Mostre que existem infinitos primos da forma $4n - 1$.

(11) Mostre que se p for primo e $p \nmid a$, então $mdc(a, p) = 1$.

(12) Utilize o algoritmo da divisão para calcular $d = mdc(a, b)$ e escrever $d = ax + by$, sendo:

(a) $a = 232$ e $b = 136$;

(b) $a = 187$ e $b = 221$;

(c) $a = -25$ e $b = 5$;

Em seguida, calcule o mínimo múltiplo comum dos pares a e b dados.

(13) (a) Mostre que $mdc(a, b)$ divide $a - b$.

(b) Mostre que $mdc(a, b) = mdc(a - b, b)$.

(14) Mostre que dois inteiros consecutivos são sempre primos entre si.

(15) Mostre que, se existem x e y inteiros tais que $ax + by = 1$ então $mdc(a, b) = 1$.

(16) Se $d = ax + by$, é verdade que $d = mdc(a, b)$?

(17) Se $d = mdc(a, b)$ e x e y são tais que $ax + by = d$, mostre que $mdc(x, y) = 1$.

(18) Mostre que $mdc(a, b) = mdc(a, b + ax)$ para todo inteiro x.

(19) Se $mdc(n, 6) = 1$, mostre que $12|(n^2 - 1)$.

(20) O mdc entre dois números inteiros positivos é 10 e o maior deles é 120. Determine todos os inteiros que satisfazem essa condição.

(21) Sejam a e b inteiros não nulos e $m > 0$ um natural. Mostre que:

(a) $mdc(ma, mb) = m \cdot mdc(a, b)$;

(b) $mmc(ma, mb) = m \cdot mmc(a, b)$.

(22) Sejam a e b inteiros não nulos tais que $mdc(a, b) = 1$. Então, para todo inteiro $m > 0$, $mdc(a^m, b^m) = 1$.

(23) (a) Mostre que, se a e b forem inteiros não simultaneamente nulos, então o $mdc(a, b)$ é o menor elemento de

$$S = \{ax + by : \ x, y \in \mathbb{Z}, \ ax + by > 0\}.$$

(b) Mostre que $mdc(a, b)$ é o único divisor comum de a e b que se escreve como combinação linear desses números.

(24) Mostre que se r e s são inteiros positivos tais que $mdc(r, s) = mmc(r, s)$ então $r = s$.

(25) Mostre que se r e s são inteiros, então $mdc(r, s)$ sempre divide $mmc(r, s)$.

2.4 Equações diofantinas

2.4.1 Exercícios

(1) Determine o menor inteiro positivo que deixa resto 16 e 27 quando dividido por 39 e 56, respectivamente.

(2) Ache a solução geral e uma solução positiva da equação $12740x + 7260y = 60$.

(3) Encontre a solução geral, caso exista, das seguintes equações diofantinas lineares:

(a) $15x + 27y = 1$;

(b) $5x - 6y = -1$;

(c) $15x - 51y = 41$;

(d) $5x + 6y = 1$;

(e) $2x + 3y = 4$.

(4) Uma caixa contém besouros e aranhas. Existem 46 patas na caixa. Quantas patas são dos besouros?

(5) Divida 100 em 2 parcelas positivas, de modo que uma seja divísivel por 7 e a outra por 11.

(6) Encontre todos os inteiros com a seguinte propriedade: quando divididos por 11 fornecem resto 6 e divididos por 7 fornecem resto 3.

2.5 Congruências

2.5.1 Exercícios

(1) Seja m um inteiro não nulo. Dados $a, b, c \in \mathbb{Z}$, mostre que se $ac \equiv bc(mod\, m)$ e $mdc(c, m) = d$, então $a \equiv b(mod\, \frac{m}{d})$.

(2) Sejam a, b inteiros quaisquer, e sejam m, d, r e s inteiros positivos. Mostre que:

(a) se $a \equiv b(mod\, m)$ e $d|m$, então $a \equiv b(mod\, d)$;

(b) Se $a \equiv b(mod\, r)$ e $a \equiv b(mod\, s)$, então $a \equiv b(mod\, mmc(r, s))$;

(c) se $ra \equiv rb(mod\, m)$, então $a \equiv b(mod\, \frac{m}{mdc(r,m)})$;

(d) se $ra \equiv rb(mod\, rm)$, então $a \equiv b(mod\, m)$.

(3) Mostre que, se $[a]_m \in \mathbb{Z}_m$ for inversível, então seu inverso é único.

(4) Mostre que o produto de dois elementos inversíveis módulo m é um elemento inversível.

(5) Mostre que se $[a]_m \cdot [c]_m = [b]_m \cdot [c]_m$ e $[c]_m$ for inversível, então $[a]_m = [b]_m$.

(6) Mostre que, se p for um número primo, então todos os elementos não nulos de $\mathbb{Z}_p$ são inversíveis.

(7) Suponha que $a \equiv b(mod\, m)$ e $c \equiv d(mod\, m)$. Mostre que $ax + cy \equiv bx + dy(mod\, m)$ para quaisquer $x, y \in \mathbb{Z}$.

(8) Mostre que, se $a \equiv b(mod\, m)$, então $a^n \equiv b^n(mod\, m)$ para todo inteiro positivo n.

(9) Se $a = (72)^6 + (72)^5 + 2$, mostre que $7|a$.

(10) Demonstre o critério de divisibilidade por 11 usando congruências.

(11) Ache o resto da divisão de $a = 531 \cdot 2 \cdot (31)^2$ por 7.

(12) Resolva as congruências:

(a) $3x \equiv 3 (mod\, 5)$;

(b) $3x \equiv 1 (mod\, 6)$;

(c) $3x \equiv 3 (mod\, 6)$;

(13) Resolva a congruência $x^2 \equiv 4 (mod\, 13)$.

(14) Mostre, por indução, que $4^n \equiv 1 + 3n (mod\, 9)$, se n for um inteiro positivo.

(15) Ache o último algarismo dos números 9^{9^9} e 7^{7^7}.

(16) Mostre que 8 é um número composto usando o Pequeno Teorema de Fermat.

(17) Mostre que 8 é um número composto utilizando o Teorema de Wilson.

(18) Verifique que $p = 341$ satisfaz o Pequeno Teorema de Fermat para $a = 2$, mas 341 não é um número primo.

(19) MOstre que 17 é um número primo utilizando o Teorema de Wilson.

(20) Mostre que 19 é um número primo utilizando o Teorema de Wilson.

CAPÍTULO 3

ANÉIS

A teoria de anéis é um dos principais assuntos dentro da álgebra abstrata e sua noção abstrata foi introduzida na segunda década do século XX. O conteúdo que será apresentado neste capítulo tem por principal objetivo estabelecer uma sequência lógica de estudos que culminaria na importante contribuição de Galois dentro da álgebra, assim como feito em [2]. Portanto, para mais detalhes sobre a teoria de anéis e a sequência lógica de estudos mencionada, sugerimos uma consulta a [1, 2, 4].

3.1 Primeiras definições

Seja A um conjunto não vazio munido de duas operações que chamaremos de adição e multiplicação e denotaremos respectivamente por $+$ e $\cdot$:

$$+ : \begin{array}{ccc} A \times A & \longrightarrow & A \\ (a,b) & \longmapsto & a+b \end{array} \qquad e \qquad \cdot : \begin{array}{ccc} A \times A & \longrightarrow & A \\ (a,b) & \longmapsto & a \cdot b. \end{array}$$

Chamaremos o sistema $(A, +, \cdot)$ de **anel** se para quaisquer $a, b, c \in A$ forem satisfeitas as seguintes propriedades:

(A1) Associatividade da adição:

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

(A2) Comutatividade da adição:

$$a+b = b+a.$$

(A3) Existência do elemento neutro na adição, isto é, existe um elemento chamado *zero*, denotado por 0, tal que

$$a+0 = 0+a = a.$$

(A4) Existência do elemento inverso na adição: dado $a \in A$, existe um elemento chamado **simétrico** (ou **oposto** ou **inverso aditivo**) de a e denotado por $(-a)$, tal que

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

(A5) Associatividade da multiplicação:

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

(A6) Distributividade da multiplicação com relação a adição:

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

Definição 3.1 *Seja $(A, +, \cdot)$ um anel.*

- *A é dito um **anel com unidade** se:*
  *$(A7)$ existe um elemento $1 \in A$, chamado **unidade**, tal que $0 \neq 1$ e $a \cdot 1 = a = 1 \cdot a$, para todo $a \in A$;*

- *A é dito um **anel comutativo** se:*
  $(A8)$ para quaisquer $a, b \in A$, $a \cdot b = b \cdot a$;

- *A é dito um **anel sem divisores de zero** se:*
  $(A9)$ para quaisquer $a, b \in A$ vale a implicação $a \cdot b = 0 \Rightarrow a = 0$ ou $b = 0$;

- *A é dito um **domínio de integridade** se A for um anel comutativo, com unidade e sem divisores de zero;*

- *A é dito um **corpo** se A for um anel comutativo com unidade e ainda for satisfeita a seguinte propriedade:*
  *$(A10)$ para todo $a \in A$, $a \neq 0$, existe $x \in A$ tal que $a \cdot x = 1$. Neste caso, chamamos x de **inverso** de a e o denotamos por a^{-1} ou $\frac{1}{a}$.*

Observação 3.1 *Observe que todo corpo é um domínio de integridade. De fato, dado um corpo A, pela definição dada acima, para ser um domínio de integridade A deve satisfazer a propriedade $(A9)$. Assim, dados $a, b \in A$ tais que $a \cdot b = 0$ vamos supor que a seja diferente de 0, daí pela propriedade $(A10)$ existe a^{-1} tal que $a \cdot a^{-1} = 1$, logo*

$$a \cdot b = 0 \Rightarrow a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \Rightarrow (a^{-1} \cdot a) \cdot b = 0 \Rightarrow b = 0.$$

Portanto A é um domínio de integridade.

Exemplo 3.1 *O conjunto $\mathbb{Z}$ dos números inteiros é um domínio de integridade.*

Exemplo 3.2 *Dado $n \in \mathbb{N}$, considere o conjunto $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$.*

Por exemplo

$$2\mathbb{Z} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$$

é o conjunto dos números pares.

- *$n\mathbb{Z}$ é um anel comutativo para todo $n \geq 1$;*
- *$n\mathbb{Z}$ é um anel sem divisores de zero para todo $n \geq 1$;*
- *$n\mathbb{Z}$ não possui unidade para todo $n \geq 2$.*

Exemplo 3.3 *Dado $n \in \mathbb{N}$, $n \geq 2$, considere o conjunto das classes dos inteiros módulo n dado por $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \ldots, \overline{n-1}\}$.*

- *$\mathbb{Z}_n$ é anel comutativo com unidade;*
- *se n não é primo então $\mathbb{Z}_n$ possui divisores de zero. De fato, por n não ser primo, existem $a, b \in \mathbb{Z}$, $1 < a, b < n$ tais que $a \cdot b = n$, logo*

$$\bar{a} \cdot \bar{b} = \bar{n} = \bar{0}$$

e $\bar{a} \neq \bar{0}$ e $\bar{b} \neq \bar{0}$;

- *se n é primo $\mathbb{Z}_n$ é um corpo. De fato, se n é primo, seja $a \in \mathbb{Z}$ com $1 < a < n$. Vamos mostrar que existe o inverso de $\bar{a}$ e como pegamos $\bar{a}$ um elemento qualquer de $\mathbb{Z}_n$ teremos provado que $\mathbb{Z}_n$ é um corpo. Como n é primo, $mdc(a, n) = 1$, logo pelo Teorema de Bezóut, existem inteiros x, y tais que*

$$ax + ny = 1 \Rightarrow \overline{ax + ny} = \bar{1} \Rightarrow \overline{ax} + \overline{ny} = \bar{1} \Rightarrow \bar{a}\bar{x} = \bar{1},$$

e daí $\bar{x}$ é o inverso de $\bar{a}$.

Neste caso também vale a recíproca da afirmação acima, isto é, se $\mathbb{Z}_n$ é corpo então n é primo. Suponha que n não fosse primo, isto é, existem $a, b \in \mathbb{Z}$, com $1 < a, b < n$ tais que $n = a \cdot b$. Daí

$$\bar{n} = \overline{a \cdot b} \Rightarrow \bar{0} = \bar{a} \cdot \bar{b}.$$

Como $\mathbb{Z}_n$ é corpo devemos ter $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$, um absurdo já que $1 < a, b < n$.

Exemplo 3.4 *Os conjuntos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ são corpos.*

Exemplo 3.5 *O conjunto* $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ *é um domínio de integridade, mas não é um corpo. De fato, para qualquer* $a \in \mathbb{Z}$*, temos que* $a \in \mathbb{Z}[\sqrt{2}]$*, pois* $a = a + 0 \cdot \sqrt{2}$*. Vamos mostrar então que qualquer elemento* $a \in \mathbb{Z} \subset \mathbb{Z}[\sqrt{2}]$*, com* $a \neq 1$ *e* $a \neq 0$ *não possui inverso multiplicativo em* $\mathbb{Z}[\sqrt{2}]$*. Suponha por contradição que dado a nessas condições, exista* $x = b_1 + b_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ *tal que* $a \cdot x = 1$*, daí teríamos*

$$a(b_1 + b_2\sqrt{2}) = 1 \Rightarrow ab_1 + ab_2\sqrt{2} = 1 \Rightarrow ab_1 = 1 \quad e \quad ab_2 = 0 \Rightarrow b_2 = 0 \quad e \quad b_1 = \frac{1}{a},$$

mas $\frac{1}{a} \notin \mathbb{Z}$*, logo* x *não pertenceria a* $\mathbb{Z}[\sqrt{2}]$*. Portanto* $\mathbb{Z}[\sqrt{2}]$ *não é um corpo.*

Em geral, se p *é primo,* $\mathbb{Z}[\sqrt{p}]$ *é um domínio de integridade, mas não é corpo.*

Exemplo 3.6 *O conjunto* $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} : a, b \in \mathbb{Q}\}$ *é um corpo para todo* p *primo. É um corpo intermediário entre* $\mathbb{Q}$ *e* $\mathbb{R}$*, isto é,*

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{p}] \subset \mathbb{R}.$$

Exemplo 3.7 *O conjunto* $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$*,* $i = \sqrt{-1}$ *é um domínio de integridade tal que* $\mathbb{Z} \subset \mathbb{Z}[i] \subset \mathbb{C}$*.*

Já o conjunto $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$ *é um corpo tal que* $\mathbb{Q} \subset \mathbb{Q}[i] \subset \mathbb{C}$*.*

Note que $\mathbb{R}[i] = \mathbb{C}$*.*

Exemplo 3.8 *Seja* $A = \mathcal{F}(\mathbb{R})$ *o conjunto das funções reais de uma variável real*

$$A = \mathcal{F}(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R}\}.$$

Definimos em A *duas operações*

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

dada por $(f + g)(x) = f(x) + g(x)$*, para todo* $x \in \mathbb{R}$*. E*

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

dada por $(f \cdot g)(x) = f(x) \cdot g(x)$*, para todo* $x \in \mathbb{R}$*. Note que a função constante zero é o elemento neutro em relação a adição de* A*, isto é, a função*

$$\begin{array}{rccc} 0_f : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & 0, \end{array}$$

é tal que $f + 0_f = f$ para todo $f \in A$. Além disso, a função constante 1 é o elemento unidade de A, isto é, a função

$$\begin{array}{rccc} 1_f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & 1, \end{array}$$

é tal que $f \cdot 1_f = f = 1_f \cdot f$ para todo $f \in A$. Com as operações definidas acima, A é um anel comutativo com unidade, porém A não é um domínio de integridade, pois A possui divisores de zero, isto é, existem f, g funções não nulas em A tais que $f \cdot g = 0_f$. Por exemplo, dados

$$f(x) = \begin{cases} 0, & se \quad x < 0 \\ x, & se \quad x \geq 0 \end{cases} \qquad e \qquad g(x) = \begin{cases} x^2, & se \quad x < 0 \\ 0, & se \quad x \geq 0. \end{cases}$$

Note que

$$(f \cdot g)(x) = \begin{cases} 0 \cdot x^2, & se \quad x < 0 \\ x \cdot 0, & se \quad x \geq 0 \end{cases} \qquad \equiv \quad 0.$$

Logo $A = \mathcal{F}(\mathbb{R})$ é um anel comutativo com unidade e com divisores de zero.

Exemplo 3.9 (Anel dos quatérnios ($Quat$)) *Considere o conjunto $Quat = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ onde*

$$i^2 = j^2 = k^2 = -1$$

$$i \cdot j = k; \quad j \cdot i = -k$$

$$j \cdot k = i; \quad k \cdot j = -i$$

$$k \cdot i = j; \quad i \cdot k = -j.$$

Definimos as operações de adição e multiplicação em $Quat$ por

$$\begin{array}{rccc} +: & Quat \times Quat & \longrightarrow & Quat \\ (a + bi + cj + dk, a' + b'i + c'j + d'k)) & & \longmapsto & (a + a') + (b + b')i + (c + c')j + (d + d')k, \end{array}$$

$$\begin{array}{rccc} \cdot: & Quat \times Quat & \longrightarrow & Quat \\ (a + bi + cj + dk, a' + b'i + c'j + d'k)) & & \longmapsto & (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i + \\ & & & (ac' + ca' + db' - bd')j + (ad' + da' + bc' - cb')k. \end{array}$$

O elemento $0 = 0 + 0i + 0j + 0k$ é o elemento neutro de $Quat$. E o elemento $1 = 1 + 0i + 0j + 0k$ é a unidade de $Quat$. Com isso, é fácil ver que $Quat$ é um anel.

Como $j \cdot i \neq i \cdot j$, $Quat$ não é comutativo. Além disso, dado $x = a + bi + cj + dk \neq 0$, considere

$$y = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} \in Quat$$

e então $x \cdot y = y \cdot x = 1$. Logo Quat é um anel não comutativo com unidade sem divisores de zero e todo elemento não nulo possui inverso. Assim, Quat não é um corpo apenas porque não é comutativo. Neste caso, dizemos que $(Quat, +, \cdot)$ é um ***anel de divisão*** *(ou* ***corpo não comutativo****).*

Note que $\mathbb{R} \subset Quat$ e existem três cópias de $\mathbb{C}$ em Quat:

$$\{a + bi : a, b \in \mathbb{R}\}, \qquad \{a + cj : a, c \in \mathbb{R}\} \quad e \quad \{a + dk : a, d \in \mathbb{R}\}.$$

3.1.1 Subanéis

Sejam $(A, +, \cdot)$ um anel e $B \subset A$. Se $(B, +, \cdot)$ for um anel, dizemos que B é um **subanel** de A, isto é, se B for um subconjunto de A que herda a estrutura de anel de A.

Proposição 3.1 *Sejam $(A, +, \cdot)$ um anel e $B \subset A$. Então B é um subanel de A se, e somente se, as seguintes condições são verificadas:*

(i) $0 \in B$ *(o elemento neutro de A pertence a B);*

(ii) $x, y \in B \Rightarrow x - y \in B$ *(B é fechado para a diferença);*

(iii) $x, y \in B \Rightarrow x \cdot y \in B$ *(B é fechado para o produto).*

Demonstração: É claro que se B é um subanel, as condiçãoes $(i), (ii)$ e (iii) são satisfeitas. Reciprocamente, seja $B \subset A$ satisfazendo $(i), (ii)$ e (iii) e vamos mostrar que B é de fato, subanel de A.

- $B \neq \emptyset$, pois $0 \in B$ por (i);
- se $x \in B$ então por (i) e (ii) $0 - x = -x \in B$;
- se $x, y \in B$, pelo item anterior e por (ii), $x - (-y) = x + y \in B$ e B é fechado para a adição;
- por (iii) B é fechado para a multiplicação.

As demais propriedades são herdadas de A e portanto B é um subanel de A. ∎

Se B é subanel de A denotamos $B \leq A$.

Exemplo 3.10 *Seguem alguns exemplos de sequências de subanéis:*

- *Para todo $n \in \mathbb{N}$, $n\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Z}[\sqrt{p}]$, para p primo;*
- *Para p primo, $\mathbb{Q} \leq \mathbb{Q}[\sqrt{p}] \leq \mathbb{R} \leq \mathbb{C} \leq Quat$;*

Exemplo 3.11 *$\mathbb{Z}_2$ não é subanel de $\mathbb{Z}_3$, pois $\mathbb{Z}_2$ não é um subcojunto de $\mathbb{Z}_3$.*

Exemplo 3.12 *$2\mathbb{Z} \leq \mathbb{Z}$, mas apesar de $\mathbb{Z}$ possuir unidade, $2\mathbb{Z}$ não possui.*

Exemplo 3.13 *Sejam $A = M_2(\mathbb{R})$ e $B = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}$. É fácil ver que $B \leq A$, porém o elemento unidade de A e B são distintos. De fato, sabemos que*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

é a unidade de A, mas é claro que

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin B.$$

Mostremos que $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ é a unidade de B. Com efeito,

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

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

para todo $a \in \mathbb{R}$.

Um subanel B de um corpo $\mathbb{K}$ que também é um corpo é dito um **subcorpo** de $\mathbb{K}$.

Exemplo 3.14 *$\mathbb{Q}[\sqrt{p}]$ é um subcorpo de $\mathbb{R}$ e $\mathbb{Q}[i]$ é um subcorpo de $\mathbb{C}$.*

Proposição 3.2 *As únicas soluções da equação $x^2 = x$ em um domínio de integridade são 0 e 1.*

Demonstração: Seja $x \in D$ um domínio de integridade tal que $x^2 = x$. Daí

$$x^2 = x \Rightarrow x^2 - x = 0 \Rightarrow x(x-1) = 0 \Rightarrow x = 0 \quad \text{ou} \quad x = 1.$$

■

Corolário 3.1 *Seja D um domínio de integridade com unidade 1 e seja $B \leq D$ com unidade $1'$. Então $1 = 1'$.*

Demonstração: Por definição de unidade $1' \neq 0$. Além disso, $1'$ é raiz de $x^2 = x$, logo pela proposição anterior $1' = 1$. ■

Definição 3.2 *Um domínio de integridade D é dito de* ***característica*** 0 *se $m = 0$ sempre que $ma = 0$ com $a \in D$, $a \neq 0$. E dizemos que D tem* ***característica finita*** *se existe $a \in D$, $a \neq 0$, tal que $ma = 0$ para algum $m \in \mathbb{N} = \{1, 2, \ldots\}$. Daí, definimos a* ***característica*** *de D como sendo o menor inteiro positvo m tal que $ma = 0$ para algum $a \in D$, $a \neq 0$.*

Proposição 3.3 *Se D é um domínio de integridade e característica de D é p, então $p \cdot x = 0$ para todo $x \in D$.*

Demonstração: Se p é a característica de D então existe $a \neq 0$ em D tal que

$$p \cdot a = 0 \Rightarrow (p \cdot 1) \cdot a = 0 \Rightarrow p \cdot 1 = 0 \quad \text{ou} \quad a = 0 \Rightarrow p \cdot 1 = 0.$$

Daí, dado $x \in D$

$$p \cdot x = (p \cdot 1) \cdot x = 0 \cdot x = 0.$$

■

Proposição 3.4 *A caracterísitca de um domínio de integridade D ou é zero ou é um número primo.*

Demonstração: Seja m a característica de D e considere $m \neq 0$, logo devemos mostrar que m é primo.

Suponha que m não seja primo, isto é, m é composto, logo existem $a, b \in \mathbb{Z}$ tais que $1 < a, b < m$ e $m = a \cdot b$. Como m é a característica de D, para todo $x \in D$ temos

$$m \cdot x = 0 \Rightarrow (a \cdot b) \cdot x = 0 \Rightarrow (a \cdot 1)(b \cdot x) = 0 \Rightarrow a = a \cdot 1 = 0 \quad \text{ou} \quad b \cdot x = 0,$$

um absurdo, pois por um lado $a \neq 0$ e por outro, se tivéssemos $b \cdot x = 0$ teríamos que b seria a característica de D, pois $b < m$. Portanto devemos ter m primo. ■

Definição 3.3 *Seja A um anel. Chamamos de* ***centro*** *de A o seguinte conjunto*

$$Z(A) = \{x \in A : x \cdot y = y \cdot x, \ \forall \ y \in A\}.$$

Exemplo 3.15 *O centro do conjunto dos número inteiros é $Z(\mathbb{Z}) = \mathbb{Z}$ enquanto o centro do anel dos quatérnios é $Z(Quat) = \mathbb{R}$.*

Proposição 3.5 *Seja A um anel. O centro $Z(A)$ de A é um subanel comutativo de A.*

Demonstração: É claro que $Z(A) \subset A$ por definição.

- $0 \in Z(A)$, pois $0 \cdot x = 0 = x \cdot 0$, para todo $x \in A$;
- sejam $a, b \in Z(A)$, daí $ay = ya$ e $by = yb$, para todo $y \in A$. Então
$$(a-b)y = ay - by = ya - yb = y(a-b) \Rightarrow (a-b) \in Z(A);$$
- sejam $a, b \in Z(A)$, então
$$(a \cdot b) \cdot y = a \cdot \underbrace{(b \cdot y)}_{\in A} = (b \cdot y) \cdot a = b \underbrace{(y \cdot a)}_{\in A} = y(a \cdot b) \Rightarrow ab \in Z(A).$$

Portanto, $Z(A)$ é subanel de A e ainda se $a, b \in Z(A) \subset A$ então $a \cdot b = b \cdot a$, logo $Z(A)$ é comutativo. ■

3.1.2 Exercícios

(1) Calcule os divisores de zero dos seguintes anéis: $\mathbb{Z}_6$, $\mathbb{Z}_8$, $\mathbb{Z}_{18}$.

(2) Seja $f : \mathbb{Z} \to \mathbb{Z}$ uma função tal que $f(x+y) = f(x) + f(y)$ e $f(x \cdot y) = f(x) \cdot f(y)$ para quaisquer x e y em $\mathbb{Z}$. Prove que ou $f = I_{\mathbb{Z}}$ ou $f \equiv 0$ é a função constante zero.

(3) Seja $f : \mathbb{Q} \to \mathbb{Q}$ uma função tal que $f(x+y) = f(x) + f(y)$ e $f(x \cdot y) = f(x) \cdot f(y)$ para quaisquer x e y em $\mathbb{Q}$. Prove que ou $f = I_{\mathbb{Q}}$ ou $f \equiv 0$ é a função constante zero.

(4) Seja $f : \mathbb{R} \to \mathbb{R}$ uma função tal que $f(x+y) = f(x) + f(y)$ e $f(x \cdot y) = f(x) \cdot f(y)$ para quaisquer x e y em $\mathbb{R}$. Prove que, se f é contínua então ou $f = I_{\mathbb{R}}$ ou $f \equiv 0$ é a função constante zero.

(5) Prove que se $(A, +, \cdot)$ é um anel qualquer então para quaisquer $x, y \in A$ são válidas as seguintes propriedades:

   (a) $0 \cdot x = x \cdot 0 = 0$
   (b) $-(x \cdot y) = (-x) \cdot y = x \cdot (-y)$
   (c) Se existe $1 \in A$, então $(-1) \cdot x = -x$.

(6) Mostre que o conjunto
$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}$$
das matrizes reais 2×2 com as operações usuais de soma e produto de matrizes é um anel com unidade não comutativo e com divisores de zero.

(7) Sejam p um número primo e $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} : \ a, b \in \mathbb{Z}\}$. Mostre que $\mathbb{Z}[\sqrt{p}]$ com soma e produto definidos por

$$(a + b\sqrt{p}) + (c + d\sqrt{p}) = (a + c) + (b + d)\sqrt{p}$$

$$(a + b\sqrt{p}) \cdot (c + d\sqrt{p}) = (ac + pbd) + (bc + ad)\sqrt{p},$$

para quaisquer $a, b, c, d \in \mathbb{Z}$, é um domínio de integridade.

(8) Mostre que o anel $\mathcal{C}[0, 1]$ das funções reais contínuas definidas em $[0, 1]$ possui divisores de zero.

(9) Seja A um domínio de integridade e $a, b, c \in A$. Prove que, se $a \neq 0$ e $ab = ac$ então $b = c$.

(10) Sejam p um número primo e

$$A = \left\{ \frac{m}{n} \in \mathbb{Q} : mdc(p, n) = 1 \right\}.$$

Mostre que A é um anel com as operações usuais de fração.

11) Sejam D um domínio de integridade e $a \in D$, $a \neq 0$. Mostre que a função $\phi_a : D \to D$ dada por $\phi_a(x) = a \cdot x$ é injetiva. Em seguida, conclua que todo domínio de integridade finito é um corpo.

(12) Seja A um anel tal que $x^2 = x$ para todo $x \in A$. Mostre que A é um anel comutativo.

(13) Sejam A um anel, B um conjunto e $f : B \to A$ uma função bijetiva de B sobre A. Se para cada $x, y \in B$ definimos

$$x + y = f^{-1}(f(x) + f(y)) \quad \text{e} \quad x \cdot y = f^{-1}(f(x) \cdot f(y))$$

então prove que:

(a) $(B, +, \cdot)$ é um anel.

(b) $f(x + y) = f(x) + f(y)$ e $f(x \cdot y) = f(x) \cdot f(y)$ para quaisquer $x, y \in B$.

(14) Sejam $(A, \bar{+}, \bar{\cdot})$ e $(B, \oplus, \odot)$ anéis. Considere o conjunto

$$A \times B = \{(a, b) : a \in A, b \in B\},$$

com as operações de soma e produto definidas por

$$(a_1, b_1) + (a_2, b_2) = (a_1 \bar{+} a_2, b_1 \oplus b_2)$$

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \bar{\cdot} a_2, b_1 \odot b_2).$$

Mostre que $(A \times B, +, \cdot)$ é um anel. Este anel é chamado **produto direto** de A com B.

(15) Prove que se definirmos no conjunto $\Im(\mathbb{R})$ de todas as funções $f : \mathbb{R} \to \mathbb{R}$ a soma usual de função e considerarmos o produto dado por $(g \cdot f)(x) = g(f(x)$, então $\Im(\mathbb{R})$ não é um anel.

(16) Seja $\{B_i\}_{i\in\mathbb{N}}$ uma sequência de subanéis de um anel A. Prove que $B = \bigcap_{i\in\mathbb{N}} B_i$ é também um subanel de A.

(17) Seja $\{B_i\}_{i\in\mathbb{N}}$ uma sequência de subanéis de um anel A. Prove que, se $B - 0 \subset B_1 \subset \ldots \subset B_n \subset \ldots$ então $B = \bigcup_{i\in\mathbb{N}} B_i$ é também um subanel de A.

(18) Mostre que $\mathbb{Z}_3$ não é subanel de $\mathbb{Z}_5$.

(19) Sejam A um anel e $a \in A$. Prove que $B = \{x \in A : x \cdot a = a \cdot x\}$ é um subanel de A.

(20) Sejam A um anel e $a \in A$. Prove que $B = \{x \in A : x \cdot a = 0\}$ é um subanel de A.

(21) Seja $\{K_i\}_{i\in\mathbb{N}}$ uma sequência de subcorpos de um corpo K. Prove que $K = \bigcap_{i\in\mathbb{N}} K_i$ é também um subcorpo de K. Mostre também que a intersecção P de todos os subcorpos de um corpo K é o menor subcorpo de K (P é chamado **corpo primo** de K).

(22) Calcule todos os subanéis de $\mathbb{Z}_{12}$.

(23) Prove que se A é um anel de divisão então $Z(A)$ o centro de A é um corpo.

(24) Seja $(A, +, \cdot)$ um anel com unidade $1 \in A$. Defina duas novas operações no conjunto A usando as operações $+$ e $\cdot$ de A por

$$a \oplus b = a + b + 1, \quad \forall\ a, b \in A$$

$$a \odot b = a \cdot b + a + b, \quad \forall\ a, b \in A.$$

(a) Mostre que $(A, \oplus, \odot)$ é um anel.

(b) Qual é o elemento zero de $(A, \oplus, \odot)$?

(c) $(A, \oplus, \odot)$ possui unidade? Qual?

(25) Mostre que o centro $Z(M_2(\mathbb{R}))$ do anel das matrizes 2×2 com entradas reais é o conjunto

$$Z(M_2(\mathbb{R})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} :\ a \in \mathbb{R} \right\}.$$

3.2 Ideais

Seja A um anel e $I \subset A$ um subanel de A. Dizemos que I é um **ideal à esquerda** de A se $a \cdot x \in I$, para todo $a \in A$ e para todo $x \in I$ (simbolicamente $A \cdot I \subset I$). Dizemos ainda que I é um **ideal à direita** de A se $x \cdot a \in I$, para todo $a \in A$ e para todo $x \in I$ (simbolicamente $I \cdot A \subset I$). Se I é um ideal à esquerda e à direita simultaneamente, dizemos que I é um **ideal** de A, isto é

$$A \cdot I \subset I \quad \text{e} \quad I \cdot A \subset I.$$

Observação 3.2 *É claro que, se A é um anel comutativo as definições acima são equivalentes.*

Exemplo 3.16 *Sejam A um anel e $x_1, x_2, \ldots, x_n \in A$. O conjunto*

$$Ax_1 + Ax_2 + \cdots + Ax_n = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n : \ a_i \in A\}$$

*é um ideal à esquerda de A chamado de **ideal à esquerda gerado por** $x_1, x_2, \ldots, x_n \in A$.*

Se A é um anel, os conjuntos $\{0\}$ e A são ideais de A e são chamados **ideais triviais** de A. Os ideais não triviais de A são chamados **ideais próprios** de A.

Exemplo 3.17 *Seja $A = M_2(\mathbb{R})$ e considere os subanéis de A dados pelos conjuntos*

$$I = \left\{ \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} : a, c \in \mathbb{R} \right\} \quad e \quad J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}.$$

- *I é ideal à esquerda de A. De fato, dados $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in A$ e $\begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} \in I$ temos*

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} a_{11}a + a_{12}c & 0 \\ a_{21}a + a_{22}c & 0 \end{pmatrix} \in I \Rightarrow AI \subset I.$$

- *J é ideal à direita de A. De fato, dados $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in A$ e $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in J$ temos*

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} aa_{11} + ba_{21} & aa_{12} + ba_{22} \\ 0 & 0 \end{pmatrix} \in J \Rightarrow JA \subset J.$$

Proposição 3.6 *Os únicos ideais de $A = M_2(\mathbb{R})$ são os triviais.*

Demonstração: Seja I um ideal de A e assuma $I \neq \{0\}$. Daí existe $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in I$ com algum $a_{ij} \neq 0$, $1 \leq i, j \leq 2$. Sejam

$$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}; \quad e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}; \quad e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}; \quad e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Sabemos que $A \cdot I \subset I$ e $I \cdot A \subset I$, daí

$$e_{1s} \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot e_{m1} = \begin{pmatrix} a_{sm} & 0 \\ 0 & 0 \end{pmatrix} \in I$$

e

$$e_{2s} \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot e_{m2} = \begin{pmatrix} 0 & 0 \\ 0 & a_{sm} \end{pmatrix} \in I$$

Logo

$$\begin{pmatrix} a_{sm} & 0 \\ 0 & a_{sm} \end{pmatrix} \in I,$$

para todos s, m, com $1 \leq s, m \leq 2$. Se $a_{sm} \neq 0$ então existe $(a_{sm})^{-1}$, logo

$$\begin{pmatrix} (a_{sm})^{-1} & 0 \\ 0 & (a_{sm})^{-1} \end{pmatrix} \cdot \begin{pmatrix} a_{sm} & 0 \\ 0 & a_{sm} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in I.$$

Assim, para todos $a, b, c, d \in \mathbb{R}$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in I$$

e portanto $I = A = M_2(\mathbb{R})$. ■

Um anel é chamado **anel simples** se seus únicos ideais são os triviais.

Proposição 3.7 *Seja $(A, +, \cdot)$ um anel com unidade. Então $I \subset A$ é um ideal (à esquerda) de A se, e somente se, as seguintes condições são verificadas:*

(i) $x + y \in I$, para todos $x, y \in I$.

(ii) $ax \in I$, para todo $x \in I$ e para todo $a \in A$.

Demonstração: É claro que se $I \subset A$ é ideal (à esquerda) então os itens (i) e (ii) seguem direto da definição. Por outro lado, suponha válidos os item (i) e (ii) e vamos mostrar que I é ideal de A. Note que devemos mostrar apenas que I é subanel de A, já que a outra condição é exatamente a hipótese (ii).

- como $0 \in A$, por (ii) $0 = 0 \cdot x \in I$;
- como $1 \in A$, $-1 \in A$, daí por (ii) $-y \in I$ se $y \in I$, logo para $x, y \in I$, por (i) temos que $x + (-y) = x - y \in I$;
- por fim, por (ii), $x \cdot y \in I$, para quaisquer $x, y \in I$.

■

Exemplo 3.18 *Seja $n \geq 0$ um inteiro, daí $n\mathbb{Z} = \{nz : \ z \in \mathbb{Z}\}$ é um ideal de $\mathbb{Z}$.*

Exemplo 3.19 *Determinação de todos os ideais de $(\mathbb{Z}, +, \cdot)$.*

Já sabemos que $\{0\}, \mathbb{Z}$ e $n\mathbb{Z}$, para todo $n \geq 0$ e n inteiro, são ideais de $\mathbb{Z}$. Mostremos que todo ideal de $\mathbb{Z}$ é da forma $n\mathbb{Z}$ para algum inteiro $n \geq 0$.

Seja I um ideal qualquer de $\mathbb{Z}$. Se $I = \{0\}$, então $I = 0\mathbb{Z}$. Suponha $I \neq \{0\}$ e seja $n = min\{x \in I : \ x > 0\}$. Como $n \in I$ e I é ideal então

$$nz \in I, \ \forall \ z \in \mathbb{Z} \Rightarrow n\mathbb{Z} \subset I.$$

Agora seja h um elemento qualquer de I. Pelo algoritmo de Euclides, existem $q, r \in \mathbb{Z}$ tais que

$$h = n \cdot q + r, \quad 0 \leq r < n.$$

Como h e $nq \in I$,

$$r = h - nq \in I.$$

Mas n é o menor inteiro positivo de I, logo

$$r \in I \quad e \quad 0 \leq r < n \Rightarrow r = 0$$

e portanto $h = qn$, ou seja, $h \in n\mathbb{Z}$ e como h é elemento qualquer de I, segue que $I = n\mathbb{Z}$.

Definição 3.4 *Seja A um anel. Um ideal $I \subset A$ é dito **ideal principal à esquerda (à direita)** se existe $\alpha \in A$ tal que $I = A\alpha$ ($I = \alpha A$). Se $I = \alpha A = A\alpha$, I é dito simplesmente **ideal principal**. Um domínio de integridade no qual todo ideal é principal é chamado **domínio principal**.*

Observe que $n\mathbb{Z}$ é ideal principal de $\mathbb{Z}$ e pelo Exemplo 3.19 vimos que $\mathbb{Z}$ é um domínio principal.

Seja A um anel e $I \subset A$ um ideal de A. Dizemos que I é um **ideal maximal** em A se $I \neq A$ e os únicos ideais de A contendo I são I e A, isto é, se $J \subset A$ é ideal e $I \subset J$ então $J = I$ ou $J = A$.

Exemplo 3.20 *Seja $A = \mathcal{C}[0, 1]$ o anel das funções contínuas $f : [0, 1] \to \mathbb{R}$ com as operações usuais de adição e multiplicação de funções. Dessa forma A é um anel comutativo com unidade. Dado $b \in [0, 1]$, considere*

$$I = \{f \in A : f(b) = 0\}.$$

Mostremos que I é um ideal maximal de A:

- *I é um ideal de A.*
  De fato, é claro que $I \subset A$ por definição e ainda:

  (i) a função constante 0 pertence a I, pois anula b;

  (ii) sejam $f, g \in I$, daí $f(b) = 0 = g(b)$. Logo

  $$(f - g)(b) = f(b) - g(b) = 0 - 0 = 0 \Rightarrow (f - g) \in I;$$

  (iii) sejam $f \in A$ e $g \in I$, logo $g(b) = 0$ e daí

  $$(f \cdot g)(b) = f(b) \cdot g(b) = f(b) \cdot 0 = 0$$

  e portanto $(f \cdot g) \in I$.

  Então I é um ideal de A.

- *I é maximal em A.*
  Seja J um ideal de A tal que $I \subset J$. Se $I \neq J$ então existe $f \in J$ tal que $f \notin I$ e daí $f(b) = t \neq 0$. Por abuso de notação, seja t a função constante t, daí

  $$h = f - t \in I,$$

  pois $h(b) = f(b) - t = t - t = 0$. Então $t = f - h \in J$, pois $f \in J$ e $h \in I \subset J$. Além disso, a função constante $t^{-1} \in A$ e daí como J é ideal

  $$t^{-1} \cdot t = 1 \in J.$$

  Logo, se $1 \in J$ então $x = x \cdot 1 \in J$, para todo $x \in A$ e então $J = A$ e consequentemente I é maximal em A.

Teorema 3.1 *Seja $(\mathbb{K}, +, \cdot)$ um anel comutativo com unidade $1 \in \mathbb{K}$. Então as seguintes condições são equivalentes:*

(i) $\mathbb{K}$ é um corpo;

(ii) $\{0\}$ é um ideal maximal em $\mathbb{K}$;

(iii) os únicos ideais de $\mathbb{K}$ são os triviais.

Demonstração: $(i) \Rightarrow (ii)$ Sejam $\mathbb{K}$ um corpo e J ideal de $\mathbb{K}$ tal que $\{0\} \subset J \subset \mathbb{K}$. Suponha $J \neq \{0\}$, daí existe $a \in J$, $a \neq 0$. Como $\mathbb{K}$ é corpo, $a^{-1} \in \mathbb{K}$ e daí $1 = a^{-1} \cdot a \in J$, logo $J = \mathbb{K}$. E portanto $\{0\}$ é maximal em $\mathbb{K}$.

$(ii) \Rightarrow (iii)$ É imediato, já que se $J \neq \{0\}$ fosse ideal próprio de $\mathbb{K}$ teríamos uma contradição ao fato de $\{0\}$ ser maximal.

$(iii) \Rightarrow (i)$ Devemos mostrar que para todo $a \in \mathbb{K}$, $a \neq 0$, existe $b \in \mathbb{K}$ tal que $ab = 1$.

Seja $a \neq 0$, $a \in \mathbb{K}$ e defina $I = \mathbb{K}a$, o ideal gerado por a. É claro que, $a = 1 \cdot a \in I$, logo $I \neq \{0\}$ e por hipótese $\mathbb{K}$ só possui ideais triviais, então $I = \mathbb{K}$. Logo $1 \in I$ e então existe $b \in \mathbb{K}$ tal que $1 = b \cdot a$. ■

3.2.1 Anel quociente

Sejam A um anel qualquer e J um ideal de A. Defina a seguinte relação em A

$$x, y \in A, x \equiv y(modJ) \Leftrightarrow x - y \in J.$$

A relação $x \equiv y(modJ)$ é lida da seguinte maneira "x é congruente a y módulo J. Mostremos que a relação definida é uma relação de equivalência em A. De fato, sejam $x, y, z \in A$.

(i) Reflexividade

$$0 = x - x \in J \Rightarrow x \equiv x(modJ);$$

(ii) Simetria

$$x \equiv y(modJ) \Rightarrow x - y \in J \Rightarrow -(x - y) = y - x \in J \Rightarrow y \equiv x(modJ);$$

(iii) Transitividade

$$x \equiv y(modJ) \text{ e } y \equiv z(modJ) \Rightarrow x-y, y-z \in J \Rightarrow x-y+(y-z) = x-z \in J \Rightarrow x \equiv z(modJ).$$

Se $x \in A$, então

$$\overline{x} = \{y \in A : \ y \equiv x(modJ)\}$$

é a **classe de equivalência** do elemento $x \in A$ relativamente a relação $\equiv (modJ)$. Note que, se $y \in \overline{x}$ então

$$y - x \in J \Rightarrow y - x = j, j \in J \Rightarrow y = x + j, j \in J.$$

Por isso, também denotamos a classe de x por

$$\overline{x} = x + J = \{x + z : \ z \in J\}.$$

Chamaremos de **conjunto quociente de A pelo ideal** J o conjunto das classes de equivalência

$$\frac{A}{J} = \{\overline{x} = x + J : \ x \in A\}.$$

Proposição 3.8 *Sejam A um anel e J um ideal de A. Se $x \equiv x'(modJ)$ e $y \equiv y'(modJ)$ então:*

(a) $x + y \equiv (x' + y')(modJ)$;

(b) $x \cdot y \equiv (x' \cdot y')(modJ)$.

Demonstração:

(a) Por hipótese $(x - x') \in J$ e $(y - y') \in J$, daí

$$x + y - (x' + y') = (x - x') + (y - y') \in J.$$

(b) Por hipótese temos

$$x \equiv x'(modJ) \Rightarrow x = x' + j_1,\ j_1 \in J \quad \text{e}$$

$$y \equiv y'(modJ) \Rightarrow y = y' + j_2,\ j_2 \in J.$$

Daí

$$x \cdot y - x' \cdot y' = (x' + j_1)(y' + j_2) - x'y' = x'j_2 + j_1y' + j_1j_2 \in J.$$

■

Corolário 3.2 *Sejam A um anel e J um ideal de A. Se $\overline{x} = \overline{x'}$ e $\overline{y} = \overline{y'}$ então*

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

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

Teorema 3.2 *Sejam A um anel e J um ideal de A. Se $\overline{x} = x + J$ e $\dfrac{A}{J} = \{\overline{x} :\ x \in A\}$, então*

(a)

$$+ :\ \frac{A}{J} \times \frac{A}{J} \longrightarrow \frac{A}{J},\quad (\overline{x}, \overline{y}) \longmapsto \overline{x} + \overline{y} = \overline{x + y} \qquad e \qquad \cdot :\ \frac{A}{J} \times \frac{A}{J} \longrightarrow \frac{A}{J},\quad (\overline{x}, \overline{y}) \longmapsto \overline{x} \cdot \overline{y} = \overline{x \cdot y}.$$

definem duas operações (adição e multiplicação) em $\dfrac{A}{J}$.

(b) $\left(\dfrac{A}{J}, +, \cdot\right)$ *é um anel (chamado* ***anel quociente de*** *A* ***por*** *J);*

(c) se 1 é a unidade de A então $\overline{1}$ é a unidade de $\dfrac{A}{J}$;

(d) se A é comutativo então $\dfrac{A}{J}$ é comutativo.

Demonstração:

(a) Pelo corolário anterior as operações $+$, e $\cdot$ estão bem definidas no conjunto $\dfrac{A}{J}$;

(b) As propriedades de anel seguem de maneira simples das definições de $+$ e $\cdot$ dadas no item (a);

(c) Dado $\overline{x} \in \dfrac{A}{J}$, temos

$$\overline{x} \cdot \overline{1} = \overline{x \cdot 1} = \overline{x} = \overline{1 \cdot x} = \overline{1} \cdot \overline{x};$$

(d) se A é comutativo $xy = yx$, para quaisquer $x, y \in A$, daí

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y} = \overline{y \cdot x} = \overline{y} \cdot \overline{x},$$

para quaisquer $\overline{x}, \overline{y} \in \dfrac{A}{J}$.

■

Teorema 3.3 *Seja A um anel comutativo com unidade $1 \in A$ e J um ideal de A. Então*

$$J \quad \textit{é um ideal maximal em} \quad A \Leftrightarrow \frac{A}{J} \quad \textit{é um corpo.}$$

Demonstração:

Sejam J um ideal maximal de A e $\overline{a} \in \dfrac{A}{J} - \{\overline{0}\}$. Devemos mostrar que existe $\overline{b} \in \dfrac{A}{J}$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$.

Note que $L = Aa$ é ideal de A não nulo, pois $1 \cdot a = a \in L$. Daí

$$J + L = \{x + y : \ x \in J, y \in L\}$$

é um ideal de A que contém J e ainda $J + L \neq J$, pois $a \in L \subset J + L$ e $\overline{a} \neq \overline{0}$, logo $a \notin J$. Como J é maximal segue então que

$$J + L = A.$$

Daí $1 \in J + L$ e então existem $j \in J$ e $\ell \in L$ tais que

$$1 = j + \ell.$$

Mas se $\ell \in L = Aa$, existe $b \in A$ tal que $\ell = ba$. Então

$$1 = j + ba \Rightarrow \overline{1} = \overline{j + ba} = \overline{j} + \overline{ba} = \overline{0} + \overline{ba} = \overline{b} \cdot \overline{a}.$$

Reciprocamente, suponha que $\dfrac{A}{J}$ seja um corpo, daí $\overline{0}, \overline{1} \in \dfrac{A}{J}$ e $\overline{0} \neq \overline{1}$. Então $\overline{1} \notin J$, pois do contrário, teríamos $\overline{1} = \overline{0}$. Daí $J \neq A$. Seja $M \neq J$ ideal de A tal que $J \subset M \subset A$, assim, existe $a \in M$, $a \notin J$, isto é, $\overline{a} \neq \overline{0}$, $\overline{a} \in \dfrac{A}{J}$. Como $\dfrac{A}{J}$ é corpo, existe $\overline{b} \in \dfrac{A}{J}$ tal que

$$\overline{a}\overline{b} = \overline{1},$$

isto é,

$$ab \equiv 1(mod J) \Leftrightarrow ab - 1 \in J \Leftrightarrow \exists\ j \in J \quad \text{tal que} \quad ab - 1 = j.$$

Logo $1 = ab - j$. Mas $a \in M$, daí $ab \in M$ e ainda $j \in J \subset M$. Então $1 = ab - j \in M$ e $M = A$. Portanto J é ideal maximal em A. ■

Exemplo 3.21 *O anel quociente dos inteiros módulo n é*

$$\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

3.2.2 Exercícios

(1) Mostre que a intersecção de ideais de um anel A é também um ideal de A.

(2) Seja $\{I_n\}_{n\in\mathbb{N}}$ uma família de ideais de um anel A. Mostre que, se $J_0 \subset J_1 \subset \ldots \subset J_n \subset \ldots$ então $J = \bigcup_{n\in\mathbb{N}} J_n$ é um ideal de A.

(3) Seja A um anel e $a \in A$. Mostre que $I = \{x \in A : x \cdot a = 0\}$ é um ideal à esquerda de A.

(4) Sejam I e J ideais de um anel A. Mostre que $I + J = \{x + y :\ x \in I,\ y \in J\}$ é um ideal de A.

(5) Seja I um ideal à esqeurda e J um ideal à direita do anel A. Mostre que

$$I \cdot J = \{\sum_{i=1}^{n} x_i \cdot y_i :\ n \in \mathbb{N}, x_i \in I, y_i \in J\}$$

é um ideal de A.

(6) Seja $(I, +, \cdot)$ um ideal de um anel $(A, +, \cdot)$ com elemento unidade 1. Mostre que:

(a) Se $1 \in I$, então $I = A$.

(b) Se $a \in A$ é inversível e $a \in I$, então $I = A$.

(7) Sejam $(I, +, \cdot)$ e $(J, +, \cdot)$ ideais de um anel $(A, +, \cdot)$ tais que $I \cap J = \{0\}$. Mostre que $a \cdot b = 0$, quaisquer que sejam $a \in I$ e $b \in J$.

(8) Seja I um ideal do anel A e $a \in A$ um elemento fixado. Mostre que o conjunto

$$\langle I, a \rangle = \{i + ra : \ i \in I \quad \text{e} \quad r \in A\}$$

é um ideal de A.

(9) Sejam A um anel comutativo e $N = \{x \in A : x^n = 0, \quad \text{para algum} \quad n \in \mathbb{N} \setminus \{0\}\}$. Mostre que N é um ideal de A (N é chamado de **radical** de A). Além disso, mostre que se $\bar{x} \in \dfrac{A}{N}$ e $\bar{x}^n = \bar{0}$ para algum inteiro $n \geq 1$ então $\bar{x} = \bar{0}$. (Sugestão: Prove que se $x^n \in \mathbb{N}$ para algum inteiro $n \geq 1$ então $x \in \mathbb{N}$.)

(10) Seja n um inteiro positivo que não é primo. Mostre que o anel $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, +, \cdot\right)$ não é um domínio de integridade.

(11) Seja A um anel comutativo com unidade $1 \in A$, e seja P um ideal de A. Dizemos que P é um **ideal primo** de A se $P \neq A$ e para todos $x, y \in A$, se $x \cdot y \in P$ então $x \in P$ ou $y \in P$. Mostre que:

(a) P é um ideal primo de A se e somente se $\dfrac{A}{P}$ é um domínio de integridade.

(b) os únicos ideias primos de $\mathbb{Z}$ são $\{0\}$ e os ideais principais $p \cdot \mathbb{Z}$, onde p é um número primo.

(c) se P é um ideal maximal de A então P é um ideal primo de A.

(12) Seja $A = \mathcal{C}[0, 1]$ o anel das funções reais contínuas (com as operações usuais de soma e produto de funções) definidas no intervalo $[0, 1]$. Mostre que, se M é um ideal maximal de A então existe $a \in [0, 1]$ tal que

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

3.3 Homomorfismos de anéis

Sejam A e B dois anéis. Uma aplicação $f : A \to B$ é um **homomorfismo** de A em B se satisfaz

(i) $f(x+y) = f(x) + f(y)$, para todos $x, y \in A$;

(ii) $f(x \cdot y) = f(x) \cdot f(y)$, para todos $x, y \in A$.

Exemplo 3.22 *Sejam A e B anéis. A aplicação*

$$\begin{array}{rccc} f: & A & \longrightarrow & B \\ & a & \longmapsto & f(a) = 0 \end{array}$$

é um homomorfismo chamado ***homomorfismo nulo****.*

Exemplo 3.23 *Seja A um anel. A aplicação*

$$\begin{array}{rccc} I_A: & A & \longrightarrow & A \\ & a & \longmapsto & I_A(a) = a \end{array}$$

é um homomorfismo chamado ***homomorfismo identidade de*** *A.*

Exemplo 3.24 *Sejam A um anel e J um ideal de A. A* ***projeção canônica***

$$\begin{array}{rccc} \pi: & A & \longrightarrow & \dfrac{A}{J} \\ & a & \longmapsto & \pi(a) = \overline{a} \end{array}$$

é tal que

$$\pi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \pi(a) + \pi(b),$$
$$\pi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \pi(a) + \pi(b),$$

isto é, π é um homomorfismo.

Exemplo 3.25 *Seja A um anel com unidade 1_A. Para todo $n \in \mathbb{Z}$, $n \geq 0$ defina:*

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & A \\ & n & \longmapsto & f(n) = \underbrace{1_A + 1_A + \cdots + 1_A}_{n \ vezes} \\ & -n & \longmapsto & f(-n) = \underbrace{(-1_A) + (-1_A) + \cdots + (-1_A)}_{n \ vezes}. \end{array}$$

Definido assim, f é um homomorfismo de anéis.

Proposição 3.9 *Sejam A e B anéis e $f: A \to B$ um homomorfismo. Então*

(a) $f(0_A) = 0_B$;

(b) $f(-a) = -f(a)$, para todo $a \in A$;

(c) se A e B são domínios de integridade então ou f é a função constante zero ou $f(1_A) = 1_B$;

(d) se A e B são corpos então ou f é a função constante zero ou f é injetiva.

Demonstração:

(a) Temos

$$f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A) \Rightarrow$$

$$f(0_A) - f(0_A) = f(0_A) + f(0_A) - f(0_A) \Rightarrow 0_b = f(0_A).$$

(b) Seja $a \in A$, pelo item (a) temos

$$0_B = f(0_A) = f(a - a) = f(a) + f(-a) \Rightarrow$$

$$0_B - f(a) = f(a) - f(a) + f(-a) \Rightarrow -f(a) = f(-a).$$

(c) Dado $a \in A$, $f(a) = f(a \cdot 1_A) = f(a) \cdot f(1_A)$. Em particular,

$$f(1_A) = f(1_A)f(1_A) \Rightarrow f(1_A)(1_B - f(1_A)) = 0_B,$$

daí, como B é domínio de integridade

$$f(1_A) = 0_B \Rightarrow f(a) = 0, \ \forall a \in A$$

ou

$$1_B - f(1_A) = 0_B \Rightarrow f(1_A) = 1_B.$$

(d) Suponha que f não seja a função constante zero e considere $a_1, a_2 \in A$ tais que $f(a_1) = f(a_2)$. Daí

$$f(a_1) - f(a_2) = 0_B \Rightarrow f(a_1 - a_2) = 0_B.$$

Se $a_1 - a_2 \neq 0$, como A é corpo, existe $x \in A$ tal que $(a_1 - a_2) \cdot x = 1$. Então

$$f(a_1 - a_2) \cdot f(x) = f(1_A) = 1_B,$$

mas por outro lado

$$f(a_1 - a_2) = 0_B \Rightarrow f(a_1 - a_2) \cdot f(x) = 0_B,$$

um absurdo, pois $0_B \neq 1_B$. Portanto $a_1 = a_2$ e f é injetiva.

■

Se $f : A \to B$ é um homomorfismo bijetor dizemos que f é um **isomorfismo**. Neste caso, dizemos que A e B são **isomorfos** e denotamos por $A \simeq B$.

Se $f : A \to A$ é um homomorfismo de A em A, ele é dito um **endomorfismo** de A. E se $f : A \to A$ é um isomorfismo de A em A, ele é dito um **automorfismo** de A. Vamos denotar os conjuntos de endomorfismos e automorfismos de A respectivamente, por:

$$End(A) = \{f : A \to A : \ f \quad \text{é endomorfismo}\} \quad \text{e}$$

$$Aut(A) = \{f : A \to A : \ f \quad \text{é automorfismo}\}.$$

Exemplo 3.26 $Aut(\mathbb{Z}) = \{I_{\mathbb{Z}}\}$.

Exemplo 3.27 $Aut(\mathbb{Q}) = \{I_{\mathbb{Q}}\}$.

Exemplo 3.28 *Seja $D = \mathbb{Z}[\sqrt{p}]$, para algum primo p. Vamos determinar $Aut(D)$. Sabemos que D é um domínio de integridade, daí pelo item (c) da Proposição 3.9, se $f \in Aut(D)$ então $f(1) = 1$. Logo $f(x) = x$, para todo $x \in \mathbb{Z}$. Assim, se $f \in Aut(D)$ e $x + y\sqrt{p}$ é um elemento qualquer de D, temos*

$$f(x + y\sqrt{p}) = x + yf(\sqrt{p}).$$

Agora note que

$$(\sqrt{p})^2 = p \Rightarrow f((\sqrt{p})^2) = f(p) \Rightarrow f(\sqrt{p}) \cdot f(\sqrt{p}) = f(p) = p \Rightarrow f(\sqrt{p}) = \sqrt{p} \quad ou \quad f(\sqrt{p}) = -\sqrt{p}.$$

No primeiro caso f é o homomorfismo identidade, enquanto no segundo caso temos

$$f(x + y\sqrt{p}) = x - y\sqrt{p}, \quad \forall\ x, y \in \mathbb{Z}.$$

Portanto

$$Aut(D) = \{I_D, \sigma\},$$

onde

$$\sigma(x + y\sqrt{p}) = x - y\sqrt{p}, \quad \forall\ x, y \in \mathbb{Z}.$$

Proposição 3.10 $Aut(\mathbb{R}) = \{I_{\mathbb{R}}\}$.

Demonstração: Como $\mathbb{R}$ é corpo, $f(1) = 1$ e daí $f(m) = m$, para todo $m \in \mathbb{Z}$. Agora sejam a, b inteiros não nulos tais que $mdc(a, b) = 1$ e note que

$$1 = f\left(b \cdot \frac{1}{b}\right) = f(b) \cdot f\left(\frac{1}{b}\right) = b \cdot f\left(\frac{1}{b}\right) \Rightarrow f\left(\frac{1}{b}\right) = \frac{1}{b}.$$

Daí

$$f\left(\frac{a}{b}\right) = f\left(a \cdot \frac{1}{b}\right) = f(a) \cdot f\left(\frac{1}{b}\right) = a \cdot \frac{1}{b} = \frac{a}{b},$$

portanto $f(x) = x$, para todo $x \in \mathbb{Q}$. Mostremos agora que f preserva a ordem em $\mathbb{R}$, isto é,

$$x < y \Rightarrow f(x) < f(y).$$

De fato,

$$x < y \Rightarrow y - x > 0 \Rightarrow y - x = \alpha^2, \quad \text{para algum} \quad \alpha \in \mathbb{R},$$

então

$$f(y) - f(x) = f(y - x) = f(\alpha^2) = f(\alpha) \cdot f(\alpha) = (f(\alpha))^2 > 0 \Rightarrow f(y) > f(x).$$

Dado $x \in \mathbb{R}$, considere $\{r_n\}_{n\geq 1}$ e $\{s_n\}_{n\geq 1}$ sequências de racionais tais que

$$r_n < x < s_m, \quad \forall\ n, m \in \mathbb{N} \quad \text{e} \quad x = \lim_{n\to\infty} r_n = \lim_{m\to\infty} s_m.$$

Assim,

$$r_n = f(r_n) < f(x) < f(s_m) = s_m, \quad \forall\ n, m \in \mathbb{N}.$$

Logo, pelo teorema do confronto, $f(x) = \lim_{n\to\infty} r_n = x$, isto é, $f \equiv I_{\mathbb{R}}$. ■

3.3.1 Núcleo e imagem de um homomorfismo

Sejam A e B anéis e $f : A \to B$ um homomorfismo entre esses anéis. Chamamos de **núcleo** de f o conjunto definido por

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

E chamamos de **imagem** de f o conjunto definido por

$$Im(f) := \{f(a) :\ a \in A\} \subset B.$$

É um exercício relativamente simples mostrar a seguinte proposição:

Proposição 3.11 *Seja $f : A \to B$ um homomorfismo de anéis. Então*

(i) $Im(f)$ é um subanel de B;

(ii) $ker(f)$ é um ideal de A;

(iii) f é injetivo se e somente se $ker(f) = \{0\}$.

Teorema 3.4 (Teorema do Homomorfismo) *Seja $f : A \to B$ um homomorfismo de anéis, então os anéis $\dfrac{A}{ker(f)}$ e $Im(f)$ são isomorfos.*

Demonstração: Defina

$$\begin{array}{rccc} \phi: & \dfrac{A}{ker(f)} & \longrightarrow & Im(f) \\ & \overline{a} & \longmapsto & \phi(a) = f(a). \end{array}$$

- ϕ está bem definida e é injetora. De fato, dados $\overline{a}, \overline{b} \in \dfrac{A}{ker(f)}$ temos

  $\overline{a} = \overline{b} \Leftrightarrow a \equiv b(mod(ker(f))) \Leftrightarrow a-b \in ker(f) \Leftrightarrow f(a-b) = 0 \Leftrightarrow f(a) = f(b) \Leftrightarrow \phi(\overline{a}) = \phi(\overline{b})$;

- é claro que ϕ é sobrejetora, pois para $f(a) \in Im(f)$, basta tomarmos $\overline{a} \in \dfrac{A}{Im(f)}$ e daí $\phi(\overline{a}) = f(a)$;

- ϕ é homomorfismo. De fato, para $\overline{a}, \overline{b} \in \dfrac{A}{ker(f)}$,

$$\phi(\overline{a} + \overline{b}) = \phi(\overline{a+b}) = f(a+b) = f(a) + f(b) = \phi(\overline{a}) + \phi(\overline{b}) \quad \text{e}$$
$$\phi(\overline{a} + \cdot\overline{b}) = \phi(\overline{a \cdot b}) = f(a \cdot b) = f(a) \cdot f(b) = \phi(\overline{a}) \cdot \phi(\overline{b}).$$

Logo ϕ é um isomorfismo e daí $\dfrac{A}{ker(f)} \simeq Im(f)$. ■

Exemplo 3.29 *Sejam $A = \mathcal{C}[0,1] = \{f : [0,1] \to \mathbb{R};\ f \quad$ é contínua$\}$ e $I = \{f \in A : f(0) = 0\}$. Já sabemos do Exemplo 3.20 que I é ideal maximal em A, logo pelo Teorema 3.3 $\dfrac{A}{I}$ é um corpo. Mostremos que $\dfrac{A}{I} \simeq \mathbb{R}$.*

Dado $a \in \mathbb{R}$, denotaremos por f_a a função constante a, isto é,

$$\begin{array}{rccc} f_a: & [0,1] & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & f_a(x) = a. \end{array}$$

Defina

$$\begin{array}{rccc} \phi: & A & \longrightarrow & \mathbb{R} \\ & f & \longmapsto & \phi(f) = f(0). \end{array}$$

- *ϕ é homomorfismo:*

$$\phi(f+g) = (f+g)(0) = f(0) + g(0) = \phi(f) + \phi(g),$$
$$\phi(f \cdot g) = (f \cdot g)(0) = f(0) \cdot g(0) = \phi(f) \cdot \phi(g);$$

- $ker(f) = \{f \in A : \ \phi(f) = 0\} = \{f \in A : \ f(0) = 0\} = I$;
- ϕ *é sobrejetora, isto é,* $Im(\phi) = \mathbb{R}$. *De fato, dado* $a \in \mathbb{R}$, $\phi(f_a) = f_a(0) = a$.

Portanto, pelo Teorema do Homomorfismo

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

3.3.2 Exercícios

(1) Sejam $f : A \to B$ e $g : B \to C$ homomorfismos de anéis. Mostre que $g \circ f : A \to C$ é um homorfismo do anel A em C.

(2) Seja $f : A \to B$ um homomorfismo de anéis. Mostre que:

(a) $Im\, f$ é um subanel de B;

(b) $Ker\, f$ é um ideal de A;

(c) f é injetivo se e somente se $Ker\, f = \{0\}$.

(3) Calcule $End(\mathbb{Z}[i])$ e $Aut([\mathbb{Q}[i])$.

(4) Mostre que $f : \mathbb{C} \to M_2(\mathbb{R})$ dada por

$$f(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

é um monomorfismo de anéis, isto é, é um homomorfismo injetivo.

(5) Sejam $A = \{a + b\sqrt{-2} : \ a, b \in \mathbb{Q}\}$ e $B = M_2(\mathbb{Q})$. Mostre que $f : A \to B$ dada por $f(a + b\sqrt{-2}) = \begin{pmatrix} a & -2b \\ b & a \end{pmatrix}$ é um homomorfismo. f é isomorfismo? Justifique.

(6) Prove que os anéis $2\mathbb{Z}$ e $3\mathbb{Z}$ não são isomorfos.

(7) Seja A um anel. Mostre que

(a) se $f, g \in End(A)$ então $(f+g) \in End(A)$, onde $(f+g)(x) = f(x)+g(x), \quad \forall\ x \in A$.

(b) se $f, g \in End(A)$ então $(f \cdot g) \in End(A)$, onde $(f \cdot g)(x) = f(g(x)), \quad \forall\ x \in A$.

(c) (End(A), $+, \cdot$) é um anel com as operações definidas em (a) e (b).

(8) Sejam A e B anéis. Defina $+$ e $\cdot$ no conjunto $A \times B = \{(a, b) : \ a \in A, b \in B\}$ de modo que $A \times B$ seja um anel com essas operações.

(9) Se $A \times B$ é o anel definido no exercício anterior. Prove que

$$\begin{array}{rcl} \pi_1 : A \times B & \to & A \\ (a,b) & \mapsto & a \end{array} \quad \text{e} \quad \begin{array}{rcl} \pi_2 : A \times B & \to & B \\ (a,b) & \mapsto & b \end{array}$$

são epimorfismos, isto é, homomorfismos sobrejetivos. Calcule os núcleos de π_1 e π_2.

(10) Seja $f : A \to B$ um homomorfismo e J um ideal de B. Prove que

$$f^{-1}(J) = \{a \in A : \ f(a) \in J\}$$

é um ideal de A.

(11) Seja $F : \mathcal{C}[0,1] \to \mathbb{R}$ definida por $F(f) = f(\frac{1}{2})$, para todo $f \in \mathcal{C}[0,1]$.

(a) Prove que F é um homomorfismo.

(b) Calcule $Im\, F$ e $Ker\,(F)$.

(c) Identifique o anel $\dfrac{\mathcal{C}[0,1]}{Ker\,(F)}$.

(12) Sejam A e B anéis, $\varphi : A \to B$ um homomorfismo de anéis e I um ideal do anel A. Defina a função

$$\begin{array}{rccc} h : & \dfrac{A}{I} & \to & \dfrac{B}{f(I)} \\ & a + I & \mapsto & f(a) + f(I). \end{array}$$

Mostre que h é um isomorfismo entre os anéis $\dfrac{A}{I}$ e $\dfrac{B}{f(I)}$

(13) Seja A um anel com unidade $1 \in A$. E seja $e \in A$, $e \neq 0$ tal que $e^2 = e$ (e diz-se um elemento **idempotente** de A). Se $A_1 = A \cdot e = \{a \cdot e : \ a \in A\}$ e se $A_2 = A \cdot (1 - e) = \{a - a \cdot e : \ a \in A\}$, então mostre que:

(a) A_1 e A_2 são subanéis de A tais que $A_1 \cap A_2 = \{0\}$.

(b) $A = A_1 \oplus A_2$ (isto é, para todo $a \in A$, existem únicos elementos $a_1 \in A_1$ e $a_2 \in A_2$ tais que $a = a_1 + a_2$).

(14) Seja A um anel com unidade $1 \in A$ e sejam $e_1, e_2, \ldots, e_n \in A \setminus \{0\}$ idempotentes de A tais que $1 = e_1 + \ldots + e_n$, $e_i \cdot e_j = 0$ se $i \neq j$, $1 \leq i, j \leq n$. Mostre que, se $A_i = A \cdot e_i = \{a \cdot e_i : \ a \in A\}$ então $A = A_1 \oplus \ldots \oplus A_n$ (isto é, para todo $a \in A$, existem únicos elementos $a_i \in A_i$, $i = 1, \ldots, n$, tais que $a = a_1 + \ldots + a_n$).

CAPÍTULO 4

POLINÔMIOS

4.1 Polinômios com coeficientes em anéis

Seja A um anel e considere $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Chamamos de **polinômio sobre** A (ou **polinômio com coeficientes em** A) em uma **indeterminada** x uma expressão do tipo

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m + \cdots ,$$

onde $a_j \in A$ e existe $n \in \mathbb{N}_0$ tal que $a_j = 0$ para todo $j \geq n$. Os elementos a_j são chamados os **coeficientes** do polinômio $p(x)$ para todo $0 \leq j < n$ e o coeficiente a_0 é chamado ainda de **termo constante** de $p(x)$.

Se $p(x) = 0 + 0x + \cdots + 0x^m + \cdots$ indicaremos $p(x)$ simplesmente por 0 e o chamaremos de **polinômio identicamente nulo** sobre A, isto é, $a_j = 0$ para todo $j \in \mathbb{N}_0$. E para $a \in A$, chamamos o polinômio $p(x) = a$ de **polinômio constante** a.

Dizemos que dois polinômios $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m + \cdots$ e $q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_kx^k + \cdots$ sobre A são iguais se, e somente se $a_j = b_j$ em $\mathbb{A}$, para todo $j \in \mathbb{N}_0$.

Se $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots$ é tal que $a_n \neq 0$ e $a_j = 0$ para todo $j > n$ dizemos que n é o **grau do polinômio** $p(x)$ e, neste caso escrevemos $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ e denotamos o grau de $p(x)$ por $gr(p(x)) = n$.

Denotaremos por $A[x]$ o conjunto de todos os polinômios com coeficientes em A em uma indeterminada x, isto é,

$$A[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : \ a_j \in A, \, 0 \leq j \leq n, \ n \in \mathbb{N}_0\}.$$

Se identificarmos os elementos $a \in A$ com os polinômios constantes $p(x) = a$ podemos pensar em $A[x]$ contendo uma cópia de A e muitas vezes por abuso de notação escreveremos e usaremos $A \subset A[x]$.

Observe que o grau do polinômio nulo não está definido, porém os graus dos demais polinômios estão bem definidos e podemos interpretar o grau como um função

$$\begin{array}{rccl} \partial: & A[x]-\{0\} & \longrightarrow & \mathbb{N}_0 \\ & p(x) & \longmapsto & \partial(p(x)) = gr(p(x)). \end{array}$$

Se $p(x)$ é um polinômio de grau n, chamamos a_n de **coeficiente líder** e se $a_n = 1$ o polinômio é chamado de **polinômio mônico**.

Exemplo 4.1 *$p(x) = \frac{1}{7} + 2x + 7x^4 + \sqrt{3}x^5$, $q(x) = \frac{3}{7}$, $f(x) = x$ são exemplos de polinômios em $\mathbb{R}[x]$.*

Exemplo 4.2 *$p(x) = -2 + 3x + 4x^7 - 3x^{12}$, $q(x) = x + x^2 + x^3$ são exemplos de polinômios em $\mathbb{Z}[x]$.*

Exemplo 4.3 *Os polinômios $h(x) = -1 + 2x + \frac{1}{3}x^4 + x^6$ e $f(x) = 1 + 2x + \frac{1}{3}x^4 + x^6$ de $\mathbb{Q}[x]$ não são iguais, pois os termos constantes dos dois polinômios são diferentes, portanto $h(x) \neq f(x)$.*

Exemplo 4.4 *Os polinômios $q(x) = 3$, $p(x) = x + x^2 - x^3$ e $f(x) = 1 - x^5$ de $\mathbb{Z}[x]$ têm, respectivamente, graus $gr(q(x)) = 0$, $gr(p(x)) = 3$ e $gr(f(x)) = 5$.*

Note que, para $p(x) \in A[x]$, temos $gr(p(x) = 0$ se, e somente se, $p(x) = a \neq 0$, $a \in A$.

Utilizando as operações de adição e multiplicação do anel A podemos definir a adição e multiplicação em $A[x]$. Sejam $p(x) = \sum_{j=0}^{n} a_j x^j$ e $q(x) = \sum_{j=0}^{n} b_j x^j$ polinômios em $A[x]$, definimos a adição destes polinômios como segue

$$p(x) + q(x) = \sum_{j=0}^{n} c_j x^j,$$

onde $c_j = a_j + b_j$, para $0 \leq j \leq n$. Observe que segue direto da definição de adição que

$$gr(p(x) + q(x)) \leq \max\{gr(p(x)), gr(q(x))\}, \quad \forall\ p(x), q(x) \in A[x] - \{0\}.$$

Exemplo 4.5 *Sejam $p(x) = 2 + 3x - x^2 - 5x^4$ e $q(x) = -3x + 4x^2 + 3x^4 - x^5$ polinômios em $\mathbb{Z}[x]$. Então*

$$\begin{aligned} p(x) + q(x) &= (2+0) + (3+(-3))x + (-1+4)x^2 + (0+0)x^3 + (-5+3)x^4 + (0+(-1))x^5 \\ &= 2 + 3x^2 - 2x^4 - x^5. \end{aligned}$$

Sejam $p(x) = \sum_{j=0}^{n} a_j x^j$ e $q(x) = \sum_{j=0}^{m} b_j x^j$ polinômios em $A[x]$, definimos a multiplicação destes polinômios como segue

$$p(x) \cdot q(x) = \sum_{j=0}^{n+m} c_j x^j,$$

onde

$$\begin{aligned}
c_0 &= a_0 \cdot b_0 \\
c_1 &= a_0 \cdot b_1 + a_1 \cdot b_0 \\
c_2 &= a_0 \cdot b_2 + a_1 b_1 + a_2 \cdot b_0 \\
&\vdots \\
c_j &= \sum_{\lambda+\mu=j} a_\lambda \cdot b_\mu \\
&\vdots \\
c_{n+m} &= a_n \cdot b_m.
\end{aligned}$$

Exemplo 4.6 *Sejam $p(x) = 2 + x - 2x^2$ e $q(x) = -1 + 3x$ polinômios em $\mathbb{Z}[x]$, então*

$$\begin{aligned}
p(x) \cdot q(x) &= (2 \cdot (-1)) + (2 \cdot 3 + 1 \cdot (-1))x + (1 \cdot 3 + (-2) \cdot (-1))x^2 + (-2 \cdot 3)x^3 \\
&= -2 + 5x + 5x^2 - 6x^3.
\end{aligned}$$

Como consequência das propriedades de adição e multiplicação do anel A temos a seguinte proposição:

Proposição 4.1 *Seja A um anel comutativo com unidade 1.*

(i) A adição e multiplicação em $A[x]$ têm as seguintes propriedades, para quaisquer $p(x), q(x), h(x)$ em $A[x]$:

- *Associativa*
$$(p(x) + q(x)) + h(x) = p(x) + (q(x) + h(x)) \quad e$$
$$(p(x) \cdot q(x)) \cdot h(x) = p(x) \cdot (q(x) \cdot h(x));$$
- *Comutativa*
$$p(x) + q(x) = q(x) + p(x) \quad e$$
$$p(x) \cdot q(x) = q(x) \cdot p(x);$$
- *Distributiva*
$$p(x) \cdot (q(x) + h(x)) = p(x) \cdot q(x) + p(x) \cdot h(x);$$

- *Existência do elemento neutro da adição. O polinômio nulo é tal que* $p(x)+0 = p(x)$ *qualquer que seja* $p(x) \in A[x]$;
- *Existência do simétrico. Dado* $p(x) = a_0 + a_1x + \cdots a_nx^n \in A[x]$*, o simétrico de* $p(x)$*é o polinômio* $-p(x) = (-a_0) + (-a_1)x + \cdots + (-a_n)x^n$;
- *Existência do elemento neutro da multiplicação. O polinômio constante 1 é tal que* $p(x) \cdot 1 = p(x)$ *qualquer que seja* $p(x) \in A[x]$.

Portanto $A[x]$ *é um anel comutativo com unidade.*

(ii) Se D *é um domínio de integridade então* $D[x]$ *é um domínio de integridade. Em particular, se* $\mathbb{K}$ *é um corpo,* $\mathbb{K}[x]$ *é um domínio de integridade.*

Assim, se $p(x)$ e $q(x)$ são polinômios não nulos em $D[x]$, onde D é um domínio de integridade e com coeficientes líderes a_n e b_m, respectivamente, então o polinômio $p(x) \cdot q(x)$ tem coeficiente líder $a_n \cdot b_m$ e portanto

$$gr(p(x) \cdot q(x)) = gr(p(x)) + gr(q(x)).$$

Na proposição anterior vimos que a natureza algébrica de A nos dá informações sobre a estrutura de $A[x]$, logo poderíamos esperar que se $\mathbb{K}$ é um corpo então $\mathbb{K}[x]$ também deveria ser um corpo. Isso não ocorre como veremos na proposição a seguir. Portanto o que temos para este caso é o que já foi enunciado no item (ii) da proposição anterior: se $\mathbb{K}$ é corpo, $\mathbb{K}[x]$ é um domínio de integridade.

Proposição 4.2 *Seja* $\mathbb{K}$ *um corpo. Os únicos polinômios invertíveis em* $\mathbb{K}[x]$ *são os polinômios constantes não nulos.*

Demonstração: Seja $p(x) \neq 0$ um polinômio em $\mathbb{K}[x]$ que possua inverso multiplicativo $q(x) \in \mathbb{K}[x]$. Daí

$$p(x) \cdot q(x) = 1.$$

Analisando o grau do produto e sabendo que $\mathbb{K}[x]$ é um domínio de integridade temos

$$gr(p(x)) + gr(q(x)) = gr(p(x) \cdot q(x)) = gr(1) = 0 \Rightarrow gr(p(x)) = 0 \quad \text{e} \quad gr(q(x)) = 0.$$

Portanto $p(x)$ deve ser um polinômio constante não nulo. ■

4.2 Algoritmo da divisão

No que segue, a menos que mencionemos o contrário, estaremos considerando o anel de polinômios $\mathbb{K}[x]$ sobre um corpo $\mathbb{K}$, que já sabemos ser um domínio de integridade. Muitos

dos resultados que veremos podem ser adaptados considerando o anel de polinômios $A[x]$ com A sendo um domínio de integridade. No entanto, na maioria teríamos que considerar polinômios com coeficientes líderes invertíveis. Para evitarmos esse trabalho utilizaremos o corpo $\mathbb{K}$ onde sabemos que todos os elementos não nulos são invertíveis.

Iniciaremos nossa discussão com a introdução do conceito de divisibilidade em $\mathbb{K}[x]$. Dados $p(x)$ e $q(x) \in \mathbb{K}[x]$, se existe $h(x) \in \mathbb{K}[x]$ tal que $p(x) = q(x) \cdot h(x)$, dizemos que $p(x)$ é **múltiplo** de $q(x)$. Nesse caso, se $q(x) \neq 0$ dizemos que $q(x)$ **divide** $p(x)$ ou que $q(x)$ é um **divisor** de $p(x)$ e escrevemos $q(x)|p(x)$.

Teorema 4.1 (Algoritmo da divisão) *Sejam $f(x), g(x) \in \mathbb{K}[x]$ e $g(x) \neq 0$. Então existem únicos $q(x), r(x) \in \mathbb{K}[x]$ tais que*

$$f(x) = q(x) \cdot g(x) + r(x),$$

onde ou $r(x) = 0$ ou $gr(r(x)) < gr(g(x))$.

Demonstração: Sejam $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$ polinômios em $\mathbb{K}[x]$, com $gr(g(x)) = m$.

- Existência:
  Se $f(x) = 0$, basta tomar $q(x) = r(x) = 0$. Suponha então $f(x) \neq 0$ de grau $gr(f(x)) = n$.

  Se $n < m$ basta tomar $q(x) = 0$ e $r(x) = f(x)$.

  Se $n \geq m$, mostremos o teorema por indução sobre $gr(f(x)) = n$. Para $n = 0$, como $n \geq m$ devemos ter $m = 0$ e portanto $f(x) = a_0 \neq 0$, $g(x) = b_0 \neq 0$ e teremos $f(x) = a_0b_0^{-1}g(x)$, daí basta tomar $q(x) = a_0b_0^{-1}$ e $r(x) = 0$.

  Suponha por hipótese de indução que o resultado é válido para todo polinômio de grau menor que n e defina o polinômio $f_1(x)$ por

  $$f_1(x) = f(x) - a_nb_m^{-1}x^{n-m} \cdot g(x).$$

  Note que $gr(f_1(x)) < gr(f(x))$, logo pela hipótese de indução, o resultado é válido para $f_1(x)$, isto é, existem $q_1(x), r_1(x)$ tais que

  $$f_1(x) = q_1(x) \cdot g(x) + r_1(x),$$

  onde $r_1(x) = 0$ ou $gr(r_1(x)) < gr(g(x))$. Daí segue que

  $$\begin{aligned} f(x) &= f_1(x) + a_nb_m^{-1}x^{n-m} \cdot g(x) \\ &= q_1(x) \cdot g(x) + r_1(x) + a_nb_m^{-1}x^{n-m} \cdot g(x) \\ &= g(x)(q_1(x) + a_nb_m^{-1}x^{n-m}) + r_1(x). \end{aligned}$$

Portanto, basta tomar $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ e $r(x) = r_1(x)$.

- Unicidade
  Sejam $q_1(x), q_2(x), r_1(x), r_2(x) \in \mathbb{K}[x]$ tais que

$$f(x) = q_1(x) \cdot g(x) + r_1(x) = q_2(x) \cdot g(x) + r_2(x),$$

onde $r_i(x) = 0$ ou $gr(r_i(x)) < gr(g(x))$, para $i =, 2$. Então temos

$$q_1(x) \cdot g(x) + r_1(x) = q_2(x) \cdot g(x) + r_2(x) \Leftrightarrow (q_1(x) - q_2(x)) \cdot g(x) = r_2(x) - r_1(x).$$

Se $q_1(x) \neq q_2(x)$,

$$gr((q_1(x) - q_2(x)) \cdot g(x)) = gr(q_1(x) - q_2(x)) + gr(g(x)) \geq gr(g(x)),$$

mas por outro lado

$$gr(r_2(x) - r_1(x)) < gr(g(x)),$$

logo temos um absurdo e portanto devemos ter $q_1(x) = q_2(x)$ e daí

$$r_1(x) = f(x) - q_1(x)g(x) = f(x) - q_2(x)g(x) = r_2(x).$$

■

Sejam $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ um polinômio não nulo em $\mathbb{K}[x]$ e $\alpha \in \mathbb{K}$. Definimos a **avaliação** de $f(x)$ em α como sendo

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n \in \mathbb{K}.$$

Se $f(\alpha) = 0$ dizemos que α é uma raiz de $f(x)$.

Proposição 4.3 *Seja $f(x) \in \mathbb{K}[x] - \{0\}$. Então $\alpha \in \mathbb{K}$ é uma raiz de $f(x)$ se, e somente se, $x - \alpha$ divide $f(x)$.*

Demonstração: Pelo algoritmo da divisão, existem $q(x), r(x) \in \mathbb{K}[x]$ tais que

$$f(x) = q(x)(x - \alpha) + r(x),$$

onde $r(x) = 0$ ou $gr(r(x)) < gr(x - \alpha) = 1$, isto é, $r(x) = a \in \mathbb{K}$ e então

$$f(x) = q(x)(x - \alpha) + a.$$

Se α é raiz de $f(x)$ temos $f(\alpha) = 0$ e daí

$$0 = f(\alpha) = q(\alpha)(\alpha - \alpha) + r = r,$$

o que mostra que $r(x) = 0$ e que portanto $x - \alpha$ divide $f(x)$.

Reciprocamente, se $x - \alpha$ divide $f(x)$, então existe $q(x) \in \mathbb{K}[x]$ tal que

$$f(x) = q(x)(x - \alpha)$$

e portanto

$$f(\alpha) = q(\alpha)(\alpha - \alpha) = q(\alpha) \cdot 0 = 0.$$

■

Proposição 4.4 *Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio não nulo em $\mathbb{K}[x]$ de grau n. Então o número de raízes de $f(x)$ em $\mathbb{K}$ é no máximo igual a $gr(f(x)) = n$.*

Demonstração: Se $f(x)$ não possuir raízes em $\mathbb{K}$ a proposição está provada. Suponhamos que $\alpha \in \mathbb{K}$ seja uma raiz de $f(x)$, daí pela Proposição 4.3

$$f(x) = q(x)(x - \alpha),$$

para algum $q(x) \in \mathbb{K}[x]$, com $gr(q(x)) = n - 1$. Logo, se β for uma raiz qualquer de $f(x)$ então

$$0 = f(\beta) = q(\beta)(\beta - \alpha),$$

e como $\mathbb{K}[x]$ é um domínio d eintegridade $q(\beta) = 0$ ou $\beta = \alpha$, isto é, as raízes de $f(x)$ são α e as raízes de $q(x)$. Vamos fazer indução sobre $gr(f(x)) = n$ para provar o resultado.

Se $n = 0$, f não possui raízes em $\mathbb{K}$ e nesse caso não temos nada para provar. Por hipótese de indução se $p(x)$ tem grau $k < n$ então $p(x)$ tem no máximo k raízes em $\mathbb{K}$. Logo $q(x)$ possui no máximo $n - 1$ raízes em $\mathbb{K}$ e daí $f(x)$ possui no máximo n raízes em $\mathbb{K}$.

■

Definição 4.1 *Seja $\mathbb{K}$ um corpo. Se $L \supset \mathbb{K}$ é um corpo, dizemos que L é uma **extensão** de $\mathbb{K}$.*

Observe que o polinômio $x^2 + 1$ não possui raízes em $\mathbb{R}$, mas possui duas raízes em $\mathbb{C} \supset \mathbb{R}$, uma extensão de $\mathbb{R}$.

Corolário 4.1 *Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio não nulo em $\mathbb{K}[x]$ de grau n. Então $f(x)$ possui no máximo n raízes em qualquer extensão L de $\mathbb{K}$.*

Demonstração: Se $f(x) \in \mathbb{K}[x]$ e $\mathbb{K} \subset L$ então $f(x) \in L[x]$ e daí basta usar a Proposição 4.4.

■

Exemplo 4.7 *O polinômio $x^3 - 2$ não possui raízes em $\mathbb{Q}$, possui apenas uma raiz em $\mathbb{R}$ e possui 3 raízes em $\mathbb{C}$.*

Assim, em uma extensão do corpo podemos obter mais raízes do polinômio, porém esse número de raízes nunca vai passar do grau do polinômio.

É comum confundirmos polinômios com funções polinomiais e muitas vezes não fazermos distinção entre essas duas coisas. Vamos apresentar um exemplo dessa diferença utilizando corpos finitos. Para isso vamos identificar os polinômios com n-uplas da seguinte forma

$$\begin{aligned} 1 &\leftrightsquigarrow (1,0,0,\ldots,0,\ldots) \\ x &\leftrightsquigarrow (0,1,0,\ldots,0,\ldots) \\ x^2 &\leftrightsquigarrow (0,0,1,\ldots,0,\ldots) \\ &\vdots \end{aligned}$$

Assim, o polinômio $p(x) = 2x^2 - 3x$ seria identificado com a n-upla

$$p(x) \leftrightsquigarrow (0,-3,2,\ldots,0,\ldots).$$

Uma função polinomial $f(x)$ em uma variável sobre $\mathbb{K}$ é identicamente nula se $f(u) = 0$ para todo $u \in \mathbb{K}$. Por exemplo, se $\mathbb{K} = \mathbb{Z}_p$, sabemos que $u^p = u$, para todo $u \in \mathbb{K}$, logo a função

$$\begin{array}{rccc} f: & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p \\ & y & \longmapsto & f(y) = y^p - y \end{array}$$

é identicamente nula em $\mathbb{Z}_p$. Mas o polinômio $g(x) = x^p - x$ não é o polinômio nulo sobre $\mathbb{Z}_p$. Em termos de uplas seria

$$g(x) \leftrightsquigarrow (0,-1,0,\ldots,0,1,0,\ldots).$$

Daí em $\mathbb{Z}_p$ existem vários polinômios cuja função polinomial correspondente é nula, por exemplo $f(x) = x^p - x$ e $q(x) = 0$, mas cujos polinômios são distintos. Vejamos que isso só ocorre para corpos finitos.

Corolário 4.2 *Sejam $f(x)$ e $g(x)$ em $\mathbb{K}[x]$, onde $\mathbb{K}$ é um corpo com infinitos elementos. Então*

$$f(x) = g(x) \Leftrightarrow f(b) = g(b), \quad \forall b \in \mathbb{K}.$$

Demonstração: É direto que

$$f(x) = g(x) \Rightarrow f(b) = g(b), \quad \forall b \in \mathbb{K}.$$

Provemos então o sentido contrário da implicação. Seja $h(x) = f(x) - g(x) \in \mathbb{K}[x]$. Por hipótese $h(b) = 0$ para todo $b \in \mathbb{K}$, e como $\mathbb{K}$ tem infinitos elementos, segue da Proposição 4.4 que $h(x) = 0$, ou seja, $f(x) = g(x)$.

■

4.2.1 Algoritmo de Briot-Ruffini

Em álgebra a divisão de um polinômio por polinômios da forma $x - \alpha$ tem uma certa importância e por essa razão iremos apresentar um método prático para a determinação do quociente e do resto da divisão de $f(x) \in \mathbb{K}[x]$ por $x - \alpha$, onde $\alpha \in \mathbb{K}$. Chamamos este método de **algoritmo de Briot-Ruffini**.

Sejam $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{K}[x]$, com $a_n \neq 0$, e $\alpha \in \mathbb{K}$. Vamos considerar também $q(x) \in \mathbb{K}[x]$ o quociente e $r \in \mathbb{K}$ o resto da divisão de $f(x)$ por $x - \alpha$, isto é

$$f(x) = q(x)(x - \alpha) + r, \quad \text{com} \quad gr(q(x)) = n - 1.$$

Assim podemos escrever o quociente $q(x)$ como

$$q(x) = q_{n-1}x^{n-1} + q_{n-2}x^{n-2} + \cdots + q_1(x) + q_0$$

e daí teremos

$$\begin{aligned} f(x) &= (q_{n-1}x^{n-1} + q_{n-2}x^{n-2} + \cdots + q_1(x) + q_0)(x - \alpha) + r \\ &= q_{n-1}x^n + (q_{n-2} - \alpha q_{n-1})x^{n-1} + \cdots + (q_0 - \alpha q_1)x + (r - \alpha q_0), \end{aligned}$$

onde, pela igualdade de polinômios, temos

$$\begin{cases} q_{n-1} = a_n \\ q_{n-2} = a_{n-1} + \alpha q_{n-1} \\ q_{n-3} = a_{n-2} + \alpha q_{n-2} \\ \vdots \\ q_1 = a_2 + \alpha q_2 \\ q_0 = a_1 + \alpha q_1 \\ r = a_0 + \alpha q_0 \end{cases}$$

Observe que nas igualdades acima é possível determinar os valores dos coeficientes de $q(x)$ a partir do coeficiente do temo de maior grau, obtido através de a_n, e depois os de graus menores a partir dos coeficientes anteriores e dos coeficientes de $f(x)$.

O algortimo de Briot-Ruffini trata-se da elaboração de uma tabela que apresenta os coeficientes de $q(x)$ e o resto obtidos usando a fórmula recursiva apresentada acima.

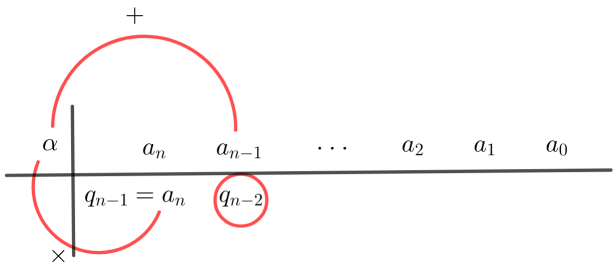
A tabela deve ter duas linhas, sendo a primeira linha composta por α e os coeficientes de $f(x)$ e na segunda linha apenas o coeficiente do termo de maior grau de $q(x)$, isto é, $q_{n-1} = a_n$, dispostos da seguinte forma

α	a_n	a_{n-1}	$\cdots$	a_2	a_1	a_0
	$q_{n-1} = a_n$					

Os demais coeficientes de $q(x)$ completarão a segunda linha da tabela e devem ser calculados utilizando as recorrências obtidas anteriormente, ou seja, o k-ésimo coeficiente q_k de $q(x)$ será dado por

$$q_k = \alpha q_{k+1} + a_{k+1}.$$

Assim, o próximo termo a ser inserido na tabela será $q_{n-2} = \alpha q_{n-1} + a_{n-1}$



Devemos continuar esse procedimento até que tenhamos

α	a_n	a_{n-1}	$\cdots$	a_2	a_1	a_0
	$q_{n-1} = a_n$	q_{n-2}	$\cdots$	q_1	q_0	r

O algoritmo pode ser usado para fazer divisões sucessivas de $f(x)$ por $x - \alpha$, quando α for raiz de $f(x)$. Dizemos que $\alpha \in \mathbb{K}$ é uma raiz de $f(x) \in \mathbb{K}[x]$ de **multiplicidade** m quando $(x-\alpha)^m$ dividir $f(x)$ e $(x-\alpha)^{m+1}$ não dividir $f(x)$ em $\mathbb{K}[x]$. Se $m = 1$ dizemos que α é uma **raiz simples** de $f(x)$ e se $m \geq 2$, α é dita uma **raiz múltipla** de $f(x)$.

4.3 Ideais principais e máximo divisor comum

Relembremos da Definição 3.4 que um ideal é principal se ele for gerado por um único elemento do anel. Na proposição a seguir veremos que todos os ideais de $\mathbb{K}[x]$ são principais.

Proposição 4.5 *$\mathbb{K}[x]$ é um domínio principal.*

Demonstração: Devemos mostrar que todo ideal de $\mathbb{K}[x]$ é principal, isto é, se J é ideal de $\mathbb{K}[x]$ devemos mostrar que existe $p(x) \in \mathbb{K}[x]$ tal que $J = \mathbb{K}[x] \cdot p(x)$.

Seja J ideal de $\mathbb{K}[x]$. Se $J = \{0\}$ então basta tomar $p(x) = 0$ o polinômio nulo. Se $J \neq \{0\}$, escolha $0 \neq v(x) \in J$ de menor grau possível.

- se $gr(v(x)) = 0$, isto é, $v(x) = a$ constante não nula, então $1 = a^{-1} \cdot a \in J$, logo $J = \mathbb{K}[x]$ e basta tomar $p(x) = 1$.
- se $gr(v(x)) > 0$, como $v(x) \in J$, é claro que $\mathbb{K}[x] \cdot v(x) \subset J$. Vamos mostrar que $J \subset \mathbb{K}[x] \cdot v(x)$, daí basta tomar $p(x) = v(x)$ e teremos $J = \mathbb{K}[x] \cdot p(x)$.

De fato, seja $f(X) \in J$, pelo algoritmo da divisão, existem $q(x), r(x) \in \mathbb{K}[x]$ tais que

$$f(x) = q(x) \cdot v(x) + r(x),$$

onde ou $r(x) = 0$ ou $gr(r(x)) < gr(v(x))$. Como $f(x0, v(x) \in J \subset \mathbb{K}[x]$ então

$$f(x) - q(x)v(x) = r(x) \in J.$$

Como $v(x)$ tem grau mínimo em J então $r(x) = 0$ e portanto

$$f(x) = q(x) \cdot v(x) \in \mathbb{K}[x] \cdot v(x).$$

■

Teorema 4.2 (Existência de mdc) *Sejam $p_1(x), \ldots, p_m(x) \in \mathbb{K}[x] - \{0\}$ e considere o ideal*

$$J = \mathbb{K}[x]p_1(x) + \cdots + \mathbb{K}[x] \cdot p_m(x) \subset \mathbb{K}[x]$$

gerado pelos polinômios não nulos $p_1(x), \ldots, p_m(x)$. Se $d(x) \in \mathbb{K}[x]$ é tal que $J = \mathbb{K}[x] \cdot d(x)$ então são válidas as seguintes propriedades:

(a) Existem $r_1(x), \ldots, r_m(x) \in \mathbb{K}[x]$ tais que

$$d(x) = r_1(x)p_1(x) + \cdots + r_m(x)p_m(x).$$

(b) $d(x)$ é um divisor comum de $p_1(x), p_2(x), \ldots, p_m(x)$.

(c) Se $d'(x)$ é um divisor comum qualquer de $p_1(x), p_2(x), \ldots, p_m(x)$ então $d'(x)$ é também um divisor de $d(x)$.

Demonstração:

(a) É direto da definição do ideal J.

(b) Para todo $i = 1, \ldots, m$ é claro que

$$p_i(x) \in \mathbb{K}[x] \cdot p_i(x) \subset \mathbb{K}[x]p_1(x) + \cdots + \mathbb{K}[x] \cdot p_m(x) = \mathbb{K}[x] \cdot d(x)$$

e portanto, existe $r_i(x) \in \mathbb{K}[x]$ tal que $p_i(x) = r_i(x) \cdot d(x)$, logo $d(x)$ é um divisor de cada $p_i(x)$.

(c) Seja $d'(x)$ um divisor comum de $p_1(x), p_2(x), \ldots, p_m(x)$ em $\mathbb{K}[x]$, isto é, existem $r_i(x) \in \mathbb{K}[x]$ tais que $p_i(x) = r_i(x) \cdot d'(x)$, para $i = 1, 2, \ldots, m$. Assim,

$$\mathbb{K}[x] \cdot p_i(x) \subset \mathbb{K}[x] \cdot d'(x), \quad \forall\ i \in \{1, 2, \ldots, m\}.$$

Daí

$$\mathbb{K}[x] \cdot d(x) = \mathbb{K}[x]p_1(x) + \cdots + \mathbb{K}[x] \cdot p_m(x) \subset \mathbb{K}[x] \cdot d'(x),$$

isto é, existe $r(x) \in \mathbb{K}[x]$ tal que $d(x) = r(x) \cdot d'(x)$.

■

Um polinômio satisfazendo as condições (b) e (c) do teorema anterior é **um máximo divisor comum** de $p_1(x), p_2(x), \ldots, p_m(x)$ em $\mathbb{K}[x]$. E note que, Se $d(x)$ é um máximo divisor de $p_1(x), p_2(x), \ldots, p_m(x)$ em $\mathbb{K}[x]$ e $a \in \mathbb{K}$, $a \neq 0$, então $a \cdot d(x)$ também é um máximo divisor comum em $\mathbb{K}[x]$ desses mesmos polinômios.

Se $p_1(x), p_2(x), \ldots, p_m(x) \in \mathbb{K}[x] - \{0\}$ então existe um único máximo divisor comum mônico de $p_1(x), p_2(x), \ldots, p_m(x)$ em $\mathbb{K}[x]$. Este é dito **o máximo divisor comum** de $p_1(x), p_2(x), \ldots, p_m(x)$ em $\mathbb{K}[x]$ e o denotamos por

$$mdc_{\mathbb{K}[x]}\{p_1(x), p_2(x), \ldots, p_m(x)\}.$$

Se $mdc_{\mathbb{K}[x]}\{p_1(x), p_2(x), \ldots, p_m(x)\} = 1$, dizemos que os polinômios são **relativamente primos** em $\mathbb{K}[x]$, e nesse caso, existem $r_1(x), \ldots, r_m(x) \in \mathbb{K}[x]$ tais que

$$r_1(x)p_1(x) + \cdots + r_m(x)p_m(x) = 1.$$

Exemplo 4.8 *Seja $A = \mathbb{Z}[x]$. Vamos mostrar que A não é um domínio principal. Ou seja, devemos mostrar que nem todos os ideias de A são principais. De fato, consideremos como contra exemplo o ideal I de A gerado por 2 e x, isto é,*

$$I = A \cdot 2 + A \cdot x = \{2p(x) + xq(x) :\ p(x), q(x) \in \mathbb{Z}[x]\}.$$

Suponha por absurdo que A é domínio principal. Daí existe $d(x) \in A$ tal que $I = A \cdot d(x)$, logo

$$A \cdot d(x) = A \cdot 2 + A \cdot x,$$

e então $d(x)$ é um máximo divisor comum de 2 e x em $\mathbb{Z}[x]$. Como 2 é primo em $\mathbb{Z}$ e 2 não é um divisor de x em $\mathbb{Z}[x]$ (já que $x = (\frac{1}{2}x) \cdot 2$ e $\frac{1}{2} \notin \mathbb{Z}$), então $d(x) = \pm 1$, assim,

$$1 = mdc\{2, x\} \quad em \quad \mathbb{Z}[x] \quad e \quad A \cdot 2 + A \cdot x = A.$$

Consequentemente, existem $p(x), q(x) \in \mathbb{Z}[x]$ tais que

$$1 = 2p(x) + xq(x),$$

o que é um absurdo, pois o termo independente do lado direito da igualdade é par enquanto o do lado esquerdo é ímpar.

4.4 Polinômios irredutíveis

Seja $f(x) \in \mathbb{K}[x]$ tal que $gr(f(x)) \geq 1$. Dizemos que $f(x)$ é um plinômio **irredutível** sobre $\mathbb{K}$ se toda vez que $f(x) = g(x) \cdot h(x)$, $g(x), h(x) \in \mathbb{K}[x]$ tivermos $g(x) = a$ uma constante em $\mathbb{K}$ ou $h(x) = b$ uma constante em $\mathbb{K}$. Se $f(x)$ não for irredtível em $\mathbb{K}$, dizemos que $f(x)$ é **redutível** sobre $\mathbb{K}$.

Exemplo 4.9 *Todo polinômio de grau 1 sobre um corpo $\mathbb{K}$ é irredutível sobre $\mathbb{K}$.*

Um polinômio $f(x) \in \mathbb{K}[x]$ pode ser irredutível sobre $\mathbb{K}$ e redutível em uma extensão $L \supset \mathbb{K}$.

Exemplo 4.10 *O polinômio $x^2 + 1$ é irredutível sobre $\mathbb{R}$ porém é redutível sobre $\mathbb{C}$, pois*

$$x^2 + 1 = (x + i)(x - i).$$

Teorema 4.3 *Sejam $\mathbb{K}$ um corpo e $p(x) \in \mathbb{K}[x]$. Então as seguintes condições são equivalentes:*

(i) $p(x)$ *é irredutível sobre* $\mathbb{K}$*;*

(ii) $J = \mathbb{K}[x] \cdot p(x)$ *é um ideal maximal em* $\mathbb{K}[x]$;

(iii) $\dfrac{\mathbb{K}[x]}{J}$ *é um corpo, onde* $J = \mathbb{K}[x] \cdot p(x)$.

Demonstração: Vamos provar a seguinte sequência de equivalências

$$(i) \Leftrightarrow (ii) \Leftrightarrow (iii).$$

Observe que $(ii) \Leftrightarrow (iii)$ segue imediatamente do Teorema 3.3. Mostremos então que $(i) \Rightarrow (ii)$. Para isso sejam $p(x) \in \mathbb{K}[x]$, $p(x)$ irredutível e $J = \mathbb{K}[x] \cdot p(x)$. Como $gr(p(x)) \geq 1$ então $J \neq \mathbb{K}[x]$. Queremos mostrar que J é maximal, então seja $I = \mathbb{K}[x] \cdot h(x)$ ideal de $\mathbb{K}[x]$ tal que $I \supset J$ e provemos que $I = J$ ou $I = \mathbb{K}[x]$. Temos

$$p(x) \in \mathbb{K}[x] \cdot p(x) = J \subset I = \mathbb{K}[x] \cdot h(x),$$

logo existe $g(x) \in \mathbb{K}[x]$ tal que $p(x) = g(x) \cdot h(x)$ e como $p(x)$ é irredutível, $g(x) = a \in \mathbb{K} - \{0\}$ ou $h(x) = b \in \mathbb{K} - \{0\}$. Se $g(x) = a \neq 0$, então $h(x) = a^{-1} \cdot p(x)$ e daí

$$I = \mathbb{K}[x] \cdot h(x) \subset \mathbb{K}[x] \cdot p(x) = J,$$

logo $I = J$. E se $h(x) = b \neq 0$, então

$$I = \mathbb{K}[x] \cdot h(x) = \mathbb{K}[x].$$

Reciprocamente, para mostrar que $(ii) \Rightarrow (i)$, seja $J = \mathbb{K}[x] \cdot p(x)$ um ideal maximal em $\mathbb{K}[x]$. Daí $J \neq \mathbb{K}[x]$ e então $gr(p(x)) \geq 1$. Suponha $g(x), h(x) \in \mathbb{K}[x]$ tais que $p(x) = g(x) \cdot h(x)$. Daí $p(x) \in I = \mathbb{K}[x] \cdot h(x)$, e portanto $J \subset I$. Como J é maximal, devemos ter $I = \mathbb{K}[x]$ ou $I = J$.

- Se $J = I$ então $h(x) \in J = \mathbb{K}[x] \cdot p(x)$ e daí $h(x) = f(x) \cdot p(x)$, para algum $f(x) \in \mathbb{K}[x]$. Logo
$$p(x) = g(x) \cdot f(x) \cdot p(x) \Rightarrow p(x)(1 - g(x) \cdot f(x)) = 0.$$
Como $\mathbb{K}[x]$ é um domínio de integridade e $p(x) \neq 0$ temos $g(x) \cdot f(x) = 1$. Então $g(x)$ é invertível em $\mathbb{K}[x]$ e pela Proposição 4.2, $g(x) = a \neq 0$, consequentemente $p(x)$ é redutível.

- Se $I = \mathbb{K}[x]$ então $h(x) = b \neq 0$ constante, logo $p(x)$ é irredutível sobre $\mathbb{K}$.

■

Exemplo 4.11 *Sejam $A = \mathbb{R}[x]$ e $I = A \cdot (x^2 + 1)$, mostremos que $\dfrac{A}{I} \simeq \mathbb{C}$.*

Sabemos que $x^2 + 1$ é irredutível em A, daí pelo teorema anterior, I é maximal em A e $L = \dfrac{A}{I}$ é um corpo, então vamos mostrar que esse corpo é isomorfo ao corpo do complexos.

Seja $p(x) \in A$, daí existem únicos $q(x), r(x) \in A$ tais que

$$p(x) = q(x)(x^2 + 1) + r(x),$$

com $r(x) = 0$ ou $gr(r(x)) < 2$, isto é, $r(x) = a + bx, \quad a, b \in \mathbb{R}$. Defina

$$\begin{array}{rccl} \phi: & A & \longrightarrow & \mathbb{C} \\ & p(x) & \longmapsto & \phi(p(x)) = a + bi. \end{array}$$

É claro que ϕ é sobrejetora, pois dado $a + bi \in \mathbb{C}$, basta tomar $p(x) = x^2 + 1 + a + bx$ e daí $\phi(p(x)) = a + bi$.

Sejam $p(x), f(x) \in A$, logo existem $q_1(x), q_2(x), r_1(x) = a_1 + b_1x, r_2(x) = a_2 + b_2x \in A$ tais que

$$p(x) = q_1(x)(x^2 + 1) + r_1(x) \quad e \quad f(x) = q_2(x)(x^2 + 1) + r_2(x).$$

Daí

$$\begin{aligned} \phi(p(x) + f(x)) = \phi(r_1(x) + r_2(x)) &= \phi((a_1 + a_2) + (b_1 + b_2)x) \\ &= (a_1 + a_2) + (b_1 + b_2)i \\ &= (a_1 + b_1i) + (a_2 + b_2i) \\ &= \phi(r_1(x)) + \phi(r_2(x)) \\ &= \phi(p(x)) + \phi(f(x)) \end{aligned}$$

e

$$\begin{aligned}\phi(p(x)\cdot f(x)) &= \phi(r_1(x)\cdot r_2(x))\\ &= \phi(r_1(x))\cdot\phi(r_2(x))\\ &= \phi(p(x))\cdot\phi(f(x)).\end{aligned}$$

Logo ϕ é um homomorfismo sobrejetor e daí pelo Teorema do Homomorfismo

$$\frac{A}{ker(\phi)} \simeq Im(\phi) = \mathbb{C}.$$

Mas note que

$$\begin{aligned}ker(\phi) &= \{p(x)\in\mathbb{R}[x]:\ \phi(p(x))=0\}\\ &= \{p(x)\in\mathbb{R}[x]:\ \phi(r(x))=0\}\\ &= \{p(x)\in\mathbb{R}[x]:\ r(x)=0\}\\ &= \{p(x)\in\mathbb{R}[x]:\ p(x)=q(x)(x^2+1), \quad \textit{para algum} \quad q(x)\in\mathbb{R}[x]\}\\ &= A(x^2+1) = I.\end{aligned}$$

Portanto $\dfrac{A}{I} \simeq \mathbb{C}$.

4.4.1 Fatoração única

Nesta seção veremos um resultado similar ao Teorema Fundamental da Aritmética que discorre sobre o anel dos números inteiros. Naquela ocasião os números primos se apresentam como os "blocos menores" que constroem os números inteiros. Agora veremos que essas partes "menores" no anel de polinômios são os polinômios irredutíveis.

Teorema 4.4 (Fatoração única) *Seja $f(x)\in\mathbb{K}[x]$ com $gr(f(x))\geq 1$. Então existem polinômios mônicos irredutíveis $p_1(x),\ldots,p_s(x)$ distintos, $a\in\mathbb{K}-\{0\}$ e números naturais $n_1,\ldots,n_s$, tais que*

$$f(x) = a\cdot p_1(x)^{n_1}\cdots p_s(x)^{n_s}.$$

Essa expressão é única a menos da ordem dos fatores.

Demonstração: Vamos mostrar que existem polinômios mônicos irredutíveis, não necessariamente distintos, $p_1(x),\ldots,p_m(x)$ tais que

$$f(x) = a\cdot p_1(x)\cdots p_m(x),$$

e essa expressão é única a menos da ordem dos fatores. A expressão do enunciado é obtida agrupando os fatores iguais.

- Existência: Indução sobre $n = gr(f(x))$.
  Se $gr(f(x)) = 1$, então $f(x) = ax + b = a(x + a^{-1}b)$, com $a, b \in \mathbb{K}$ e $a \neq 0$. Suponhamos que $gr(f(x)) = n \geq 2$ e que o teorema seja válido para polinômios em $\mathbb{K}[x]$ não constantes com grau menor do que n. Vamos mostrar que vale para $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Se $f(x)$ é iredutível então

  $$f(x) = a_n(x^n + \cdots + a_n^{-1}a_1 x + a_n^{-1}a_0)$$

  e está provado o resultado. Vamos então supor $f(x)$ redutível. Daí existem $g(x), h(x) \in \mathbb{K}[x]$ não constantes tais que

  $$f(x) = g(x) \cdot h(x),$$

  com $1 \leq gr(g(x)), gr(h(x)) < n = gr(f(x))$. Por hipótese de indução

  $$g(x) = b \cdot p_1(x) \cdots p_r(x),$$

  com $p_1(x), \ldots, p_r(x)$ mônicos e irredutíveis e $b \in \mathbb{K} - \{0\}$ e também

  $$h(x) = c \cdot p_{r+1}(x) \cdots p_{r+\ell}(x),$$

  com $p_{r+1}, \ldots, p_{r+\ell}$ mônicos e irredutíveis e $c \in \mathbb{K} - \{0\}$. Assim,

  $$\begin{aligned} f(x) &= b \cdot p_1(x) \cdots p_r(x) \cdot c \cdot p_{r+1}(x) \cdots p_{r+\ell}(x) \\ &= a \cdot p_1(x) \cdots p_r(x) \cdot p_{r+1}(x) \cdots p_{r+\ell}(x), \end{aligned}$$

  onde $a = b \cdot c \in \mathbb{K} - \{0\}$ e $p_1(x), \ldots, p_{r+\ell}(x)$ são mônicos irredutíveis.

- Unicidade:
  Suponha

  $$f(x) = a \cdot p_1(x) \cdots p_m(x) = b \cdot q_1(x) \cdots q_r(x),$$

  $a, b \in \mathbb{K} - \{0\}$ e $p_1(x), \ldots, p_m(x), q_1(x), \ldots, q_r(x)$ mônicos e irredutíveis. Como a e b são iguais ao coeficiente de maior grau de $f(x)$ então temos

  $$p_1(x) \cdots p_m(x) = q_1(x) \cdots q_r(x).$$

  Como $p_1(x)$ divide o polinômio à esquerda da igualdade, então $p_1(x)$ divide $q_1(x) \cdots q_r(x)$. Como $p_1(x)$ é irredutível, então $p_1(x)$ divide q_j para algum $j = 1, \ldots, r$. Daí $q_j(x) = u \cdot p_1(x)$ para algum $u \in \mathbb{K} - \{0\}$. Como $q_j(x)$ é mônico, $u = 1$ e $q_j(x) = p_1(x)$. Reenumerando os polinômios $q_1(x) \cdots q_r(x)$, se necessário, podemos supor $p_1(x) = q_1(x)$. Faremos indução sobre m. Se $m = 1$, então $r = 1$. Se $m > 1$, cancelamos $p_1(x)$, obtendo

  $$p_2(x) \cdots p_m(x) = q_2(x) \cdots q_r(x)$$

  e, por hipótese de indução, $m - 1 = r - 1$, que é equivalente a $m = r$, e cada $p_j(x)$ é igual a $q_j(x)$.

■

4.5 Polinômios com coeficientes inteiros

Na seção anterior foi possível notar a importância dos polinômios irredutíveis que pode até ser comparada dentro dos anéis de polinômios com a importância dos números primos no anel dos números inteiros. Finalizaremos este capítulo com alguns resultados que nos dão critérios para determinar se um polinômio é irredutível sobre determinados anéis. O principal resultado dessa seção é o critério de Eisenstein sobre a redutibilidade de polinômios com coeficientes inteiros.

Vejamos inicialmente um resultado que nos dá condições suficientes para que um polinômio $f(x) \in \mathbb{Q}[x]$ seja irredutível sobre $\mathbb{Q}$. Observe que, dado um polinômio $f(x) \in \mathbb{Q}[x]$ se multiplicarmos $f(x)$ pelo mínimo múltiplo comum dos denominadores dos coeficientes de $f(x)$, podemos supor que $f(x)$ seja um polinômio em $\mathbb{Z}[x]$.

Lema 4.1 (Lema de Gauss) *Seja $f(x) \in \mathbb{Z}[x]$ irredutível sobre $\mathbb{Z}$, então $f(x)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração: Suponha $f(x)$ irredutível sobre $\mathbb{Z}$, mas $f(x) = g(x) \cdot h(x)$, onde $g(x), h(x) \in \mathbb{Q}[x]$ e $1 \leq gr(g(x)), gr(h(x)) < gr(f(x))$. É claro que existe inteiro positivo m tal que

$$m \cdot f(x) = g_1(x) \cdot h_1(x),$$

onde $g_1(x), h_1(x) \in \mathbb{Z}[x]$. Assim,

$$g_1(x) = a_0 + a_1x + \cdots + a_rx^r, \quad a_i \in \mathbb{Z},$$

$$h_1(x) = b_0 + b_1x + \cdots + b_sr^s, \quad b_i \in \mathbb{Z}.$$

Seja p um primo tal que $p|m$.

Afirmação: $p|a_i$, para todo $i \in \{1, \ldots, r\}$ ou $p|b_j$, para todo $j \in \{1, \ldots, s\}$.

De fato, do contrário existiriam $i \in \{1, \ldots, r\}$ e $j \in \{1, \ldots, s\}$ tais que $p \nmid a_i$ e $p \nmid b_j$. Consideremos i e j menores possíveis com esta propriedade. Como $p|m$ então P divide o coeficiente de x^{i+j} do polinômio $mf(x) = g_1(x) \cdot h_1(x)$, isto é,

$$p|(b_0a_{i+j} + b_1a_{i+j-1} + \cdots + b_ja_i + \cdots + b_{i+j-1}a_1 + b_{i+j}a_0).$$

Pela nossa escolha de i e j temos que p divide cada parcela, exceto b_ja_i, do coeficiente de x^{i+j} de $g_1(x) \cdot h_1(x)$. Como p divide toda a expressão, então p também deve dividir b_ja_i, mas p é primo, logo

$$p|b_ja_i \Rightarrow p|b_j \quad \text{ou} \quad p|a_i,$$

uma contradição. Assim, se p é primo e $p|m$ então $p|a_i$, para todo $i \in \{1, \ldots, r\}$ ou $p|b_j$, para todo $j \in \{1, \ldots, s\}$.

Sem perda de generalidade, vamos supor que $p|a_i$, para todo $i \in \{1, \ldots, r\}$. Assim $g_1(x) = p \cdot g_2(x)$, onde $g_2(x) \in \mathbb{Z}[x]$, e se $m = p \cdot m_1$ temos

$$pm_1 f(x) = pg_2(x)h_1(x) \Rightarrow m_1 f(x) = g_2(x)h_1(x).$$

Como o número de fatores primos de m é finito, prosseguindo no argumento acima (ou por indução sobre o número de fatores primos de m) chegaremos que

$$f(x) = g^*(x) \cdot h^*(x),$$

onde $g^*(x), h^*(x) \in \mathbb{Z}[x]$ e $g^*(x), h^*(x)$ são múltiplos racionais de $g(x)$ e $h(x)$, respectivamente, contradizendo a irredutibilidade de $f(x)$ sobre $\mathbb{Z}$.

■

Teorema 4.5 (Critério de Eisenstein) *Seja $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ um polinômio em $\mathbb{Z}[x]$. Suponhamos que exista um inteiro primo p tal que:*

(i) $p \nmid a_n$;

(ii) $p|a_0, a_1, \ldots, a_{n-1}$;

(iii) $p^2 \nmid a_0$.

Então $f(x)$ é irredutível sobre $\mathbb{Q}$.

Demonstração: Pelo Lema de Gauss é suficiente mostrar que $f(x)$ é irredutível sobre $\mathbb{Z}$. Suponhamos por contradição que

$$f(x) = g(x) \cdot h(x),$$

com $g(x0, h(x) \in \mathbb{Z}[x]$ e $1 \leq gr(g(x)), gr(h(x)) < gr(f(x)) = n$. Sejam

$$g(x) = b_0 + b_1 x + \cdots + b_r x^r \in \mathbb{Z}[x], \quad gr(g(x)) = r,$$

$$h(x) = c_0 + c_1 x + \cdots + c_s x^s \in \mathbb{Z}[x], \quad gr(h(x)) = s.$$

Assim, $n = r + s$. Temos també que $a_0 = b_0 \cdot c_0$ e daí por hipótese $p|a_0$, logo $p|b_0$ ou $p|c_0$, mas como $p^2 \nmid a_0$ então p divide apenas um dos inteiros b_0 e c_0. Sem perda de generalidade suponha que $p|b_0$ e $p \nmid c_0$.

Temos ainda que $a_n = b_r c_s$ é o coeficiente de $x^n = x^{r+s}$ e como $p \nmid a_n$ então $p \nmid b_r$.

Como $p|b_0$ e $p \nmid b_r$ podemos escolher b_i o primeiro coeficiente de $g9x)$ tal que $p \nmid b_i$. Note que

$$a_i = b_0 \cdot c_i + b_1 \cdot c_{i-1} + \cdots + b_i \cdot c_0$$

e como $p|b_0, \ldots, b_{i-1}$, $p \nmid b_i$ e $p \nmid c_0$ então $p \nmid a_i$, logo $i = n$, o que é um absurdo pois $1 \leq i \leq r < n$. ∎

Exemplo 4.12 *Seja $f(x) = x^3 + 2x + 10$. O critério de Eisenstein se aplica para o primo $p = 2$, portanto $f(x)$ é irredutível sobre $\mathbb{Q}$.*

Exemplo 4.13 *Sejam p um número primo qualquer e $p(x) = x^n - p$ um polinômio de grau $n \geq 1$ sobre $\mathbb{Q}$. O próprio primo p se aplica no critério de Eisenstein e portanto $p(x)$ é irredutível sobre $\mathbb{Q}$.*

Agora observe que se $a \in \mathbb{K}$, a aplicação

$$\begin{array}{rccc} \psi: & \mathbb{K}[x] & \longrightarrow & \mathbb{K}[x] \\ & f(x) & \longmapsto & \psi(f(x)) = f(x+a) \end{array}$$

é um automorfismo de $\mathbb{K}[x]$. Logo, $f(x)$ é irredutível sobre $\mathbb{K}$ se, e somente se, $f(x+a)$ é irredutível sobre $\mathbb{K}$.

Exemplo 4.14 *Seja p um número primo e seja $q(x) \in \mathbb{Z}[x]$ o polinômio*

$$q(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Vamos mostrar que $q(x)$ é irredutível sobre $\mathbb{Q}$.

$$\begin{aligned} q(x+1) &= (x+1)^{p-1} + (x+1)^{p-2} + \cdots + (x+1) + 1 \\ &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{x^p + \left(\begin{array}{c} p \\ 1 \end{array} \right) x^{p-1} + \cdots + \left(\begin{array}{c} p \\ p-1 \end{array} \right) x + 1 - 1}{x} \\ &= x^{p-1} + \left(\begin{array}{c} p \\ 1 \end{array} \right) x^{p-2} + \cdots + \left(\begin{array}{c} p \\ p-2 \end{array} \right) x + p. \end{aligned}$$

Note que o primo p pode ser usado no critério de Eisenstein no polinômio acima. Portanto $q(x+1)$ é irredutível sobre $\mathbb{Q}$ e consequentemente $q(x)$ é irredutível sobre $\mathbb{Q}$.

Proposição 4.6 *Sejam p um número primo e $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ o corpo contendo p elementos. Se $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ vamos definir o polinômio $\overline{f}(x) \in \mathbb{Z}_p[x]$ do seguinte modo*

$$\overline{f}(x) = \overline{a_0} + \overline{a_1} x + \cdots + \overline{a_n} x^n,$$

onde $\overline{a_i} = a_i + p\mathbb{Z}$ é a classe de equivalência, módulo p, cujo representante é $a_i \in \mathbb{Z}$. Então

(a)

$$\begin{array}{rccc} \phi: & \mathbb{Z}[x] & \longrightarrow & \mathbb{Z}_p[x] \\ & f(x) & \longmapsto & \overline{f}(x) \end{array}$$

é um homomorfismo (sobrejetivo) do domínio $\mathbb{Z}[x]$ sobre o domínio $\mathbb{Z}_p[x]$.

(b) Se $p \nmid a_n$ e $\overline{f}(x)$ é irredutível sobre $\mathbb{Z}_p$ então $f(x)$ é irredutível sobre $\mathbb{Q}$. (Observe que se $f(x)$ é mônico, então $p \nmid a_n = 1$ é sempre satisfeita.)

Demonstração:

(a) A demonstração do item (a) é direta, dada a definição de $\overline{f}$.

(b) Sejam $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $gr(f(x)) = n$ e p primo tal que $p \nmid a_n$. Suponha que $f(x) \in \mathbb{Z}[x]$ seja redutível sobre $\mathbb{Q}$. Então sabemos, pelo Lema de Gauss, que $f(x)$ é redutível sobre $\mathbb{Z}$, logo existem

$$g(x) = b_0 + b_1x + \cdots + b_rx^r \in \mathbb{Z}[x], \quad gr(g(x)) = r, \quad 1 \leq r < n \quad \text{e}$$

$$h(x) = c_0 + c_1x + \cdots + c_sx^s \in \mathbb{Z}[x], \quad gr(h(x)) = s, \quad 1 \leq s < n,$$

tais que $f(x) = g(x) \cdot h(x)$. Daí

$$\overline{f}(x) = \overline{g}(x) \cdot \overline{h}(x),$$

onde $\overline{g}(x), \overline{h}(x) \in \mathbb{Z}_p[x]$. Além disso, como $a_n = b_r \cdot c_s$ e $p \nmid a_n$ segue que $p \nmid b_r$ e $p \nmid c_s$ e portante $\overline{b_r} \neq \overline{0}$ e $\overline{c_s} \neq \overline{0}$, isto é, $gr(\overline{g}(x)) = r$ e $gr(\overline{h}(x)) = s$, logo $\overline{f}(x)$ é redutível sobre $\mathbb{Z}_p$. Pela contrapositiva está demonstrada a proposição.

■

Exemplo 4.15 *Seja $f(x) = x^3 + 6x^2 + 5x + 25$. Mostremos que $f(x)$ é irredutível sobre $\mathbb{Q}$. Note que se escolhermos o primo $p = 2$ temos*

$$\overline{f}(x) \in \mathbb{Z}_2[x] \Rightarrow \overline{f}(x) = x^3 + x + \overline{1} \quad e \quad 2 \nmid 1.$$

Além disso, $\overline{f}(x)$ é um polinômio de grau 3 que não possui raízes em $\mathbb{Z}_2$, já que

$$\overline{f}(\overline{0}) = \overline{1} \quad e \quad \overline{f}(\overline{1}) = \overline{1}.$$

Logo $\overline{f}(x)$ é irredutível em $\mathbb{Z}_2[x]$ e pela proposição anterior segue que $f(x)$ é irredutível sobre $\mathbb{Q}$.

Exemplo 4.16 *Seja* $f(x) = x^3 + 17x^2 + 6x + 4$. *Mostremos que* $f(x)$ *é irredutível sobre* $\mathbb{Q}$. *Note que se escolhermos o primo* $p = 3$ *temos*

$$\overline{f}(x) \in \mathbb{Z}_3[x] \Rightarrow \overline{f}(x) = x^3 + \overline{2}x^2 + \overline{1} \quad e \quad 3 \nmid 1.$$

Além disso, $\overline{f}(x)$ *é um polinômio de grau 3 que não possui raízes em* $\mathbb{Z}_3$, *já que*

$$\overline{f}(\overline{0}) = \overline{1}, \quad \overline{f}(\overline{1}) = \overline{1} \quad e \quad \overline{f}(\overline{2}) = \overline{2}.$$

Logo $\overline{f}(x)$ *é irredutível em* $\mathbb{Z}_3[x]$ *e pela proposição anterior segue que* $f(x)$ *é irredutível sobre* $\mathbb{Q}$.

4.6 Exercícios

(1) Determine $q(x)$ e $r(x)$ tais que $f(x) = q(x) \cdot g(x) + r(x)$, onde $r(x) = 0$ ou $\partial r(x) < \partial g(x)$ e $f(x), g(x) \in \mathbb{R}[x]$.

(a) $f(x) = x^3 + x - 1, \quad g(x) = x^2 + 1;$

(b) $f(x) = x^3 + 1, \quad g(x) = x + 1;$

(c) $f(x) = x^5 - 1, \quad g(x) = x - 1;$

(d) $f(x) = x^4 - 2, \quad g(x) = x^2 - 2;$

(2) Sejam $f(x), g(x) \in \mathbb{Z}[x]$ e $g(x) = b_0 + b_1x + \ldots + b_mx^m$ onde $b_m = 1$. Prove que existem $q(x), r(x) \in \mathbb{Z}[x]$ tais que $f(x) = q(x) \cdot g(x) + r(x)$ onde $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

(3) Seja $f(x) \in \mathbb{K}[x] - \{0\}$, $\mathbb{K}$ corpo, e seja $L \supset \mathbb{K}$ uma extensão de $\mathbb{K}$. Prove que, se $\alpha \in L$ é uma raiz de $f(x)$ então existe $q(x) \in L[x]$ tal que $f(x) = (x - \alpha) \cdot q(x)$.

(4) Seja $\mathbb{K}$ um corpo. Dizemos que $\mathbb{K}$ é um corpo **algebricamente fechado** se para todo $f(x) \in \mathbb{K}[x]$, existe $\alpha \in \mathbb{K}$ tal que $f(\alpha) = 0$. Prove que $\mathbb{R}$ não é um corpo algebricamente fechado.

(5) Prove que se $\mathbb{K}$ é algebricamente fechado, então todo polinômio $f(x) \in \mathbb{K}[x]$ de grau $n \geq 1$ pode ser fatorado em $\mathbb{K}$ do seguinte modo:

$$f(x) = c \cdot (x - \alpha_1) \cdot (x - \alpha_2) \ldots (x - \alpha_n),$$

onde $c \in \mathbb{K}$, e $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ são raízes de $f(x)$.

(6) Calcule todas as raízes em $\mathbb{K} = \mathbb{Z}_5$ do polinômio $f(x) = x^5 + \bar{3}x^3 + x^2 + \bar{2}x \in \mathbb{Z}[x]$.

(7) Seja $\mathbb{K}$ um corpo e $L \supset \mathbb{K}$ uma extensão de $\mathbb{K}$. Se $\alpha \in L$ e $f(x) \in \mathbb{K}[x]$, $f(x) = a_0 + a_1x + \ldots + a_nx^n$ definimos $f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n \in L$.

(a) Prove que $\mathbb{K}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{K}[x]\}$ é um domínio de integridade tal que

$$\mathbb{K} \subset \mathbb{K}[\alpha] \subset L.$$

(b) Prove que

$$\begin{array}{rccc} \psi: & \mathbb{K}[x] & \to & \mathbb{K}[\alpha] \\ & f(x) & \mapsto & f(\alpha) \end{array}$$

é um homomorfismo sobrejetivo.

(c) Prove que $J = \{f(x) \in \mathbb{K}[x] : f(\alpha) = 0\}$ é um ideal de $\mathbb{K}[x]$.

(d) Prove que $\dfrac{\mathbb{K}[x]}{J} \simeq \mathbb{K}[\alpha] \subset L$.

(8) Prove que $\mathbb{Q}[\sqrt{2}] = \{f(\sqrt{2}) : f(x) \in \mathbb{Q}[x]\}$ é igual a $\{x + y\sqrt{2} : x, y \in \mathbb{Q}\}$. Prove que o ideal $J = \{f(x) \in \mathbb{Q}[x] : f(\sqrt{2}) = 0\}$ é um ideal maximal de $\mathbb{Q}[x]$ e conclua pelo exercício anterior que $\mathbb{Q}[\sqrt{2}]$ é um corpo (generalize para $\sqrt{p}$, p primo).

(9) Seja $\mathbb{K}$ um corpo e $a \in \mathbb{K}$. Prove que

$$\begin{array}{rccc} \phi: & \mathbb{K}[x] & \to & \mathbb{K}[x] \\ & p(x) & \mapsto & \phi(p(x)) = p(x+a) \end{array}$$

é um automorfismo de $\mathbb{K}[x]$.

(10) Sejam $\mathbb{K}$ um corpo, $f(x) \in \mathbb{K}[x]$ e $a \in \mathbb{K}$. Prove que o resto da divisão de $f(x)$ por $g(x) = x - a$ é $f(a)$.

(11) Calcule $mdc_{\mathbb{C}[x]}\{f(x), g(x)\}$ para os seguintes pares de polinômios em $\mathbb{C}[x]$:

(a) $f(x) = (x-2)^3(x-5)^4(x-i)$; $\quad g(x) = (x-1)(x-2)(x-5)^3$

(b) $f(x) = (x^2+1)(x^2-1)$; $\quad g(x) = (x+i)^3(x^3-1)$

(12) Calcule $mdc_{\mathbb{Q}[x]}\{f(x), g(x)\}$ para os seguintes pares de polinômios em $\mathbb{Q}[x]$:

(a) $f(x) = x^3 - 6x^2 + x + 4$; $\quad g(x) = x^5 - 6x + 1$

(b) $f(x) = x^2 + 1$; $\quad g(x) = x^6 + x^3 + x + 1$

(13) Sejam $f(x), g(x) \in \mathbb{K}[x] - \{0\}$ e $a \in \mathbb{K} - \{0\}$. Então prove que $d(x)$ é um mdc de $f(x)$ e $g(x)$ em $\mathbb{K}[x]$ se e somente se $a \cdot d(x)$ é um mdc de $f(x)$ e $g(x)$ em $\mathbb{K}[x]$.

(14) Calcule $q(x), r(x)$ tais que $f(x) = q(x) \cdot g(x) + r(x)$ onde ou $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.

(a) $f(x) = x^5 - x^3 + 3x - 5; \quad g(x) = x^2 + 7 \in \mathbb{Q}[x]$.

(b) $f(x) = x^5 - x^3 + 3x - 5; \quad g(x) = x - 2 \in \mathbb{Q}[x]$.

(c) $f(x) = x^5 - x^3 + \bar{3}x - \bar{5}; \quad g(x) = x + \bar{2} \in \mathbb{Z}_5[x]$.

(15) Sejam $\mathbb{K}$ um corpo e $f(x) \in \mathbb{K}[x] - \{0\}$. Prove que, se $f(x)$ é um polinômio de grau maior ou igual a 2 e possui uma raiz $a \in \mathbb{K}$ então $f(x)$ é redutível sobre $\mathbb{K}$.

(16) Prove que todo polinômio de grau ímpar sobre $\mathbb{R}$ possui uma raiz em $\mathbb{R}$ (Sugestão: use o teorema do valor intermediário). Conclua que se $f(x) \in \mathbb{R}[x]$ tem grau ímpar então $f(x)$ é redutível sobre $\mathbb{R}$.

(17) Determine todos os n de modo que $x^2 + \bar{2}$ divide $x^5 - \bar{10}x + \bar{12}$ em $\mathbb{Z}_n$.

(18) Determine todos os polinômios de grau 2 que sejam irredutíveis sobre $\mathbb{K} = \mathbb{Z}_5$.

(19) Mostre que $x^3 + x + \bar{1} \in \mathbb{Z}_5[x]$ é irredutível sobre $\mathbb{Z}_5$.

(20) Mostre que o polinômio $p(x) = x^3 - 2$ é irredutível sobre o corpo $\mathbb{Q}$.

(21) Sejam $\mathbb{K}$ um corpo, $p(x) \in \mathbb{K}[x]$ um polinômio irredutível sobre $\mathbb{K}$ e $f(x) \in \mathbb{K}[x] - \{0\}$. Prove que, se $f(x)|p(x)$ então ou $f(x) = a$ constante não nula ou $p(x) = b \cdot f(x)$ com $b \in \mathbb{K} - \{0\}$.

(22) Sejam $\mathbb{K}$ um corpo e $p(x) \in \mathbb{K}[x]$ um polinômio irredutível sobre $\mathbb{K}$. Se $f(x), g(x) \in \mathbb{K}[x]$ e $p(x)|f(x) \cdot g(x)$, prove que $p(x)|f(x)$ ou $p(x)|g(x)$.

(23) Decomponha o polinômio $x^4 - 5x^2 + 6$ em produto de fatores irredutíveis sobre os seguintes corpos $\mathbb{K}$:

(a) $\mathbb{K} = \mathbb{Q}$

(b) $\mathbb{K} = \mathbb{Q}[\sqrt{2}]$

(c) $\mathbb{K} = \mathbb{R}$

(24) Decomponha sobre o corpo $\mathbb{K} = \mathbb{Z}_3$ os seguintes polinômios como produto de irredutíveis:

(a) $x^2 + x + \bar{1}$

(b) $x^3 + x + \bar{2}$

(25) Prove que o polinômio $x^2 - \bar{3}$ é irredutível sobre o corpo $\mathbb{K} = \mathbb{Z}_5$. Mais ainda, se $J = \mathbb{Z}_5[x] \cdot p(x)$, onde $p(x) = x^2 - \bar{3}$ então o corpo $\dfrac{\mathbb{Z}_5}{J}$ possui exatamente 25 elementos.

(26) Prove que o polinômio $p(x) = x^3 + x + \bar{1}$ é irredutível sobre $\mathbb{Z}_5$. e mostre que o corpo $\dfrac{\mathbb{Z}_5}{J}$ possui exatamente 125 elementos, onde $J = \mathbb{Z}_5[x] \cdot p(x)$.

(27) Sejam $p(x)$ um polinômio irredutível de grau n sobre o corpo $\mathbb{Z}_p$, p primo, e seja $J = \mathbb{Z}_p[x] \cdot p(x)$. Prove que $\dfrac{\mathbb{Z}_p[x]}{J}$ é um corpo contendo exatamente p^n elementos.

(28) (a) Prove que $p(x) = x^2 + \bar{1}$ é irredutível sobre $\mathbb{K} = \mathbb{Z}_7$ e construa um corpo com 49 elementos.

(b) Prove que $p(x) = x^2 + \bar{1}$ é redutível sobre $\mathbb{K} = \mathbb{Z}_{11}$ e construa um corpo com 121 elementos.

(c) Prove que $p(x) = x^2 + \bar{1}$ é redutível sobre $\mathbb{K} = \mathbb{Z}_5$.

(d) Prove que $p(x) = x^3 - \bar{9}$ é irredutível sobre $\mathbb{K} = \mathbb{Z}_{31}$ e construa um corpo com $(31)^3$ elementos.

(29) Prove que os seguintes polinômios $f(x) \in \mathbb{Z}[x]$ são irredutíveis osbre $\mathbb{Q}$.

(a) $f(x) = x^4 + 2x^3 + 2x^2 + 2x + 2$
(b) $f(x) = x^7 - 31$
(c) $f(x) = x^6 + 15$
(d) $f(x) = x^3 + 6x^2 + 5x + 25$
(e) $f(x) = x^4 + 8x^3 + x^2 + 2x + 5$
(f) $f(x) = x^4 + 10x^3 + 20x^2 + 30x + 22$

(30) Determine quais dos seguintes polinômios são irredutíveis sobre $\mathbb{Q}$:

(a) $x^3 - x + 1$
(b) $x^3 + 2x + 10$
(c) $x^3 - 2x^2 + x + 15$
(d) $x^4 + 2$
(e) $x^4 - 2$
(f) $x^4 - x + 1$

(31) Determine quais dos seguintes polinômios sobre os seguintes corpos $\mathbb{K}$ são irredutíveis:

(a) $x^7 + 22x^3 + 11x^2 - 44x + 33; \quad \mathbb{K} = \mathbb{Q}$
(b) $x^3 - 7x^2 + 3x + 3; \quad \mathbb{K} = \mathbb{Q}$
(c) $x^4 - \bar{5}; \quad \mathbb{K} = \mathbb{Z}_{17}$
(d) $x^3 - \bar{5}; \quad \mathbb{K} = \mathbb{Z}_{11}$
(e) $x^4 + \bar{7}; \quad \mathbb{K} = \mathbb{Z}_{17}$

CAPÍTULO 5

APÊNDICE

5.1 Relações

5.1.1 Relação de equivalência

5.1.2 Relação de ordem

5.1.3 Exercícios

(1) Seja $X = \{1, 2, 3\}$. Considere as seguintes relações em X:

$$R_1 = \{(1,1), (2,2), (3,3)\}$$

$$R_2 = \{(1,1), (1,2), (1,3), (2,2), (2,3), (3,3)\}$$

$$R_3 = \{(1,2), (1,3), (2,1), (2,3), (3,1), (3,2), (3,3)\}$$

$$R_4 = X \times X$$

$$R_5 = \emptyset$$

Quais são reflexivas? E simétricas? E transitivas? E antissimétricas?

(2) $\emptyset \subset A \times A$, logo $\emptyset$ é uma relação em A. É de equivalência?

(3) Seja $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

(a) Represente no plano cartesiano os pontos da seguinte relação em X:

$$\Delta_X = \{(x, y) \in X \times X : x = y\}.$$

(Esse conjunto é conhecido como *diagonal* do conjunto X.)

(b) Mostre que Δ_X é uma relação de equivalência sobre X.

(c) Seja S_0 uma relação de equivalência sobre X com a propriedade de estar contida em qualquer outra relação de equivalência sobre X. Mostre que $S_0 = \Delta$. [Dica: basta mostrar que $\Delta_X \subset S_0$.]

(d) Mostre que $X \times X$ é uma relação de equivalência sobre X.

(4) (a) Seja

$$S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : \text{ existe } \quad n \in \mathbb{Z} \quad \text{tal que } \quad \frac{x}{y} = 3^n\}.$$

Mostre que S satisfaz as propriedades simétrica e transitiva, mas não satisfaz a propriedade reflexiva (atenção: o problema não é o número 3 na base da potência)

(b) Sejam X um conjunto não vazio e S uma relação sobre X que satisfaça as propriedades simétrica e transitiva. O raciocínio a seguir "demonstra" que uma relação que seja simétrica e transitiva é também reflexiva.

Sejam $x, y \in X$, se $(x, y) \in S$, pela propriedade simétrica, concluímos que $(y, x) \in S$. Usando agora a propriedade transitiva com os pares $(x, y) \in S$ e $(y, x) \in S$, vemos que $(x, x) \in S$. Assim, S é reflexiva.

O item (a) desta questão é um exemplo de que esse raciocínio está errado. Encontre o erro.

(5) Dados os conjuntos X e $S \subset X \times X$ a seguir, demonstre que S é uma relação de equivalência sobre X ou explique qual a propriedade que falta para não ser uma relação de equivalência.

(a) $X = \mathbb{Z}, \quad R = \{(a, b) \in X \times X : a - b \quad \text{é múltiplo de} \quad 3\}$

(b) $X = \{\text{retas do plano cartesiano}\}, \quad R = \{(a, b) \in X \times X : a \quad \text{é paralela a} \quad b\}$

(c) $X = \{\text{retas do plano cartesiano}\}, \quad R = \{(a, b) \in X \times X : a \quad \text{é perpendicular a} \quad b\}$

(d) $X = \{\text{pontos do plano cartesinao, exceto a origem}\}, \quad R = \{(a, b) \in X \times X : a \quad \text{pertence a reta que passa pela origem e por} \quad b\}$

(e) $X = \{\text{pessoas do mundo que têm alguma profissão}\}, \quad R = \{(a, b) \in X \times X : a \quad \text{tem a mesma profissão que} \quad b\}$

(f) $X = \{\text{pessoas desta faculdade}\}, \quad R = \{(a, b) \in X \times X : a \quad \text{é amigo de} \quad b\}$

(g) $X = \mathbb{R}, \quad R = \{(a, b) \in X \times X : a \geq b\}$

(6) Seja $X = \{1, 2, 3, 4, 5, 6\}$. Faça o que se pede em cada item e desenhe os diagramas de flechas.

(a) Dê exemplos de relações sobre X que sejam simétricas e antissimétricas ao mesmo tempo.

(b) Dê exemplos de relações sobre X que sejam simétricas e não sejam antissimétricas.

(c) Dê exemplos de relações sobre X que não sejam simétricas e sejam antissimétricas.

(d) Dê exemplos de relações sobre X que não sejam simétricas e nem antissimétricas.

(7) Pode acontecer de uma relação de equivalência ser também uma relação de ordem parcial (ou total)? Se sim, construa exemplos e, caso contrário, justifique.

(8) Considere o conjunto $X = \{x \in \mathbb{Z} : 0 \leq x \leq 50\}$. Defina sobre X a seguinte relação:

$$R = \{(a, b) \in X \times X : a - b \quad \text{é múltiplo de} \quad 4\}.$$

(a) Mostre que R é uma relação de equivalência.

(b) Descreve as classes de equivalência e escreva o conjunto quociente X/R.

(9) As relações definidas a seguir são de equivalência. Determine o que se pede em cada caso.

(a) $S = \{(a, b) \in X \times X : a - b \quad \text{é múltiplo de} \quad 5\}$, onde $X = \{0, 1, 2, 3, \ldots, 30\}$. Descreva as classes de equivalência e obtenha o conjunto quociente X/S.

(b) $S = \{(a, b) \in X \times X : a - b \quad \text{é múltiplo de} \quad 6\}$, onde $X = \{0, 1, 2, 3, \ldots, 35\}$. Descreva as classes de equivalência e obtenha o conjunto quociente X/S.

(10) Seja $X = \{x \in \mathbb{Z} : 0 \leq x \leq 20\}$ e defina sobre X a relação

$$S = \{(x, y) \in X \times X : \text{existe} \quad n \in \mathbb{Z} \quad \text{tal que} \quad x - y = 4n\}.$$

Determine o conjunto quociente X/S.

(11) Seja S uma relação de equivalência definida sobre um conjunto não vazio X. Sejam $x, y \in X$. Demonstre que as afirmações a seguir são equivalentes:

(i) xSy;

(ii) $x \in \overline{y}$;

(iii) $y \in \overline{x}$;

(iv) $\overline{x} = \overline{y}$.

(12) Verifique se cada um dos conjuntos a seguir é totalmente ordenado segundo a relação de divisibilidade.

(a) $X = \{1, 18, 3, 6\}$

(b) $X = \{4, 16, 5\}$

(c) $X = \{-1, 1, -5, 5, -20, 20\}$

(d) $X = \mathbb{Z}$

(13) Seja X um conjunto não vazio e seja $\mathcal{P}$ uma família de subconjuntos de X. Defina sobre $\mathcal{P}$ a relação de inclusão dada por $S = \{(F_1, F_2) \in \mathcal{P} \times \mathcal{P} : F_1 \subset F_2\}$, onde F_1, F_2 são elementos em $\mathcal{P}$.

(a) Mostre que S é reflexiva.

(b) Mostre que S é antissimétrica.

(c) Mostre que S é transitiva.

(d) Verifique se S é uma relação de ordem total sobre $\mathcal{P}$.

(14) Considere $X = \mathbb{N} \times \mathbb{N}$ e defina relação

$$S = \{((x, y), (z, t)) \in X \times X : x \quad \text{divide} \quad z \quad \text{e} \quad y \leq t\}$$

sobre X, em que o símbolo $\leq$ é a desigualdade "menor que ou igual a" no sentido usual.

(a) Demonstre que S satisfaz a propriedade reflexiva.

(b) Demonstre que S satisfaz a propriedade antissimétrica.

(c) Demonstre que S satisfaz a propriedade transitiva.

(d) Discuta porque S é uma relação de ordem parcial, mas não total sobre X.

(15) ***Ordem Lexicográfica.*** Considere $\mathbb{C}$ o conjunto dos números complexos e sejam $x = a + bi$, $y = c + di$ dois de seus elementos, onde $a, b, c, d \in \mathbb{R}$. Defina sobre $\mathbb{C}$ a seguinte relação:

$$S = \{(x, y) \in \mathbb{C} \times \mathbb{C} : a < c \quad \text{ou} \quad (a = c \quad \text{e} \quad b \leq d)\},$$

onde o símbolo $\leq$ é a desigualdade "menor que ou igual a" no sentido usual.

(a) Demonstre que S satisfaz a propriedade reflexiva.

(b) Demonstre que S satisfaz a propriedade antissimétrica.

(c) Demonstre que S satisfaz a propriedade transitiva.

(d) Demonstre que S é uma relação de ordem total sobre $\mathbb{C}$.

5.2 Estruturas definidas por uma operação

5.2.1 Exercícios

(1) Em cada caso a seguir, verifique se a operação $*$ sobre X é associativa, comutativa e tem elemento neutro. Determine também o conjuntos dos elementos regulares para a operação dada. Para as operações que possuem elemento neutro, determine os elementos simetrizáveis:

(a) $X = \mathbb{R}$ e $x * y = \dfrac{x+y}{2}$

(b) $X = \mathbb{R}$ e $x * y = x$

(c) $X = \mathbb{R}$ e $x * y = \sqrt{x^2 + y^2}$

(d) $X = \mathbb{R}^*$ e $x * y = \dfrac{x}{y}$

(2) Em cada caso a seguir está definida uma operação sobre $\mathbb{Z} \times \mathbb{Z}$. Verifique se ela é associativa, comutativa e tem elemento neutro. Determine também o conjuntos dos elementos regulares para a operação dada. Para as operações que possuem elemento neutro, determine os elementos simetrizáveis:

(a) $(a, b) * (c, d) = (ac, 0)$

(b) $(a, b) \triangle (c, d) = (a + c, b + d)$

(c) $(a, b) \odot (c, d) = (ac, ad + bc)$

(d) $(a, b) \oslash (c, d) = (a + c, bd)$

(3) Estabeleça as condições sobre $m, n \in \mathbb{Z}$ de modo que a operação $*$ sobre $\mathbb{Z}$ dada pela lei $x * y = mx + ny$:

(a) seja associativa;

(b) seja comutativa;

(c) admita elemento neutro.

(4) Mostre que nenhum elemento de $\mathbb{R}$ é regular para a operação $*$ assim definida:

$$x * y = x^2 + y^2 - xy.$$

(5) Em cada caso a seguir está definida uma operação $*$ sobre X. Faça a tábua da operação:

(a) $X = \{1, 2, 3, 6\}$ e $x * y = \text{mdc}(x, y)$

(b) $X = \{1, 3, 9, 27\}$ e $x * y = \text{mmc}(x, y)$

(c) $X = \{1, \sqrt{2}, \frac{3}{2}\}$ e $x * y = \min(x, y)$

(d) $X = \{3\sqrt{2}, \pi, \frac{7}{2}\}$ e $x * y = \max(x, y)$

(6) Em cada caso a seguir está definida uma operação $*$ sobre $X = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. Construa a tábua da operação.

(a) $x * y = x \cup y$

(b) $x * y = x \cap y$

(c) $x * y = (x \cup y) - (x \cap y)$

(7) Construa as tábuas das operações $*$ e $\triangle$ sobre $X = \{0, 1, 2, 3\}$ assim definidas:

(a) $x * y =$ resto da divisão em $\mathbb{Z}$ de $x + y$ por 4.

(b) $x \triangle y =$ resto da divisão em $\mathbb{Z}$ de $x \cdot y$ por 4.

(8) Construa as tábuas das operações $\oplus$ e $\odot$ sobre $X = \{0, 1, 2, 3, 4\}$ assim definidas:

(a) $x \oplus y =$ resto da divisão em $\mathbb{Z}$ de $x + y$ por 5.

(b) $x \odot y =$ resto da divisão em $\mathbb{Z}$ de $x \cdot y$ por 5.

(9) A partir da tábua abaixo, da operação $\odot$ sobre $X = \{1, 2, 3, 4\}$, calcule os seguintes elementos:

$\odot$	1	2	3	4
1	1	1	1	1
2	1	2	3	4
3	1	3	4	2
4	1	4	2	3

(a) $(3 \odot 4) \odot 2$

(b) $3 \odot (4 \odot 2)$

(c) $(4 \odot (3 \odot 3)) \odot 4$

(d) $(4 \odot 3) \odot (3 \odot 4)$

(e) $((4 \odot 3) \odot 3) \odot 4$

(10) Construa a tábua da operação de intersecção sobre a família de conjuntos $\mathcal{F} = \{A, B, C, D\}$, sabendo que

$$A \cap B = B,\ B \cap C = C,\ C \cap D = D.$$

Em seguida, estabeleça:

(a) qual é o elemento neutro;

(b) que elementos são simetrizáveis;

(c) que elementos são regulares.

(11) Nos itens a seguir verifique qual a maior estrutura (semigrupo, monóide ou grupo) que os conjuntos com as operações indicadas possuem:

(a) O conjunto $\wp(X)$ das partes de um conjunto X, com a operação de união de conjuntos.

(b) O conjunto $\wp(X)$ das partes de um conjunto X, com a operação de intersecção de conjuntos.

(c) O conjunto $\mathbb{Z}$ dos números inteiros, com a operação de subtração.

(d) O conjunto $\mathbb{N}^*$ dos números naturais não nulos, com a operação de potenciação.

(e) O conjunto $\mathbb{Q}$ dos números racionais, com a operação de divisão.

(12) Verifique se os conjuntos abaixo com as operações dadas são grupos:

(a) o conjunto dos números ímpares com a multiplicação.

(b) o conjunto dos múltiplos de 3 com a adição.

(c) conjunto dos números da forma $a + b\sqrt{2}$, onde $a, b \in \mathbb{R}$ com a adição.

(d) conjunto dos polinômios da forma $ax + b$, onde $a, b \in \mathbb{N}$ com a adição.

(e) conjunto dos inteiros não positivos $\mathbb{Z}_-$, com a adição.

(f) conjunto $C = \{-2, -1, 0, 1, 2\}$, com a adição.

(g) conjunto $A = \{1, -1\}$, com a multiplicação.

(13) Sabemos que em $\mathbb{Z}$, $m \equiv n (\mathrm{mod}\, 5)$ se e somente se, $m - n = 5k$, para algum $k \in \mathbb{Z}$. Desta relação de equivalência em $\mathbb{Z}$, vem o conjunto quociente $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Faça a tábua da adição em $\mathbb{Z}_5$. Logo em seguida, determine a estrutura (semigrupo, monóide ou grupo) de $\mathbb{Z}_5$.

(14) Defina em $\mathbb{Z}$ a operação $\odot$ da seguinte forma:

$$a \odot b = a + b - ab.$$

Qual a estrutura (semigrupo, monóide ou grupo) de $\mathbb{Z}$ com a operação $\odot$?

(15) Defina em $\mathbb{Z}$ a operação $\oplus$ da seguinte forma:

$$a \oplus b = a + b^2.$$

Qual a estrutura (semigrupo, monóide ou grupo) de $\mathbb{Z}$ com a operação $\oplus$?

(16) Mostre que $\mathbb{R}$ dotado da operação $*$ tal que $x * y = \sqrt[3]{x^3 + y^3}$ é um grupo abeliano.

(17) Mostre que $\mathbb{R}$ munido da operação $\triangle$ tal que $x \triangle y = x + y - 3$ é um grupo abeliano.

(18) Mostre que $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$ é um grupo aditivo abeliano. Estabeleça as condições sobre a e b para que $\mathbb{Q}[\sqrt{2}]$ seja também um grupo multiplicativo.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] GARCIA, A. e LEQUAIN, Y. *Elementos de Álgebra*. Projeto Euclides, IMPA, Rio de Janeiro, 2010.

[2] GONÇALVES, A. *Introdução à Álgebra*. Projeto Euclides, IMPA, Rio de Janeiro, 2006.

[3] HEFEZ, A. *Elementos de Aritmética*. 2ª Edição, Textos Universitários, SBM, Rio de Janeiro, 2006.

[4] HEFEZ, A. *Curso de álgebra*. 5. Edição, Coleção Matemática Universitária, IMPA, Rio de Janeiro, 2016.

[5] HEFEZ, A. e VILLELA, M. L. T. *Polinômios e equações algébricas*. 2. Edição, Coleção PROFMAT, SBM, Rio de Janeiro, 2018.

[6] SANTOS, J. P. O., *Introdução à Teoria dos Números*, 3. edição, Coleção Matemática Universitária, IMPA, Rio de Janeiro, RJ, 2018.

[7] SILVA, J. C. e GOMES, O. R. *Estruturas algébricas para licenciatura. Elementos de aritmética superior*. 1ª ed., volume 2, Editora Edgard Blücher, São Paulo, 2018.

[8] SILVA, J. C. e GOMES, O. R. *Estruturas algébricas para licenciatura. Elementos de álgebra moderna*. 1. Edição, volume 3, Editora Edgard Blücher, São Paulo, (2020).

[9] TENGAN, E., et al., *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*, 5. edição, Projeto Euclides, IMPA, Rio de Janeiro, RJ, 2018.

[10] VIDIGAL, A., et al., *Fundamentos de Álgebra*, Editora UFMG, Belo Horizonte, MG, 2005.