LENIMAR NUNES DE ANDRADE

INTRODUÇÃO À ÁLGEBRA: QUESTÕES COMENTADAS E RESOLVIDAS

1^{a} edição
ISBN 978-85-917238-0-5

João Pessoa
Edição do Autor
2014

Prefácio

Este texto foi elaborado para a disciplina "Introdução à Álgebra" que passou a ser ministrada na UAB/UFPB a partir de 2010. É um complemento de outro texto que contenha o desenvolvimento detalhado da teoria. Dedica-se principalmente a alunos dos cursos de Licenciatura ou Bacharelado em Matemática, Física, Química ou Engenha Elétrica (Telecomunicações).

No início, fazemos um pequeno resumo dos assuntos vistos ao longo do semestre: operações binárias, grupos, anéis, corpos e polinômios. Depois, iniciamos a resolução de vários exercícios relacionados com os esses temas para ajudar na fixação do conteúdo. No final, são apresentados alguns testes do tipo múltipla escolha.

É importante observar que os exercícios foram colocados em ordem crescente de dificuldade. Os que iniciam com "A" (Ex.: A1, A2, etc.) são os mais fáceis, os que iniciam com "B" (Ex.: B1, B2, etc.) são os "médios" e os que iniciam com "C" são os mais difíceis.

João Pessoa, 8 de janeiro de 2014

Lenimar Nunes de Andrade

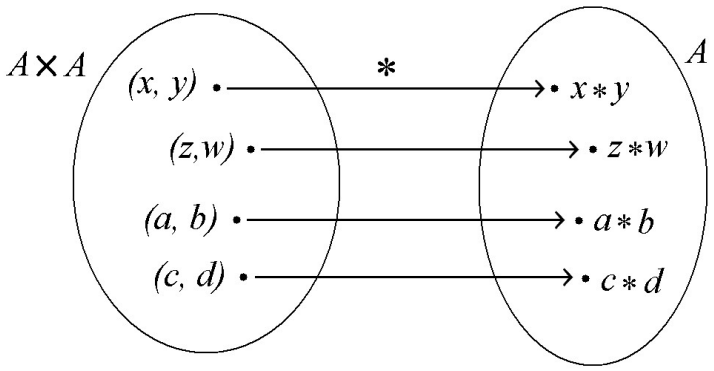
Sumário

Capítulo 1

Resumo da teoria

1.1 Operações binárias

Uma **operação binária** $*$ (ou simplesmente uma **operação** $*$) sobre um conjunto $A \neq \emptyset$ é uma função de $A \times A$ em A que associa a cada par $(x, y) \in A \times A$ um único elemento de A que é denotado por $x * y$.



Comutatividade

Uma operação $*$ sobre A é **comutativa** quando

$$x * y = y * x, \ \forall x, y \in A$$

Exemplos

- A adição de inteiros é comutativa, ou seja, $x + y = y + x$, $\forall x, y \in \mathbb{Z}$.
- A multiplicação de inteiros também é comutativa, ou seja, $x \cdot y = y \cdot x$, $\forall x, y \in \mathbb{Z}$.
- A multiplicação de matrizes não é uma operação comutativa, isto é, existem matrizes A e B tais que $AB \neq BA$.

- A composição de funções também não é uma operação comutativa, isto é, existem funções f e g tais que $f \circ g \neq g \circ f$.

Associatividade

Uma operação $*$ sobre A é **associativa** quando

$$x * (y * z) = (x * y) * z, \ \forall x, y, z \in A$$

Exemplos

- A adição de números reais é associativa, ou seja, $x + (y + z) = (x + y) + z$, $\forall x, y, z \in \mathbb{R}$.
- A multiplicação de números reais é associativa, ou seja, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, $\forall x, y, z \in \mathbb{R}$.
- A subtração de números reais não é uma operação associativa. Por exemplo, $5 - (2 - 1) = 5 - 1 = 4$ e $(5 - 2) - 1 = 3 - 1 = 2$ de onde temos que $5 - (2 - 1) \neq (5 - 2) - 1$.

Elemento neutro

Um elemento $e \in A$ é denominado **elemento neutro** para a operação $*$ sobre A quando

$$x * e = e * x = x, \ \forall x \in A$$

Exemplos

- O 0 (zero) é o elemento neutro da adição de inteiros.
- O 1 (um) é o elemento neutro da multiplicação de inteiros.
- A matriz identidade $n \times n$ é o elemento neutro da operação de multiplicação de matrizes $n \times n$.
- A operação de potenciação $x * y = x^y$ definida sobre os inteiros positivos não tem elemento neutro.

Elemento inverso

Se uma operação $*$ sobre A possuir elemento neutro e, então um elemento $x \in A$ é denominado **invertível** (ou simetrizável) quando existir $x^{-1} \in A$ tal que

$$x * x^{-1} = x^{-1} * x = e$$

Exemplos

- Todo $x \in \mathbb{Z}$ possui um inverso com relação à operação de adição de inteiros: é o inteiro $-x$. Por exemplo, o inverso (aditivo) de 3 é o -3.
- Na multiplicação usual dos números racionais, todo $x = \frac{p}{q} \in \mathbb{Q}$ possui um inverso (multiplicativo) que é o elemento $x^{-1} = \frac{q}{p}$, com exceção apenas do 0 (zero) que não tem inverso com relação à multiplicação.

Distributividade

Sejam $*$ e $\oplus$ duas operações definidas sobre um conjunto $A \neq \emptyset$. Dizemos que $*$ é **distributiva** com relação a $\oplus$ quando

$$x * (y \oplus z) = x * y \oplus x * z, \ \forall x, y, z \in A$$

e

$$(x \oplus y) * z = x * z \oplus y * z, \ \forall x, y, z \in A.$$

Exemplo

No conjunto dos números inteiros, a multiplicação é distributiva com relação à adição porque:

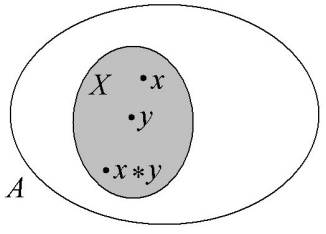
- $x \cdot (y + z) = x \cdot y + x \cdot z$
- $(x + y) \cdot z = x \cdot z + y \cdot z$

para quaisquer $x, y, z \in \mathbb{Z}$.

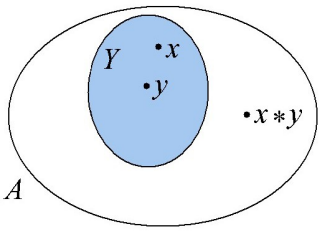
Parte fechada

Consideremos um conjunto $A \neq \emptyset$, $X \neq \emptyset$ um subconjunto de A e $*$ uma operação definida sobre A. Dizemos que X é **parte fechada** de A com relação à operação $*$ quando

$$\forall x, y \in X \Rightarrow x * y \in X.$$



X é parte fechada para $*$



Y não é parte fechada para $*$

Tábua de uma operação

A **tábua** de uma operação $*$ definida sobre um conjunto finito $A = \{a_1, a_2, \cdots, a_n\}$ é uma tabela onde o resultado da operação $a_i * a_j$ é colocado na i-ésima linha e j-ésima coluna.

$*$	a_1	a_2	a_3	a_4	a_5
a_1	$a_1 * a_1$	$a_1 * a_2$	$a_1 * a_3$	$a_1 * a_4$	$a_1 * a_5$
a_2	$a_2 * a_1$	$a_2 * a_2$	$a_2 * a_3$	$a_2 * a_4$	$a_2 * a_5$
a_3	$a_3 * a_1$	$a_3 * a_2$	$a_3 * a_3$	$a_3 * a_4$	$a_3 * a_5$
a_4	$a_4 * a_1$	$a_4 * a_2$	$a_4 * a_3$	$a_4 * a_4$	$a_4 * a_5$
a_5	$a_5 * a_1$	$a_5 * a_2$	$a_5 * a_3$	$a_5 * a_4$	$a_5 * a_5$

1.2 Grupos

Um **grupo** é um conjunto $G \neq \emptyset$ no qual está definida uma operação $*$ que satisfaz às seguintes propriedades:

- $*$ é associativa, ou seja, $x * (y * z) = (x * y) * z$, $\forall x, y, z \in G$
- $*$ admite elemento neutro, ou seja, $\exists e \in G$ tal que $x * e = e * x = x$, $\forall x \in G$
- Para cada elemento $x \in G$, $\exists x^{-1} \in G$ tal que $x * x^{-1} = x^{-1} * x = e$

Além disso, se $*$ for comutativa, então o grupo G é denominado *comutativo* ou *abeliano*.

Exemplos

- O conjunto dos inteiros $\mathbb{Z}$ com a adição usual é um grupo.
- O conjunto dos números reais não nulos $\mathbb{R}^*$ com a operação de multiplicação usual é um grupo.

Grupos de permutações

Sejam E um conjunto não vazio e S_E o conjunto de todas as funções bijetoras $f : E \longrightarrow E$. Com a operação $\circ$ de composição de funções, $(S_E, \circ)$ é um grupo denominado **grupo de permutações sobre** E.

Notação

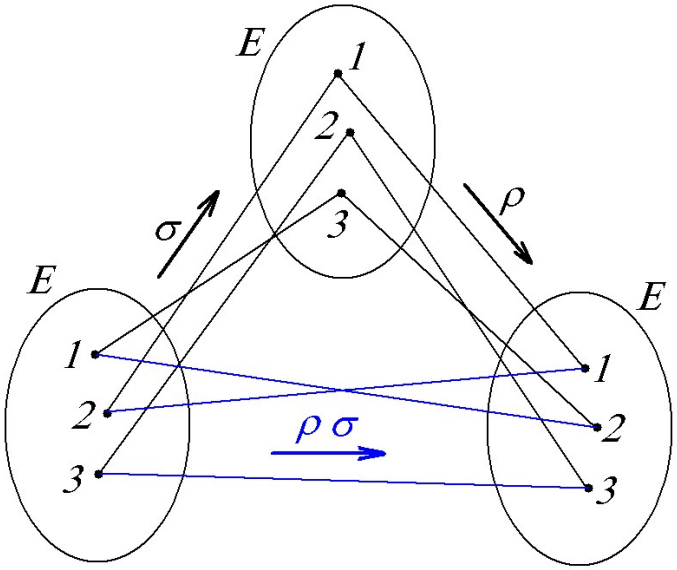
Em particular, quando $E = \{1, 2, \cdots, n\}$, onde n é um inteiro positivo fixado, S_E é denotado por S_n. Se $f : E \longrightarrow E$ for tal que $f(i) = a_i$, para todo $i \in E$, então f costuma ser denotada na forma

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$$

O total de funções que podem ser construídas dessa forma é de $n!$.

Exemplo

Sejam $E = \{1, 2, 3\}$ e $\sigma, \rho \in S_3$ definidas por $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ e $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Então $\rho \circ \sigma = \rho\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.



Grupos de classes de restos

Sejam $n > 1$ um inteiro e $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$, onde $\bar{a} = \{a+kn \mid k \in \mathbb{Z}\}$, $\forall a \in \mathbb{Z}$. O conjunto $\mathbb{Z}_n$ é denominado conjunto das **classes de restos módulo** n. Definindo-se a seguinte operação de adição sobre $\mathbb{Z}_n$

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

então $(\mathbb{Z}_n, +)$ é um grupo abeliano.

Exemplo

Escolhendo $n = 5$, temos que em $\mathbb{Z}_5$ são válidas as igualdades:

- $\bar{1} + \bar{2} = \bar{3}$, $\bar{2} + \bar{2} = \bar{4}$, $\bar{0} + \bar{3} = \bar{3}$
- $\bar{2} + \bar{3} = \bar{0}$, $\bar{4} + \bar{3} = \bar{2}$, $\bar{3} + \bar{3} = \bar{1}$

Subgrupos

Seja $(G, *)$ um grupo. Um subconjunto não vazio $H \subset G$ que seja fechado com relação à operação $*$ é denominado um **subgrupo** de G quando $(H, *)$ também for um grupo.

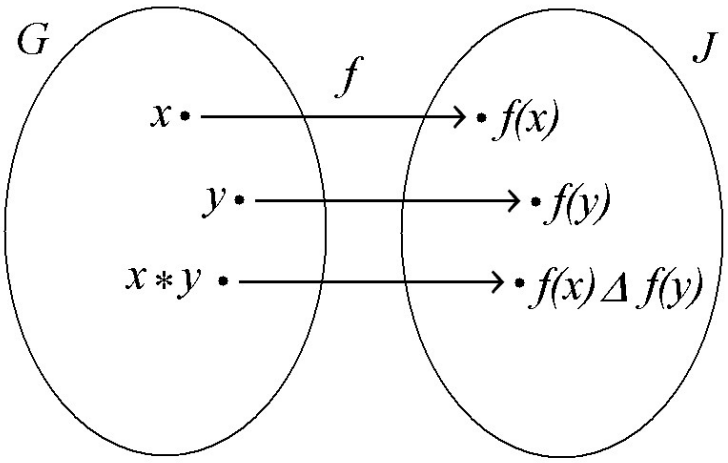
Exemplos

- $H = (\mathbb{Q}, +)$ é um subgrupo de $G = (\mathbb{R}, +)$
- O conjunto H dos inteiros pares com a operação de adição usual é um subgrupo de $G = (\mathbb{Z}, +)$.
- O conjunto $H = (\mathbb{R}_+^*, \cdot)$ dos números reais positivos com a operação de multiplicação usual é um subgrupo de $G = (\mathbb{R}^*, \cdot)$
- O conjunto $N = (\mathbb{R}_-^*, \cdot)$ dos reais negativos com a multiplicação não é subgrupo de $G = (\mathbb{R}^*, \cdot)$, porque N não é fechado com relação à multiplicação.

1.3 Homomorfismo de grupos

Uma função f de um grupo $(G, *)$ em um grupo (J, Δ) chama-se um **homomorfismo** quando

$$f(x * y) = f(x) \Delta f(y), \ \forall x, y \in G.$$



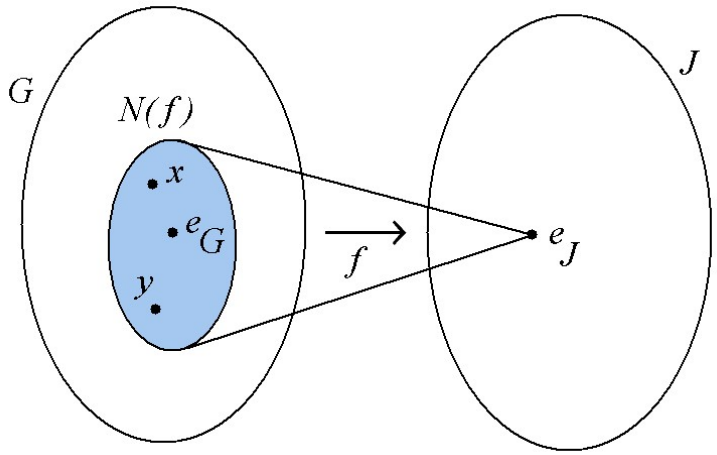
Exemplos

- Se $G = J = (\mathbb{Z}, +)$, então $f : G \longrightarrow J$, $f(x) = 2x$ é um homomorfismo de grupos porque $f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$, $\forall x, y \in G$.
- Se $G = (\mathbb{Q}^*, \cdot)$ e $J = (\mathbb{R}^*, \cdot)$, então $f : \mathbb{Q} \longrightarrow \mathbb{R}$, $f(x) = x^2$ é um homomorfismo de grupos porque $f(x \cdot y) = (x \cdot y)^2 = x^2 \cdot y^2 = f(x) \cdot f(y)$, $\forall x, y \in \mathbb{Q}$.
- Sejam $G = (\mathbb{R} \times \mathbb{R}, +)$, $J = (\mathbb{R}^*, \cdot)$ e $g : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}^*$, $g(x, y) = 2^{x-y}$. Para quaisquer $(a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$, temos que: $g((a, b) + (c, d)) = g(a + c, b + d) = 2^{(a+c)-(b+d)} = 2^{(a-b)+(c-d)} = 2^{a-b} \cdot 2^{c-d} = g(a, b) \cdot g(c, d)$. Logo, g é um homomorfismo de G em J.

Núcleo de um homomorfismo

Se $f : G \to J$ for um homomorfismo de grupos, o **núcleo** de f, denotado por $N(f)$, é o conjunto de todos os elementos do domínio G cujas imagens através de f são iguais ao elemento neutro de J:

$$N(f) = \{x \in G \mid f(x) = e_J\}$$



Exemplos

Vamos determinar o núcleo de cada um dos homomorfismos dos exemplos anteriores.

- Seja $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{R}, +)$, $f(x) = 2x$. O elemento neutro do contradomínio de f é o 0 (zero). Se $x \in N(f)$, então $f(x) = 0 \Rightarrow 2x = 0 \Rightarrow x = 0$. Logo, o núcleo de f é formado apenas pelo 0 (zero), isto é, $N(f) = \{0\}$.

- Sejam $G = (\mathbb{Q}^*, \cdot)$, $J = (\mathbb{R}^*, \cdot)$, $f : G \longrightarrow J$, $f(x) = x^2$. O elemento neutro de J é o 1 (um). Se $x \in N(f)$, então devemos ter $f(x) = 1$, ou seja, $x^2 = 1 \Rightarrow x = \pm 1$. Logo, $N(f) = \{-1, 1\}$.
- Sejam $G = (\mathbb{R} \times \mathbb{R}, +)$, $J = (\mathbb{R}^*, \cdot)$, $g : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}^*$, $g(x, y) = 2^{x-y}$. Se $(x, y) \in N(g)$, então $g(x, y) = 1$ = elemento neutro de $J \Rightarrow 2^{x-y} = 1 \Rightarrow 2^{x-y} = 2^0$ $\Rightarrow x - y = 0 \Rightarrow x = y$. Logo, $N(g) = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y\} = \{(x, x) \mid x \in \mathbb{R}\}$.

Isomorfismo de grupos

Um **isomorfismo** de um grupo G em um grupo J é um homomorfismo de G em J que também é uma função bijetora. Se existir um isomorfismo de G em J então dizemos que G e J são isomorfos e denotamos isso por $G \simeq J$.

Exemplo

A função $f(x) = \log(x)$ é um isomorfismo de $G = (\mathbb{R}_+^*, \cdot)$ em $J = (\mathbb{R}, +)$ porque:

- $f : \mathbb{R}_+^* \longrightarrow \mathbb{R}$, $f(x) = \log(x)$ é bijetora;
- Para quaisquer $x, y \in \mathbb{R}_+^*$ temos: $f(x \cdot y) = \log(x \cdot y) = \log(x) + \log(y) = f(x) + f(y)$.

Potências e múltiplos

Em um grupo multiplicativo $(G, \cdot)$ com elemento neutro e, dados $x \in G$ e $n \in \mathbb{Z}$, definimos a potência x^n da seguinte forma:

$$x^n = \begin{cases} x^{n-1} \cdot x, & \text{se } n \geq 1 \\ e, & \text{se } n = 0 \\ (x^{-1})^{-n}, & \text{se } n < 0 \end{cases}$$

Pela definição, $x^0 = e$, $x^n = \underbrace{x \cdot x \cdot x \cdot \cdots \cdot x}_{n \text{ fatores}}$ se $n > 0$ e $x^n = \underbrace{x^{-1} \cdot x^{-1} \cdot x^{-1} \cdot \cdots \cdot x^{-1}}_{(-n) \text{ fatores}}$ se $n < 0$.

Múltiplos

Em um grupo aditivo $(G, +)$ com elemento neutro 0, dados $x \in G$ e $n \in \mathbb{Z}$, definimos o múltiplo nx da seguinte forma:

$$nx = \begin{cases} (n-1)x + x, & \text{se } n \geq 1 \\ 0, & \text{se } n = 0 \\ (-n)(-x), & \text{se } n < 0 \end{cases}$$

Pela definição, $0x = 0$, $nx = \underbrace{x + x + x + \cdots + x}_{n \text{ parcelas}}$ se $n > 0$ e $nx = \underbrace{(-x) + (-x) + (-x) + \cdots + (-x)}_{(-n) \text{ parcelas}}$ se $n < 0$.

A definição de múltiplo é muito parecida com a de potência.

1.4 Grupos cíclicos

Grupo gerado por um elemento

Seja x um elemento de um grupo multiplicativo $(G, \cdot)$. O **grupo gerado por** x, denotado por $[x]$ (ou por $\langle x \rangle$) é o conjunto de todas as potências de expoente inteiro de x:

$$[x] = \{x^k \mid k \in \mathbb{Z}\} = \{\ldots, x^{-3}, x^{-2}, x^{-1}, x, e, x, x^2, x^3, \ldots\}$$

Se $(J, +)$ for um grupo aditivo e $y \in J$, então $[y]$ é o conjunto de todos os múltiplos de y:

$$[y] = \{ky \mid k \in \mathbb{Z}\} = \{\ldots, -3y, -2y, -y, 0, y, 2y, 3y, \ldots\}$$

Exemplo

Em $G = (\mathbb{Q}^*, \cdot)$, temos: $[2] = \{2^k \mid k \in \mathbb{Z}\} = \{\ldots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \ldots\}$

Grupos cíclicos

Um grupo G é denominado **cíclico** se existir $x \in G$ tal que $G = [x]$. Neste caso, todos os elementos de G são potências (ou múltiplos) de x que é denominado um *gerador* de G.

Exemplos

- $(\mathbb{Z}, +)$ é um grupo cícliclo porque todo inteiro é múltiplo de 1, ou seja, $\mathbb{Z} = [1]$. Um grupo cíclico pode ter mais de um gerador. Note que neste caso temos também $\mathbb{Z} = [-1]$.
- $(\mathbb{Z}_5^*, \cdot)$ é um grupo cíclico gerado por $\bar{2}$ porque $[\bar{2}] = \{\bar{2}^0, \bar{2}^1, \bar{2}^2, \bar{2}^3\} = \{\bar{1}, \bar{2}, \bar{4}, \bar{3}\} = \mathbb{Z}_5^*$.

- O grupo multiplicativo dos reais, $(\mathbb{R}^*, \cdot)$, não é um grupo cíclico porque não existe um número real x tal que todo número real seja igual a alguma potência de x.

Classes laterais

Consideremos um grupo $(G, *)$, um subgrupo $H \subset G$ e $x \in G$.

- A **classe lateral à esquerda**, módulo H, definida por x, denotada por $x * H$, é o conjunto definido por
$$x * H = \{x * h \mid h \in H\}$$
- A **classe lateral à direita**, módulo H, definida por x, denotada por $H * x$, é o conjunto definido por
$$H * x = \{h * x \mid h \in H\}$$

As classes laterais à esquerda podem coincidir ou não com as classes à direita. Podemos ter $x * H = H * x$ ou $x * H \neq H * x$, dependendo do x e do H.

Exemplo 1

Sejam $G = (\mathbb{Z}_8, +)$ e um subgrupo $H = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$.

- A classe lateral à esquerda definida pelo elemento $\bar{1}$ é: $\bar{1} + H = \bar{1} + \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\} = \{\bar{1} + \bar{0}, \bar{1} + \bar{2}, \bar{1} + \bar{4}, \bar{1} + \bar{6}\} = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.
- A classe lateral à esquerda definida pelo elemento $\bar{2}$ é: $\bar{2} + H = \bar{2} + \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\} = \{\bar{2} + \bar{0}, \bar{2} + \bar{2}, \bar{2} + \bar{4}, \bar{2} + \bar{6}\} = \{\bar{2}, \bar{4}, \bar{6}, \bar{0}\}$.

Exemplo 2

Consideremos $G = (\mathbb{R}^*, \cdot)$ e um subgrupo $H = \{3^k \mid k \in \mathbb{Z}\}$, ou seja, $H = \{\cdots, \frac{1}{9}, \frac{1}{3}, 1, 3, 9, 27, \cdots\}$. A classe lateral à direita definida pelo elemento $\sqrt{2} \in G$ é: $H \cdot \sqrt{2} = \{3^k \cdot \sqrt{2} \mid k \in \mathbb{Z}\} = \{\cdots, \frac{\sqrt{2}}{9}, \frac{\sqrt{2}}{3}, \sqrt{2}, 3\sqrt{2}, 9\sqrt{2}, 27\sqrt{2}, \cdots\}$.

Índice de H em G

Sejam G um grupo finito e H um subgrupo de G. O **índice de H em G** é o número de classes laterais distintas módulo H em G e é denotado por $(G : H)$.

Exemplo

Sejam $G = (\mathbb{Z}_6, +)$ e $H = \{\bar{0}, \bar{3}\}$. As classes laterais módulo H são:

- $\bar{0} + H = \{\bar{0} + \bar{0}, \bar{0} + \bar{3}\} = \{\bar{0}, \bar{3}\}$
- $\bar{1} + H = \{\bar{1} + \bar{0}, \bar{1} + \bar{3}\} = \{\bar{1}, \bar{4}\}$
- $\bar{2} + H = \{\bar{2} + \bar{0}, \bar{2} + \bar{4}\} = \{\bar{2}, \bar{5}\}$

As outras classes $\bar{3} + H = \{\bar{3}, \bar{0}\}$, $\bar{4} + H = \{\bar{4}, \bar{1}\}$, etc. coincidem com as anteriores. Dessa forma, temos um total de 3 classes laterais distintas e, consequentemente, $(G : H) = 3$.

Subgrupo normal e grupo quociente

Sendo $(G, *)$ um grupo, um subgrupo N de G é denominado **normal** quando $x * N = N * x$ para todo $x \in G$. Neste caso, denotaremos N normal em G por $N \lhd G$.

Grupo quociente

Consideremos $N \lhd G$. O conjunto de todas as classes laterais módulo N é um grupo com a operação definida por

$$(aN)(bN) = (ab)N, \ \forall a, b \in G$$

e é denominado **grupo quociente** de G por N. O grupo quociente de G por N é denotado por G/N.

1.5 Principais proposições

Teorema de Lagrange

Se G for um grupo finito e H um subgrupo de G, então a ordem de H é um divisor da ordem de G e o quociente da divisão é igual ao índice de H em G. Em símbolos: $o(G) = o(H) \cdot (G : H)$.

Teorema do Homomorfismo

Seja $f : G \longrightarrow J$ um homomorfismo de grupos sobrejetor. Se N for o núcleo de f, então $N \lhd G$ e $G/N \simeq J$.

1.6 Anéis

Seja $A \neq \emptyset$ um conjunto com duas operações: uma adição $(+)$ e uma multiplicação $(\cdot)$. Dizemos que $(A, +, \cdot)$ *é um anel* quando

- A é um grupo abeliano com relação à adição:
  - $\forall x, y, z \in A,\ x + (y + z) = (x + y) + z$
  - $\forall x, y \in A,\ x + y = y + x$
  - Existe $0 \in A$ tal que $x + 0 = x,\ \forall x \in A$
  - Para todo $x \in A$, existe $(-x) \in A$ tal que $x + (-x) = 0$
- A multiplicação é associativa: $\forall x, y, z,\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- A multiplicação é distributiva com relação à adição: $x \cdot (y + z) = x \cdot y + x \cdot z$ e $(x + y) \cdot z = x \cdot z + y \cdot z$ para quaisquer $x, y, z \in A$.

Exemplos

- O conjunto dos números inteiros $\mathbb{Z}$ é um anel com relação às operações de adição e multiplicação de inteiros usuais.
- Também são anéis os seguintes conjuntos numéricos: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$.
- Sendo n um inteiro positivo, O conjunto dos múltiplos de n

  $$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$$

  é um anel com as operações de adição e multiplicação usuais dos inteiros.
- Dado $n > 1$ um inteiro, o conjunto $M_{n\times n}(\mathbb{Z})$ das matrizes quadradas $n \times n$ com elementos em $\mathbb{Z}$ é um anel com relação à adição e à multiplicação de matrizes definidas de forma usual.

Exemplo

- Dado n um inteiro positivo, o conjunto das classes de restos módulo n,

  $$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\},$$

  é um anel com relação às operações de adição e multiplicação definidas da seguinte forma:

  $$\bar{x} + \bar{y} = \overline{x + y}$$

  e

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

  para quaisquer $\bar{x}, \bar{y} \in \mathbb{Z}_n$.

Subanéis

Seja $(A, +, \cdot)$ um anel e $S \neq \emptyset$ um subconjunto de A. Dizemos que S é um *subanel* de A quando $(S, +, \cdot)$ também for um anel com as operações de A restritas ao conjunto S.

Exemplos

- O conjunto dos múltiplos de 2, $2\mathbb{Z}$, é um subanel de $\mathbb{Z}$ com as operações de adição e multiplicação de inteiros usuais.
- Em geral, $(n\mathbb{Z}, +, \cdot)$ é um subanel de $(\mathbb{Z}, +, \cdot)$ para qualquer inteiro positivo n.

Subanéis

A proposição a seguir fornece um critério bastante útil para se determinar se um conjunto $S \neq \emptyset$ é subanel de um anel A.

Proposição

Sejam $(A, +, \cdot)$ e $S \neq \emptyset$ um subconjunto de A. Então, S é um subanel de A se, e somente se, S for fechado com relação à subtração e à multiplicação de A, ou seja, se, e somente se, $x - y \in S$ e $x \cdot y \in S$ para quaisquer $x, y \in S$.

Observação

Em um anel A, a diferença $x - y$ de dois elementos $x, y \in A$ é definida como sendo $x - y = x + (-y)$.

Subanéis

Exemplo

Consideremos no anel $A = (M_{2\times 2}(\mathbb{R}), +, \cdot)$ o conjunto $S = \left\{ \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \mid x, y \in \mathbb{Q} \right\}$.

- É claro que $S \neq \emptyset$ porque, por exemplo, $\begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix} \in S$.
- Além disso, dados dois elementos quaisquer de S, $M = \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix}$ e $N = \begin{bmatrix} z & 0 \\ t & 0 \end{bmatrix}$, temos que $M - N = \begin{bmatrix} x - z & 0 \\ y - t & 0 \end{bmatrix} \in S$ e $M \cdot N = \begin{bmatrix} x \cdot z & 0 \\ y \cdot z & 0 \end{bmatrix} \in S$.

- Usando a Proposição anterior, concluímos que S é um subanel de A.

Anéis comutativos

Um anel $(A, +, \cdot)$ é denominado *comutativo* se a sua multiplicação for comutativa, ou seja, se $x \cdot y = y \cdot x$, $\forall x, y \in A$.

Exemplos

- O anel dos inteiros $(\mathbb{Z}, +, \cdot)$ é um anel comutativo porque $x \cdot y = y \cdot x$, $\forall x, y \in \mathbb{Z}$.
- Também são comutativos os seguintes anéis: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_m$ com as operações usuais de adição e multiplicação definidas em cada um desses conjuntos.
- Dado $n > 1$ um inteiro, o anel $(M_{n\times n}(\mathbb{R}), +, \cdot)$ das matrizes quadradas $n \times n$ com elementos em $\mathbb{R}$ não é comutativo.

Anéis com unidade

Um *anel com unidade* é um anel A cuja multiplicação possui elemento neutro, denotado por 1_A ou simplesmente por 1, e denominado a *unidade* do anel.

Exemplos

- O número 1 é a unidade dos anéis $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$. Logo, esses são exemplos de anéis com unidade.
- Dado $m \geq 2$ inteiro, $(\mathbb{Z}_m, +, \cdot)$ é um anel com unidade. Neste caso, a unidade é a classe $\overline{1}$.
- Sendo n um inteiro maior do que 1, o anel $(n\mathbb{Z}, +, \cdot)$ não possui unidade.

Anéis de integridade

Um anel comutativo com unidade A é denominado *anel de integridade* quando

$$\forall x, y \in A,\ x \cdot y = 0 \Rightarrow x = 0 \text{ ou } y = 0.$$

Definição

Dizemos que $x \neq 0$ e $y \neq 0$ em um anel A são *divisores próprios de zero* quando $x \cdot y = 0$.

Observação

De acordo com as definições anteriores, um anel de integridade é um anel comutativo com unidade que não tem divisores próprios do zero.

Exemplos

- No anel dos inteiros $\mathbb{Z}$, se $x, y \in \mathbb{Z}$ são tais que $x \cdot y = 0$, então temos que $x = 0$ ou $y = 0$. Logo, $\mathbb{Z}$ é um anel de integridade.
- Também são anéis de integridade: $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.
- Em $\mathbb{Z}_8$, os elementos $\bar{2}$ e $\bar{4}$ são diferentes de $\bar{0}$, mas $\bar{2} \cdot \bar{4} = \bar{8} = \bar{0}$. Logo, $\bar{2}$ e $\bar{4}$ são divisores próprios do zero em $\mathbb{Z}_8$ e, consequentemente, $\mathbb{Z}_8$ não é anel de integridade.
- Em $A = M_{2\times2}(\mathbb{Z})$ consideremos os elementos $X = \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}$ e $Y = \begin{bmatrix} 0 & 3 \\ 0 & 0 \end{bmatrix}$. X e Y não são matrizes nulas, no entanto $X \cdot Y = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Logo, X e Y são divisores próprios do zero e A não é anel de integridade.

1.7 Corpos

Um anel comutativo com unidade K é denominado um *corpo* se todo elemento não nulo de K possuir inverso multiplicativo, ou seja,

$$\forall x \in K, x \neq 0 \Rightarrow \exists x^{-1} \in K \text{ tal que } x \cdot x^{-1} = 1.$$

Exemplos

- Os anéis $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são exemplos de corpos (com as operações de adição e multiplicação usuais).
- $\mathbb{Z}$ não é um corpo, porque nem todo elemento de $\mathbb{Z}$ possui inverso multiplicativo. Por exemplo, $2 \in \mathbb{Z}$ e não existe $y \in \mathbb{Z}$ tal que $2 \cdot y = 1$.
- Se p for um inteiro primo positivo, então $\mathbb{Z}_p$ é um corpo.

Proposição

Todo corpo é um anel de integridade.

Observação

A recíproca da proposição anterior não é válida, ou seja, nem todo anel de integridade é um corpo. O exemplo mais conhecido dessa situação é o anel dos inteiros $\mathbb{Z}$.

Proposição

Todo anel de integridade finito é um corpo.

1.8 Homomorfismos de anéis

Uma função $f : A \longrightarrow B$ de um anel A em um anel B é denominada **homomorfismo de anéis** quando forem verificadas as duas seguintes propriedades:

- $\forall x, y \in A$, $f(x + y) = f(x) + f(y)$;
- $\forall x, y \in A$, $f(x \cdot y) = f(x) \cdot f(y)$

Exemplo

Sejam $A = \mathbb{R}$, $B = \mathbb{R} \times \mathbb{R}$ e a função $f : A \longrightarrow B$, $f(x) = (0, x)$.

- Se $x, y \in \mathbb{R}$, então $f(x + y) = (0, x + y) = (0, x) + (0, y) = f(x) + f(y)$
- Temos também: $f(x \cdot y) = (0, x \cdot y) = (0, x) \cdot (0, y) = f(x) \cdot f(y)$.

Logo, f é um homomorfismo do anel A no anel B.

Homomorfismos de anéis

O **núcleo** de um homomorfismo $f : A \longrightarrow B$, denotado por $N(f)$ ou por $\ker(f)$, é definido como sendo o conjunto de todos os elementos de A cuja imagem pela f é igual ao zero do anel B:

$$N(f) = \{x \in A \mid f(x) = 0_B\}$$

Exemplo

Com relação ao exemplo anterior, vamos determinar o seu núcleo. Suponhamos $a \in N(f)$. Então pela definição de núcleo, f(a) = (0, 0) = zero do anel B. Como $f(a) = (0, a)$, temos que $(0, a) = (0, 0)$ de onde resulta que $a = 0$. Assim, o núcleo de f é o conjunto $N(f) = \{0\}$.

Homomorfismos de anéis

Propriedades

Seja $f : A \longrightarrow B$ um homomorfismo de anéis. São válidas as seguintes propriedades:

- $f(0_A) = 0_B$ onde 0_A representa o zero do anel A e 0_B é o zero de B;
- $f(-x) = -f(x)$, $\forall x \in A$;
- $f(x - y) = f(x) - f(y)$, $\forall x, y \in A$;
- f é uma função injetora se, e somente se, $N(f) = \{0_A\}$;
- Se S é um subanel de A, então $f(S)$ é um subanel de B.
- Se f for uma função sobrejetora e A possuir unidade 1_A, então o mesmo acontece com B e a unidade de B é $1_B = f(1_A)$;
- Se f for sobrejetora, A tiver unidade e x for invertível (com relação à multiplicação), então $f(x)$ também é invertível e $f(x^{-1}) = [f(x)]^{-1}$.

Isomorfismos de anéis

Um **isomorfismo** de um anel A em um anel B é uma função $f : A \longrightarrow B$ que é um homomorfismo e bijetora.

Observações

- Se existir um isomorfismo de anéis $f : A \longrightarrow B$, então $f^{-1} : B \longrightarrow A$ também é um isomorfismo.
- Quando existir um isomorfismo de A em B, então diremos que A e B são *isomorfos* e denotamos isso por $A \simeq B$.
- Se A e B forem anéis isomorfos, então eles têm as mesmas propriedades, a diferença entre eles é basicamente os nomes dos elementos.

Ideais

Em um anel comutativo A, um subconjunto não vazio $I \subset A$ é um **ideal** em A quando ele satisfizer às seguintes propriedades:

- $x - y \in I$, $\forall x, y \in I$;
- $a \cdot x \in I$, $\forall x \in I$ e $\forall a \in A$

Exemplo

- Sejam $A = \mathbb{Z}$ e $I = 2\mathbb{Z}$ = conjunto dos inteiros pares.
  - É claro que $I \neq \emptyset$, porque $0 \in I$;
  - Se $x, y \in I$, então $x = 2m$ e $y = 2n$ com $m, n \in \mathbb{Z}$. Daí, temos que $x - y = 2m - 2n = 2(m - n) \in I$;
  - Se $a \in A$, então $a \cdot x = a \cdot (2m) = 2(a \cdot m) \in I$.

  Portanto, $2\mathbb{Z}$ é um ideal em $\mathbb{Z}$.
- Em geral, $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ é um ideal em $\mathbb{Z}$, $\forall n \in \mathbb{Z}$.

Ideais

- Sejam A um anel comutativo e $a_1, a_2, \cdots, a_n \in A$, onde $n \geq 1$ é um inteiro. O conjunto formado por todas as combinações do tipo $x_1 \cdot a_1 + x_2 \cdot a_2 + \cdots + x_n \cdot a_n$, com $x_1, x_2, \cdots, x_n \in A$ é um ideal em A que é denominado **ideal gerado** por $a_1, a_2, \cdots, a_n$ e é denotado por $\langle a_1, a_2, \cdots, a_n \rangle$.
- Quando $I = \langle a \rangle = \{x \cdot a \mid x \in A\}$ for um ideal geral por um único elemento a de um anel comutativo A, então I é denominado **ideal principal** gerado por a.

Exemplos

- O conjunto dos números pares é um ideal principal de $\mathbb{Z}$ porque é gerado pelo $2 \in \mathbb{Z}$.
- Em geral, $I = n\mathbb{Z}$ é um ideal principal de $\mathbb{Z}$ e $I = \langle n \rangle$.

1.9 Anéis-quocientes

Seja I um ideal em um anel comutativo A. O **anel quociente** de A por I é o conjunto

$$A/I = \{x + I \mid x \in A\}$$

com as operações de adição e multiplicação definidas a seguir:

- Adição: $(x + I) + (y + I) = (x + y) + I$, $\forall x, y \in A$
- Multiplicação: $(x + I) \cdot (y + I) = (x \cdot y) + I$, $\forall x, y \in A$

Exemplo

Consideremos o anel $A = \mathbb{Z}$ e o ideal $I = 5\mathbb{Z}$ = múltiplos de 5 (operações de adição e multiplicação usuais). Temos que:

- $0 + I = \{\cdots, -15, -10, -5, 0, 5, 10, 15, \cdots\} = I$
- $1 + I = \{\cdots, -14, -9, -4, 1, 6, 11, 16, \cdots\}$
- $2 + I = \{\cdots, -13, -8, -3, 2, 7, 12, 17, \cdots\}$
- $3 + I = \{\cdots, -12, -7, -2, 3, 8, 13, 18, \cdots\}$
- $4 + I = \{\cdots, -11, -6, -1, 4, 9, 14, 19, \cdots\}$
- $5 + I = \{\cdots, -10, -5, 0, 5, 10, 15, 20, \cdots\} = I$

Portanto, o anel-quociente de A por I é

$$A/I = \{I, 1 + I, 2 + I, 3 + I, 4 + I\}.$$

- Sendo $A/I = \{I, 1 + I, 2 + I, 3 + I, 4 + I\}$, alguns exemplos de adição entre seus elementos são $(2+I)+(1+I) = (2+1)+I = 3+I$ e $(2+I)+(4+I) = (2+4)+I = 6 + I = 1 + I$.
- Todas as possíveis adições entre seus elementos podem ser observadas na seguinte tábua:

$+$	I	$1 + I$	$2 + I$	$3 + I$	$4 + I$
I	I	$1 + I$	$2 + I$	$3 + I$	$4 + I$
$1 + I$	$1 + I$	$2 + I$	$3 + I$	$4 + I$	I
$2 + I$	$2 + I$	$3 + I$	$4 + I$	I	$1 + I$
$3 + I$	$3 + I$	$4 + I$	I	$1 + I$	$2 + I$
$4 + I$	$4 + I$	I	$1 + I$	$2 + I$	$3 + I$

- Sendo $A/I = \{I, 1+I, 2+I, 3+I, 4+I\}$, alguns exemplos de multiplicação entre seus elementos são $(2 + I) \cdot I = (2 + I) \cdot (0 + I) = (2 \cdot 0) + I = 0 + I = I$ e $(2 + I) \cdot (4 + I) = (2 \cdot 4) + I = 8 + I = 3 + I$.
- Todas as possíveis multiplicações entre seus elementos podem ser observadas na seguinte tábua:

$\cdot$	I	$1 + I$	$2 + I$	$3 + I$	$4 + I$
I	I	I	I	I	I
$1 + I$	I	$1 + I$	$2 + I$	$3 + I$	$4 + I$
$2 + I$	I	$2 + I$	$4 + I$	$1 + I$	$3 + I$
$3 + I$	I	$3 + I$	$1 + I$	$4 + I$	$2 + I$
$4 + I$	I	$4 + I$	$3 + I$	$2 + I$	$1 + I$

Observações e teoremas

Observação 1

Um ideal em um anel A é um tipo particular de subanel de A, mas nem todo subanel é um ideal.

Observação 2

Todo anel possui pelo menos dois ideais: o próprio anel e o conjunto unitário formado só pelo zero; esses são chamados os **ideais triviais** do anel. Em um corpo K, seus únicos ideais são os triviais: $\{0\}$ e K.

Teorema 1

O núcleo $N(f)$ de um homomorfismo de anéis $f : A \longrightarrow B$ é um ideal em A.

Teorema 2

Se $f : A \longrightarrow B$ é uma função sobrejetora que também é um homomorfismo de anéis, então $A/N(f)$ e B são anéis isomorfos.

1.10 Polinômios

Seja A um anel. Uma *sequência de elementos em A* é uma função $f : \mathbb{N} \longrightarrow A$. que costuma ser representada na forma $f = (a_0, a_1, a_2, \cdots)$, ou de forma mais simplificada $f = (a_i)$.

Nesse formato, estamos representando $f(k)$ por a_k, para todo $k \in \mathbb{N}$. O elemento $a_k \in A$ é denominado o *k-ésimo termo* da sequência.

Exemplos

- $f = (-3, 0, 1, \pi, 5, 6, -10, \sqrt{3}, \sqrt{3}, 5, \cdots)$ é uma sequência de elementos em $\mathbb{R}$
- $g = (\bar{1}, \bar{2}, \bar{3}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{0}, \bar{0}, \cdots, \bar{0}, \bar{0}, \cdots)$ é uma sequência de elementos em $\mathbb{Z}_5$.

Definição

Consideremos duas sequências $f = (a_i)$ e $g = (b_i)$.

- **Igualdade:** Dizemos que $f = g$ quando $a_i = b_i$ para todo $i \in \mathbb{N}$.
- **Adição:** A *soma* de f com g é uma sequência $h = (c_i)$ tal que $c_i = a_i + b_i$ para todo $i \in \mathbb{N}$.

- **Multiplicação:** O *produto* de f por g é uma sequência $j = (d_i)$ tal que $d_i = \sum_{k=0}^{i} a_{i-k}b_k$ para todo $i \in \mathbb{N}$.

Observação

O produto das sequências $f = (a_i)$ e $g = (b_i)$ é uma sequência $h = (d_i)$ cujos termos são: $d_0 = a_0b_0$, $d_1 = a_1b_0 + a_0b_1$, $d_2 = a_2b_0 + a_1b_1 + a_0b_2$, $d_3 = a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3$, $\cdots$

$$d_k = a_kb_0 + a_{k-1}b_1 + a_{k-2}b_2 + \cdots + a_0b_k$$

Definição

Em um anel A, uma sequência $(a_1, a_2, a_3, \cdots)$ com $a_i \in A$ para todo $i \in \mathbb{N}$ é denominada **polinômio sobre** A quando existir um índice $s \in \mathbb{N}$ tal que $a_k = 0$ para todo $k > s$. O conjunto de todos os polinômios com coeficientes no anel A é denotado por $A[x]$.

Observação

Uma sequência que é um polinômio tem todos os seus termos nulos a partir de certa ordem. Por isso, um polinômio também é denominado **sequência quase-nula**. Os termos de um polinômio também são chamados de **coeficientes**.

Exemplo

$f = (5, 6, 9, -3, 0, 0, \cdots, 0, \cdots)$, onde $a_k = 0$ se $k > 3$ é um polinômio sobre o anel $\mathbb{Z}$.

1.11 Grau de um polinômio

Consideremos $f = (a_i)$ um polinômio não nulo. O **grau de** f é o maior índice dos termos não nulos de f, ou seja, é definido como sendo igual a n se $a_n \neq 0$ e $a_k = 0$ para todo $k > n$. Neste caso, o termo a_n é denominado **coeficiente dominante de** f. O polinômio nulo $o = (0, 0, 0, \cdots, 0, \cdots)$ não tem grau definido.
Notação: O grau de um polinômio f é denotado por ∂f ou por $gr(f)$.

Exemplos

- O termo não nulo de $p = (5, -2, 1, 8, 0, 0, \cdots, 0, \cdots) \in \mathbb{Z}[x]$ que tem o maior índice é o $a_3 = 8$; logo, o grau de p é 3, ou seja, $\partial p = 3$.

- O termo não nulo de $q = (\bar{2}, \bar{0}, \bar{0}, \bar{3}, \bar{1}, \bar{0}, \bar{0}, \cdots, \bar{0}, \cdots) \in \mathbb{Z}_5[x]$ que tem o maior índice é o $a_4 = \bar{1}$; logo, $\partial q = 4$.
- Em um anel A, se $a \in A$, então o polinômio do tipo $c = (a, 0, 0, 0, \cdots, 0, \cdots)$ é um polinômio de grau 0 e é denominado *polinômio constante* em $A[x]$.

1.12 Notação usual

Seja A um anel com unidade. O polinômio

$$x = (0, 1, 0, 0, \cdots, 0, \cdots)$$

é denominado **indeterminada** sobre A.

Usando a definição de produto de polinômios, temos:

- $x^2 = x \cdot x = (0, 0, 1, 0, 0, 0, \cdots, 0, \cdots)$
- $x^3 = x^2 \cdot x = (0, 0, 0, 1, 0, 0, \cdots, 0, \cdots)$
- $x^4 = x^3 \cdot x = (0, 0, 0, 0, 1, 0, \cdots, 0, \cdots)$, etc.

Dado um polinômio qualquer $f = (a_0, a_1, a_2, \cdots, a_n, 0, 0, \cdots)$ de $A[x]$ temos que $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$. Essa notação é considerada a usual para indicar um polinômio f.

Exemplos

- O polinômio $p = (-3, \sqrt{2}, 3, 4, -5, 1, 0, 0, 0, \cdots, 0, \cdots) \in \mathbb{R}[x]$ é denotado na forma usual por $p = -3 + \sqrt{2}x + 3x^2 + 4x^3 - 5x^4 + x^6$ ou por $p(x) = -3 + \sqrt{2}x + 3x^2 + 4x^3 - 5x^4 + x^6$;
- O polinômio $q = (4, 5, -3, 2, 7, 0, 0, 0, \cdots, 0, \cdots) \in \mathbb{Z}[x]$ é denotado na forma usual por $q = 4 + 5x - 3x^2 + 2x^3 + 7x^4$ ou por $q(x) = 4 + 5x - 3x^2 + 2x^3 + 7x^4$;
- O polinômio $q = (\bar{2}, \bar{3}, \bar{0}, \bar{0}, \bar{1}, \bar{7}, \bar{0}, \bar{0}, \bar{0}, \cdots, \bar{0}, \cdots) \in \mathbb{Z}_8[x]$ é denotado na forma usual por $f = \bar{2} + \bar{3}x + x^4 + \bar{7}x^5$ ou por $f(x) = \bar{2} + \bar{3}x + x^4 + \bar{7}x^5$.

Os graus dos polinômios $p(x)$, $q(x)$ e $f(x)$ anteriores são: $\partial p = 6$, $\partial q = 4$ e $\partial f = 5$.

Proposições básicas

- A soma e o produto de dois polinômios de $A[x]$ dá como resultado um polinômio de $A[x]$.
- Se A for um anel, então $A[x]$ também é.
- Se A for um anel comutativo, então $A[x]$ também é.
- Se A for um anel com unidade, então $A[x]$ também é.
- Se A for um anel de integridade, então $A[x]$ também é.
- Em geral, $A[x]$ não é um corpo (mesmo que A seja um corpo).
- Se $p = \partial f$ e $q = \partial g$, então $\partial(f + g) = \max(p, q)$ e $\partial(f \cdot g) \leq p + q$. Se A for um anel de integridade ou um corpo, então $\partial(f \cdot g) = p + q$.
- Todo anel A é isomorfo ao subanel de $A[x]$ formado por todos os polinômios constantes.

Divisão de polinômios

Sendo A um anel comutativo com unidade, dados dois polinômios f e g em $A[x]$, dizemos que f *divide* g quando existir $h \in A[x]$ tal que $g = f \cdot h$.
Notação: Denotamos *"f divide g"* por $f \mid g$ e *"f não divide g"* por $f \nmid g$.

Observação

f *divide* g é considerado o mesmo que: f *é divisor de* g ou g *é divisível por* f ou g *é múltiplo de* f.

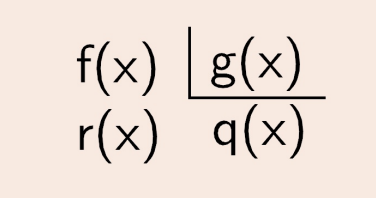
Exemplo

Sejam $f(x) = x - 2$ e $g(x) = x^2 - 5x + 6 = (x - 2) \cdot (x - 3)$. Considerando $h(x) = x - 3$, temos que $g(x) = f(x) \cdot h(x)$ e daí concluímos que $f(x) \mid g(x)$.

Teorema (Algoritmo da Divisão)

Seja K um corpo. Dados dois polinômios $f, g \in K[x]$, existe um único $q \in K[x]$ (denominado **quociente**) e um único $r \in K[x]$ (denominado **resto**) tais que

$$f = g \cdot q + r \text{ e } r = 0 \text{ ou } \partial r < \partial g.$$



Exemplo

Dividir $f(x) = 6x^4 + 5x^3 - 10x^2 + 7x - 8$ por $g(x) = x^2 - 2x + 1$.

Dividindo $6x^4$ por x^2 obtemos $6x^2$. Multiplicamos $6x^2$ por $g(x)$ e subtraimos o produto de $f(x)$. Repetimos esse procedimento até obtermos um polinômio de grau menor do que o grau de $g(x)$.

$$\begin{array}{rl} 6x^4 + 5x^3 - 10x^2 + 7x - 8 & \big| \; x^2 - 2x + 1 \\ \underline{-6x^4 + 12x^3 - 6x^2} & \\ 17x^3 - 16x^2 + 7x & \\ \underline{-17x^3 + 34x^2 - 17x} & \\ 18x^2 - 10x - 8 & \\ \underline{-18x^2 + 36x - 18} & \\ 26x - 26 & \end{array} \qquad 6x^2 + 17x + 18$$

Obtivemos quociente $q(x) = 6x^2 + 17x + 18$ e resto $r(x) = 26x - 26$. Observe que $f(x) = g(x) \cdot q(x) + r(x)$.

Raízes de polinômios

Sejam A um anel comutativo com unidade, $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ e $s \in A$.

- O *valor de f em s*, denotado por $f(s)$, é o seguinte elemento de A: $f(s) = a_0 + a_1 \cdot s + a_2 \cdot s^2 + \cdots + a_n \cdot s^n$.
- Quando $f(s) = 0$, dizemos que s é uma *raiz* do polinômio f.

Exemplo

Sejam $f(x) = 4 + x^2 - x^3$, $r = 2$ e $s = 3$. Temos:

- $f(r) = f(2) = 4 + 2^2 - 2^3 = 0$
- $f(s) = f(3) = 4 + 3^2 - 3^3 = -14$

Portanto, r é uma raiz do polinômio $f(x)$, mas s não é.

Proposição

Sejam A um anel comutativo com unidade, $f \in A[x]$ e $g = x - s \in A[x]$.

- O resto da divisão de f por g é igual a $f(s)$;
- f é divisível por g se, e somente se, $f(s) = 0$ (ou seja, s é raiz de $f(x)$).

Exemplos

- Em $\mathbb{Z}[x]$, dados $f = x^2 + 5x + 3$ e $g = x - 4$, então o resto da divisão de f por g é $f(4) = 4^2 + 5 \cdot 4 + 3 = 39$.
- Consideremos $f(x) = x^3 - 8$ e $g(x) = x - 2$. O resto da divisão de $f(x)$ por $g(x)$ é igual a $f(2) = 2^3 - 8 = 0$. Isso significa que a divisão é exata e que 2 é raiz de $f(x)$

Raízes racionais

Seja $a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0 = 0$ uma equação polinomial de coeficientes inteiros. Se $\frac{p}{q}$ for uma raiz racional dessa equação com $p, q \in \mathbb{Z}$, então p é um divisor de a_0 e q é um divisor de a_n.

Exemplo

Consideremos a equação $12x^6 - x^5 + 23x^4 - 2x^3 + 58x^2 - 5x - 5 = 0$.

- Os divisores do termo independente de x são ± 1 e ± 5.
- Os divisores do coeficiente do termo de maior grau são ± 1, ± 2 ± 3, $\pm 4, \pm 6$ e ± 12.
- Logo, as possíveis raízes racionais da equação são: ± 1, $\pm\frac{1}{2}$, $\pm\frac{1}{3}$, $\pm\frac{1}{4}$, $\pm\frac{1}{6}$, $\pm\frac{1}{12}$, ± 5, $\pm\frac{5}{2}$, $\pm\frac{5}{3}$, $\pm\frac{5}{4}$, $\pm\frac{5}{6}$ e $\pm\frac{5}{12}$.
- Substituindo na equação, verificamos que somente $\frac{1}{3}$ e $-\frac{1}{4}$ são raízes.

Exemplo

Determine todas as raízes da equação

$$f(x) = 2x^4 + 5x^3 - 17x^2 - 35x + 21 = 0.$$

Solução

- Os divisores de 21 são: ± 1, ± 3, ± 7 e ± 21
- Os divisores de 2 são: ± 1 e ± 2
- Dividindo-se os divisores de 21 pelos divisores de 2, obtemos as possíveis raízes racionais da equação dada: ± 1, ± 3, ± 7, ± 21, $\pm\frac{1}{2}$, $\pm\frac{3}{2}$, $\pm\frac{7}{2}$ e $\pm\frac{21}{2}$
- Por substituição direta, temos que somente $\frac{1}{2}$ e -3 são raízes
- Daí, temos que $f(x)$ é divisível por $2(x - \frac{1}{2})(x - (-3)) = 2x^2 + 5x - 3$.
- Efetuando-se a divisão de

$$f(x) = 2x^4 + 5x^3 - 17x^2 - 35x + 21$$

por

$$g(x) = 2x^2 + 5x - 3,$$

obtemos quociente igual a $(x^2 - 7)$ e resto igual a zero.

- As raízes de $x^2 - 7$ são $\pm\sqrt{7}$
- Concluímos, então, que todas as raízes da equação dada são $\pm\sqrt{7}$, $\frac{1}{2}$ e -3, ou seja, seu conjunto-solução é:

$$S = \{-\sqrt{7},\ \sqrt{7}, \frac{1}{2}, -3\}$$

1.13 Polinômios irredutíveis

Seja K um corpo e $p \in K[x]$. Dizemos que o polinômio p é *irredutível* em $K[x]$ (ou *irredutível sobre* K) quando p não é um polinômio constante e, se existirem $f, g \in K[x]$ tais que $p = f \cdot g$, então f é constante ou g é constante. Um polinômio que não é irredutível sobre K é denominado *redutível* sobre K.

Observação

Os polinômios redutíveis sobre K são aqueles polinômios que podem ser fatorados, ou seja, escritos como produto de dois polinômios não constantes de $K[x]$.

Exemplos

- Todo polinômio de grau 1 é irredutível em $\mathbb{R}[x]$.

- $f = x^2 - 9$ é redutível em $\mathbb{R}[x]$ porque é possível escrevê-lo como produto de dois polinômios não constantes: $f = (x+3)(x-3)$. Note que essa fatoração não é única pois temos também $f = (2x + 6)(\frac{1}{2}x - \frac{3}{2})$, entre outras possibilidades.
- Se K for um corpo e $f(x) \in K[x]$ com $\partial f \geq 2$ possuir uma raiz $r \in K$, então $f(x)$ é redutível sobre K porque pode ser escrito na forma $(x - r)g(x)$ onde $g(x) \in K[x]$ e $\partial g \geq 1$.
- $f(x) = x^2 - 5$ é irredutível sobre $\mathbb{Q}$ mas é redutível sobre $\mathbb{R}$ porque $f(x) = \underbrace{(x - \sqrt{5})}_{\in \mathbb{R}[x]} \cdot \underbrace{(x + \sqrt{5})}_{\in \mathbb{R}[x]}$.

Teorema (Critério de Eisenstein)

Seja $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$ um polinômio de coeficientes inteiros. Se existir um inteiro primo p tal que

- $p \mid a_0$, $p \mid a_1$, $p \mid a_2$, $\cdots$, $p \mid a_{n-1}$
- $p \nmid a_n$
- $p^2 \nmid a_0$

então $f(x)$ é irredutível sobre $\mathbb{Z}$.

Exemplo

Seja $f(x) = 7x^5 + 110x^4 - 22x^3 + 44x^2 - 11x + 66$. Considerando o primo $p = 11$ temos que $p \mid 66$, $p \mid (-11)$, $p \mid 44$, $p \mid (-22)$, $p \mid 110$, $p \nmid 7$ e $p^2 \nmid 66$. Logo, $f(x)$ é irredutível sobre $\mathbb{Z}$, ou seja, $f(x)$ não pode ser fatorado como produto de dois polinômios não constantes de coeficientes inteiros.

Capítulo 2

Operações binárias

A1) Considere a operação $\boxdot$ definida sobre o conjunto $A = \{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}$ cuja tábua está mostrada a seguir:

$\boxdot$	$\heartsuit$	$\spadesuit$	$\diamondsuit$	$\clubsuit$
$\heartsuit$	$\diamondsuit$	$\clubsuit$	$\heartsuit$	$\spadesuit$
$\spadesuit$	$\clubsuit$	$\heartsuit$	$\spadesuit$	$\diamondsuit$
$\diamondsuit$	$\heartsuit$	$\spadesuit$	$\diamondsuit$	$\clubsuit$
$\clubsuit$	$\spadesuit$	$\diamondsuit$	$\clubsuit$	$\heartsuit$

Verifique:

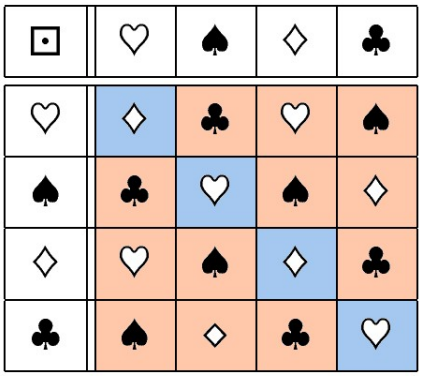
a) se $\boxdot$ tem elemento neutro;

b) se $\boxdot$ é comutativa;

c) quais são os elementos de A que são invertíveis.

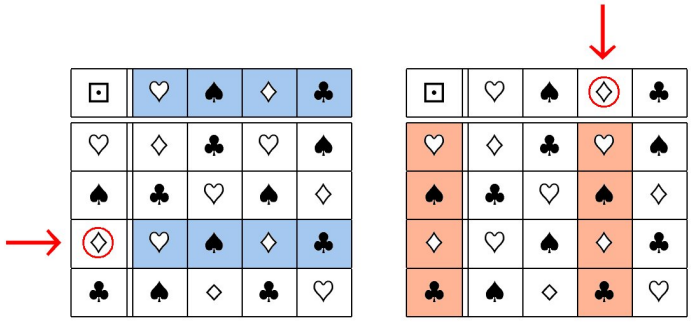
Solução:

a) Primeiramente, vamos verificar se a operação $\boxdot$ é comutativa. Para isso, verificamos que a parte da tábua que está acima da diagonal que vai do canto superior esquerdo ao inferior direito é simétrica com relação à parte que está abaixo da diagonal.



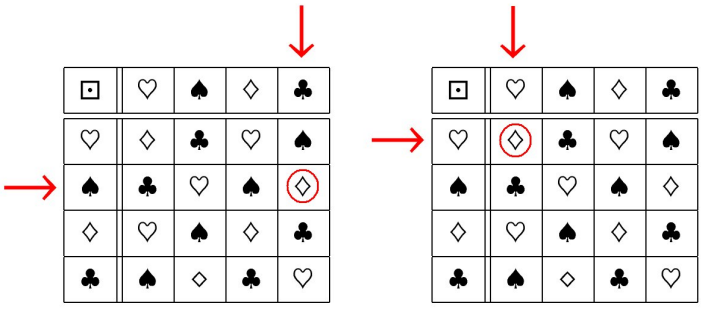
Como há uma simetria entre a parte que está acima e a que está abaixo da diagonal, concluímos que a operação é comutativa: $\heartsuit \boxdot \diamondsuit = \diamondsuit \boxdot \heartsuit$, $\spadesuit \boxdot \heartsuit = \heartsuit \boxdot \spadesuit$, $\clubsuit \boxdot \diamondsuit = \diamondsuit \boxdot \clubsuit$, etc.

b) Agora, vamos verificar se a operação tem elemento neutro. Observamos a primeira linha da tábua (o cabeçalho) e verificamos se ela se repete em algum lugar. Ela se repete na linha do elemento $\diamondsuit$. Isso signifca que: $\diamondsuit \boxdot \heartsuit = \heartsuit$, $\diamondsuit \boxdot \spadesuit = \spadesuit$, $\diamondsuit \boxdot \diamondsuit = \diamondsuit$ e $\diamondsuit \boxdot \clubsuit = \clubsuit$. Logo, $\diamondsuit$ é um elemento neutro à esquerda para a operação $\boxdot$.



Observamos novamente a tábua para ver se a primeira coluna se repete em algum lugar. Verificamos que ela se repete no elemento $\diamondsuit$. Isso significa que $\diamondsuit$ é um elemento neutro à direita. Portanto, $\diamondsuit$ é o elemento neutro da operação $\boxdot$.

c) Como $\diamondsuit$ é o elemento neutro da operação, verificamos na tábua quais são os pares de elementos (x, y) tais que $x \boxdot y = \diamondsuit$.



Temos os seguintes resultados: $\spadesuit \boxdot \clubsuit = \diamondsuit$, $\heartsuit \boxdot \heartsuit = \diamondsuit$ e $\diamondsuit \boxdot \diamondsuit = \diamondsuit$. Isso significa que $\spadesuit^{-1} = \clubsuit$, $\clubsuit^{-1} = \spadesuit$, $\heartsuit^{-1} = \heartsuit$ e $\diamondsuit^{-1} = \diamondsuit$, ou seja, todos os elementos de A são invertíveis.

A2) Considere a operação $\star$ (*"estrela"*) definida sobre o conjunto $B = \{1, 2, 3, 4, 5\}$ cuja tábua está mostrada a seguir:

$\star$	1	2	3	4	5
1	1	1	1	1	1
2	1	2	2	2	2
3	1	2	3	3	3
4	1	2	3	4	4
5	1	2	3	4	5

Verifique se $\star$ tem elemento neutro, se é comutativa e quais são os elementos de B que são invertíveis.

Solução:

- A primeira linha da tabela se repete na última linha, a linha que corresponde ao elemento 5. Note que a primeira coluna se repete também na coluna que corresponde ao elemento 5. Isso significa que o $e = 5$ é o único elemento neutro dessa operação.
- A tabela é simétrica com relação à diagonal que inicia na parte superior esquerda e termina na parte inferior direita. Logo, a operação é comutativa.
- O elemento neutro e aparece na tábua apenas uma única vez, como resultado da operação $5 \star 5 = 5 = e$. Isso significa que o 5 é o único elemento invertível e o inverso do 5 é igual a ele mesmo.

A3) Sejam $A = \{0, 1, 2, 3, 4\} \subset \mathbb{N}$ e as operações $\oplus$ e $\odot$ definidas por

- $x \odot y$ = resto da divisão de xy por 5;
- $x \oplus y$ = resto da divisão de $x + y$ por 5.

Construa a tábua dessas duas operações sobre o conjunto A.

Solução: Alguns exemplos:

- $3 \odot 4$ = resto da divisão de 12 por 5 = 2,

- $2 \odot 3$ = resto da divisão de 6 por 5 = 1,
- $4 \oplus 3$ = resto da divisão de 7 por 5 = 2, etc.

Prosseguindo dessa forma, obtemos as seguintes tabelas:

$\odot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

A4) Seja $X = \{1, 2, 3\}$ e $\mathcal{F}$ o conjunto de todas as funções $f : X \longrightarrow X$ que são constantes. Construa a tábua da operação de composição de funções definida em $\mathcal{F}$ e verifique se tem elemento neutro.

Solução: Como X só tem 3 elementos, então só podem existir 3 funções constantes definidas de X em X:

- $f_1 : X \longrightarrow X$, $f_1(x) = 1$;
- $f_2 : X \longrightarrow X$, $f_2(x) = 2$;
- $f_3 : X \longrightarrow X$, $f_3(x) = 3$;

Agora, observe que $(f_1 \circ f_2)(x) = f_1(f_2(x)) = f_1(2) = 1 = f_1(x)$; logo, $f_1 \circ f_2 = f_1$. De modo análogo, obtemos: $f_1 \circ f_3 = f_1$, $f_2 \circ f_3 = f_2$, etc. Resumimos tudo isso na seguinte tabela:

$\circ$	f_1	f_2	f_3
f_1	f_1	f_1	f_1
f_2	f_2	f_2	f_2
f_3	f_3	f_3	f_3

Observando a tábua, vemos que a primeira linha da tábua (o cabeçalho) não se repete em lugar algum; logo, a operação **não tem elemento neutro à esquerda.** Por outro lado, note que a primeira coluna se repete 3 vezes na tábua; isso significa que **a operação tem 3 elementos neutros à direita:** f_1, f_2 e f_3. Concluímos então que a operação não tem elemento neutro.

A5) Considere a seguinte operação $*$ definida sobre o conjunto dos números racionais:

$$x * y = \frac{x + y}{2}.$$

Verifique se $*$ é comutativa, se é associativa, se tem elemento neutro e se existem elementos invertíveis.

Solução:

- Para quaisquer $x, y \in \mathbb{Q}$, temos $x * y = \frac{x+y}{2} = \frac{y+x}{2} = y * x$, logo, a operação é comutativa.
- $1 * (2 * 3) = 1 * \frac{2+3}{2} = 1 * \frac{5}{2} = \frac{1+\frac{5}{2}}{2} = \frac{7}{4}$ e $(1 * 2) * 3 = \frac{1+2}{2} * 3 = \frac{3}{2} * 3 = \frac{\frac{3}{2}+3}{2} = \frac{9}{4}$; logo, $1 * (2 * 3) \neq (1 * 2) * 3$ e daí concluímos que a operação não é associativa.
- Suponhamos que e seja o elemento neutro dessa operação. Então, por exemplo, $e * 0 = 0$ e $e * 1 = 1 \Rightarrow \frac{e+0}{2} = 0$ e $\frac{e+1}{2} = 1$, ou seja, $e = 0$ e $e = 1$, o que é impossível. Logo, a operação não tem elemento neutro.
- Se a operação não tem elemento neutro, então não faz sentido a definição de elemento invertível.

A6) Considere a seguinte operação $\oplus$ definida sobre o conjunto dos números reais não negativos:

$$x \oplus y = \sqrt{x^2 + y^2}.$$

Verifique se $\oplus$ é comutativa, se é associativa, se tem elemento neutro e se existem elementos invertíveis.

Solução:

- Para quaisquer $x, y \in \mathbb{R}_+$ temos $x \oplus y = \sqrt{x^2 + y^2} = \sqrt{y^2 + x^2} = y \oplus x$. Logo, a operação é comutativa.
- Para quaisquer $x, y, z \in \mathbb{R}_+$ temos $x \oplus (y \oplus z) = x \oplus \sqrt{y^2 + z^2} = \sqrt{x^2 + \left(\sqrt{y^2 + z^2}\right)^2} = \sqrt{x^2 + y^2 + z^2}$ e $(x \oplus y) \oplus z = \sqrt{x^2 + y^2} \oplus z = \sqrt{\left(\sqrt{x^2 + y^2}\right)^2 + z^2} = \sqrt{x^2 + y^2 + z^2}$. Logo, $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ o que significa que $\oplus$ é associativa.
- Supondo que e seja o elemento neutro, temos $e \oplus x = x$, ou seja, $\sqrt{e^2 + x^2} = x$ para todo x real não negativo. Elevando a última igualdade ao quadrado, obtemos: $e^2 + x^2 = x^2$ e, daí, chegamos a $e^2 = 0$, ou seja, $e = 0$. Assim, o zero é o elemento neutro da operação. Vejamos: $x \oplus 0 = \sqrt{x^2 + 0^2} = \sqrt{x^2} = x$ para todo x real não negativo.
- Dado um real não negativo a, seu inverso (simétrico) é o real não negativo b tal que $a \oplus b = 0 =$ elemento neutro. Daí, obtemos que $\sqrt{a^2 + b^2} = 0$ o que implica

$a^2 + b^2 = 0$. A única possibilidade para a última equação é $a = 0$ e $b = 0$. Assim, o único elemento invertível é o zero e o inverso é ele mesmo.

A7) Considere a seguinte operação $*$ definida sobre o conjunto dos números reais:

$$x * y = 2^{x \cdot y}.$$

Verifique se $*$ é comutativa, se é associativa e se tem elemento neutro.

Solução:

- Para quaisquer $x, y \in \mathbb{R}$, temos $x * y = 2^{x \cdot y} = 2^{y \cdot x} = y * x$. Logo, $*$ é comutativa.
- $0*(1*2) = 2^{0 \cdot (1*2)} = 2^0 = 1$ e $(0*1)*2 = 2^{0 \cdot 1} * 2 = 2^0 * 2 = 1*2 = 2^{1 \cdot 2} = 2^2 = 4$. Logo, $0 * (1 * 2) \neq (0 * 1) * 2$ o que significa que $*$ não é associativa.
- Suponhamos que exista um elemento neutro e para essa operação. Então, devemos ter $e * x = x$ para todo $x \in \mathbb{R}$. Daí, temos $2^{ex} = x$. Escolhendo dois valores distintos para x, por exemplo, $x = 1$ e $x = 2$, substituindo na equação anterior, obtemos: $2^e = 1$ e $2^{2e} = 2$ que implicam em $e = 0$ e $2e = 1$ que é um absurdo. Logo, não existe elemento neutro para essa operação.

A8) Sendo $a, b \in \mathbb{R}$, mostre com detalhes que $(a + b)^2 = a^2 + 2ab + b^2$ identificando todas as propriedades da adição ou multiplicação utilizadas. O quadrado de x, denotado por x^2 é definido como sendo igual a $x \cdot x$.

Solução:

- $(a + b)^2 = (a + b) \cdot (a + b)$ *(definição de quadrado)*
- $(a+b)\cdot\underbrace{(a + b)}_{z} = a\underbrace{(a + b)}_{z} + b\underbrace{(a + b)}_{z}$ *(distributividade à direita da multiplicação com relação à adição)*
- $a(a + b) + b(a + b) = (a \cdot a + a \cdot b) + (b \cdot a + b \cdot b)$ *(distributividade à esquerda da multiplicação com relação à adição)*
- $(a \cdot a + a \cdot b) + (b \cdot a + b \cdot b) = (a^2 + a \cdot b) + (a \cdot b + b^2)$ *(definição de quadrado e comutatividade da multiplicação)*
- $\underbrace{(a^2 + ab)}_{x} + (ab + b^2) = (\underbrace{(a^2 + ab)}_{x} + ab) + b^2$ *(associatividade da adição)*

- $((a^2 + ab) + ab) + b^2 = (a^2 + (ab + ab)) + b^2$ *(associatividade da adição)*
- $(a^2 + (ab + ab)) + b^2 = (a^2 + 2ab) + b^2$
- $(a^2 + 2ab) + b^2 = a^2 + 2ab + b^2$ *(associatividade da adição)*

Observação. O objetivo deste exercício é mostrar que várias propriedades da adição e da multiplicação estão "escondidas" em uma fórmula tão conhecida como essa do quadrado da soma. É essencial, por exemplo, a multiplicação ser comutativa para que a fórmula seja válida. Por exemplo, com matrizes quadradas A e B não é válida a fórmula $(A + B)^2 = A^2 + 2AB + B^2$ em geral.

B1) Quantas operações diferentes é possível definir em um conjunto A que tenha exatamente n elementos? Entre essas operações, quantas são comutativas?

Solução: Uma operação fica perfeitamente determinada se conhecermos sua tábua. Se o conjunto $A = \{a_1, a_2, \cdots, a_n\}$ tem n elementos, então definir a operação é atribuir um valor a cada $\bullet$ na seguinte tábua:

$*$	a_1	a_2	$\cdots$	a_n
a_1	$\bullet$	$\bullet$	$\cdots$	$\bullet$
a_2	$\bullet$	$\bullet$	$\cdots$	$\bullet$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n	$\bullet$	$\bullet$	$\cdots$	$\bullet$

Como a quantidade total de $\bullet$ é n^2, e cada uma pode ser preenchida com n opções, então há um total de $\underbrace{n \cdot n \cdot n \ldots n}_{n^2 \text{ fatores}} = n^{(n^2)}$ possíveis operações.

Se a operação for comutativa, então ao preenchermos a diagonal e a parte acima da diagonal, a operação já fica determinada. A parte que está abaixo da diagonal fica determinada por simetria. O total de $\bullet$ que está na diagonal e acima dela é de $1 + 2 + 3 + \cdots + n$, ou seja, $\frac{n(n+1)}{2}$. Como cada $\bullet$ pode ser preenchida com n opções, temos que o total de operações comutativas é de $\underbrace{n \cdot n \cdot n \cdots n}_{\frac{n(n+1)}{2} \text{ fatores}} = n^{\frac{n(n+1)}{2}}$ operações.

Observação. A quantidade de operações é um número gigantesco, mesmo para valores pequenos de n. Por exemplo, quando $n = 4$ há um total de $n^{(n^2)} = 4^{16} = 4294967296$ (mais de 4 bilhões) operações que podem ser definidas; entre elas, um total de $n^{\frac{n(n+1)}{2}} = 4^{10} = 1048576$ (mais de 1 milhão) são comutativas.

B2) Determine $a, b, c \in \mathbb{R}$ para que a operação $*$ sobre $\mathbb{R}$ definida por

$$x * y = ax + by + cxy$$

tenha elemento neutro.

Solução: Suponhamos que o elemento neutro dessa operação seja e. Então, por exemplo, temos que $e * 0 = 0$ e também $0 * e = 0$. Usando a definição de $*$, temos: $ae + b \cdot 0 + ce \cdot 0 = 0$ e $a \cdot 0 + be + ce \cdot 0 = 0$, ou seja, $ae = 0$ e $be = 0$. Como $e * e = e$, devemos ter também que $ae + be + ce^2 = e \Rightarrow ce^2 = e$.

- (1° caso) Suponhamos $e \neq 0$. Então a partir de $ae = 0$ e $be = 0$, obtemos $a = 0$ e $b = 0$. A partir de $ce^2 = e$, obtemos $ce = 1$, ou seja, $c \neq 0$ e $e = \frac{1}{c}$. Assim, neste caso, a operação fica definida como sendo $x * y = cxy$, onde c é qualquer número real não nulo.
- (2° caso) Suponhamos $e = 0$. A partir de 1 * 0 = 1 obtemos a + 0 + 0 = 1 e a partir de 0 * 1 = 1 obtemos 0 + b + 0 = 1. Portanto, devemos ter a = 1 e b = 1. Portanto, $x * y = x + y + cxy$.

Concluímos dessa forma que a operação $*$ tem elemento neutro quando $a = b = 0$ e $c \neq 0$ (neste caso, o elemento neutro é $\frac{1}{c}$) ou quando $a = b = 1$ e $c \in \mathbb{R}$ (neste caso, o elemento neutro é o zero).

B3) Verifique se a operação $*$ sobre $\mathbb{Z} \times \mathbb{Z}$ definida por

$$(a, b) * (c, d) = (ac, ad + bc)$$

é comutativa, se existe elemento neutro e determine todos os elementos invertíveis.

Solução:

- Para quaisquer (a, b) e (c, d) pertencentes a $\mathbb{Z} \times \mathbb{Z}$ temos $(a, b) * (c, d) = (ac, ad + bc) = (ca, cb + da) = (c, d) * (a, b)$, logo, $*$ é comutativa.
- Suponhamos que a operação tenha elemento neutro $e = (e_1, e_2)$. Então, se $x = (a, b)$ for um elemento genérico de $\mathbb{Z} \times \mathbb{Z}$, temos que $e * x = x$, isto é, $(e_1, e_2) * (a, b) = (a, b) \Rightarrow (e_1 a, e_1 b + e_2 a) = (a, b) \Rightarrow e_1 a = a, e_1 b + e_2 a = b$. Em particular, escolhendo $(a, b) = (1, 1)$, temos $e_1 = 1$, $e_1 + e_2 = 1$ o que implica em $e_2 = 0$. Logo, $e = (1, 0)$ é um "candidato" a elemento neutro da operação. Vejamos: $e * x = (1, 0) * (a, b) = (1 \cdot a, 1 \cdot b + 0 \cdot a) = (a, b)$. Logo, $(1, 0)$ é realmente o elemento neutro da operação.
- Dado $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, se (x, y) for o elemento inverso de (a, b), então devemos ter $(a, b) * (x, y) = (1, 0)$ = elemento neutro $\Rightarrow (ax, ay + bx) = (1, 0)$ $\Rightarrow ax = 1, ay + bx = 0$. Como a e x são inteiros, então $ax = 1$ implica $a = 1, x = 1$ ou $a = -1, x = -1$.

- ◦ (1° caso:) Se $a = 1$ e $x = 1$, então $1 \cdot y + b \cdot 1 = 0 \Rightarrow y = -b$. Logo, o inverso de $(1, b)$ é o elemento $(1, -b)$.
- ◦ (2° caso:) Se $a = -1$ e $x = -1$, então $-1 \cdot y + b \cdot (-1) = 0 \Rightarrow y = -b$. Assim, o inverso de $(-1, b)$ é o elemento $(-1, -b)$.

Concluímos dessa forma que os elementos invertíveis são da forma $(1, b)$ ou $(-1, b)$, com $b \in \mathbb{Z}$ e seus inversos são dados por: $(1, b)^{-1} = (1, -b)$ e $(-1, b)^{-1} = (-1, -b)$.

C1) Seja E um conjunto com uma operação $*$ que admite elemento neutro. Mostre que $*$ é comutativa e associativa se, e somente se, $x*(y*z) = (x*z)*y$ para quaisquer $x, y, z \in E$.

Solução: ($\Rightarrow$) Suponhamos $*$ comutativa e associativa. Então para quaisquer $x, y, z \in E$ temos

- $x * (y * z) = x * (z * y)$ *(porque $*$ é comutativa)*
- $x * (z * y) = (x * z) * y$ *(porque $*$ é associativa)*
- Logo, $x * (y * z) = (x * z) * y$.

($\Leftarrow$) Suponhamos $x * (y * z) = (x * z) * y$ para quaisquer $x, y, z \in E$. Em particular, escolhendo $x = e$ = elemento neutro, temos que $e * (y * z) = (e * z) * y$, ou seja, $y * z = z * y$ para quaisquer $y, z \in E$. Isso significa que a operação $*$ é comutativa. Como $x * (\underbrace{y * z}_{z*y}) = (x * z) * y \Rightarrow x * (z * y) = (x * z) * y$ para quaisquer $x, y, z \in E$. Logo, $*$ é associativa.

C2) Uma operação $*$ em um conjunto $E \neq \emptyset$ é denominada *totalmente não associativa* quando

$$(x * y) * z \neq x * (y * z), \ \forall x, y, z \in E.$$

a) Mostre que se $*$ é totalmente não associativa, então $*$ não é comutativa;

b) Mostre que a potenciação $a * b = a^b$ é totalmente não associativa em $E = \{n \in \mathbb{N} \mid n \geq 3\}$.

Solução:

a) Sejam $\alpha \in E$ e $\beta = \alpha * \alpha$. Como $*$ é totalmente não associativa, temos que $(\underbrace{\alpha * \alpha}_{\beta}) * \alpha \neq \alpha * (\underbrace{\alpha * \alpha}_{\beta})$, ou seja, $\beta * \alpha \neq \alpha * \beta$ o que mostra que $*$ não é comutativa.

b) Suponhamos que existissem três inteiros a, b, c maiores ou iguais a 3 tais que $(a * b) * c = a * (b * c)$, ou seja, $(a^b)^c = a^{(b^c)}$ que é equivalente a $a^{(bc)} = a^{(b^c)}$. Daí, obtemos $bc = b^c$. Resta mostrar agora que essa última igualdade é impossível se b e c forem inteiros maiores ou iguais a 3. Consideremos, então, dois casos: $b < c$ e $b \geq c$.

   - Se $b < c$, multiplicando por c, obtemos: $bc < c^2 \Rightarrow b^c < c^2 \Rightarrow 3^c < c^2$ e essa desigualdade é impossível se $c \geq 3$.
   - Se $b \geq c$, então multiplicando por b, obtemos: $b^2 \geq bc \Rightarrow b^2 \geq b^c \Rightarrow 2 \geq c$ que também é impossível.

Capítulo 3

Grupos e subgrupos

A1) Consideremos o conjunto $\mathbb{R}$ com a operação $\oplus$ definida por $x \oplus y = x + y - 5$ para quaisquer $x, y \in \mathbb{R}$. Mostre que $G = (\mathbb{R}, \oplus)$ é um grupo abeliano.

Solução: Inicialmente, vamos mostrar que a operação $\oplus$ é associativa, tem elemento neutro e todo elemento de G tem inverso.

- Para quaisquer $x, y, z \in G$, temos:
  - $x \oplus (y \oplus z) = x \oplus (y + z - 5) = x + (y + z - 5) - 5 = x + y + z - 10$
  - $(x \oplus y) \oplus z = (x + y - 5) \oplus z = (x + y - 5) + z - 5 = x + y + z - 10$

  Logo, $x \oplus (y \oplus z) = (x \oplus y) \oplus z$.

- Suponhamos que $\oplus$ tenha elemento neutro e. Então $e \oplus x = x$ para todo $x \in \mathbb{R}$ o que implica em $e + x - 5 = x$ de onde obtemos $e = 5$. (*Podemos agora comprovar que $e = 5$ é realmente o elemento neutro dessa operação: $e \oplus x = 5 \oplus x = 5 + x - 5 = x$ e $x \oplus e = x + 5 - 5 = x$ para todo $x \in \mathbb{R}$.*)

- Dado $x \in \mathbb{R}$, vamos determinar $y = x^{-1}$. Por definição, temos $x \oplus y = e$, ou seja, $x + y - 5 = 5$. Daí, obtemos que $y = -x + 10$, isto é, $x^{-1} = -x + 10$. (*Comprovando: $x \oplus x^{-1} = x \oplus (-x + 10) = x + (-x + 10) - 5 = 5 = e$ e $x^{-1} \oplus x = (-x + 10) \oplus x = (-x + 10) + x - 5 = 5 = 5$. Logo, $(-x + 10)$ é realmente o inverso de x com relação à operação $\oplus$.*)

Agora, vamos mostrar que $\oplus$ é comutativa:

- $x \oplus y = x + y - 5 = y + x - 5 = y \oplus x$ para quaisquer $x, y \in G$.

Fica mostrado assim que $(G, \oplus)$ é um grupo abeliano.

A2) Consideremos o conjunto $A = \{a + b\sqrt{3} \in \mathbb{R}^* \mid a, b \in \mathbb{Q}\}$.

a) Dê exemplo de elementos desse conjunto;

b) Verifique se ele é fechado com relação à operação de multiplicação usual dos números reais;

c) Verifique se A é um grupo multiplicativo abeliano.

Solução:

a) Todo racional não nulo como $1, -1, \frac{1}{2}, -\frac{3}{7}$ pertencem ao conjunto A. Além desses, qualquer combinação do tipo $a + b\sqrt{3} \neq 0$ com $a, b \in \mathbb{Q}$ como $1 + 2\sqrt{3}$, $-\sqrt{3}$, $5\sqrt{3}$, $-8 - 4\sqrt{3}$, $\frac{1}{3} + \frac{11}{9}\sqrt{3}$ também pertencem a A.

b) Sejam $x = a + b\sqrt{3}$ e $y = c + d\sqrt{3}$ dois elementos de A. Vamos verificar se o produto xy também pertence a A. Usando as diversas propriedades da adição e da multiplicação usuais em $\mathbb{R}$, podemos desenvolver o produto xy da seguinte forma: $xy = (a + b\sqrt{3})(c + d\sqrt{3}) = ac + ad\sqrt{3} + bc\sqrt{3} + bd(\sqrt{3})^2 = (\underbrace{ac + 3bd}_{\in \mathbb{Q}}) + (\underbrace{ad + bc}_{\in \mathbb{Q}})\sqrt{3} \in A$. Logo, A é fechado com relação à multiplicação.

c)
- Como a multiplicação é associativa em $\mathbb{R}$, ou seja, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ para quaisquer $x, y, z \in \mathbb{R}$, temos que, em particular, a multiplicação é associativa em $A \subset \mathbb{R}$, ou seja, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ para quaisquer $x, y, z \in A$.
- O elemento neutro da multiplicação em A é o $1 \in A$.
- Dado $x = a + b\sqrt{3} \in A$ vamos verificar se existe $y \in A$ tal que $x \cdot y = y \cdot x = 1$. Para verificar se $y = \frac{1}{x} = \frac{1}{a+b\sqrt{3}} \in A$, racionalizamos o denominador de y, multiplicando numerador e denominador por $(a - b\sqrt{3})$:

$$y = \frac{1 \cdot (a - b\sqrt{3})}{(a + b\sqrt{3})(a - b\sqrt{3})} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} = \underbrace{\frac{a}{a^2 - 3b^2}}_{\in \mathbb{Q}} + \underbrace{\frac{(-b)}{a^2 - 3b^2}}_{\in \mathbb{Q}}\sqrt{3} \in A.$$

- Como a multiplicação é comutativa em $\mathbb{R}$ então, em particular, também é comutativa em A, ou seja, $x \cdot y = y \cdot x$ para quaisquer $x, y \in A$.

Portanto, fica mostrado assim que $(A, \cdot)$ é um grupo abeliano.

A3) Seja $\mathcal{F} = \{f : \mathbb{R} \longrightarrow \mathbb{R} \mid f(x) = ax + b, a, b \in \mathbb{R}, a \neq 0\}$. Mostre que $\mathcal{F}$ é um grupo não abeliano com relação à composição de funções.

Solução:

- Para quaisquer funções f, g, h de $\mathbb{R}$ em $\mathbb{R}$, temos que $f \circ (g \circ h) = (f \circ g) \circ h$. Logo, em particular, a composição de funções é associativa sobre o conjunto $\mathcal{F}$.
- Quando $a = 1$ e $b = 0$ temos que $f(x) = x \in \mathcal{F}$ é o elemento neutro da composição de funções.
- Dada $f(x) = ax + b$ com $a, b \in \mathbb{R}$ e $a \neq 0$, a função inversa de f é a função $f^{-1} : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f^{-1}(x) = \frac{1}{a}x - \frac{b}{a}$ que é um elemento de $\mathcal{F}$.
- Dadas $f, g \in \mathcal{F}$ definidas por $f(x) = ax + b$ e $g(x) = cx + d$ temos que $(f \circ g)(x) = f(g(x)) = f(cx + d) = a(cx + d) + b = (ac)x + (ad + b)$ e $(g \circ f)(x) = g(f(x)) = g(ax + b) = c(ax + b) + d = (ac)x + (bc + d)$ de onde percebemos que, em geral, $f \circ g \neq g \circ f$. Portanto, a operação $\circ$ não é comutativa sobre $\mathcal{F}$.
  Outra opção seria escolher um contra-exemplo para mostrar que $\circ$ não é comutativa, por exemplo, $f(x) = 2x + 1$ e $g(x) = 3x - 4$ temos $(f \circ g)(x) = 6x - 7$ e $(g \circ f)(x) = 6x - 1$.

A4) Dê exemplo de um grupo G e elementos $x, y \in G$ tais que $(xy)^{-1} \neq x^{-1}y^{-1}$.

Solução: No grupo $G = GL_2(\mathbb{R})$ escolhamos dois elementos como por exemplo $x = \begin{bmatrix} 2 & 1 \\ 3 & 0 \end{bmatrix}$ e $y = \begin{bmatrix} 0 & 1 \\ 5 & 7 \end{bmatrix}$. Então $x^{-1} = \begin{bmatrix} 0 & \frac{1}{3} \\ 1 & -\frac{2}{3} \end{bmatrix}$, $y^{-1} = \begin{bmatrix} -\frac{7}{5} & \frac{1}{5} \\ 1 & 0 \end{bmatrix}$, $x^{-1}y^{-1} = \begin{bmatrix} \frac{1}{3} & 0 \\ -\frac{31}{15} & \frac{1}{5} \end{bmatrix}$, $xy = \begin{bmatrix} 5 & 9 \\ 0 & 3 \end{bmatrix}$, $(xy)^{-1} = \begin{bmatrix} \frac{1}{5} & -\frac{3}{5} \\ 0 & \frac{1}{3} \end{bmatrix}$. Logo, $(xy)^{-1} \neq x^{-1}y^{-1}$.

Observação. Se $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R})$, então $M^{-1} = \frac{1}{\det(M)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$.

Observação. Como $(xy)^{-1} \neq x^{-1}y^{-1} \Rightarrow y^{-1}x^{-1} \neq x^{-1}y^{-1}$, temos que esse tipo de exemplo só é possível com grupos não abelianos.

A5) Sejam a, b, c elementos de um grupo $(G, *)$ com elemento neutro e. Determine as soluções $x \in G$ das seguintes equações:

a) $c^{-1} * x * c = e$ b) $b * x * b^{-1} = b$

c) $c * x * a * c = b$ d) $a * b^{-1} * x * b * a^{-1} = a * b$

Solução:

a) Multiplicando por c à esquerda e por c^{-1} à direita, obtemos: $c^{-1} * x * c = e \Rightarrow \underbrace{c * c^{-1}}_{=e} * x * \underbrace{c * c^{-1}}_{=e} = \underbrace{c * e * c^{-1}}_{=e} \Rightarrow x = e$. Neste caso, o uso de parênteses pode ser eliminado porque a operação $*$ é associativa.

b) Multiplicando por b^{-1} à esquerda e por b à direita, obtemos: $b * x * b^{-1} = b \Rightarrow \underbrace{b^{-1} * b}_{=e} * x * \underbrace{b^{-1} * b}_{=e} = \underbrace{b^{-1} * b}_{=e} * b \Rightarrow x = b$.

c) Multiplicando por c^{-1} à esquerda e à direita, obtemos: $c * x * a * c = b \Rightarrow \underbrace{c^{-1} * c}_{=e} * x * a * \underbrace{c * c^{-1}}_{=e} = c^{-1} * b * c^{-1} \Rightarrow x * a = c^{-1} * b * c^{-1}$. Multiplicando por a^{-1} à direita, obtemos $x * \underbrace{a * a^{-1}}_{=e} = c^{-1} * b * c^{-1} * a^{-1} \Rightarrow x = c^{-1} * b * c^{-1} * a^{-1}$ é a única solução da equação.

d) Multiplicando por a^{-1} à esquerda e por a à direita, obtemos: $a * b^{-1} * x * b * a^{-1} = a * b \Rightarrow \underbrace{a^{-1} * a}_{=e} * b^{-1} * x * b * \underbrace{a^{-1} * a}_{=e} = \underbrace{a^{-1} * a}_{=e} * b * a^{-1} \Rightarrow b^{-1} * x * b = b * a^{-1}$. Multiplicando por b à esquerda e por b^{-1} à direita, obtemos: $\underbrace{b * b^{-1}}_{=e} * x * \underbrace{b * b^{-1}}_{=e} = b * b * a^{-1} * b^{-1} \Rightarrow x = b * b * a^{-1} * b^{-1}$. Denotando $b * b$ por b^2 temos que a solução dessa equação também pode ser escrita na forma $x = b^2 * a^{-1} * b^{-1}$.

Observação. Não podemos mudar a ordem dos fatores em cada caso porque não sabemos se a operação é comutativa. Dessa forma, não é correto escrever a solução da última equação como sendo $x = b * a^{-1}$ depois do "cancelamento" errado de b^2 com b^{-1}.

A6) Determine $x \in S_5$ que seja solução da equação $a^2 x b^{-1} = c$, onde $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$ e $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}$.

Solução: A equação dada é $aaxb^{-1} = c$. Multiplicando por $a^{-1}a^{-1}$ à esquerda e por b à direita, obtemos: $a^{-1}\underbrace{a^{-1}a}_{=e}ax\underbrace{b^{-1}b}_{=e} = a^{-1}a^{-1}cb \Rightarrow \underbrace{a^{-1}a}_{=e}x = a^{-1}a^{-1}cb$

$\Rightarrow x = a^{-1}a^{-1}cb$. Para calcular a^{-1}, basta trocar as linhas e, depois, reordenar as colunas: $a^{-1} = \begin{pmatrix} 4 & 5 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$. Assim, podemos agora calcular o valor de x:

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$$

Seguimos os seguintes "caminhos", começando sempre na permutação mais à direita e terminando na que estiver mais à esquerda:

- $1 \mapsto 1, 1 \longrightarrow 5, 5 \longrightarrow 2, 2 \longrightarrow 4$; logo, $x : 1 \mapsto 4$.
- $2 \mapsto 2, 2 \longrightarrow 4, 4 \longrightarrow 1, 1 \longrightarrow 3$; logo, $x : 2 \mapsto 3$.
- $3 \mapsto 4, 4 \longrightarrow 1, 1 \longrightarrow 3, 3 \longrightarrow 5$; logo, $x : 3 \mapsto 5$.
- $4 \mapsto 3, 3 \longrightarrow 3, 3 \longrightarrow 5, 5 \longrightarrow 2$; logo, $x : 4 \mapsto 2$.
- $5 \mapsto 5, 5 \longrightarrow 2, 2 \longrightarrow 4, 4 \longrightarrow 1$; logo, $x : 5 \mapsto 1$.

Portanto,

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 2 & 1 \end{pmatrix}.$$

A7) Seja $(G, *)$ um grupo para o qual $(x * y)^2 = x^2 * y^2$, $\forall x, y \in G$. Mostre que G é abeliano. *Observação: Se $a \in G$, então a^2 é o mesmo que $a * a$.*

Solução: Para quaisquer $x, y \in G$, a igualdade dada é equivalente a $x * y * x * y = x * x * y * y$. Multiplicando por x^{-1} à esquerda e por y^{-1} à direita, obtemos: $\underbrace{x^{-1} * x}_{= e} * y * x * \underbrace{y * y^{-1}}_{= e} = \underbrace{x^{-1} * x}_{= e} * x * y * \underbrace{y * y^{-1}}_{= e} \Rightarrow y * x = x * y$. Como x e y são dois elementos genéricos, concluímos que o grupo é abeliano.

A8) Seja $(G, *)$ um grupo com elemento neutro e para o qual $x^2 = e$, $\forall x \in G$. Mostre que G é abeliano.

Solução: Sejam x, y dois elementos genéricos de G. Por hipótese, neste grupo, todo elemento elevado ao quadrado é igual ao elemento neutro, logo, $x^2 = e$, $y^2 = e$ e $(x * y)^2 = e$. Como $(x * y)^2 = e$ é o mesmo que $x * y * x * y = e$, multiplicando por x

à esquerda e por y à direita, obtemos $\underbrace{x*x}_{=e}*y*x*\underbrace{y*y}_{=e} = x*e*y \Rightarrow y*x = x*y$.

Logo, G é abeliano.

A9) Em cada caso, verifique se H é subgrupo de G.

a) $H = \{x \in \mathbb{Q} \mid x > 0\}$, $G = (\mathbb{R}^*, \cdot)$

b) $H = \{x \in \mathbb{Q} \mid x < 0\}$, $G = (\mathbb{R}^*, \cdot)$

c) $H = \{7k \mid k \in \mathbb{Z}\}$, $G = (\mathbb{Z}, +)$

d) $H = \{a + b\sqrt{2} \in \mathbb{R}^* \mid a, b \in \mathbb{Q}\}$, $G = (\mathbb{R}^*, \cdot)$

e) $H = \{a + b\sqrt[3]{2} \in \mathbb{R}^* \mid a, b \in \mathbb{Q}\}$, $G = (\mathbb{R}^*, \cdot)$

f) $H = \{a + b\sqrt[3]{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$, $G = (\mathbb{R}, +)$

Solução: Se H não for um subgrupo de G, então apresentamos um contra-exemplo como justificativa. Se H for subgrupo de G, então mostramos que ele não é vazio e que $a, b \in H \Rightarrow a * b^{-1} \in H$.

a) $H \neq \emptyset$ porque, por exemplo, $1 \in H$. Sejam $a = \frac{p}{q}$ e $b = \frac{r}{s}$ dois elementos genéricos de H com $p, q, r, s \in \mathbb{Z}^*$. Então $a \cdot b^{-1} = (\frac{p}{q}) \cdot (\frac{r}{s})^{-1} = \frac{p}{q} \cdot \frac{s}{r} = \frac{ps}{qr} \in H$. Logo, H é subgrupo de G.

b) H não é fechado com relação à multiplicação usual dos números reais. Por exemplo, $-2 \in H$ e $-5 \in H$, mas $(-2)\cdot(-5) = 10 \notin H$. Logo, H não é subgrupo de G.

c) H é o conjunto de todos os múltiplos de 7. $H \neq \emptyset$, porque, por exemplo, $14 \in H$. Sejam $a, b \in H$. Então $a = 7m$ e $b = 7n$ onde $m, n \in \mathbb{Z}$. Daí, temos que $a + (-b) = a - b = 7m - 7n = 7(m - n)$ também é um múltiplo de 7, ou seja, $a - b \in H$. Logo, H é um subgrupo de G.

d) Escolhendo, por exemplo, $a = 1$ e $b = 2$, obtemos que $1 + 2\sqrt{2} \in H$. Logo, $H \neq \emptyset$. Sejam $\alpha = a + b\sqrt{2}$ e $\beta = c + d\sqrt{2}$ dois elementos genéricos de H, com $a, b, c, d \in \mathbb{Q}$. Então, $\alpha \cdot \beta^{-1} = \dfrac{\alpha}{\beta} = \dfrac{a + b\sqrt{2}}{c + d\sqrt{2}} = \dfrac{(a + b\sqrt{2})(c - d\sqrt{2})}{(c + d\sqrt{2})(c - d\sqrt{2})} = \dfrac{(ac - 2bd) + (bc - ad)\sqrt{2}}{c^2 - 2d^2} = \underbrace{\dfrac{ac - 2bd}{c^2 - 2d^2}}_{\in \mathbb{Q}} + \underbrace{\dfrac{bc - ad}{c^2 - 2d^2}}_{\in \mathbb{Q}}\sqrt{2} \in H$. Logo, H é subgrupo de G. Note que para mostrar que $\alpha \cdot \beta^{-1} \in H$ é indispensável usar a *racionalização* do denominador da fração.

e) H não é fechado com relação à multiplicação usual dos números reais. Por exemplo, $\sqrt[3]{2} \in H$ e $2\sqrt[3]{2} \in H$, mas $(\sqrt[3]{2}) \cdot (2\sqrt[3]{2}) = 2\sqrt[3]{4} \notin H$. Logo, H não é subgrupo de G.

f) $H \neq \emptyset$ porque, por exemplo, $4 - 5\sqrt[3]{2} \in H$. Sejam $\alpha = a + b\sqrt[3]{2}$ e $\beta = c + d\sqrt{2}$ dois elementos de H, onde $a, b, c, d \in \mathbb{Q}$. Temos que $\alpha + (-\beta) = \alpha - \beta = (a + b\sqrt[3]{2}) - (c + d\sqrt[3]{2}) = \underbrace{(a-c)}_{\in \mathbb{Q}} + \underbrace{(b-d)}_{\in \mathbb{Q}}\sqrt[3]{2} \in H$. Logo, H é subgrupo de G.

A10) Uma função $f : \mathbb{R} \longrightarrow \mathbb{R}$ chama-se *par* quando $f(-x) = f(x)$, $\forall x \in \mathbb{R}$. Verifique se o conjunto $\mathcal{P}$ de todas as funções pares de $\mathbb{R}$ em $\mathbb{R}$ é um subgrupo de $(\mathbb{R}^{\mathbb{R}}, +)$.

Solução: Considerando $f(x) = x^2$, temos que $\mathcal{P} \neq \emptyset$. Sejam $f, g \in \mathcal{P}$. Vamos verificar se $f + (-g) = f - g \in \mathcal{P}$. Como f e g são pares, temos $f(-x) = f(x)$ e $g(-x) = g(x)$. Daí, temos que $(f-g)(-x) = f(-x) - g(-x) = f(x) - g(x) = (f-g)(x)$, $\forall x \in \mathbb{R}$. Logo, $f - g \in \mathcal{P}$ e concluímos que $\mathcal{P}$ é um subgrupo de $(\mathbb{R}^{\mathbb{R}}, +)$.

Observação. De modo análogo, temos também que o conjunto das *funções ímpares* ($f(-x) = -f(x)$, $\forall x \in \mathbb{R}$) é um subgrupo de $(\mathbb{R}^{\mathbb{R}}, +)$.

B1) Seja E o conjunto dos números reais não negativos e $*$ a operação sobre E definida por:

$$x * y = \frac{x + y}{1 + xy}.$$

a) Verifique se a operação $*$ é associativa;

b) Verifique se $(E, *)$ é um grupo.

Solução:

a) Sejam $a, b, c \in E = \mathbb{R}_+$. Temos que:

- $a * (b * c) = \frac{a+(b*c)}{1+a\cdot(b*c)} = \frac{a+\frac{b+c}{1+bc}}{1+a\cdot\frac{b+c}{1+bc}} = \frac{a+abc+b+c}{1+bc+ab+ac}$
- $(a * b) * c = \frac{(a*b)+c}{1+(a*b)\cdot c} = \frac{\frac{a+b}{1+ab}+c}{1+c\cdot\frac{a+b}{1+ab}} = \frac{a+b+c+abc}{1+ab+ac+bc}$

Logo, a operação $*$ é associativa sobre o conjunto E.

b) Como a operação $*$ é associativa, para $(E, *)$ ser um grupo, $*$ precisa ter elemento neutro e todo elemento deve ser invertível.

- Seja $x \in E$. Temos que $x * 0 = \frac{x+0}{1+x\cdot 0} = x$ e $0 * x = \frac{0+x}{1+0\cdot x} = x$. Logo, o zero é o elemento neutro de $*$.
- Dado $x \in E$, suponhamos que exista $y = x^{-1} \in E$ tal que $x * y = 0 =$ elemento neutro de $*$. Então $\frac{x+y}{1+xy} = 0 \Rightarrow x + y = 0 \Rightarrow y = -x$. A única possibilidade de se ter $x \in \mathbb{R}_+$ e $y \in \mathbb{R}_+$ é quando $x = y = 0$. Isso significa que o único elemento invertível é o zero.

Logo, E não é um grupo com a operação $*$.

B2) Sejam H_1 e H_2 subgrupos de um grupo G. Mostre que a interseção $H_1 \cap H_2$ também é um subgrupo de G.

Solução:

- Como H_1 e H_2 são subgrupos de G, cada um deles deve conter o elemento neutro $e \in G$, ou seja, $e \in H_1$ e $e \in H_2$. Logo, $e \in H_1 \cap H_2$ o que mostra que $H_1 \cap H_2 \neq \emptyset$.
- Sejam $a, b \in H_1 \cap H_2$. Então, $a, b \in H_1$ e $a, b \in H_2$. Como H_1 é subgrupo de G, $a, b \in H_1 \Rightarrow a * b^{-1} \in H_1$. De modo análogo, $a, b \in H_2 \Rightarrow a * b^{-1} \in H_2$. Portanto, $a * b^{-1} \in H_1 \cap H_2$.

Fica mostrado dessa forma que $H_1 \cap H_2$ é um subgrupo de G.

B3) Dê exemplo de dois subgrupos H_1 e H_2 de um grupo G e tais que a união $H_1 \cup H_2$ não seja subgrupo de G.

Solução: Seja $G = (\mathbb{Z}, +)$ o grupo aditivo dos inteiros. Para todo $n \in \mathbb{Z}$ fixado, o conjunto dos múltiplos de n é um subgrupo de $\mathbb{Z}$. Escolhamos H_1 como sendo o conjunto dos múltiplos de 3 e H_2 como sendo os múltiplos de 5. $H_1 \cup H_2$ é o conjunto dos inteiros que são múltiplos de 3 ou de 5:

$$H_1 \cup H_2 = \{0, \pm 3, \pm 5, \pm 6, \pm 9, \pm 10, \pm 12, \pm 15, \pm 18, \pm 20, \cdots\}$$

O conjunto $H_1 \cup H_2$ não é fechado com relação à soma (por exemplo, $3 \in H_1 \cup H_2$ e $5 \in H_1 \cup H_2$, mas $3 + 5 = 8 \notin H_1 \cup H_2$) e, consequentemente, não é um subgrupo de G.

B4) Verifique se $\mathcal{R}$, o conjunto das matrizes da forma $\begin{bmatrix} \cos(\theta) & \text{sen}(\theta) \\ -\text{sen}(\theta) & \cos(\theta) \end{bmatrix}$ com $\theta \in \mathbb{R}$, é um subgrupo do grupo multiplicativo $GL_2(\mathbb{R})$.

Solução: É claro que $\mathcal{R} \neq \emptyset$ porque basta escolher qualquer valor para θ para obtermos um elemento de $\mathcal{R}$. Por exemplo, escolhendo $\theta = 0$, obtemos $\begin{bmatrix} \cos 0 & \operatorname{sen} 0 \\ -\operatorname{sen} 0 & \cos 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathcal{R}$.

Sejam $A = \begin{bmatrix} \cos(\alpha) & \operatorname{sen}(\alpha) \\ -\operatorname{sen}(\alpha) & \cos(\alpha) \end{bmatrix}$ e $B = \begin{bmatrix} \cos(\beta) & \operatorname{sen}(\beta) \\ -\operatorname{sen}(\beta) & \cos(\beta) \end{bmatrix}$ dois elementos de $\mathcal{R}$. Então $B^{-1} = \begin{bmatrix} \cos(\beta) & -\operatorname{sen}(\beta) \\ \operatorname{sen}(\beta) & \cos(\beta) \end{bmatrix}$ e $AB^{-1} = \begin{bmatrix} \cos(\alpha) & \operatorname{sen}(\alpha) \\ -\operatorname{sen}(\alpha) & \cos(\alpha) \end{bmatrix} \begin{bmatrix} \cos(\beta) & -\operatorname{sen}(\beta) \\ \operatorname{sen}(\beta) & \cos(\beta) \end{bmatrix}$, ou seja, $AB^{-1} = \begin{bmatrix} \cos(\alpha)\cos(\beta) + \operatorname{sen}(\alpha)\operatorname{sen}(\beta) & \operatorname{sen}(\alpha)\cos(\beta) - \cos(\alpha)\operatorname{sen}(\beta) \\ \cos(\alpha)\operatorname{sen}(\beta) - \operatorname{sen}(\alpha)\cos(\beta) & \cos(\alpha)\cos(\beta) + \operatorname{sen}(\alpha)\operatorname{sen}(\beta) \end{bmatrix}$ que é equivalente a $AB^{-1} = \begin{bmatrix} \cos(\alpha-\beta) & \operatorname{sen}(\alpha-\beta) \\ -\operatorname{sen}(\alpha-\beta) & \cos(\alpha-\beta) \end{bmatrix}$. Como $\alpha - \beta \in \mathbb{R}$, temos que $AB^{-1} \in \mathcal{R}$. Portanto, $\mathcal{R}$ é um subgrupo de $GL_2(\mathbb{R})$.

Observação. Essas matrizes que formam o conjunto $\mathcal{R}$ são conhecidas pelo nome de *matrizes de rotação* porque ao multiplicarmos um ponto $P = (x, y)$ do plano por $M = \begin{bmatrix} \cos(\theta) & -\operatorname{sen}(\theta) \\ \operatorname{sen}(\theta) & \cos(\theta) \end{bmatrix}$, o resultado corresponde a um ponto $P' = P \cdot M$ que é igual ao ponto P rotacionado de θ radianos em torno da origem.

B5) Identifique todos os elementos invertíveis de $\mathbb{Z}_{12}$ com relação à multiplicação $\bar{x} \cdot \bar{y} = \overline{xy}$.

Solução: Suponhamos que $\bar{a} \in \mathbb{Z}_{12}$ seja invertível e seja $\bar{b}$ o seu inverso multiplicativo. Então $\bar{a} \cdot \bar{b} = \bar{1}$ = elemento neutro de $\mathbb{Z}_{12}$, temos que $\overline{ab} = \bar{1} \Rightarrow ab - 1 = 12k$, onde $k \in \mathbb{Z} \Rightarrow ab - 12k = 1$. Conseguimos assim uma combinação linear dos inteiros a e 12 dando 1 como resultado. Portanto, $\operatorname{mdc}(a, 12) = 1$.
Por outro lado, se $\operatorname{mdc}(a, 12) = 1$, então existem $x, y \in \mathbb{Z}$ tais que $ax + 12y = 1 \Rightarrow \overline{ax + 12y} = \bar{1} \Rightarrow \bar{a}\bar{x} + \underbrace{\overline{12}\bar{y}}_{=\bar{0}} = \bar{1} \Rightarrow \bar{a}\bar{x} = \bar{1}$, ou seja, $\bar{a}$ é invertível.
Assim, mostramos que $\bar{a} \in \mathbb{Z}_{12}$ é invertível se, e somente se, $\operatorname{mdc}(a, 12) = 1$. Concluímos então que os elementos invertíveis de $\mathbb{Z}_{12}$ são $\bar{1}, \bar{5}, \bar{7}$ e $\overline{11}$. Como $\bar{1} \cdot \bar{1} = \bar{1}$, $\bar{5} \cdot \bar{5} = \bar{1}$ e $\bar{7} \cdot \overline{11} = \bar{1}$ temos que $(\bar{1})^{-1} = \bar{1}$, $(\bar{5})^{-1} = \bar{5}$, $(\bar{7})^{-1} = \overline{11}$ e $(\overline{11})^{-1} = \bar{7}$.

Observação. Seja $\bar{a} \in \mathbb{Z}_{12}$ tal que $\operatorname{mdc}(a, 12) > 1$, por exemplo, $a = 3$. Então, dividindo 12 por $\operatorname{mdc}(a, 12)$ obtemos 4 como quociente, ou seja, $3 \cdot 4 = 12$. Daí, $\overline{3 \cdot 4} = \overline{12}$, isto é, $\bar{3} \cdot \bar{4} = \bar{0}$. Se $\bar{3}$ fosse invertível em $\mathbb{Z}_{12}$, obteríamos $(\bar{3})^{-1} \cdot (\bar{3} \cdot \bar{4}) = (\bar{3})^{-1} \cdot \bar{0} \Rightarrow (\underbrace{(\bar{3})^{-1} \cdot \bar{3}}_{=\bar{1}}) \cdot \bar{4} = \bar{0} \Rightarrow \bar{4} = \bar{0}$ o que é absurdo. Fica mostrado assim que $\bar{4}$

não é invertível. Da mesma forma, poderia ser mostrado também que $\bar{2}$, $\bar{3}$, $\bar{6}$, $\bar{8}$, $\bar{9}$ e $\overline{10}$ não são invertíveis.

Observação. Este exercício pode ser generalizado: um elemento $\bar{a} \in \mathbb{Z}_n$ é invertível se, e somente se, $\text{mdc}(a, n) = 1$.

B6) Suponhamos H um subgrupo do grupo aditivo $\mathbb{Z}$. Mostre que existe $n \in \mathbb{N}$ tal que $H = \{kn \mid k \in \mathbb{Z}\}$, isto é, existe um número natural n tal que H é formado por todos os múltiplos de n.

Solução:

- Se $H = \{0\}$, então basta considerar $n = 0$: neste caso, todo elemento de H é múltiplo de 0.
- Suponhamos $H \neq \{0\}$. Seja r um elemento não nulo de H. Como H é um grupo, $x \in H \Leftrightarrow -x \in H$. Assim, H contém inteiros positivos. Seja n o menor inteiro positivo de H. Se h for um elemento positivo de H, então, dividindo h por n obtemos um quociente q e um resto r tal que $0 \leq r < n$, ou seja, $h = nq + r$. Daí, obtemos que $r = h - nq$. Como $h \in H$ e $nq \in H$, temos que $r \in H$. Não podemos ter $r > 0$ porque assim r seria um elemento positivo menor do que n (não pode porque n é o menor elemento elemento positivo de H). Concluímos então que $r = 0$, ou seja, que $h = nq$. Isso mostra que h é múltiplo de n.
- Se h fosse negativo, então $-h > 0$ e daí $-h$ seria um múltiplo de n o que implica que h também é múltiplo de n.

Se h for um elemento genérico de H, ficou mostrado que em qualquer situação h é múltiplo de um número natural n. Isso significa que $H = \{kn \mid k \in \mathbb{Z}\}$.

Capítulo 4

Homomorfismos, isomorfismos, grupos cíclicos

A1) Em cada caso, verifique se $f : G \longrightarrow J$ é um homomorfismo.

a) $G = (\mathbb{Z}, +)$, $J = (\mathbb{Z}, +)$, $f(x) = 7x$

b) $G = (\mathbb{Z}, +)$, $J = (\mathbb{Z}, +)$, $f(x) = 7x + 1$

c) $G = (\mathbb{Z}, +)$, $J = (\mathbb{Z}, +)$, $f(x) = 7x^2$

d) $G = (\mathbb{R}, +)$, $J = (\mathbb{R}, +)$, $f(x) = |x|$

e) $G = (\mathbb{R}, \cdot)$, $J = (\mathbb{R}, \cdot)$, $f(x) = |x|$

f) $G = (\mathbb{R}, +)$, $J = (\mathbb{R} \times \mathbb{R}, +)$, $f(x) = (2x, 3x)$

g) $G = (\mathbb{R} \times \mathbb{R}, +)$, $J = (\mathbb{R}, +)$, $f(x, y) = 4x - 5y$

h) $G = (GL_2(\mathbb{Z}), +)$, $J = (Z, +)$, $f(X) = \text{tr}(X) =$ traço de X

A operação de adição em $\mathbb{R} \times \mathbb{R}$ dos itens f) e g) é definida da seguinte forma: $(a, b) + (c, d) = (a + c, b + d)$ para quaisquer $a, b, c, d \in \mathbb{R}$.

Solução: Se f for um homomorfismo, devemos mostrar que $f(x*y) = f(x)\Delta f(y)$, $\forall x, y \in G$. Se f não for homomorfismo, devemos mostrar um contra-exemplo, ou seja, escolher valores particulares de $a, b \in G$ tais que $f(a * b) \neq f(a)\Delta f(b)$. Aqui, $*$ representa a operação de G e Δ é a operação de J.

a) Para quaisquer $x, y \in \mathbb{Z}$, temos: $f(x + y) = 7(x + y) = 7x + 7y = f(x) + f(y)$. Logo, f é um homomorfismo de $\mathbb{Z}$ em $\mathbb{Z}$.

b) Neste caso, temos por exemplo que $f(1) = 8$, $f(2) = 15$, $f(1 + 2) = f(3) = 22$ e $f(1) + f(2) = 23$. Logo, $f(1 + 2) \neq f(1) + f(2)$. Logo, f não é homomorfismo.

c) Por exemplo, $f(1) = 7$, $f(3) = 63$, $f(1+3) = f(4) = 112$ e $f(1) + f(3) = 70$. Logo, $f(1+3) \neq f(1)+f(3)$ e daí temos que f não é homomorfismo de grupos.

d) Por exemplo, $f(-2) = 2$, $f(2) = 2$, $f(-2+2) = f(0) = 0$, $f(-2)+f(2) = 2+2 = 4$. Logo, $f(-2+2) \neq f(-2)+f(2) \Rightarrow f$ não é homomorfismo.

e) Para quaisquer $x, y \in \mathbb{R}$, temos $f(x \cdot y) = |x \cdot y| = |x| \cdot |y| = f(x) \cdot f(y)$. Logo, f é um homomorfismo de G em J.

f) Sejam $x, y \in \mathbb{R}$. Temos que: $f(x+y) = (2(x+y), 3(x+y)) = (2x+2y, 3x+3y)$. Por outro lado, $f(x)+f(y) = (2x, 3x)+(2y, 3y) = (2x+2y, 3x+3y)$. Logo, $f(x+y) = f(x)+f(y)$ de onde concluímos que f é um homomorfismo de grupos.

g) Sejam (a,b) e (c,d) dois elementos genéricos de $\mathbb{R} \times \mathbb{R}$. Temos: $f(a,b)+f(c,d) = (4a-5b)+(4c-5d) = 4a+4c-5b-5d$. Por outro lado, $f((a,b)+(c,d)) = f(a+c, b+d) = 4(a+c)-5(b+d) = 4a+4c-5b-5d$. Logo, $f((a,b)+(c,d)) = f(a,b)+f(c,d) \Rightarrow f$ é homomorfismo de G em J.

h) Para quaisquer $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$ e $Y = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in G$, temos: $X + Y = \begin{bmatrix} a+r & b+s \\ c+t & d+u \end{bmatrix}$ e $f(X)+f(Y) = \text{tr}(X)+\text{tr}(Y) = (a+d)+(r+u) = a+d+r+u$. Por outro lado, $f(X+Y) = \text{tr}(X+Y) = (a+r)+(d+u) = a+r+d+u$. Logo, $f(X+Y) = f(X)+f(Y) \Rightarrow f$ é um homomorfismo de grupos. (*OBS.: O traço de uma matriz quadrada é definido como sendo a soma dos elementos da diagonal principal*).

A2) Considere $G = \mathbb{Z} \times \mathbb{Z}$ com a seguinte operação de adição: $(a,b)+(c,d) = (a+c, b+d)$. Mostre que $f : G \longrightarrow G$, $f(x,y) = (0, 3x+5y)$ é um homomorfismo, determine seu núcleo e dê alguns exemplos de elementos de $N(f)$.

Solução: Sejam $(a,b),(c,d) \in G$. Temos: $f((a,b)+(c,d)) = f(a+c, b+d) = (0, 3(a+c)+5(b+d)) = (0, 3a+3c+5b+5d) = (0, (3a+5b)+(3c+5d)) = (0, 3a+5b)+(0, 3c+5d) = f(a,b)+f(c,d)$. Logo, f é um homomorfismo.
Se $(x,y) \in N(f)$, então $f(x,y) = (0,0) =$ elemento neutro do contradomínio de $f \Rightarrow (0, 3x+5y) = (0,0) \Rightarrow 3x+5y = 0$, de onde concluímos que

$$N(f) = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid 3x+5y = 0\}.$$

Por exemplo, $(0,0), (5,-3), (-5,3), (-10,6) \in N(f)$.

A3) Sejam $G = (GL_3(\mathbb{R}), \cdot)$, $J = (\mathbb{R}, \cdot)$ e $f : G \longrightarrow J$ definida por $f(X) = \det(X) =$ determinante de X.

a) Mostre que f é um homomorfismo;

b) Determine $N(f)$ e dê exemplo de elementos do núcleo de f.

Solução: a) Sejam $X, Y \in G$. Temos: $f(XY) = \det(XY) = \det(X)\det(Y) = f(X)f(Y)$. Fica mostrado dessa forma que f é um homomorfismo de grupos.
b) Seja A um elemento genérico do núcleo de f. Então, A é uma matriz quadrada 3×3 tal que $f(A) = \det(A) = 1 =$ elemento neutro de J. Portanto,

$$N(f) = \{A \in GL_3(\mathbb{R}) \mid \det(A) = 1\}.$$

Assim, qualquer matriz 3×3 de elementos reais cujo determinante seja igual a 1 pertencem ao núcleo de f. Por exemplo, $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 2 & 0 & 0 \\ 7 & 3 & 0 \\ 5 & -4 & \frac{1}{6} \end{bmatrix}$ e $\begin{bmatrix} -1 & 0 & 0 \\ 0 & 9 & 10 \\ 0 & 1 & 1 \end{bmatrix}$ pertencem a $N(f)$.

A4) Mostre que um grupo G é abeliano se, e somente se, $f : G \longrightarrow G$ definida por $f(x) = x^{-1}$ é um homomorfismo.

Solução: ($\Rightarrow$) Suponhamos G um grupo abeliano e sejam $x, y \in G$. Então, $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y)$. Logo, f é um homomorfismo.
($\Leftarrow$) Suponhamos que f seja um homomorfismo de G em G. Então, para quaisquer $x, y \in G$, temos: $f(xy) = f(x)f(y) \Rightarrow (xy)^{-1} = x^{-1}y^{-1}$. Calculando-se o inverso de cada membro da igualdade anterior, obtemos: $((xy)^{-1})^{-1} = (x^{-1}y^{-1})^{-1} \Rightarrow xy = (y^{-1})^{-1}(x^{-1})^{-1} \Rightarrow xy = yx$, e daí, concluímos que G é um grupo abeliano.

A5) Seja G um grupo e $g \in G$. Mostre que $f : G \longrightarrow G$ definida por $f(x) = g^{-1}xg$ é isomorfismo de G em G (neste caso, f é denominado *automorfismo* de G).

Solução: Sejam $x, y \in G$ dois elementos genéricos.

- $f(xy) = g^{-1}(xy)g = g^{-1}xeyg = g^{-1}x\underbrace{gg^{-1}}_{=e}yg = f(x)f(y)$; logo, f é um homomorfismo.
- Suponhamos $f(x) = f(y)$. Então $g^{-1}xg = g^{-1}yg$. Multiplicando-se por g à esquerda e por g^{-1} à direita, obtemos: $\underbrace{gg^{-1}}_{=e}x\underbrace{gg^{-1}}_{=e} = \underbrace{gg^{-1}}_{=e}y\underbrace{gg^{-1}}_{=e} \Rightarrow x = y$; logo, f é uma função injetora.

- Dado $b \in G$ = contradomínio de f, considere o elemento $a = gbg^{-1} \in G$ = domínio de f. Então, $f(a) = f(gbg^{-1}) = \underbrace{g^{-1}(g}_{=e} b \underbrace{g^{-1})g}_{=e} = b$; logo, f é uma função sobrejetora.

Dos três itens mostrados acima, concluímos que f é um isomorfismo de grupos.

A6) Sejam $G = \{2^m 3^n \mid m, n \in \mathbb{Z}\}$ e $J = \left\{ \begin{bmatrix} m & n \\ -n & m \end{bmatrix} \mid m, n \in \mathbb{Z} \right\}$.

a) Mostre que $(G, \cdot)$ é um subgrupo de $(\mathbb{R}_+^*, \cdot)$;

b) Mostre que $(J, +)$ é subgrupo de $(M_{2\times 2}(\mathbb{R}), +)$;

a) Mostre que G é isomorfo a J.

Solução:

a) Escolhendo $m = n = 1$, obtemos $6 = 2^1 \cdot 3^1 \in G$ o que implica que G não é um conjunto vazio. Sejam $x, y \in G$. Existem $m, n, r, s \in \mathbb{Z}$ tais que $x = 2^m 3^n$ e $y = 2^r 3^s \Rightarrow x \cdot y^{-1} = 2^m 3^n 2^{-r} 3^{-s} = 2^{m-r} 3^{n-s}$. Como $m - r \in \mathbb{Z}$ e $n - s \in \mathbb{Z}$, temos $x \cdot y^{-1} \in G$ de onde concluímos que G é um subgrupo de $(\mathbb{R}_+^+, \cdot)$.

b) Escolhendo $m = 2$ e $n = 0$ obtemos $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \in J \Rightarrow J \neq \emptyset$. Sejam $X, Y \in J$. Existem $m, n, r, s \in \mathbb{Z}$ tais que $X = \begin{bmatrix} m & n \\ -n & m \end{bmatrix}$ e $Y = \begin{bmatrix} r & s \\ -s & r \end{bmatrix} \Rightarrow X + (-Y) = X - Y = \begin{bmatrix} m & n \\ -n & m \end{bmatrix} - \begin{bmatrix} r & s \\ -s & r \end{bmatrix} = \begin{bmatrix} m-r & n-s \\ -n+s & m-r \end{bmatrix}$. Como $m - r \in \mathbb{Z}$, $n - s \in \mathbb{Z}$ e $-n + s = -(n - s)$ temos que $X - Y \in J$. Logo, J é um subgrupo de $(M_{2\times 2}(\mathbb{R}), +)$.

c) Para mostrar que existe isomorfismo entre G e J, devemos ser capazes de encontrar uma função $f : G \longrightarrow J$ que seja bijetora e homomorfismo de grupos. Seja $f : G \longrightarrow J$ definida por $f(2^m 3^n) = \begin{bmatrix} m & n \\ -n & m \end{bmatrix}$.

- Sejam $m, n, r, s \in \mathbb{Z}$ tais que $f(2^m 3^n) = f(2^r 3^s)$. Daí, temos $\begin{bmatrix} m & n \\ -n & m \end{bmatrix} = \begin{bmatrix} r & s \\ -s & r \end{bmatrix} \Rightarrow m = r$ e $n = s \Rightarrow 2^m 3^n = 2^r 3^s$. Isso mostra que f é uma função injetora.
- Dado um elemento genérico $Y \in J$, temos que Y é da forma $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, onde $a, b \in \mathbb{Z}$. Escolhendo $x = 2^a 3^b \in G$ temos que $f(x) = f(2^a 3^b) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = Y$. Logo, f é uma função sobrejetora.

- Sejam $x, y \in G$. Existem $m, n, r, s \in \mathbb{Z}$ tais que $x = 2^m 3^n$ e $y = 2^r 3^s$. Temos: $f(x \cdot y) = f(2^m 3^n 2^r 3^s) = f(2^{m+r} 3^{n+s}) = \begin{bmatrix} m+r & n+s \\ -n-s & m+r \end{bmatrix} = \begin{bmatrix} m & n \\ -n & m \end{bmatrix} + \begin{bmatrix} r & s \\ -s & r \end{bmatrix} = f(2^m 3^n) + f(2^r 3^s) = f(x) + f(y)$. Logo, f é um homomorfismo de grupos.

Como f é injetora, sobrejetora e é um homomorfismo, temos que f é um isomorfismo de G em J, ou seja, $G \simeq J$.

A7) Descreva os seguintes grupos cíclicos:

- $H = [-3]$ em $(\mathbb{Z}, +)$
- $J = [-3]$ em $(\mathbb{Q}^*, \cdot)$
- $K = [\bar{3}]$ em $(\mathbb{Z}_7{}^*, \cdot)$

Solução: Se o grupo for multiplicativo, então o grupo cíciclo gerado por x é o conjunto de todas as potências de expoente inteiro de x; se o grupo for aditivo, então o grupo gerado por x é o conjunto de todos os múltiplos de x. Sendo assim, temos:

- $H = [-3]$ = múltiplos de $-3 = \{-3k \mid k \in \mathbb{Z}\} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$
- $J = [-3]$ = potências de $-3 = \{(-3)^k \mid k \in \mathbb{Z}\} = \{\ldots, 1/9, -1/3, 1, -3, 9, \ldots\}$
- $K = [\bar{3}]$ = potências de $\bar{3}$ em $\mathbb{Z}_7{}^*$. Como $\bar{3}^0 = \bar{1}$, $\bar{3}^1 = \bar{3}$, $\bar{3}^2 = \bar{9} = \bar{2}$, $\bar{3}^3 = \overline{27} = \bar{6}$, $\bar{3}^4 = \bar{3}^3 \cdot \bar{3} = \overline{18} = \bar{4}$, $\bar{3}^5 = \bar{3}^4 \cdot \bar{3} = \overline{12} = \bar{5}$, $\bar{3}^6 = \bar{3}^5 \cdot \bar{3} = \overline{15} = \bar{1}$ = elemento neutro de $(\mathbb{Z}_7^*, \cdot)$. Logo, $K = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\} = \mathbb{Z}_7{}^*$.

A8) Verifique se os grupos G e J são isomorfos em cada um dos seguintes casos:

a) $G = (\mathbb{Z}_3, +)$, $J = (\mathbb{Z}_6, +)$

b) $G = (S_3, \circ)$, $J = (\mathbb{Z}_6, +)$

c) $G = (\mathbb{R}^*, \cdot)$, $J = (\mathbb{R}, +)$

d) $G = (\mathbb{Z}, +)$, $J = (\mathbb{R}, +)$.

Solução: Quando dois grupos são isomorfos, eles têm muitas propriedades em comum. Por exemplo, se um deles tiver n elementos, então o outro também tem que ter n elementos; se um for abeliano, o outro também é abeliano; se determinado tipo de equação tem solução em um deles, então uma equação equivalente também tem solução no outro. Desse modo, para mostrar que dois grupos não podem ser isomorfos, basta detectar alguma propriedade algébrica que um tenha e que o outro não tenha.

a) $\mathbb{Z}_3$ tem 3 elementos, enquanto que $\mathbb{Z}_6$ tem 6 elementos. Logo, não pode existir bijeção entre eles e, daí, G não é isomorfo a J.

b) S_3 é um grupo não abeliano com 6 elementos e $\mathbb{Z}_6$ é abeliano com 6 elementos. Logo, não podem ser isomorfos.

c) Em J, a equação $x + x = -1$ tem solução $x = -1/2 \in J$. Em G, uma equação equivalente a essa seria $x \cdot x = -1$ que não tem solução em $\mathbb{R}^*$. Logo, G não é isomorfo a J.

d) $\mathbb{Z}$ é um conjunto enumerável, enquanto que $\mathbb{R}$ é não enumerável. Logo, não pode existir bijeção entre eles e, daí, concluímos que os grupos G e J não são isomorfos.

B1) a) Dê exemplo de um isomorfismo do grupo $G = (\mathbb{R}, +)$ em $J = (\mathbb{R}_+^*, \cdot)$.
b) Mostre que não existe isomorfismo do grupo $G = (\mathbb{Q}, +)$ em $J = (\mathbb{Q}_+^*, \cdot)$.
(*Sugestão: Supondo* $f : G \longrightarrow J$ *isomorfismo e* $x \in G$ *tal que* $f(x) = 2$*, calcule* $f(\frac{x}{2} + \frac{x}{2})$).

Solução:

a) Considere a função exponencial $f : \mathbb{R} \longrightarrow \mathbb{R}_+^*$, $f(x) = e^x$. Temos que f é bijetora e $f(x + y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$. Logo, f é um isomorfismo de G em J.

b) Suponhamos que exista um isomorfismo $f : \mathbb{Q} \longrightarrow \mathbb{Q}_+^*$. Como f é bijetora $\Rightarrow$ f sobrejetora, escolhendo $2 \in J$ temos que existe $x \in G = \mathbb{Q}$ tal que $f(x) = 2$. Como $x = \frac{x}{2} + \frac{x}{2}$ temos que $f(x) = f(\frac{x}{2} + \frac{x}{2}) = f(\frac{x}{2}) \cdot f(\frac{x}{2}) = f(\frac{x}{2})^2 \Rightarrow f(\frac{x}{2})^2 = 2$ o que é um absurdo porque $f(\frac{x}{2}) \in \mathbb{Q}_+^*$ e não existe número racional positivo que elevado ao quadrado dê um resultado igual a 2. Logo, não pode existir o isomorfismo de G em J.

B2) Considere os elementos $x = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ e $y = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ pertencentes ao grupo multiplicativo $GL_2(\mathbb{Q})$. Calcule $o(x)$, $o(y)$ e $o(xy)$.

Solução: Temos que $xy = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Para calcular as ordens de x, y e xy devemos calcular suas potências de expoentes inteiros e observar se existe alguma potência que dê igual à matriz identidade.

- $x = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \Rightarrow x^2 = x \cdot x = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$
  $\Rightarrow x^3 = x^2 \cdot x = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$
  $\Rightarrow x^4 = x^3 \cdot x = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Assim, 4 é o menor expoente positivo n para o qual x^n = elemento neutro, logo, $o(x) = 4$.
- $y = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \Rightarrow y^2 = y \cdot y = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}$
  $\Rightarrow y^3 = y^2 \cdot y = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Assim, 3 é o menor expoente positivo m para o qual y^m = elemento neutro, logo, $o(y) = 3$.
- $xy = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \Rightarrow (xy)^2 = (xy)(xy) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \Rightarrow (xy)^3 = (xy)^2(xy) = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \Rightarrow (xy)^4 = (xy)^3(xy) = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix} \Rightarrow (xy)^5 = (xy)^4(xy) = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 5 \\ 0 & 1 \end{bmatrix}$. E assim, as potências de x não se repetem e nem coincidem com a matriz identidade. Logo, $o(x) = 0$.

Observação. Casos como esse só ocorrem em grupos não abelianos. Pode-se mostrar que se G for abeliano e $x, y \in G$, então $o(xy) = \text{mmc}(o(x), o(y))$.

Observação. Observando-se o desenvolvimento do terceiro item, podemos chegar à conclusão de que $(xy)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$. Essa é uma igualdade verdadeira, mas para demonstrá-la é preciso usar o Princípio de Indução Finita.

B3) Mostre que todo grupo cíclico infinito possui exatamente dois elementos geradores.

Solução: Suponhamos que G seja um grupo multiplicativo cíclico infinito.

- Existe $x \in G$ tal que todo elemento de G é da forma x^n para algum $n \in \mathbb{Z}$, ou seja, $G = [x] = \{x^n \mid n \in \mathbb{Z}\}$.
- Como $x^n = (x^{-1})^{-n}$ temos que todo elemento de G também é potência de x^{-1}, ou seja, $G = [x^{-1}]$.
- Neste caso, não podemos ter $x = x^{-1}$ porque isso implicaria $x \cdot x = x \cdot x^{-1} \Rightarrow x^2 = e \Rightarrow G = \{e, x\}$ o que seria um absurdo porque G é infinito. Logo, $x \neq x^{-1}$ o que significa que G tem pelo menos dois geradores: x e x^{-1}.
- Se G possuir outro gerador, digamos $G = [y]$, então x deve ser igual a alguma potência de y e também y deve ser igual a alguma potência de x, ou seja, $y = x^r$ e $x = y^s$ onde $r, s \in \mathbb{Z} \Rightarrow x = y^s = (x^r)^s = x^{rs} \Rightarrow x^{rs} \cdot x^{-1} = x \cdot x^{-1} \Rightarrow x^{rs-1} = e$.
- Se $rs - 1 \neq 0$, então teríamos uma potência de x com expoente inteiro dando igual ao elemento neutro; isso limitaria a quantidade de elementos de G o que seria um absurdo porque G é infinito.
- Temos $rs - 1 = 0$. Como r e s são inteiros, temos $r = s = 1$ ou $r = s = -1$. Em um caso, temos $y = x$ e no outro caso temos $y = x^{-1}$. Portanto, y sendo um gerador de G, y deve coincidir com x ou com x^{-1}.

Fica mostrado dessa forma que G sendo cíclico infinito tem exatamente dois geradores: x e x^{-1}.

Observação. Se tivéssemos usado a notação aditiva, então teríamos usado múltiplos de x no lugar de potências de x. No final, chegaríamos à mesma conclusão: que G tem exatamente dois geradores, x e $-x$.

C1) Seja σ a seguinte permutação de S_{10}:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 7 & 5 & 9 & 4 & 10 & 2 & 6 & 3 & 1 \end{pmatrix}.$$

Calcule a ordem de σ e a potência σ^{2010}.

Solução: Para calcular a ordem de σ,devemos calcular suas potências de expoentes inteiros e verificar se alguma coincide com a identidade.

$$\sigma^2 = \sigma\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 7 & 5 & 9 & 4 & 10 & 2 & 6 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 7 & 5 & 9 & 4 & 10 & 2 & 6 & 3 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 2 & 4 & 3 & 9 & 1 & 7 & 10 & 5 & 8 \end{pmatrix},$$

As composições utilizadas no cálculo de $\sigma^2 = \sigma\sigma$ foram as seguintes:

- $1 \longrightarrow 8$ e $8 \longrightarrow 6$; logo, $1 \longrightarrow 6$ (ou seja: *"o 1 é levado por σ para o 8, depois o 8 é levado para o 6; logo, o 1 é levado na composição $\sigma\sigma$ para o 6"*)
- $2 \longrightarrow 7$ e $7 \longrightarrow 2$; logo, $2 \longrightarrow 2$
- $3 \longrightarrow 5$ e $5 \longrightarrow 4$; logo, $3 \longrightarrow 4$
- $4 \longrightarrow 9$ e $9 \longrightarrow 3$; logo, $4 \longrightarrow 3$
- etc.

$$\sigma^3 = \sigma^2\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 2 & 4 & 3 & 9 & 1 & 7 & 10 & 5 & 8 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 7 & 5 & 9 & 4 & 10 & 2 & 6 & 3 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 7 & 9 & 5 & 3 & 8 & 2 & 1 & 4 & 6 \end{pmatrix},$$

$$\sigma^4 = \sigma^3\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 7 & 9 & 5 & 3 & 8 & 2 & 1 & 4 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 7 & 5 & 9 & 4 & 10 & 2 & 6 & 3 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix} = e = \text{ identidade.}$$

Logo, $o(\sigma) = 4$. Isso significa que as potências de expoentes inteiros se repetem de 4 em 4: $\sigma^5 = \sigma^4\sigma = e\sigma = \sigma$, $\sigma^6 = \sigma^4\sigma^2 = e\sigma^2 = \sigma^2$, $\sigma^7 = \sigma^4\sigma^3 = e\sigma^3 = \sigma^3$, $\sigma^8 = \sigma^4\sigma^4 = ee = e$, etc. Se o expoente r for múltiplo de 4, então $\sigma^r = e$. Dividindo-se 2010 por 4, obtemos quociente 502 e resto igual a 2, ou seja, $2010 = 4 \times 502 + 2$. Daí,

$$\sigma^{2010} = \sigma^{4\times 502+2} = \underbrace{(\sigma^4)}_{=e}{}^{502}\sigma^2 = e\sigma^2 = \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 2 & 4 & 3 & 9 & 1 & 7 & 10 & 5 & 8 \end{pmatrix}.$$

C2) Seja G um grupo multiplicativo com elemento neutro e. Sendo $a, b \in G$ diferentes do elemento neutro tais que $a^5 = e$ e $aba^{-1} = b^2$, calcule $o(b)$.

Solução: Para calcularmos a ordem de b, devemos de algum modo saber quais são suas potências de expoentes inteiros positivos.

- $b^2 \cdot b^2 = (aba^{-1})(aba^{-1}) = ab(a^{-1}a)ba^{-1} = abeba^{-1} = a\underbrace{b^2}_{aba^{-1}}a^{-1} = a(aba^{-1})a^{-1} = a^2ba^{-2}$, ou seja, $b^4 = a^2ba^{-2}$.

- Temos também que $b^4 \cdot b^4 = (a^2ba^{-2})(a^2ba^{-2}) = a^2b(a^{-2}a^2)ba^{-2} = a^2beba^{-2} = a^2 \underbrace{b^2}_{aba^{-1}} a^{-2} = a^2(aba^{-1})a^{-2} = a^3ba^{-3}$, ou seja, $b^8 = a^3ba^{-3}$.
- De modo semelhante, calculamos $b^{16} = b^8 \cdot b^8$ e $b^{32} = b^{16} \cdot b^{16}$ e obtemos os seguintes resultados: $b^{16} = a^4ba^{-4}$ e $b^{32} = a^5ba^{-5}$. Como $a^5 = e$, obtemos finalmente que $b^{32} = ebe^{-1} \Rightarrow b^{32} = b$ que multiplicando-se por b^{-1} fornece: $b^{-1}b^{32} = b^{-1}b$, ou seja $b^{31} = e$.

Temos daí que a ordem de b é um divisor de 31. Como b não é o elemento neutro e 31 é primo, temos finalmente que $o(b) = 31$.

Capítulo 5

Classes laterais, subgrupos normais, grupos-quocientes

A1) Seja $H = [a]$ um subgrupo de $G = GL_2(\mathbb{R})$, onde $a = \begin{bmatrix} 0 & -2 \\ \frac{1}{2} & 0 \end{bmatrix}$, e seja $x = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$. Calcule as classes laterais xH e Hx e verifique se $H \lhd G$.

Solução: As potências de expoente inteiro de a são:

- $a^2 = a \cdot a = \begin{bmatrix} 0 & -2 \\ \frac{1}{2} & 0 \end{bmatrix}\begin{bmatrix} 0 & -2 \\ \frac{1}{2} & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$
- $a^3 = a^2 \cdot a = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & -2 \\ \frac{1}{2} & 0 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ -\frac{1}{2} & 0 \end{bmatrix}$
- $a^4 = a^3 \cdot a = \begin{bmatrix} 0 & 2 \\ -\frac{1}{2} & 0 \end{bmatrix}\begin{bmatrix} 0 & -2 \\ \frac{1}{2} & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = e =$ elemento neutro de $GL_2(\mathbb{R})$.

Portanto, $o(a) = 4$ e $H = \{e, a, a^2, a^3\}$ e, daí, temos que $xH = \{x, xa, xa^2, xa^3\} \Rightarrow$

$$xH = \left\{\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 1 & -2 \\ \frac{3}{2} & 0 \end{bmatrix}, \begin{bmatrix} -1 & -2 \\ 0 & -3 \end{bmatrix}, \begin{bmatrix} -1 & 2 \\ -\frac{3}{2} & 0 \end{bmatrix}\right\}$$

e $Hx = \{x, ax, a^2x, a^3x\} \Rightarrow$

$$Hx = \left\{\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 0 & -6 \\ \frac{1}{2} & 1 \end{bmatrix}, \begin{bmatrix} -1 & -2 \\ 0 & -3 \end{bmatrix}, \begin{bmatrix} 0 & 6 \\ -\frac{1}{2} & -1 \end{bmatrix}\right\}.$$

Como $xH \neq Hx$, concluímos que H não é um subgrupo normal de G.

A2) Sejam G um grupo finito, H um subgrupo de G e K um subgrupo de H. Mostre que $(G : K) = (G : H)(H : K)$.

Solução: Usando três vezes o Teorema de Lagrange, temos:

- H subgrupo de $G \Rightarrow o(G) = (G : H)o(H)$
- K subgrupo de $H \Rightarrow o(H) = (H : K)o(K)$
- K subgrupo de $G \Rightarrow o(G) = (G : K)o(K)$

Substituindo o $o(H)$ da segunda equação e o $o(G)$ da terceira equação na primeira, temos: $(G : K)o(K) = (G : H)(H : K)o(K)$ o que implica $(G : K) = (G : H)(H : K)$.

A3) Sejam $G = (\mathbb{Z}_{12}, +)$ e $H = \{\bar{0}, \bar{4}, \bar{8}\}$ um subgrupo de G. Construa a tábua do grupo-quociente $(G/H, +)$, identifique seu elemento neutro e os inversos (aditivos) de $\bar{1} + H$ e $\bar{2} + H$.

Solução: As classes laterais à esquerda módulo H são:

- $\bar{0} + H = \{\bar{0} + \bar{0}, \bar{0} + \bar{4}, \bar{0} + \bar{8}\} = \{\bar{0}, \bar{4}, \bar{8}\} = H$
- $\bar{1} + H = \{\bar{1} + \bar{0}, \bar{1} + \bar{4}, \bar{1} + \bar{8}\} = \{\bar{1}, \bar{5}, \bar{9}\}$
- $\bar{2} + H = \{\bar{2} + \bar{0}, \bar{2} + \bar{4}, \bar{2} + \bar{8}\} = \{\bar{2}, \bar{6}, \overline{10}\}$
- $\bar{3} + H = \{\bar{3} + \bar{0}, \bar{3} + \bar{4}, \bar{3} + \bar{8}\} = \{\bar{3}, \bar{7}, \overline{11}\}$
- $\bar{4} + H = \{\bar{4} + \bar{0}, \bar{4} + \bar{4}, \bar{4} + \bar{8}\} = \{\bar{4}, \bar{8}, \bar{0}\} = H$ e, a partir daqui, todas as classes laterais são repetições das anteriores: $\bar{5} + H = \bar{1} + H$, $\bar{6} + H = \bar{2} + H$, etc.

Logo, $G/H = \{H, \bar{1} + H, \bar{2} + H, \bar{3} + H\}$. Lembrando que a adição em G/H é definida por $(\bar{a} + H) + (\bar{b} + H) = (\bar{a} + \bar{b}) + H$, a sua tábua é:

$+$	H	$\bar{1} + H$	$\bar{2} + H$	$\bar{3} + H$
H	H	$\bar{1} + H$	$\bar{2} + H$	$\bar{3} + H$
$\bar{1} + H$	$\bar{1} + H$	$\bar{2} + H$	$\bar{3} + H$	H
$\bar{2} + H$	$\bar{2} + H$	$\bar{3} + H$	H	$\bar{1} + H$
$\bar{3} + H$	$\bar{3} + H$	H	$\bar{1} + H$	$\bar{2} + H$

O elemento neutro do grupo-quociente G/H é o H. Como $(\bar{1} + H) + (\bar{3} + H) = H$ temos que o inverso aditivo de $\bar{1} + H$ é o $\bar{3} + H$. Como $(\bar{2} + H) + (\bar{2} + H) = H$ temos que o inverso de $\bar{2} + H$ é o próprio $\bar{2} + H$.

A4) Sejam $G = ([x], \cdot)$ e $H = ([x^2], \cdot)$ onde x é um elemento de um grupo $(J, \cdot)$ tal que $o(x) = 8$.

a) H é normal em G ?

b) Descreva G/H e calcule sua ordem $o(G/H)$

c) Construa a tábua de G/H e calcule $(x^3H)^{-1}$ e $(x^5H)^2$

Solução:

a) O grupo G é cíclico, logo, é abeliano. Sendo assim, qualquer subgrupo é normal em G.

b) A partir de $G = [x]$ com $o(x) = 8$, obtemos $G = \{e, x, x^2, x^3, x^4, x^5, x^6, x^7\}$ onde e é o elemento neutro, e, a partir de $H = [x^2]$, obtemos $H = \{e, x^2, x^4, x^6\}$. Como $o(G) = 8$ e $o(H) = 4$, temos $o(G/H) = (G : H) = o(G)/o(H) = 8/4 = 2$. As possíveis classes laterais à esquerda módulo H são $eH = H$ e $xH = \{x, x^3, x^5, x^7\}$. Logo, $G/H = \{H, xH\}$.

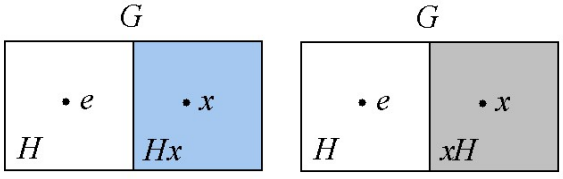
c) Temos que $H \cdot H = eH \cdot eH = (e \cdot e)H = eH = H$, $H \cdot xH = eH \cdot xH = (e \cdot x)H = xH$, $xH \cdot H = xH \cdot eH = (x \cdot e)H = xH$, $xH \cdot xH = (x \cdot x)H = x^2H = H$, porque $x^2 \in H$. Logo, a tábua de G/H é:

$\cdot$	H	xH
H	H	xH
xH	xH	H

O elemento neutro de G/H é a classe $eH = H$. Como $(x^3H) \cdot (xH) = x^4H = H$, temos que $(x^3H)^{-1} = xH$. Temos também que $(x^5H)^2 = (x^5H)(x^5H) = (x^5 \cdot x^5)H = x^{10}H = x^2H = H$.

A5) Sejam G um grupo e H um subgrupo de G tal que $(G : H) = 2$. Mostre que $H \triangleleft G$.

Solução: Sejam x um elemento de G e e o elemento neutro. Se $x \in H$, então $xH = Hx = H$. Suponhamos $x \notin H$. Como só existem duas classes laterais (porque $(G : H) = 2$) temos que as classes laterais à esquerda são eH e xH e as classes laterais à direita são He e Hx. Sendo e o elemento neutro, temos $eH = He = H$. Daí, $G = H \cup Hx = H \cup xH$.



Como $H \cap Hx = \emptyset$ e $H \cap xH = \emptyset$, concluímos que $Hx = xH$. Portanto, $H \lhd G$.

B1) Seja H um subgrupo de G e sejam x e y dois elementos quaisquer de G. Mostre que se $xH = yH$, então $Hx^{-1} = Hy^{-1}$.

Solução: ($\Rightarrow$) Suponhamos $xH = yH$.

- Seja $a \in Hx^{-1}$. Então $a = hx^{-1}, h \in H \Rightarrow a^{-1} = xh^{-1} \Rightarrow a^{-1} \in xH = yH \Rightarrow a^{-1} = yh_2 \Rightarrow a = h_2^{-1}y^{-1} \Rightarrow a \in Hy^{-1}$. Logo, $Hx^{-1} \subset Hy^{-1}$.
- Seja $b \in Hy^{-1}$. Então existe $h \in H$ tal que $b = hy^{-1} \Rightarrow b^{-1} = yh^{-1} \in yH = xH \Rightarrow b^{-1} = xh_2$, onde $h_2 \in H \Rightarrow b = h_2^{-1}x^{-1} \in Hx^{-1}$. Logo, $Hy^{-1} \subset Hx^{-1}$.

Fica mostrado então que $Hx^{-1} = Hy^{-1}$.

Observação. Analogamente, pode-se mostrar que $Hx^{-1} = Hy^{-1} \Rightarrow xH = yH$.

B2) Seja G um grupo e H um subgrupo de G. Mostre que $H \lhd G$ se, e somente se, $x^{-1}Hx = H$, $\forall x \in G$, onde $x^{-1}Hx = \{x^{-1}hx \mid h \in H\}$.

Solução: ($\Rightarrow$) Suponhamos $H \lhd G$.

- Então, $Hx = xH$ e também $Hx^{-1} = x^{-1}H$, $\forall x \in G$.
- Se $y \in x^{-1}Hx$, então existe $h \in H$ tal que $y = x^{-1}hx \Rightarrow xy = xx^{-1}hx = hx \in Hx = xH \Rightarrow xy = xh_2$, com $h_2 \in H$, de onde obtemos que $y = h_2 \in H$. Logo, $x^{-1}Hx \subset H$.
- Se $y \in H$, então $yx^{-1} \in Hx^{-1} = x^{-1}H$. Então, existe $h_3 \in H$ tal que $yx^{-1} = x^{-1}h_3 \Rightarrow y = x^{-1}h_3x \in x^{-1}Hx$. Logo, $H \subset x^{-1}Hx$.

Fica mostrado dessa forma que $x^{-1}Hx \subset H$ e $H \subset x^{-1}Hx$ o que implica $x^{-1}Hx = H$. ($\Leftarrow$) Suponhamos $x^{-1}Hx = H$, $\forall x \in G$. Como a igualdade anterior é válida para todo $x \in G$, então também é válida com x^{-1} no lugar do x: $(x^{-1})^{-1}Hx^{-1} = H$, ou seja, $xHx^{-1} = H$.

- Seja $y \in xH$. Existe $h \in H$ tal que $y = xh \Rightarrow x^{-1}y = h \Rightarrow x^{-1}y \in x^{-1}Hx \Rightarrow x^{-1}y = x^{-1}h_2x$, onde $h_2 \in H, \Rightarrow y = h_2x \Rightarrow y \in Hx$. Logo, $xH \subset Hx$.
- Seja $y \in Hx$. Existe $h_3 \in H$ tal que $y = h_3x \Rightarrow yx^{-1} = h_3 \in H \Rightarrow yx^{-1} \in xHx^{-1} \Rightarrow yx^{-1} = xh_4x^{-1}$ onde $h_4 \in H \Rightarrow y = xh_4 \Rightarrow y \in xH$. Logo, $Hx \subset xH$.

Fica mostrado então que $xH \subset Hx$ e $Hx \subset xH \Rightarrow xH = Hx, \forall x \in G \Rightarrow H \lhd G$.

B3) Sejam M e N subgrupos normais em um grupo G tais que $M \cap N = \{e\}$. Mostre que $xy = yx, \forall x \in M$ e $\forall y \in N$.

Solução: Em um grupo multiplicativo, mostrar que dois elementos a e b são iguais é o mesmo que mostrar que ab^{-1} é igual ao elemento neutro. Vamos calcular quanto é $(xy)(yx)^{-1} = (xy)(x^{-1}y^{-1})$.

- Como $M \lhd G$, temos $yMy^{-1} = M$ (ver ex. B1) o que implica $(y \underbrace{x^{-1}}_{\in M} y^{-1}) \in M$
- Como $N \lhd G$, temos $xNx^{-1} = N$ o que implica $(x \underbrace{y}_{\in N} x^{-1}) \in N$
- $(\underbrace{x}_{\in M} \underbrace{yx^{-1}y^{-1}}_{\in M}) \in M$ e $(\underbrace{xyx^{-1}}_{\in N} \underbrace{y^{-1}}_{\in N}) \in N \Rightarrow xyx^{-1}y^{-1} \in M \cap N = \{e\} \Rightarrow xyx^{-1}y^{-1} = e$

Fica mostrado dessa forma que $(xy)(yx)^{-1} = e$, ou seja, $xy = yx, \forall x \in M, \forall y \in N$.

B4) Sejam H um subgrupo normal em um grupo G e $N \lhd G$. Mostre que $N \lhd H$ e $H/N \lhd G/N$.

Solução:

- Suponhamos $N \lhd G$. Então, $xN = Nx, \forall x \in G$ e, em particular, $xN = Nx, \forall x \in H$. Logo, $N \lhd H$.
- Seja hN um elemento qualquer de H/N e gN um elemento qualquer de G/N. Temos que $(gN)^{-1}(hN)(gN) = (g^{-1}N)(hN)(gN) = (\underbrace{g^{-1}hg}_{\in H \text{ porque } H \lhd G})N \in H/N$. Isso mostra que $(gN)^{-1}(G/N)(gN) \subset G/N$ e, pelo exercício B2, temos que $H/N \lhd G/N$.

C1) Suponhamos N subgrupo de H e H subgrupo de G. Mostre que se $N \lhd G$, então $\dfrac{G/N}{H/N} \simeq G/H$. (*Sugestão: considere o homomorfismo* $\varphi : G/N \longrightarrow G/H$ *definido por* $\varphi(xN) = xH$).

Solução: Seja $\varphi : G/N \longrightarrow G/H, \varphi(xN) = xH$. Temos:

- Para quaisquer $aN, bN \in G/N$, $\varphi((aN)(bN)) = \varphi((ab)N) = (ab)H = (aH)(bH) = \varphi(aN)\varphi(bN)$. Logo, φ é um homomorfismo de grupos.
- Vamos calcular o núcleo de φ. Se $aN \in G/N$ for tal que $\varphi(aN) = H =$ elemento neutro de $G/H \Rightarrow aH = H \Rightarrow a \in H$. Logo, $N(\varphi) = \{aN \mid a \in H\} = H/N$.
- Dado $aH \in G/H =$ contradomínio de φ, considerando $aN \in G/N =$ domínio de φ, temos que $\varphi(aN) = aH$. Logo, φ é uma função sobrejetora.

Usando o Teorema do Homomorfismo para a função φ, temos que $\frac{G/N}{N(\varphi)} \simeq \text{Im}(\varphi)$ o que implica

$$\frac{G/N}{H/N} \simeq G/H.$$

Observação. O grupo-quociente G/N também pode ser denotado na forma $\frac{G}{N}$.

Capítulo 6

Anéis, subanéis, anéis de integridade, corpos

A1) Sejam $A = \mathbb{Z}\times\mathbb{Z}$, $(a,b)\oplus(c,d) = (a+c, b+d)$, $(a,b)\otimes(c,d) = (ac-bd, ad+bc)$, onde $a,b,c,d \in \mathbb{Z}$. Mostre que $(A,\oplus,\otimes)$ é um anel, verifique se é comutativo e se tem unidade.

Solução: Sejam $(a,b),(c,d),(e,f)$ três elementos genéricos de A. Temos que:

- $(a,b)\oplus(c,d) = (a+c,b+d) = (c+a,d+b) = (c,d)\oplus(a,b)$; logo, $\oplus$ é comutativa.
- $[(a,b)\oplus(c,d)]\oplus(e,f) = (a+c,b+d)\oplus(e,f) = ((a+c)+e,(b+d)+f) = (a+(c+e),b+(d+f)) = (a,b)\oplus(c+e,d+f) = (a,b)\oplus[(c,d)\oplus(e,f)]$; logo, $\oplus$ é associativa.
- $(a,b)\oplus(0,0) = (a+0,b+0) = (a,b)$; logo, $\oplus$ tem elemento neutro $(0,0)$.
- $(a,b)\oplus(-a,-b) = (a+(-a),b+(-b)) = (0,0)$; logo, todo elemento (a,b) possui um inverso aditivo $(-a,-b)$.
- $[(a,b)\otimes(c,d)]\otimes(e,f) = (ac-bd,ad+bc)\otimes(e,f) = ((ac-bd)e-(ad+bc)f,\ (ac-bd)f+(ad+bc)e) =$ $\boxed{(ace - bde - adf - bcf,\quad acf - bdf + ade + bce)}$
  e
  $(a,b)\otimes[(c,d)\otimes(e,f)] = (a,b)\otimes(ce-df,cf+ed) = (a(ce-df)-b(cf+ed), a(cf+ed)+b(ce-df)) =$ $\boxed{(ace-adf- bcf - bed,\ acf+aed + bce - bdf)}$ Logo, $[(a,b)\otimes(c,d)]\otimes(e,f) = (a,b)\otimes[(c,d)\otimes(e,f)]$ o que significa que $\otimes$ é associativa.
- $(a,b)\otimes(c,d) = (ac-bd,ad+bc) = (ca-db,cb+da) = (c,d)\otimes(a,b)$; logo, $\otimes$ é comutativa.
- $(a,b)\otimes[(c,d)\oplus(e,f)] = (a,b)\otimes(c+e,d+f) = (a(c+e)-b(d+f), a(d+f)+b(c+e)) = (ac+ae-bd-bf,\ ad+af+bc+be)$
  e
  $(a,b)\otimes(c,d)\oplus(a,b)\otimes(e,f) = (ac-bd,ad+bc)\oplus(ae-bf,af+be) = (ac-bd+ae-bf,\ ad+bc+af+be)$. Logo, $(a,b)\otimes[(c,d)\oplus(e,f)] =$

$(a,b) \otimes (c,d) \oplus (a,b) \otimes (e,f)$. Como $\otimes$ é comutativa, temos também que $[(c,d) \oplus (e,f)] \otimes (a,b) = (a,b) \otimes [(c,d) \oplus (e,f)] = (a,b) \otimes (c,d) \oplus (a,b) \otimes (e,f) = (c,d) \otimes (a,b) \oplus (e,f) \otimes (a,b)$. Portanto, $\otimes$ é distributiva com relação a $\oplus$.

- $(a,b) \otimes (1,0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a - 0, 0 + b) = (a,b)$. Logo, $\otimes$ tem elemento neutro (unidade) que é o $(1,0)$.

Todos os itens anteriores juntos mostram que $(A, \oplus, \otimes)$ é um anel comutativo com unidade.

Observação. As operações $\oplus$ e $\otimes$ definidas entre (a,b) e (c,d) neste exercício são semelhantes às que são definidas nos números complexos $a + bi$ e $c + di$. Veja os seguintes exemplos:

- Em A temos:
  - $(1,2) \oplus (3,4) = (1 + 3, 2 + 4) = (4,6)$
  - $(1,2) \otimes (3,4) = (1 \cdot 3 - 2 \cdot 4, 1 \cdot 4 + 2 \cdot 3) = (-5, 10)$
- Em $\mathbb{C}$ temos:
  - $(1 + 2i) + (3 + 4i) = (1 + 3) + (2 + 4)i = 4 + 6i$
  - $(1 + 2i)(3 + 4i) = 1 \cdot 3 + 1 \cdot 4i + 3 \cdot 2i + 8i^2 = 3 + 4i + 6i - 8 = -5 + 10i$.

A2) Seja $\mathcal{F} = \{f : \mathbb{R} \longrightarrow \mathbb{R} \mid f \text{ é contínua } \}$ e $+, \cdot, \circ$ as seguintes operações:

- $(f + g)(x) = f(x) + g(x)$
- $(f \cdot g)(x) = f(x) \cdot g(x)$
- $(f \circ g)(x) = f(g(x))$

a) Mostre que $(\mathcal{F}, +, \cdot)$ é um anel comutativo, com unidade, mas que não é de integridade;

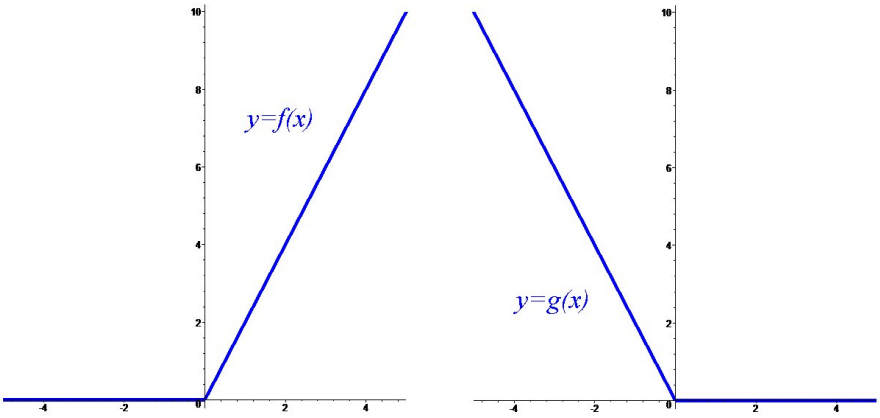
b) Mostre que $(\mathcal{F}, +, \circ)$ não é um anel.

Solução:

a) Sejam f, g e h três funções contínuas de $\mathbb{R}$ em $\mathbb{R}$, elementos genéricos de $\mathcal{F}$. Temos que as seguintes propriedades são válidas:
  - $f(x) + g(x) = g(x) + f(x)$, $\forall x \in \mathbb{R}$
  - $(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x))$, $\forall x \in \mathbb{R}$
  - $f(x) + O(x) = f(x)$, $\forall x \in \mathbb{R}$, onde $O(x)$ representa a função nula: $O(x) = 0$.

- $f(x) + (-f(x)) = O(x)$, $\forall x \in \mathbb{R}$
- $(f(x) \cdot g(x)) \cdot h(x) = f(x) \cdot (g(x) \cdot h(x))$, $\forall x \in \mathbb{R}$
- $f(x) \cdot (g(x) + h(x)) = f(x) \cdot g(x) + f(x) \cdot h(x)$ e $(f(x) + g(x)) \cdot h(x) = f(x) \cdot h(x) + g(x) \cdot h(x)$, $\forall x \in \mathbb{R}$
- $f(x) \cdot g(x) = g(x) \cdot f(x)$, $\forall x \in \mathbb{R}$
- $f(x) \cdot I(x) = f(x)$, $\forall x \in \mathbb{R}$, onde $I(x)$ é a função constante 1: $I(x) = 1$.

Logo, $(\mathcal{F}, +, \cdot)$ é um anel comutativo com unidade. Para mostrar que $\mathcal{F}$ não é anel de integridade, devemos mostrar exemplos de duas funções contínuas não nulas cujo produto é nulo. Por exemplo, sejam $f, g : \mathbb{R} \longrightarrow \mathbb{R}$ definidas por $f(x) = |x| + x$ e $g(x) = |x| - x$. Veja gráficos a seguir.



Temos que f e g não são funções nulas, mas $(f \cdot g)(x) = f(x) \cdot g(x) = (|x| + x)(|x| - x) = |x|^2 - x^2 = x^2 - x^2 = 0$, $\forall x \in \mathbb{R}$.

b) Para mostrar que $(\mathcal{F}, +, \circ)$ não é um anel, basta encontrar exemplos de funções em que falhe alguma das propriedades de anel. Por exemplo, consideremos $f : \mathbb{R} \longrightarrow \mathbb{R}$, $g : \mathbb{R} \longrightarrow \mathbb{R}$ e $h : \mathbb{R} \longrightarrow \mathbb{R}$ definidas por $f(x) = x^2$, $g(x) = 3x$ e $h(x) = x + 1$. Temos que:

1. $(f \circ (g + h))(x) = (f(g + h))(x) = f(3x + x + 1) = f(4x + 1) = (4x + 1)^2 = 16x^2 + 8x + 1$,
2. $(f \circ g + f \circ h)(x) = (f \circ g)(x) + (f \circ h)(x) = f(g(x)) + f(h(x)) = f(3x) + f(x+1) = (3x)^2 + (x + 1)^2 = 10x^2 + 2x + 1$.

Logo, $f \circ (g + h) \neq f \circ g + f \circ h$. Isso significa que a "multiplicação" $\circ$ não é distributiva com relação à adição $+$ definidas no conjunto $\mathcal{F}$, e, consequente, ele não é um anel.

A3) Verifique se os conjuntos A a seguir são subanéis de $(\mathbb{Q}, +, \cdot)$:

a) $3\mathbb{Z}$

b) $\mathbb{Q} - \mathbb{Z}$

c) $\{m + \frac{1}{5}n \,|\, m, n \in \mathbb{Z}\}$

d) $\{-1, 0, 1\}$

Solução:

a) O subconjunto $3\mathbb{Z} \subset \mathbb{Q}$ é formado por todos os múltiplos de 3. É claro que ele não é vazio porque, por exemplo, $3 \in 3\mathbb{Z}$. Sejam $x, y \in 3\mathbb{Z}$. Então existem $m, n \in \mathbb{Z}$ tais que $x = 3m$ e $y = 3n$. Daí, $x - y = 3m - 3n = 3(m - n) \in 3\mathbb{Z}$ e $x \cdot y = (3m)(3n) = 9mn = 3(3mn) \in 3\mathbb{Z}$. Logo, $3\mathbb{Z}$ é um subanel de $\mathbb{Q}$.

b) $A = \mathbb{Q} - \mathbb{Z}$ é formado pelos números racionais que não são inteiros, ou seja, formado pelas frações $p/q \in \mathbb{Q}$ tais que $p/q \notin \mathbb{Z}$. Por exemplo, $3/2 \in A$ e $1/2 \in A$, mas $3/2 - 1/2 = 1 \notin A$. Logo, A não é fechado com relação à subtração, de onde concluímos que A não é subanel de $\mathbb{Q}$.

c) Seja $A = \{m + \frac{1}{5}n \,|\, m, n \in \mathbb{Z}\}$. Escolhendo (aleatoriamente) $m = n = 1$ e, depois, $m = 0, n = 2$ temos que $x = 1 + \frac{1}{5} \cdot 1 = \frac{6}{5}$ e $y = 0 + \frac{1}{5} \cdot 2 = \frac{2}{5}$ são dois elementos de A. No entanto, $x \cdot y = \frac{6}{5} \cdot \frac{2}{5} = \frac{12}{25}$. Se esse último elemento pertencesse a A, existiriam $m, n \in \mathbb{Z}$ tais que $\frac{12}{25} = m + \frac{1}{5}n \Rightarrow 12 = 25m + 5n$ o que é um absurdo porque 12 não é múltiplo de 5 enquanto que $25m + 5n = 5(5m + n)$ é múltiplo de 5. Concluímos dessa forma que $\frac{12}{25} \notin A$ e, consequentemente, A não é subanel de $\mathbb{Q}$.

d) Se $A = \{-1, 0, 1\}$, escolhendo $x = 1$ e $y = -1$ temos que $x - y = 2 \notin A$. Logo, A não é subanel de $\mathbb{Q}$.

A4) Seja A um anel. Mostre que:

a) Se $(\alpha + \beta)^2 = \alpha^2 + 2\alpha\beta + \beta^2$ para quaisquer $\alpha, \beta \in A$, então A é um anel comutativo.

b) Dê exemplo de um anel A e elementos $\alpha, \beta \in A$ tais que $(\alpha+\beta)^2 \neq \alpha^2+2\alpha\beta+\beta^2$.

Solução:

a) Usando a propriedade distributiva da multiplicação com relação à adição temos que se α e β são dois elementos genéricos de um anel A, então $(\alpha + \beta)^2 = (\alpha + \beta)(\alpha + \beta) = \alpha(\alpha + \beta) + \beta(\alpha + \beta) = \alpha^2 + \alpha\beta + \beta\alpha + \beta^2$. Utilizamos também a propriedade associativa da adição para poder retirarmos os parênteses da expressão. Se no anel A é válido também que $(\alpha+\beta)^2 = \alpha^2+2\alpha\beta+\beta^2$, então

temos que $\alpha^2+2\alpha\beta+\beta^2 = \alpha^2+\alpha\beta+\beta\alpha+\beta^2$. Somando-se $(-\alpha^2)$, $(-\beta^2)$ e $(-\alpha\beta)$ a ambos os membros e simplificando, obtemos: $\alpha\beta = \beta\alpha$, de onde podemos concluir que o anel é comutativo.

b) Basta escolher dois elementos que não comutem em um anel A que não seja comutativo. Por exemplo, sejam $A = M_{2\times2}(\mathbb{R})$, $\alpha = \begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix} \in A$ e $\beta = \begin{bmatrix} 0 & 1 \\ 1 & 3 \end{bmatrix} \in A$. Temos $\alpha^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\alpha\beta = \begin{bmatrix} 2 & 7 \\ -1 & -3 \end{bmatrix}$, $\beta^2 = \begin{bmatrix} 1 & 3 \\ 3 & 10 \end{bmatrix}$, $\alpha+\beta = \begin{bmatrix} 1 & 3 \\ 1 & 2 \end{bmatrix}$ o que implica em $(\alpha+\beta)^2 = \begin{bmatrix} 4 & 9 \\ 3 & 7 \end{bmatrix}$ e $\alpha^2+2\alpha\beta+\beta^2 = \begin{bmatrix} 6 & 17 \\ 1 & 5 \end{bmatrix}$, de onde podemos observar que $(\alpha+\beta)^2 \neq \alpha^2+2\alpha\beta+\beta^2$.

A5) Verifique se $(S,+,\cdot)$ é um subcorpo de $(\mathbb{R},+,\cdot)$ em cada um dos seguintes casos:

a) $S = \{a+b\sqrt{3} \mid a,b \in \mathbb{Z}\}$

b) $S = \{a\sqrt{2}+b\sqrt{3} \mid a,b \in \mathbb{Q}\}$

c) $S = \{a+b\sqrt[3]{3} \mid a,b \in \mathbb{Q}\}$

(OBS.: S é um subcorpo de K quando ambos são corpos e $S \subset K$)

Solução:

a) consideremos um elemento de S e vamos verificar se esse elemento tem inverso multiplicativo em S. Por exemplo, seja $x = \sqrt{3} \in S$. Temos que $x^{-1} = \frac{1}{\sqrt{3}} = \frac{\sqrt{3}}{3} = \frac{1}{3}\sqrt{3} \notin S$ (porque $\frac{1}{3} \notin \mathbb{Z}$) $\Rightarrow S$ não é subcorpo de $\mathbb{R}$.

b) Para o conjunto ser um subcorpo, entre outras propriedades, ele precisa ser fechado para a multiplicação. Escolhendo-se $a = 1$, $b = 0$ e depois $a = 2$, $b = 0$, obtemos que $x = \sqrt{2}$ e $y = 2\sqrt{2}$ são dois elementos de S. Como $x \cdot y = \sqrt{2} \cdot 2\sqrt{2} = 4 \notin S$, temos que S não é subcorpo de $\mathbb{R}$.

c) Seja $x = \sqrt[3]{3} \in S$. Temos que $x^{-1} = \frac{1}{\sqrt[3]{3}} = \frac{\sqrt[3]{3^2}}{\sqrt[3]{3}\sqrt[3]{3^2}} = \frac{\sqrt[3]{9}}{3} \notin S$. Logo, S não é um subcorpo de $\mathbb{R}$.

A6) Mostre que:

a) $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ é um subcorpo de $\mathbb{R}$;

b) Existe uma infinidade de corpos $\mathbb{K}$ tais que $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{R}$.

Solução:

a) Escolhendo $a = b = 1$ temos que $1 + \sqrt{2} \in \mathbb{Q}[\sqrt{2}] \Rightarrow \mathbb{Q}[\sqrt{2}] \neq \emptyset$. Sejam $x = a + b\sqrt{2}$ e $y = c + d\sqrt{2}$ dois elementos genéricos de $\mathbb{Q}[\sqrt{2}]$. Temos que:

- $x - y = (a + b\sqrt{2}) - (c + d\sqrt{2}) = \underbrace{(a - c)}_{\in\mathbb{Q}} + \underbrace{(b - d)}_{\in\mathbb{Q}}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$
- $x \cdot y = (a + b\sqrt{2})(c + d\sqrt{2}) = \underbrace{(ac + 2bd)}_{\in\mathbb{Q}} + \underbrace{(ad + bc)}_{\in\mathbb{Q}}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

Fica mostrado dessa forma que $\mathbb{Q}[\sqrt{2}]$ é um subanel de $\mathbb{R}$. Para ser subcorpo, faltam ainda outras propriedades:

- Escolhendo $a = 1$ e $b = 0$ temos que $1 = 1 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}] \Rightarrow \mathbb{Q}[\sqrt{2}]$ tem unidade
- $x \cdot y = (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$ e $y \cdot x = (c + d\sqrt{2})(a + b\sqrt{2}) = (ca + 2db) + (da + cb)\sqrt{2} \Rightarrow x \cdot y = y \cdot x \Rightarrow \mathbb{Q}[\sqrt{2}]$ é comutativo
- Seja $x = m + n\sqrt{2}$ um elemento não nulo de $\mathbb{Q}[\sqrt{2}]$. O inverso multiplicativo x^{-1} é igual a $\frac{1}{m+n\sqrt{2}} = \frac{m-n\sqrt{2}}{(m+n\sqrt{2})(m-n\sqrt{2})} = \underbrace{\frac{m}{m^2-2n^2}}_{\in\mathbb{Q}} + \underbrace{\frac{-n}{m^2-2n^2}}_{\in\mathbb{Q}}\sqrt{2}$ que é um elemento de $\mathbb{Q}[\sqrt{2}]$.

b) De modo semelhante ao que foi feito no item (a), podemos mostrar que se p for um primo positivo, $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} \,|\, a, b \in \mathbb{Q}\}$ é um subcorpo de $\mathbb{R}$. Obtemos, dessa forma, uma infinidade de corpos $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{7}]$, $\cdots$ todos contidos em $\mathbb{R}$ e contendo o conjunto $\mathbb{Q}$.

A7) Dê exemplo de um anel A e um subanel B tais que:

a) $\exists 1_A, \exists 1_B$ mas $1_A \neq 1_A$;

b) $\exists 1_A$, mas $\nexists 1_B$.

Solução:

a) Consideremos $A = M_{2\times 2}\mathbb{R}$ e $B = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} | a \in \mathbb{R} \right\}$. Temos que B é um subanel de A, $1_A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $1_B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ e $1_A \neq 1_B$.

b) Sejam $B = 2\mathbb{Z}$ = inteiros pares e $A = \mathbb{Z}$ com as operações de adição e multiplicação usuais. Temos que B é subanel de A, existe $1_A = 1 \in \mathbb{Z}$, mas não existe 1_B.

A8) Mostre detalhadamente que se A for um anel de integridade e $a \in A$ for tal que $a^2 = 1$, então $a = 1$ ou $a = -1$.

Solução: Se $a^2 = 1$, então somando-se (-1) a ambos os membros, obtemos: $a^2 + (-1) = 1 + (-1) \Rightarrow a^2 - 1 = 0$. Como $(a+1)(a-1) = a^2 + a - a - 1 = a^2 - 1$, temos que $(a+1)(a-1) = 0$. Como A é um anel de integridade, temos $a + 1 = 0$ ou $a - 1 = 0$. Somando-se (-1) e 1 às igualdades anteriores, concluímos que $a = -1$ ou $a = 1$.

A9) Mostre detalhadamente que se A for um anel de integridade e $a \in A$ for tal que $a^2 = a$, então $a = 0$ ou $a = 1$.

Solução: Se $a^2 = a$, então somando-se $(-a)$ a ambos os membros, obtemos: $a^2 + (-a) = a + (-a) \Rightarrow a^2 - a = 0 \Rightarrow a(a-1) = 0$. Como A é um anel de integridade, temos $a = 0$ ou $a - 1 = 0$. Somando-se 1 à igualdade anterior, concluímos que $a = 0$ ou $a = 1$.

A10) Em um anel A, um elemento $x \in A$ é denominado *nilpotente* quando existir $n \in \mathbb{N}$ tal que $x^n = 0$. Mostre que o único elemento nilpotente de um anel de integridade é o zero.

Solução: Suponhamos x um elemento nilpotente de um anel A.

- Se $x^n = 0$, onde $x \in A$ e $n \in \mathbb{N}$, então não podemos ter $n = 0$ porque, se assim fosse, a potência x^n não seria igual a 0.
- Se $n = 1$, então $x^n = 0 \Rightarrow x = 0$.
- Se $n > 1$, então $x^n = 0 \Rightarrow \underbrace{x \cdot x \cdot x \cdot \cdots \cdot x}_{n \text{ fatores}} = 0$. Como A é um anel de integridade, temos $x = 0$.

Observação. Sendo A um anel de integridade, se $x_1, x_2 \in A$ são tais que $x_1 \cdot x_2 = 0$, então $x_1 = 0$ ou $x_2 = 0$. Isso pode ser generalizado (por Indução) para uma

quantidade de k fatores, com $k > 1$: se $x_i \in A$, com $i \in \{1, 2, \cdots, k\}$ são tais que $x_1 \cdot x_2 \cdot \cdots \cdot x_k = 0$, então existe $j \in \{1, 2, \cdots, k\}$ tal que $x_j = 0$.

A11) No corpo Z_{11}, resolva:

a) a equação $x^3 = x$;

b) o sistema de equações $\begin{cases} \bar{2}x + \bar{3}y &= \bar{1} \\ \bar{5}x - \bar{2}y &= \bar{8} \end{cases}$

Solução:

a) Como 11 é primo, $\mathbb{Z}_{11}$ é um corpo. Logo, podemos usar as propriedades (comutativa, distributiva, etc.) da adição e multiplicação para escrever a equação na seguinte forma: $x^3 = x \Rightarrow x^3 - x = \bar{0} \Rightarrow x(x^2 - \bar{1}) = \bar{0} \Rightarrow x(x + \bar{1})(x - \bar{1}) = \bar{0}$. Como $\mathbb{Z}_{11}$ é um anel de integridade, temos que $x = \bar{0}$ ou $x + \bar{1} = \bar{0}$ ou $x - \bar{1} = \bar{0}$, ou seja, $x = \bar{0}$ ou $x = -\bar{1} = \overline{10}$ ou $x = \bar{1}$. Logo, o conjunto-solução da equação é $S = \{\bar{0}, \bar{1}, \overline{10}\}$.

b) Multiplicando-se a primeira equação por $\bar{2}$, a segunda por $\bar{3}$ e somando-se as duas equações, podemos eliminar a variável y:
$\begin{cases} \bar{4}x + \bar{6}y &= \bar{2} \\ \bar{15}x - \bar{6}y &= \bar{24} \end{cases} \Rightarrow \begin{cases} \bar{4}x + \bar{6}y &= \bar{2} \\ \bar{4}x - \bar{6}y &= \bar{2} \end{cases} \Rightarrow (\bar{4}x + \bar{6}y) + (\bar{4}x - \bar{6}y) = \bar{2} + \bar{2}$
$\Rightarrow \bar{8}x = \bar{4} \Rightarrow x = (\bar{8})^{-1} \cdot \bar{4}$. Como $\bar{8} \cdot \bar{7} = \overline{56} = \bar{1}$, temos que $(\bar{8})^{-1} = \bar{7}$. Daí, $x = \bar{7} \cdot \bar{4} = \overline{28} = \bar{6}$. Substituindo-se $x = \bar{6}$ na primeira equação do sistema, obtemos: $\bar{2} \cdot \bar{6} + \bar{3}y = \bar{1} \Rightarrow \bar{3}y = \bar{1} - \overline{12} \Rightarrow \bar{3}y = -\overline{11} = \bar{0} \Rightarrow y = (\bar{3})^{-1} \cdot \bar{0} \Rightarrow y = \bar{0}$. Portanto, a solução do sistema é $x = \bar{6}$, $y = \bar{0}$.

A12) Determine todos os divisores de zero do anel $\mathbb{Z}_{15}$.

Solução: $\bar{a}$ e $\bar{b}$ são divisores de zero de $\mathbb{Z}_{15}$ se eles forem não nulos e $\bar{a} \cdot \bar{b} = \bar{0}$, ou seja, $\overline{a \cdot b} = \bar{0} \Rightarrow a \cdot b$ é um múltiplo de 15 $\Rightarrow a, b \in \{3, 5, 6, 9, 10, 12\}$, um conjunto formado por divisores de 15 e seus múltiplos maiores do que 1 e menores do que 15. Portanto, os divisores de zero de $\mathbb{Z}_{15}$ são $\bar{3}$, $\bar{5}$, $\bar{6}$, $\bar{9}$, $\overline{10}$, $\overline{12}$.

B1) Seja A um anel no qual $x^2 = x$ para todo $x \in A$. Mostre que $x = -x$ para todo $x \in A$. (*Sugestão: calcule* $(x + x)^2$.)

Solução: Em um anel A, se $a, b \in A$, então $(a + b)^2 = (a + b)(a + b) = a(a+b) + b(a+b) = a^2 + ab + ba + b^2$. Se $a = b = x$, então $(x+x)^2 = x^2 + x \cdot x + x \cdot x + x^2 =$

$x^2+x^2+x^2+x^2 = x+x+x+x$. Por outro lado, $(x+x)^2 = x+x$. Logo, $x+x = x+x+x+x$. Somando-se $(-x)+(-x)+(-x)$ aos dois membros dessa última igualdade, obtemos: $(-x)+x+(-x)+x+(-x) = (-x)+x+(-x)+x+(-x)+x+x \Rightarrow -x = x$ para todo $x \in A$.

Observação. Note que utilizamos as propriedades associativa da adição e distributiva da multiplicação com relação à adição no desenvolvimento acima.

B2) Seja A um anel no qual $x^2 = x$ para todo $x \in A$. Mostre que A é um anel comutativo. (*Sugestão: calcule* $(x+y)^2$.)

Solução: Como $(x+y)^2 = x^2+xy+yx+y^2$, temos que $(x+y)^2 = x+xy+yx+y$. Por outro lado, $(x+y)^2 = x+y$ e daí $x+xy+yx+y = x+y$. Somando-se $(-x)+(-y)$ aos dois membros da última igualdade, obtemos: $x+(-x)+xy+yx+y+(-y) = x+(-x)+y+(-y)$, ou seja, $xy+yx = 0$. Usando o exercício B1, temos $yx = -yx$. Portanto, $xy-yx = 0$ de onde obtemos que $xy = yx$ para quaisquer $x, y \in A$, ou seja, o anel A é comutativo.

B3) No anel $\mathbb{Z}_8$, determine todas as soluções da equação $x^2 - \bar{1} = \bar{0}$.

Solução: Em todo anel comutativo, é válido o seguinte *produto notável*: $(a+b)(a-b) = a^2-b^2$. Logo, a equação dada pode ser escrita na forma $(x+\bar{1})(x-\bar{1}) = \bar{0}$. Portanto, duas soluções são obtidas quando $x+\bar{1} = \bar{0}$ ou quando $x-\bar{1} = \bar{0}$, ou seja, quando $x = -\bar{1} = \bar{7}$ ou $x = \bar{1}$. Em um anel de integridade, essas seriam as únicas soluções. Mas $\mathbb{Z}_8$ não é anel de integridade porque seus divisores de zero são $\bar{2}$, $\bar{4}$ e $\bar{6}$. Logo, também podemos obter soluções da equação dada quando $x+\bar{1}$ ou $x-\bar{1}$ coincidem com esses divisores de zero. Dessa forma, obtemos as seguintes possíveis soluções:

- $x+\bar{1} = \bar{2} \Rightarrow x = \bar{1}$
- $x+\bar{1} = \bar{4} \Rightarrow x = \bar{3}$
- $x+\bar{1} = \bar{6} \Rightarrow x = \bar{5}$
- $x-\bar{1} = \bar{2} \Rightarrow x = \bar{3}$
- $x-\bar{1} = \bar{4} \Rightarrow x = \bar{5}$
- $x-\bar{1} = \bar{6} \Rightarrow x = \bar{7}$

Por substituição direta na equação, podemos verificar que $x = \bar{3}$ não é uma raiz da equação, enquanto que $\bar{1}$, $\bar{5}$ e $\bar{7}$ são raízes. Portanto, o conjunto-solução da equação $x^2 - \bar{1} = \bar{0}$ é $S = \{\bar{1}, \bar{5}, \bar{7}\}$.

B4) No corpo $\mathbb{Z}_{101}$, determine o inverso multiplicativo do elemento $\overline{43}$.

Solução: Como 101 é primo, o mdc$(101, 43) = 1$. Logo, existem $a, b \in \mathbb{Z}$ tais que $101a + 43b = 1$. Para calcular a e b, podemos usar o método das divisões sucessivas para o cálculo do máximo divisor comum, dispostas no seguinte diagrama onde fizemos $x = 101$ e $y = 43$:

	2	2	1	6	2
x	y	15	13	2	1
15	13	2	1	0	

Observando as divisões indicadas nesse diagrama, temos:

(a) $x = 2 \cdot y + \boxed{15}$

(b) $y = 2 \cdot \boxed{15} + 13$

(c) $15 = 1 \cdot 13 + 2$

(d) $13 = 6 \cdot 2 + 1$

Do item (a), temos que $15 = x - 2y$ que substituído em (b) fornece $y = 2 \cdot (x - 2y) + 13$, ou seja, $y = 2x - 4y + 13 \Rightarrow 5y - 2x = 13$. Do item (c), temos $2 = 15 - 13$ que substituindo em (d) fornece $13 = 6 \cdot (15 - 13) + 1$ que é equivalente a $7 \cdot 13 - 6 \cdot 15 = 1$, ou seja, $7(5y - 2x) - 6(x - 2y) = 1$ que equivale a $\underbrace{47}_{=b}\, y\, \underbrace{-20}_{=a}\, x = 1 \Rightarrow \overline{47y - 20x} = \bar{1} \Rightarrow \overline{47} \cdot \bar{y} - \underbrace{\overline{20} \cdot \bar{x}}_{=\bar{0}} = \bar{1} \Rightarrow \overline{47} \cdot \overline{43} = \bar{1}$ de onde concluímos que o inverso multiplicativo de $\overline{47}$ em $\mathbb{Z}_{101}$ é o elemento $\overline{43}$.

Capítulo 7

Homomorfismos de anéis, ideais, anéis-quocientes

A1) Consideremos o anel $A = \mathbb{Z}$ e o ideal $I = 4\mathbb{Z}$ = múltiplos de 4 (operações de adição e multiplicação usuais). Construa as tábuas de adição e multiplicação do anel-quociente A/I.

Solução: Temos que:

- $0 + I = \{\cdots, -12, -8, -4, 0, 4, 8, 12, \cdots\} = I$
- $1 + I = \{\cdots, -11, -7, -3, 1, 5, 9, 13, \cdots\}$
- $2 + I = \{\cdots, -10, -6, -2, 2, 6, 10, 14, \cdots\}$
- $3 + I = \{\cdots, -9, -5, -1, 3, 7, 11, 15, \cdots\}$
- $4 + I = \{\cdots, -8, -4, 0, 4, 8, 12, 16, \cdots\} = I$

Portanto, o anel-quociente de A por I é

$$A/I = \{I, 1 + I, 2 + I, 3 + I\}.$$

Alguns exemplos de adição entre seus elementos são $(2+I)+(1+I) = (2+1)+I = 3+I$ e $(2 + I) + (4 + I) = (2 + 4) + I = 6 + I = 2 + I$ e todas as possíveis adições entre seus elementos podem ser observadas na seguinte tábua:

$+$	I	$1 + I$	$2 + I$	$3 + I$
I	I	$1 + I$	$2 + I$	$3 + I$
$1 + I$	$1 + I$	$2 + I$	$3 + I$	I
$2 + I$	$2 + I$	$3 + I$	I	$1 + I$
$3 + I$	$3 + I$	I	$1 + I$	$2 + I$

Alguns exemplos de multiplicação entre seus elementos são $(2+I)\cdot I = (2+1)\cdot(0+I) = 2\cdot 0 + I = 0 + I = I$ e $(3+I)+(2+I) = (3\cdot 2) + I = 6 + I = 2 + I$ e todas as possíveis multiplicações entre seus elementos podem ser observadas na seguinte tábua:

$\cdot$	I	$1+I$	$2+I$	$3+I$
I	I	I	I	I
$1+I$	I	$1+I$	$2+I$	$3+I$
$2+I$	I	$2+I$	I	$2+I$
$3+I$	I	$3+I$	$2+I$	$1+I$

A2) Dê exemplo de um homomorfismo de anéis $f : A \longrightarrow B$ tal que $f(1_A) \neq 1_B$.

Solução: Sejam $A = B = \mathbb{Z}$. Então $1_A = 1_B = 1$. Consideremos a função nula $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, $f(x) = 0$, que é um homomorfismo de A em B. Como $f(1) = 0$, temos que $f(1_A) \neq 1_B$.

Observação. Esse tipo de exemplo só é possível quando a função f não for sobrejetora.

A3) Considere os anéis $A = (\mathbb{R}, +, \cdot)$ com operações usuais e $B = (\mathbb{R}, \oplus, \odot)$ onde $x \oplus y = x + y + 1$ e $x \odot y = x + y + xy$.

a) Mostre que $f : A \longrightarrow B$ definida por $f(x) = x - 1$ é um isomorfismo de anéis;

b) Mostre que $f : A \longrightarrow A$ definida por $f(x) = x - 1$ não é um isomorfismo de anéis.

Solução:

a) Sejam $x, y \in A$. Então:

- $f(x+y) = x+y-1$ e $f(x)\oplus f(y) = f(x)+f(y)+1 = (x-1)+(y-1)+1 = x+y-1$. Logo, $f(x + y) = f(x) \oplus f(y)$.
- $f(x\cdot y) = xy - 1$ e $f(x)\odot f(y) = f(x) + f(y) + f(x)f(y) = (x-1) + (y-1) + (x-1)(y-1) = x+y-2+xy-x-y+1 = xy-1$. Logo, $f(x\cdot y) = f(x)\odot f(y)$. Portanto, f é um homomorfismo de anéis.
- Suponhamos $f(x) = f(y)$. Então, $x-1 = y-1 \Rightarrow x = y$. Logo, f é injetora.
- Dado $y \in B = \mathbb{R}$, considerando $x = y + 1 \in A = \mathbb{R}$, temos: $f(x) = x - 1 = (y + 1) - 1 = y$. Logo, f é sobrejetora.

Ficou mostrado nos itens anteriores que f é um isomorfismo de anéis.

b) Com as operações usuais, o elemento neutro da adição de A é o 0. Como $f(0) = -1 \neq 0$ temos que f não é isomorfismo de anéis.

A4) Verifique se $(I, +, \cdot)$ é um ideal do anel $(A, +, \cdot)$ em cada um dos seguintes casos:

a) $I = \mathbb{Z}$, $A = \mathbb{Q}$;

b) $I = 3\mathbb{Z}$, $A = \mathbb{Z}$;

c) $I = 2\mathbb{Z}$, $A = \mathbb{Z}$ com as operações de adição usual de inteiros e multiplicação definida por $x \cdot y = 0$ para quaisquer $x, y \in \mathbb{Z}$.

d) $I =$ elementos de $\mathbb{Z}$ que são divisores de 100 e $A = \mathbb{Z}$.

e) $I = 3\mathbb{Z} \cup 7\mathbb{Z}$, $A = \mathbb{Z}$

f) $I = \{f : \mathbb{R} \longrightarrow \mathbb{R} \mid f(-1) = 0\}$, $A = \mathbb{R}^{\mathbb{R}}$.

g) $I = \{f : \mathbb{R} \longrightarrow \mathbb{R} \mid f(3) = f(4) = 0\}$, $A = \mathbb{R}^{\mathbb{R}}$.

h) $I = \{f : \mathbb{R} \longrightarrow \mathbb{R} \mid f(1) + f(2) = 0\}$, $A = \mathbb{R}^{\mathbb{R}}$

Solução:

a) Sejam $x = 1 \in I$ e $a = \frac{1}{3} \in A$. Como $a \cdot x = \frac{1}{3} \notin I$, temos que I não é ideal de A.

b) É claro que $I \neq \emptyset$ porque, por exemplo, $3 \in I$. Sejam $x, y \in I$. Então, $x = 3m$ e $y = 3n$ com $m, n \in \mathbb{Z}$. Daí, temos $x - y = 3m - 3n = 3(m - n) \in I$. Se $a \in \mathbb{Z}$, temos $a \cdot x = 3(am) \in I$. Logo, I é um ideal de A.

c) É claro que $I \neq \emptyset$ porque, por exemplo, $2 \in I$. Sejam $x, y \in I$. Então, $x = 2m$ e $y = 2n$ com $m, n \in \mathbb{Z}$. Daí, temos $x - y = 2m - 2n = 2(m - n) \in I$. Se $a \in \mathbb{Z}$, temos $a \cdot x = 0 \in I$. Logo, I é um ideal de A.

d) Dois divisores de 100 são $x = 5$ e $y = 10$. Como $x + y = 15$ não é divisor de 100, temos que I não é ideal de A.

e) I é formado pelos inteiros que são múltiplos de 3 ou múltiplos de 7. Dois elementos de I são $x = 3$ e $y = 14$. Como $x + y = 17 \notin I$ temos que I não é ideal de A.

f) A função nula pertence a I; logo, $I \neq \emptyset$. Se $f, g \in I$, então $f(-1) = 0$ e $g(-1) = 0$. Daí, $(f - g)(-1) = f(-1) - g(-1) = 0 - 0 = 0$; logo, $f - g \in I$. Se $h \in A$, então $(f \cdot h)(-1) = f(-1) \cdot h(-1) = 0 \cdot h(-1) = 0$. Logo, $f \cdot h \in I$. Portanto, I é um ideal de A.

g) A função nula pertence a I; logo, $I \neq \emptyset$. Se $f, g \in I$, então $f(3) = f(4) = g(3) = g(4) = 0$. Daí, $(f-g)(3) = f(3) - g(3) = 0 - 0 = 0$ e $(f-g)(4) = f(4) - g(4) = 0 - 0 = 0$; logo, $f - g \in I$. Se $h \in A$, então $(f \cdot h)(3) = f(3) \cdot h(3) = 0 \cdot h(3) = 0$ e $(f \cdot h)(4) = f(4) \cdot h(4) = 0 \cdot h(4) = 0$.. Logo, $f \cdot h \in I$. Portanto, I é um ideal de A.

h) Sejam $f(x) = -2x + 3$ e $h(x) = x$. Então, $f(1) + f(2) = 1 + (-1) = 0 \Rightarrow f \in I$ e $g(x) = h(x) \cdot f(x) = x(-2x + 3) = -2x^2 + 3x \Rightarrow g(1) + g(2) = 1 + (-2) = -1 \neq 0 \Rightarrow g = h \cdot f \notin I$. Logo, I não é ideal de A.

A5) Seja $A = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Mostre que se $f : A \longrightarrow A$ for um isomorfismo de anéis, então $f(\sqrt{2}) = \sqrt{2}$ ou $f(\sqrt{2}) = -\sqrt{2}$.

Solução: Se f for isomorfismo de anéis, então $f(1) = 1$ o que implica $f(2) = f(1+1) = f(1) + f(1) = 1 + 1 = 2$ e daí obtemos $2 = f(2) = f(\sqrt{2} \cdot \sqrt{2}) = f(\sqrt{2}) \cdot f(\sqrt{2}) = [f(\sqrt{2})]^2 \Rightarrow [f(\sqrt{2})]^2 = 2$ de onde concluímos que $f(\sqrt{2}) = \pm\sqrt{2}$.

A6) Verifique se $f : \mathbb{Q} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Q}$ tal que $f(x, y) = (y, x)$ é um isomorfismo de anéis.

Solução: Sejam $X = (a, b)$ e $Y = (c, d)$ dois elementos do domínio de f.

- $f(X + Y) = f((a, b) + (c, d)) = f(a + c, b + d) = (b + d, a + c) = (b, a) + (d, c) = f(a, b) + f(c, d) = f(X) + f(Y)$
- $f(X \cdot Y) = f((a, b) \cdot (c, d)) = f(ac, bd) = (bd, ac) = (b, a) \cdot (d, c) = f(a, b) \cdot f(c, d) = f(X) \cdot f(Y)$; logo, f é um homomorfismo de anéis.
- $f(X) = f(Y) \Rightarrow f(a, b) = f(c, d) \Rightarrow (b, a) = (d, c) \Rightarrow b = d$ e $a = c \Rightarrow (a, b) = (c, d) \Rightarrow X = Y$; logo, f é injetora
- Dado $W = (r, s) \in \mathbb{Z} \times \mathbb{Q}$, consideremos $Z = (s, r) \in \mathbb{Q} \times \mathbb{Z}$. Temos que $f(Z) = f(s, r) = (r, s) = W$; logo, f é sobrejetora.

Desse modo, fica mostrado que f é um isomorfismo de anéis.

A7) Sejam $\mathbb{K}$ um corpo e para cada $a \in \mathbb{K}$ considere a função $f_a : \mathbb{K} \longrightarrow \mathbb{K}$ tal que $f_a(x) = axa^{-1}$.

a) Mostre que f_a é um isomorfismo de anéis.

b) Se b for outro elemento de $\mathbb{K}$, então calcule a composta $f_a \circ f_b$.

Solução:

a) Sejam $x, y \in \mathbb{K}$. Temos:

- $f_a(x+y) = a(x+y)a^{-1} = (ax+ay)a^{-1} = axa^{-1} + aya^{-1} = f_a(x) + f_a(y)$
- $f_a(x \cdot y) = a(x \cdot y)a^{-1} = ax(a^{-1}a)ya^{-1} = (axa^{-1})(aya^{-1}) = f_a(x) \cdot f_a(y)$. Assim, este item, juntamente com o item anterior, mostra que f_a é um homomorfismo de anéis.
- Se $f_a(x) = f_a(y)$, então $axa^{-1} = aya^{-1}$. Multiplicando-se à esquerda por a^{-1} e à direita por a, obtemos $a^{-1}axa^{-1}a = a^{-1}aya^{-1}a \Rightarrow 1 \cdot x \cdot 1 = 1 \cdot y \cdot 1 \Rightarrow x = y$. Logo, f_a é injetora.
- Dado $s \in \mathbb{K}$ (contradomínio de f), seja $r = a^{-1}sa$ pertencente a $\mathbb{K}$ (domínio de f) temos que $f_a(r) = ara^{-1} = a(a-1sa)a^{-1} = 1 \cdot s \cdot 1 = s$. Logo, f_a é sobrejetora.

Fica mostrado dessa forma que f_a é um isomorfismo de $\mathbb{K}$ em $\mathbb{K}$.

b) Se $a, b, x \in \mathbb{K}$, então $(f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(b^{-1}a^{-1}) = (ab)x(ab)^{-1} = f_{ab}(x)$. Portanto, $f_a \circ f_b = f_{ab}$.

B1) Mostre que se $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ é um isomorfismo de anéis, então f é a função identidade.

Solução: Como f é um isomormorfismo, temos que f é um homomorfismo e $f(a+b) = f(a) + f(b)$ para quaisquer $a, b \in \mathbb{Z}$.

- Sendo f um homomorfismo, temos $f(0) = 0$
- Sendo f também sobrejetora, temos $f(1) = 1$
- $f(2) = f(1+1) = f(1) + f(1) = 1 + 1 = 2$
- $f(3) = f(2+1) = f(2) + f(1) = 2 + 1 = 3$
- $f(4) = f(3+1) = f(3) + f(1) = 3 + 1 = 4$, etc.
- Supondo $f(k) = k$, temos que $f(k+1) = f(k) + f(1) = k + 1$. Logo, por indução, $f(n) = n$ para todo $n \in \mathbb{N}$.
- Se $m \in \mathbb{Z}$ for tal que $m < 0$, então $-m \in \mathbb{N}$ e daí $f(-m) = -m$ pelo que foi mostrado no item anterior. Como $f(-m) + f(m) = f((-m) + m) = f(0) = 0$, temos que $f(-m) = -f(m) \Rightarrow -m = -f(m) \Rightarrow f(m) = m$.

Concluímos então que $f(x) = x$, $\forall x \in \mathbb{Z}$, ou seja, f é a função identidade em $\mathbb{Z}$.

B2) Seja $f : A \longrightarrow B$ um homomorfismo de anéis e P um ideal primo de B. Mostre que $f^{-1}(P)$ é um ideal primo de A.

Solução: Inicialmente, vamos mostrar que $f^{-1}(P)$ é um ideal de A. Depois, mostramos que é um ideal primo.

- Como $0 \in P$ e $f(0) = 0$ temos que $f^{-1}(P) \neq \emptyset$ porque $f^{-1}(P)$ contém pelo menos o elemento 0.
- Se $a, b \in f^{-1}(P)$, então $f(a), f(b) \in P \Rightarrow f(a) - f(b) \in P \Rightarrow f(a-b) \in P \Rightarrow a - b \in f^{-1}(P)$.
- Se $a \in f^{-1}(P)$ e $x \in A$, então $f(a) \in P$ e $f(x) \in B \Rightarrow f(a) \cdot f(x) \in P \Rightarrow f(a \cdot x) \in P \Rightarrow a \cdot x \in f^{-1}(P)$. Logo, $f^{-1}(P)$ é um ideal de A.
- Suponhamos $x, y \in A$ tais que $x \cdot y \in f^{-1}(P)$. Então, $f(x \cdot y) \in P \Rightarrow f(x) \cdot f(y) \in P$. Como P é primo, temos $f(x) \in P$ ou $f(y) \in P \Rightarrow x \in f^{-1}(P)$ ou $y \in f^{-1}(P)$. Logo, $f^{-1}(P)$ é um ideal primo de A.

B3) Mostre que $(2\mathbb{Z}, +, \cdot)$ e $(3\mathbb{Z}, +, \cdot)$ não são anéis isomorfos.

Solução: Suponhamos que exista um isomorfismo $f : 2\mathbb{Z} \longrightarrow 3\mathbb{Z}$. Então $f(2) = 3n$ para algum $n \in \mathbb{Z}$. Como $f(0) = 0$ e f é injetora, temos que $n \neq 0$. Usando o fato de que f é um homomorfismo de anéis, temos:

- $f(4) = f(2+2) = f(2) + f(2) = 3n + 3n = 6n$
- $f(4) = f(2 \cdot 2) = f(2) \cdot f(2) = (3n)(3n) = 9n^2$

o que implica em $6n = 9n^2 \Rightarrow 2 \cdot 3n = 3n \cdot 3n$. Como $3\mathbb{Z}$ é um anel de integridade e $3n \neq 0$, podemos cancelar o $3n$ nos dois membros da última igualdade de onde obtemos: $2 = 3n$. Essa última igualdade é um absurdo porque o segundo membro é um múltiplo de 3 e o primeiro membro não é. Portanto, não pode existir isomorfismo de $2\mathbb{Z}$ em $3\mathbb{Z}$.

B4) Verifique se $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ e $\mathbb{Q}[\sqrt{7}] = \{a + b\sqrt{7} \mid a, b \in \mathbb{Q}\}$ são anéis isomorfos (com as operações de adição e multiplicação usuais).

Solução: Suponhamos que exista um isomorfismo $f : \mathbb{Q}[\sqrt{5}] \longrightarrow \mathbb{Q}[\sqrt{7}]$.

Como f é um homomorfismo sobrejetor, temos $f(1) = 1$ o que implica em $f(5) = f(1+1+1+1+1) = f(1)+f(1)+f(1)+f(1)+f(1) = 1+1+1+1+1 = 5$. O elemento $\sqrt{5}$ é levado pela f para um elemento $a + b\sqrt{7}$ com $a, b \in \mathbb{Q}$, isto é, $f(\sqrt{5}) = a + b\sqrt{7}$. Elevando-se ao quadrado, obtemos: $[f(\sqrt{5})]^2 = (a + b\sqrt{7})^2 \Rightarrow f(\sqrt{5}) \cdot f(\sqrt{5}) = a^2 + 2ab\sqrt{7} + (\sqrt{7})^2 \Rightarrow f(\sqrt{5} \cdot \sqrt{5}) = a^2 + 2ab\sqrt{7} + 7 \Rightarrow f(5) = a^2 + 2ab\sqrt{7} + 7 \Rightarrow 5 = a^2 + 2ab\sqrt{7} + 7$

- Não podemos ter $a = 0$ porque isso implicaria $5 = 0 + 0 + 7$ que é absurdo.
- Não podemos ter $b = 0$ porque isso implicaria $5 = a^2 + 7 \Rightarrow a^2 = -2$ que é absurdo porque não existe número racional cujo quadrado seja igual a -2.
- Assim, $a \neq 0$ e $b \neq 0$ o que implica $ab \neq 0$.

Como $2ab\sqrt{7} = -a^2 - 2$, temos $\sqrt{7} = \frac{-a^2-2}{2ab}$ o que é absurdo porque $\sqrt{7}$ é irracional, enquanto que $\frac{-a^2-2}{2ab}$ é racional. Portanto, não pode existir isomorfismo f de $\mathbb{Q}[\sqrt{5}]$ em $\mathbb{Q}[\sqrt{7}]$

C1) Determine todos os possíveis isomorfismos do anel $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ nele mesmo.

Solução: Seja $f : \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}\times\mathbb{Z}$ um isomorfismo de anéis. Então, $f(0,0) = (0,0)$ e $f(1,1) = (1,1)$. Vamos calcular os valores de $f(0,1)$ e $f(1,0)$. Se esses valores forem conhecidos, a partir deles, podemos calcular todos os outros. Temos que:

- Suponhamos $f(0,1) = (a,b)$. Então, $(0,1) \cdot (0,1) = (0 \cdot 0, 1 \cdot 1) = (0,1) \Rightarrow f[(0,1)\cdot(0,1)] = f(0,1) \Rightarrow f(0,1)\cdot f(0,1) = f(0,1) \Rightarrow (a,b)\cdot(a,b) = (a,b) \Rightarrow (a^2, b^2) = (a,b) \Rightarrow a^2 = a$ e $b^2 = b \Rightarrow (\ a = 0$ ou $a = 1)$ e $(b = 0$ ou $b = 1) \Rightarrow f(0,1) = (0,1)$ ou $f(0,1) = (1,0)$. Note que, sendo f injetora, não podemos ter $f(0,1) = (0,0)$, nem $f(0,1) = (1,1)$.
- Suponhamos $f(1,0) = (c,d)$. Usando argumentos semelhantes aos do item anterior, a partir de $(1,0) \cdot (1,0) = (1,0)$, chegamos a $(c^2, d^2) = (c,d)$ o que implica em $f(1,0) = (0,1)$ ou $f(1,0) = (1,0)$.

Portanto, temos dois casos a considerar:

Caso 1: $f(0,1) = (0,1)$ e $f(1,0) = (1,0)$

- Neste caso, temos $f(0,2) = f[(0,1) + (0,1)] = f(0,1) + f(0,1) = (0,1) + (0,1) = (0,2)$, $f(0,3) = f[(0,2)+(0,1)] = f(0,2)+f(0,1) = (0,2)+(0,1) = (0,3)$, etc.
- Supondo $f(0,k) = (0,k)$, temos $f(0,k+1) = f[(0,k) + (0,1)] = f(0,k) + f(0,1) = (0,k) + (0,1) = (0,k+1)$. Logo, por indução, $f(0,n) = (0,n)$, $\forall n \in \mathbb{N}$.

- Se m for um inteiro negativo, então $-m$ é positivo e $f(0,-m) = (0,-m)$. Como $f(0,0) = (0,0)$, temos que $f[(0,m) + (0,-m)] = f(0,0) = (0,0) \Rightarrow f(0,m) + f(0,-m) = (0,0) \Rightarrow f(0,m) + (0,-m) = (0,0) \Rightarrow f(0,m) = -(0,-m) \Rightarrow f(0,m) = (0,m)$. Portanto, $f(0,y) = (0,y)$, $\forall y \in \mathbb{Z}$.
- A partir de $f(1,0) = (1,0)$, usando um cálculo semelhante ao item anterior, obtemos $f(2,0) = (2,0)$, $f(3,0) = (3,0)$, etc. e chegamos a $f(x,0) = (x,0)$, $\forall x \in \mathbb{Z}$.
- Portanto, $f(x,y) = f[(x,0) + (0,y)] = f(x,0) + f(0,y) = (x,0) + (0,y) \Rightarrow f(x,y) = (x,y)$.

Caso 2: $f(0,1) = (1,0)$ e $f(1,0) = (0,1)$

- Este caso é semelhante ao anterior: a partir de $f(0,1) = (1,0)$, calculamos $f(0,2) = (2,0)$, $f(0,3) = (3,0)$, etc. e chegamos a $f(0,y) = (y,0)$, $\forall y \in \mathbb{Z}$.
- A partir de $f(1,0) = (0,1)$, chegamos a $f(2,0) = (0,2)$, $f(3,0) = (0,3)$, etc. e chegamos a $f(x,0) = (0,x)$, $\forall x \in \mathbb{Z}$.
- Daí, $f(x,y) = f(x,0) + f(0,y) = (0,x) + (y,0) \Rightarrow f(x,y) = (y,x)$.

Portanto, as funções $f(x,y) = (y,x)$ e $g(x,y) = (x,y)$, sendo homomorfismos de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z} \times \mathbb{Z}$ e bijetoras, são os únicos isomorfismos de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z} \times \mathbb{Z}$.

Capítulo 8

Polinômios

A1) Determine A e B reais de modo que a igualdade

$$\frac{3x+1}{(x-2)(x+2)} = \frac{A}{x-2} + \frac{B}{x+2}$$

se verifique para todo $x \in \mathbb{R} - \{2, -2\}$.

Solução: Multiplicando-se os dois membros da igualdade por $(x-2)(x+2)$, obtemos $3x+1 = A(x+2) + B(x-2)$ que é equivalente a $3x+1 = (A+B)x + (2A-2B)$. Comparando os coeficientes nos dois membros da última igualdade, obtemos: $\begin{cases} A+B &= 3 \\ 2A-2B &= 1 \end{cases}$. Multiplicando-se a primeira equação por 2 e somando-se com a segunda, obtemos: $(2A+2B) + (2A-2B) = 6+1$, ou seja, $4A = 7$. Daí, obtemos $A = \frac{7}{4}$, que substituindo na primeira equação fornece $\frac{7}{4} + B = 3 \Rightarrow B = -\frac{7}{4} + 3 \Rightarrow B = \frac{5}{4}$. Portanto, $A = \frac{7}{4}$ e $B = \frac{5}{4}$.

A2) Determine o quociente $q(x)$ e o resto $r(x)$ da divisão de $f(x)$ por $g(x)$ em cada caso a seguir:

a) $f(x) = x^4 + 7x^3 - 5x^2 + 10x - 3$, $g(x) = x^2 + 2$

b) $f(x) = x^3 + 6x^2 + 9x - 11$, $g(x) = x^2 + x + 1$

Solução:

a) Dividimos x^4 por x^2 e obtemos como resultado x^2. Multiplicamos x^2 por (x^2+2) e obtemos $x^4 + 2x^2$. Subtraímos esse resultado de $f(x)$, ou seja, somamos $f(x)$ com $-x^4 - 2x^2$ e o resultado dessa operação inicia com $7x^3$. Repetimos o procedimento de divisão por x^2, etc. até obtermos um resultado com grau menor do que 2.

$$\begin{array}{rrr|l} x^4+7x^3-5x^2+10x-3 & & & x^2+2 \\ \cline{4-4} -x^4 & -2x^2 & & x^2+7x-7 \\ \cline{1-2} 7x^3-7x^2+10x & & & \\ -7x^3 & -14x & & \\ \cline{1-2} -7x^2-4x-3 & & & \\ 7x^2 & +14 & & \\ \cline{1-2} -4x+11 & & & \end{array}$$

O quociente da divisão é $q(x) = x^2 + 7x - 7$ e o resto é $r(x) = -4x + 11$.

b) Dividimos x^3 por x^2 e obtemos x. Multiplicamos x por $(x^2 + x + 1)$ e subtraímos de $f(x)$. Prosseguimos de maneira semelhante até obtermos um resultado de grau menor do que 2.

$$\begin{array}{rrr|l} x^3+6x^2+9x-11 & & & x^2+x+1 \\ \cline{4-4} -x^3-x^2-x & & & x+5 \\ \cline{1-3} 5x^2+8x-11 & & & \\ -5x^2-5x-5 & & & \\ \cline{1-3} 3x-16 & & & \end{array}$$

O quociente é $q(x) = x + 5$ e o resto é $r(x) = 3x - 16$.

Em qualquer caso observe que $f(x) = g(x) \cdot q(x) + r(x)$.

A3) Determine o valor de $a \in \mathbb{R}$ para que a divisão de

$$f(x) = x^4 + 2ax^3 + (a-2)x^2 + 5ax - 3$$

por $g(x) = x + 2$ apresente resto igual a -6.

Solução: O resto da divisão de $f(x)$ por $x + 2 = x - (-2)$ é igual a $f(-2) = 16 - 16a + 4(a-2) - 10a - 3 = -22a + 5$. Devemos ter $-22a + 5 = -6$ o que implica $-22a = -11$, ou seja, $a = \frac{1}{2}$.

A4) Determine $\bar{a} \in \mathbb{Z}_5$ de modo que $f(x) = \bar{2}x^3 + x^2 - \bar{3}x + \bar{a} \in \mathbb{Z}_5[x]$ seja divisível por $g(x) = x + \bar{1} \in \mathbb{Z}_5[x]$.

Solução: O resto da divisão de $f(x)$ por $x + \bar{1} = x - (-\bar{1})$ é igual a $f(-\bar{1}) = -\bar{2} + \bar{1} + \bar{3} + \bar{a} = \bar{2} + \bar{a}$. Para que o resto da divisão seja nulo, devemos ter $\bar{2} + \bar{a} = \bar{0}$, ou seja, $\bar{a} = -\bar{2} = \bar{3}$.

A5) Determine o resto da divisão de $f(x) = 7x^5 + ax^3 + bx^2 + 4x + 1 \in \mathbb{R}[x]$ por $x - 2$, sabendo o quociente da divisão é $q(x) = 7x^4 + cx^3 + dx^2 + ex + 25 \in \mathbb{R}[x]$.

Solução: O resto da divisão por um polinômio de grau 1 só pode ter resto constante. Suponhamos que o resto dessa divisão seja $r(x) = k \in \mathbb{R}$. Devemos ter $f(x) = q(x) \cdot (x - 2) + r(x)$, ou seja,

$$7x^5 + ax^3 + bx^2 + 4x + 1 = (7x^4 + cx^3 + dx^2 + ex + 25) \cdot (x - 2) + k.$$

O termo independente de x do lado esquerdo da última igualdade é igual a 1. Por outro lado, o termo independente de x do lado direito é igual a $25 \cdot (-2) + k$. Logo, $25 \cdot (-2) + k = 1 \Rightarrow k - 50 = 1 \Rightarrow \boxed{k = 51}$.

A6) Considere a equação de coeficientes inteiros $25x^6 + bx^5 + cx^4 + dx^3 + ex^2 + 49 = 0$ e o conjunto

$$A = \left\{ \frac{7}{10}, \frac{8}{5}, \frac{25}{49}, \frac{7}{25}, \frac{7}{3}, \frac{19}{7}, \frac{3}{25}, \frac{49}{5}, \frac{7}{8}, \frac{17}{5} \right\}.$$

Quais os elementos de A que podem ser raízes dessa equação?

Solução: Sendo $p, q \in \mathbb{Z}$, para que $\frac{p}{q}$ seja raiz da equação dada, devemos ter $p \mid 49$ e $q \mid 25$. Portanto, dos elementos de A, os únicos que têm chance de serem raízes são o $\frac{7}{25}$ e o $\frac{49}{5}$.

A7) Determine as raízes das seguintes equações polinomiais:

a) $15x^3 + 22x^2 - 15x + 2 = 0$

b) $4x^4 + 19x^3 + 23x^2 + 41x - 12 = 0$

Solução:

a) O termo independente de x da equação $f(x) = \boxed{15}x^3 + 22x^2 - 15x + \boxed{2} = 0$ é 2 e o coeficiente do termo de maior grau é 15.

- Os divisores de 2 são $\pm 1, \pm 2$
- Os divisores de 15 são $\pm 1, \pm 3, \pm 5, \pm 15$
- As possíveis raízes racionais da equação são os divisores de 2 divididos pelos divisores de 15, ou seja, são $\pm 1, \pm\frac{1}{3}, \pm\frac{1}{5}, \pm\frac{1}{15}, \pm 2, \pm\frac{2}{3}, \pm\frac{2}{5}, \pm\frac{2}{15}$
- Substituindo cada uma das possíveis raízes em $f(x)$ obtemos $f(-2) = 0$, $f(\frac{1}{5}) = 0$ e $f(\frac{1}{3}) = 0$.

Logo, as raízes da equação são -2, $\frac{1}{5}$ e $\frac{1}{3}$.

b) O termo independente de x da equação $f(x) = \boxed{4}x^4 + 19x^3 + 23x^2 + 41x\boxed{-12} = 0$ é -12 e o coeficiente do termo de maior grau é 4.

- Os divisores de 12 (ou -12) são ±1, ±2, ±3, ±4, ±6, ±12
- Os divisores de 4 são ±1, ±2, ±4
- As possíveis raízes racionais da equação são os divisores de 12 divididos pelos divisores de 4, ou seja, são ±1, $\pm\frac{1}{2}$, $\pm\frac{1}{4}$, ±2, ±3, $\pm\frac{3}{2}$, $\pm\frac{3}{4}$, ±4, ±6, ±12
- Substituindo cada uma das possíveis raízes em $f(x)$ obtemos $f(-4) = 0$ e $f(\frac{1}{4}) = 0$.
- Logo, -4 e $\frac{1}{4}$ são raízes o que implica que $f(x)$ é divisível pelo polinômio $4(x-(-4))(x-\frac{1}{4}) = 4x^2 + 15x - 4$.
- Dividindo-se $f(x)$ por $4x^2 + 15x - 4$ obtemos quociente igual a $x^2 + x + 3$
- As outras raízes de $f(x)$, além do -4 e $\frac{1}{4}$, são as raízes de $x^2 + x + 3 = 0$ que são raízes complexas: $x = \frac{-1\pm\sqrt{1-12}}{2} = \frac{-1\pm\sqrt{-11}}{2} = \frac{-1\pm\sqrt{11}i}{2}$.

Logo, as raízes da equação são -4, $\frac{1}{4}$ e $-\frac{1}{2} \pm \frac{\sqrt{11}}{2}i$.

A8) Um resultado conhecido como *Critério de Eisenstein* pode ser aplicado para se saber da irredutibilidade de um tipo particular de polinômio de coeficientes inteiros, é enunciado na seguinte forma:
Seja $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ para o qual existe um inteiro primo p tal que

- $p \mid a_0,\ p \mid a_1,\ p \mid a_2,\ \cdots,\ p \mid a_{n-1}$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$,

então $f(x)$ é irredutível sobre $\mathbb{Z}$. Veja também o exercício C1.
Usando esse resultado, verifique se os seguintes polinômios são irredutíveis sobre $\mathbb{Z}$:

a) $f(x) = 5x^9 + 7x^4 - 49x^3 + 14x^2 - 7x + 21$

b) $g(x) = x^6 + 20x^5 - 14x^4 + 8x^3 + 50x^2 - 44x + 10$

c) $h(x) = 4x^4 - 121x^3 + 22x^2 - 44x + 33$

d) $j(x) = 3x^7 + 100x^6 - 90x^5 + 80x^4 - 70x^3 + 30x^2 - 40x + 15$

Solução:

a) Consideremos o primo $p = 7$. Temos: $p \mid 7$, $p \mid (-49)$, $p \mid 14$, $p \mid (-7)$, $p \mid 21$, $p \nmid 5$, $p^2 \nmid 21$. Logo, pelo Critério de Eisenstein, $f(x)$ é irredutível sobre $\mathbb{Z}$.

b) Consideremos o primo $p = 2$. Temos: $p \mid 20$, $p \mid (-14)$, $p \mid 8$, $p \mid 50$, $p \mid (-44)$, $p \mid 10$, $p \nmid 1$, $p^2 \nmid 10$. Logo, pelo Critério de Eisenstein, $f(x)$ é irredutível sobre $\mathbb{Z}$.

c) Consideremos o primo $p = 11$. Temos: $p \mid (-121)$, $p \mid 22$, $p \mid (-44)$, $p \mid 33$, $p \nmid 4$, $p^2 \nmid 33$. Logo, pelo Critério de Eisenstein, $f(x)$ é irredutível sobre $\mathbb{Z}$.

d) Consideremos o primo $p = 5$. Temos: $p \mid 100$, $p \mid (-90)$, $p \mid 80$, $p \mid (-70)$, $p \mid 30$, $p \mid (-40)$, $p \mid 15$, $p \nmid 3$, $p^2 \nmid 15$. Logo, pelo Critério de Eisenstein, $f(x)$ é irredutível sobre $\mathbb{Z}$.

A9) Mostre que os seguintes polinômios são redutíveis sobre A:

a) $f(x) = x^2 + \bar{1}$, $A = \mathbb{Z}_5$

b) $g(x) = x^2 + x + \bar{2}$, $A = \mathbb{Z}_4$

c) $h(x) = x^4 - 4$, $A = \mathbb{R}$

d) $j(x) = x^3 - 8$, $A = \mathbb{R}$

e) $k(x) = 10x^3 + 13x^2 - 13x + 2$, $A = \mathbb{Q}$

f) $h(x) = x^4 + 4$, $A = \mathbb{Z}$

g) $j(x) = x^4 + x^2 + 1$, $A = \mathbb{Z}$

Solução: Em cada caso, devemos mostrar que é possível fatorar o polinômio dado escrevendo-o como produto de dois polinômios não constantes de $A[x]$. Em alguns casos, podemos utilizar conhecidas fórmulas como $a^2 + 2ab + b^2 = (a + b)^2$, $a^2 - b^2 = (a + b)(a - b)$, etc.

a) Por substituição direta em $f(x)$ dos elementos de $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$, obtemos: $f(\bar{0}) = \bar{1}$, $f(\bar{1}) = \bar{2}$, $f(\bar{2}) = \bar{5} = \bar{0}$, $f(\bar{3}) = \overline{10} = \bar{0}$ e $f(\bar{4}) = \overline{17} = \bar{2}$. Logo, as raízes de $f(x)$ em $\mathbb{Z}_5$ são $\bar{2}$ e $\bar{3}$ o que implica em $f(x) = (x - \bar{2})(x - \bar{3}) = (x + \bar{3})(x + \bar{2})$.

b) Substituindo-se cada elemento de $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}$ em $g(x)$, obtemos: $g(\bar{0}) = \bar{2}$, $g(\bar{1}) = \bar{4} = \bar{0}$, $g(\bar{2}) = \bar{8} = \bar{0}$, $g(\bar{3}) = \overline{14} = \bar{2}$. Logo, as raízes de $g(x)$ em $\mathbb{Z}_4$ são $\bar{1}$ e $\bar{2}$. Logo, $g(x) = (x - \bar{1})(x - \bar{2}) = (x + \bar{3})(x + \bar{2})$.

c) $h(x) = x^4 - 4 = (x^2)^2 - 2^2 = (x^2 + 2)(x^2 - 2)$

d) Como $j(2) = 2^3 - 8 = 0$ temos que 2 é raiz de $j(x)$. Isso significa que $j(x)$ é divisível por $x-2$. A divisão de $j(x)$ por $x-2$ deixa resto nulo e quociente igual a $x^2 + 2x + 4$. Logo, $j(x) = (x - 2)(x^2 + 2x + 4)$.

e) As possíveis raízes racionais de $k(x)$ são os divisores de 2 divididos pelos divisores de 10, ou seja, são ± 1, ± 2, $\pm\frac{1}{2}$, $\pm\frac{1}{5}$, $\pm\frac{2}{5}$, $\pm\frac{1}{10}$. Substituindo diretamente em $k(x)$ verificamos que somente -2, $\frac{1}{5}$ e $\frac{1}{2}$ são raízes. Portanto, $k(x) = 10(x-(-2))(x-\frac{1}{5})(x-\frac{1}{2}) = (x+2)(5x-1)(2x-1)$.

f) Para que x^4+4 seja o quadrado de algum outro polinômio, falta somar um termo $4x^2$. Para não alterar o polinômio, somamos e subtraímos o mesmo termo: $h(x) = x^4+4 = x^4+4+4x^2-4x^2 = (x^4+2x^2+4)-4x^2 = (x^2+2)^2-(2x)^2 = ((x^2+2)-2x)(x^2+2)+2x) = (x^2-2x+2)(x^2+2x+2)$.

g) Vamos *"completar o quadrado"* em $j(x)$. Para isso, devemos somar x^2 para obtermos x^4+2x^2+1 que é um quadrado perfeito. Portanto, $j(x) = x^4+x^2+1 = x^4+x^2+x^2+1-x^2 = (x^4+2x^2+1)-x^2 = (x^2+1)^2-x^2 = ((x^2+1)+x)((x^2+1)-x) = (x^2+x+1)(x^2-x+1)$.

A10) Escreva o polinômio $f(x) = x^4 - 7x^2 + 10$ como um produto de fatores irredutíveis sobre os seguintes corpos K:

a) $K = \mathbb{Q}$

b) $K = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

c) $K = \mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$

d) $K = \mathbb{R}$

Solução:

a) Inicialmente, vamos tentar resolver a equação $x^4 - 7x^2 + 10 = 0$ (que é conhecida pelo nome de *equação biquadrada*). Fazendo $x^2 = y$, obtemos $y^2 - 7y + 10 = 0$ que é uma equação do segundo grau na variável y, cujas raízes são $y = \frac{7 \pm \sqrt{49-40}}{2} \Rightarrow y = 2$ ou $y = 5$. Daí, temos $y^2 - 7y + 10 = (y-2)(y-5) \Rightarrow$ $\boxed{f(x) = (x^2-2)(x^2-5)}$. Os polinômios x^2-2 e x^2-7 não têm raízes racionais; logo, são irredutíveis sobre $\mathbb{Q}$.

b) Em $\mathbb{Q}[\sqrt{2}]$ o polinômio x^2-2 pode ser fatorado na forma $x^2-2 = (x+\sqrt{2})(x-\sqrt{2})$. Logo, em $\mathbb{Q}[\sqrt{2}]$, a fatoração de $f(x)$ como produto de irredutíveis é $\boxed{f(x) = (x+\sqrt{2})(x-\sqrt{2})(x^2-5)}$.

c) Em $\mathbb{Q}[\sqrt{5}]$ o polinômio x^2-5 pode ser fatorado na forma $x^2-5 = (x+\sqrt{5})(x-\sqrt{5})$. Logo, em $\mathbb{Q}[\sqrt{5}]$, a fatoração de $f(x)$ como produto de irredutíveis é $\boxed{f(x) = (x^2-2)(x+\sqrt{5})(x-\sqrt{5})}$.

d) Em $\mathbb{R}]$ o polinômio x^2-2 pode ser fatorado na forma $x^2-2=(x+\sqrt{2})(x-\sqrt{2})$ e x^2-5 como $x^2-5=(x+\sqrt{5})(x-\sqrt{5})$. Logo, em $\mathbb{R}$, a fatoração de $f(x)$ como produto de irredutíveis é $\boxed{f(x)=(x+\sqrt{2})(x-\sqrt{2})(x+\sqrt{5})(x-\sqrt{5})}$.

B1) Dados $n\in\mathbb{N}$, $n\geq 2$ e um inteiro primo $p>0$, mostre que $\sqrt[n]{p}$ é irracional.

Solução: Se $a=\sqrt[n]{p}$, então $a^n=p\Rightarrow a^n-p=0\Rightarrow a$ é raiz da equação $f(x)=x^n-p=0$. As possíveis raízes racionais dessa equação são os divisores de p: $1,-1,p,-p$. Como $f(1)=1-p\neq 0$, $f(-1)=(-1)^n-p\neq 0$, $f(p)=p^n-p\neq 0$ e $f(-p)=(-p)^n-p\neq 0$ temos que a equação não possui raiz racional. Concluímos, então, que a é irracional.

B2) Seja $P(x)=(2x^2+x+1)(-3+7x-x^2)+(x^3-2)(-13+2x)\in\mathbb{Z}[x]$

a) Mostre que $P(x)$ é um polinômio constante;

b) Racionalize o denominador de $\dfrac{1}{1+\sqrt[3]{2}+2\sqrt[3]{4}}$. (*Sugestão: calcule* $P(\sqrt[3]{2})$).

Solução:

a) Efetuando-se todas as operações que estão indicadas em $P(x)$, obtemos: $P(x)=-6x^2-3x-3+14x^3+7x^2+7x-2x^4-x^3-x^2-13x^3+26+2x^4-4x=23$. Logo, $P(x)$ é constante e é igual a 23.

b) Sabemos que $P(\sqrt[3]{2})=23$. Substituindo-se $x=\sqrt[3]{2}$ na expressão de $P(x)$ dada no enunciado, obtemos: $(2(\sqrt[3]{2})^2+\sqrt[3]{2}+1)\cdot(-3+7\sqrt[3]{2}-(\sqrt[3]{2})^2))+\underbrace{((\sqrt[3]{2})^3-2)}_{=0}\cdot(-13+2\sqrt[3]{2})=23\Rightarrow -3+7\sqrt[3]{2}-\sqrt[3]{4}=\frac{23}{2\sqrt[3]{4}+\sqrt[3]{2}+1}$ de onde obtemos finalmente que

$$\frac{1}{1+\sqrt[3]{2}+2\sqrt[3]{4}}=\frac{-3+7\sqrt[3]{2}-\sqrt[3]{4}}{23}$$

B3) Seja $\frac{p}{q}\in\mathbb{Q}$, $\text{mdc}(p,q)=1$, uma raiz da equação polinomial de coeficientes inteiros

$$f(x)=a_nx^n+\cdots+a_1x+a_0=0.$$

Mostre que p é um divisor de a_0 e que q é um divisor de a_n.

Solução: Supondo $\frac{p}{q}$ uma raiz e substituindo-a na equação, obtemos:

$a_n(\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} \cdots + a_1(\frac{p}{q}) + a_0 = 0$. Multiplicando-se os dois membros por q^n, obtemos $a_n p^n + a_{n-1} q p^{n-1} + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$. Isolando-se $a_n p^n$ no primeiro membro e, depois, isolando-se também $a_0 q^n$, obtemos:

- $a_0 q^n = \underbrace{-a_n p^n - a_{n-1} q p^{n-1} - \cdots - a_1 p q^{n-1}}_{\text{múltiplo de } p} \Rightarrow p \mid a_0 q^n$. Como $\text{mdc}(p, q) = 1$, temos $p \mid a_0$
- $a_n p^n = \underbrace{-a_{n-1} q p^{n-1} - \cdots - a_1 p q^{n-1} - a_0 q^n}_{\text{múltiplo de } q} \Rightarrow q \mid a_n p^n$. Como $\text{mdc}(p, q) = 1$, temos $q \mid a_n$

B4) Onde está o erro? Seja x uma raiz da equação $x^2 + x + 1 = 0$. Então, $x \neq 0$ e, por isso, podemos dividir os dois membros da equação por x e obtemos $x + 1 + \frac{1}{x} = 0$. Da equação inicial temos $x + 1 = -x^2$ o que implica $-x^2 + \frac{1}{x} = 0$, ou seja, $x^2 = \frac{1}{x}$ que é equivalente a $x^3 = 1$. A partir daí, obtemos $x = 1$. Substituindo essa solução na equação $x^2 + x + 1 = 0$ original, obtemos $3 = 0$. Como a conclusão não está correta, onde foi cometido um erro?

Solução: Foi mostrado no enunciado que toda raiz da equação $x^2 + x + 1 = 0$ também é raiz de $x^3 = 1$. No entanto, a recíproca não é verdadeira: nem toda raiz de $x^3 = 1$ é raiz de $x^2 + x + 1 = 0$. As raízes de $x^2 + x + 1 = 0$ são r_1 e r_2 e as raízes de $x^3 = 1$ são 1, r_1 e r_2. O erro no enunciado está na afirmação de que a raiz $x = 1$ da equação $x^3 = 1$ também é raiz de $x^2 + x + 1$.

C1) Considere $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Mostre que se existir um inteiro primo p tal que

- $p \mid a_0,\ p \mid a_1, \cdots, p \mid a_{n-1}$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$,

então $f(x)$ é irredutível sobre $\mathbb{Z}$.

Solução: Suponhamos $f(x)$ redutível. Então existem polinômios $g(x), h(x)$ pertencentes a $\mathbb{Z}[x]$ tais que $f(x) = g(x) \cdot h(x)$ e $1 \leq \partial g < n$, $1 \leq \partial h < n$. Sejam $g(x) = b_r x^r + \cdots + b_1 x + b_0 \in \mathbb{Z}[x]$ e $h(x) = c_s x^s + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$, onde $r = \partial g$, $s = \partial h$ e $r + s = n$.
Como $a_0 = b_0 c_0$ e $p \mid a_0$, temos que p é um divisor de b_0 ou de c_0, mas não pode

ser divisor simultaneamente de b_0 e c_0 porque $p^2 \nmid a_0$. Temos então dois casos a considerar: caso 1 em que $p \mid b_0$ e $p \nmid c_0$ e um caso 2 em que $p \nmid b_0$ e $p \mid c_0$.
Suponhamos $p \mid b_0$ e $p \nmid c_0$. Como $a_n = b_r \cdot c_s$ e $p \nmid a_n$, temos $p \nmid b_r$. Seja b_i o primeiro coeficiente (de menor índice i) de $g(x)$ tal que $p \nmid b_i$; isso significa que $p \mid b_0, \cdots p \mid b_{i-1}$. Como $\underbrace{a_i}_{\text{múltiplo de } p} = \underbrace{b_0c_i + b_1c_{i-1} + \cdots + b_{i-1}c_1}_{\text{múltiplo de } p} + b_ic_0$, temos que b_ic_0 é um múltiplo de p, o que é um absurdo porque $p \nmid b_i$ e $p \nmid c_0$.
De modo semelhante, o caso 2 também leva a um absurdo. Concluímos então que o polinômio $f(x)$ é irredutível sobre $\mathbb{Z}$.

Observação. Esta proposição é conhecida pelo nome de *Critério de Eisenstein.*

C2) Mostre que o número

$$\sqrt[3]{\frac{25}{8} + \frac{11\sqrt{2}}{4}} + \sqrt[3]{\frac{25}{8} - \frac{11\sqrt{2}}{4}}$$

é inteiro.

Solução: Antes de tudo, note que essa soma de raízes cúbicas é um número real. Sejam $a = \sqrt[3]{\frac{25}{8} + \frac{11\sqrt{2}}{4}}$, $b = \sqrt[3]{\frac{25}{8} - \frac{11\sqrt{2}}{4}}$ e $x = a + b$. Então, temos que:

- $x^3 = (a+b)^3 = a^3+3a^2b+3ab^2+b^3 = a^3+b^3+3ab\underbrace{(a+b)}_{=x} \Rightarrow x^3 = a^3+b^3+3abx.$
- $a^3 + b^3 = \left(\sqrt[3]{\frac{25}{8} + \frac{11\sqrt{2}}{4}}\right)^3 + \left(\sqrt[3]{\frac{25}{8} - \frac{11\sqrt{2}}{4}}\right)^3 = \left(\frac{25}{8} + \frac{11\sqrt{2}}{4}\right) + \left(\frac{25}{8} - \frac{11\sqrt{2}}{4}\right) = \frac{25}{4}$
- $ab = \left(\sqrt[3]{\frac{25}{8} + \frac{11\sqrt{2}}{4}}\right)\left(\sqrt[3]{\frac{25}{8} - \frac{11\sqrt{2}}{4}}\right) = \sqrt[3]{\left(\frac{25}{8}\right)^2 - \left(\frac{11\sqrt{2}}{4}\right)^2} = \sqrt[3]{\frac{625}{64} - \frac{121\cdot 2}{16}} = \sqrt[3]{\frac{625-968}{64}}$
  $= \sqrt[3]{-\frac{343}{64}} = -\frac{7}{4}.$
- Portanto, $x^3 = \frac{25}{4} + 3x \cdot (-\frac{7}{4}) \Rightarrow 4x^3 = 25 - 21x \Rightarrow 4x^3 + 21x - 25 = 0.$
- As possíveis raízes racionais dessa equação são os divisores de 25 divididos pelos divisores de 4.
- Testando uma por uma, temos que $x = 1$ é uma raiz racional da equação.
- Dividindo-se $4x^3 + 21x - 25$ por $x - 1$, obtemos $4x^2 + 4x + 25$ que não tem raiz real (porque $\Delta = 4^2 - 4 \cdot 4 \cdot 25 < 0$). Portanto, a única raiz real da equação é $x = 1$.

Concluímos que

$$\sqrt[3]{\frac{25}{8}+\frac{11\sqrt{2}}{4}}+\sqrt[3]{\frac{25}{8}-\frac{11\sqrt{2}}{4}}=1.$$

Capítulo 9

Exercícios de revisão

Neste capítulo, apresentamos uma pequena lista de exercícios dos mais diversos temas que são úteis para se fazer uma revisão rápida dos assuntos.

1) Seja $\otimes$ a operação sobre $\mathbb{R}$ definida por $x \otimes y = x + y + xy$. Verifique se essa operação é comutativa, se é associativa e se tem elemento neutro.

Solução:

- Para quaisquer $x, y \in \mathbb{R}$, $x \otimes y = x + y + xy = y + x + yx = y \otimes x$. Logo, a operação $\otimes$ é comutativa.
- Para quaisquer $x, y, z \in \mathbb{R}$, temos:
  - $x \otimes (y \otimes z) = x \otimes (y + z + yz) = x + (y + z + yz) + x(y + z + yz) = x + y + z + xy + xz + yz + xyz$
  - $(x \otimes y) \otimes z = (x + y + xy) \otimes z = (x + y + xy) + z + (x + y + xy)z = x + y + z + xy + xz + yz + xyz$.

  Logo, $x \otimes (y \otimes z) = (x \otimes y) \otimes z$, de onde concluímos que $\otimes$ é associativa.
- $0 \otimes x = x \otimes 0 = x + 0 + x \cdot 0 = x, \forall x \in \mathbb{R}$. Logo, o 0 (zero) é o elemento neutro da operação.

2) Consideremos o conjunto dos números reais $\mathbb{R}$ com a operação definida por $x * y = \sqrt[3]{x^3 + y^3}$. Mostre que $G = (\mathbb{R}, *)$ é um grupo abeliano.

Solução:

- $x * y = \sqrt[3]{x^3 + y^3} = \sqrt[3]{y^3 + x^3} = y * x$, $\forall x, y \in \mathbb{R}$. Logo, $*$ é comutativa.
- Sejam $x, y, z \in \mathbb{R}$ três elementos genéricos.
  - $x * (y * z) = x * \sqrt[3]{y^3 + z^3} = \sqrt[3]{x^3 + \left(\sqrt[3]{y^3 + z^3}\right)^3} = \sqrt[3]{x^3 + y^3 + z^3}$
  - $(x * y) * z = \sqrt[3]{x^3 + y^3} * z = \sqrt[3]{\left(\sqrt[3]{x^3 + y^3}\right)^3 + z^3} = \sqrt[3]{x^3 + y^3 + z^3}$

  Logo, $x * (y * z) = (x * y) * z$, ou seja, a operação $*$ é associativa.
- $0 * x = x * 0 = \sqrt[3]{x^3 + 0^3} = \sqrt[3]{x^3} = x$, $\forall x \in \mathbb{R}$, logo, 0 (zero) é o elemento neutro.
- Dado $x \in \mathbb{R}$, $y = -x$ é tal que $y * x = x * y = \sqrt[3]{x^3 + y^3} = \sqrt[3]{x^3 + (-x)^3} = \sqrt[3]{x^3 - x^3} = \sqrt[3]{0} = 0 =$ elemento neutro. Logo, $-x$ é o elemento inverso de x.

Os quatro itens anteriores demonstram que $(G, *)$ é um grupo abeliano.

3) Verifique se H é subgrupo de G nos seguintes casos:

a) $H = (\mathbb{R} - \mathbb{Q}, +)$, $G = (\mathbb{R}, +)$

b) $H = (\{2^m 3^n 5^r \mid m, n, r \in \mathbb{Z}\}, \cdot)$, $G = (\mathbb{Q}^*, \cdot)$

c) $H = \left(\left\{\begin{bmatrix} 0 & a \\ b & a-b \end{bmatrix} \mid a, b \in \mathbb{R}\right\}, +\right)$, $G = (M_{2\times 2}(\mathbb{R}), +)$

Solução:

a) O conjunto H é o conjunto dos números irracionais. Dados dois irracionais, por exemplo, $x = 2 - \sqrt{3}$ e $y = 2 + \sqrt{3}$, temos $x + y = (2 - \sqrt{3}) + (2 + \sqrt{3}) = 4 \notin H$. Logo, o conjunto dos irracionais não é fechado para a adição de números reais e, consequentemente, não formam um subgrupo de $\mathbb{R}$.

b) Escolhendo $m = n = r = 0$, temos $x = 2^0 3^0 5^0 = 1 \in H \Rightarrow H \neq \emptyset$. Sejam $a, b \in H$. Existem $m_1, n_1, r_1, m_2, n_2, r_2 \in \mathbb{Z}$ tais que $a = 2^{m_1} 3^{n_1} 5^{r_1}$ e $b = 2^{m_2} 3^{n_2} 5^{r_2}$ $\Rightarrow a \cdot b^{-1} = 2^{m_1} 3^{n_1} 5^{r_1} 2^{-m_2} 3^{-n_2} 5^{-r_2} = 2^{m_1 - m_2} 3^{n_1 - n_2} 5^{r_1 - r_2} \in H$. Logo, H é um subgrupo de G.

c) Escolhendo $a = b = 0$, temos que $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in H \Rightarrow H \neq \emptyset$. Sejam $X, Y \in H$. Existem $a, b, c, d \in \mathbb{R}$ tais que $X = \begin{bmatrix} 0 & a \\ b & a-b \end{bmatrix}$ $Y = \begin{bmatrix} 0 & c \\ d & c-d \end{bmatrix}$. Como $X + (-Y) = X - Y = \begin{bmatrix} 0 & a-c \\ b-d & (a-c)-(b-d) \end{bmatrix} \in H$, temos que H é um subgrupo de G.

4) Dadas as permutações $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ e $c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$, determine a solução $x \in S_4$ da equação $axb^{-3} = c^2$.

Solução: Multiplicando a equação dada por a^{-1} à esquerda e por b^3 à direita, obtemos $\underbrace{a^{-1}a}_{=e} x \underbrace{b^{-3}b^3}_{=e} = a^{-1}c^2b^3 \Rightarrow x = a^{-1}c^2b^3$. Temos que:

- $a^{-1} = \begin{pmatrix} 4 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$
- $b^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$
- $c^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ = elemento neutro;

Portanto, $x = a^{-1}c^2b^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ é a solução procurada da equação dada.

5) Consideremos os grupos $G = (\mathbb{R}\times\mathbb{R}, +)$, $J = (\mathbb{R}, +)$ a função $\varphi : G \longrightarrow J$ definida por $\varphi(x, y) = 3x-5y$. Mostre que φ é um homomorfismo de grupos e determine $N(\varphi)$.

Solução:

- Sejam $a = (x, y)$ e $b = (z, w)$ dois elementos genéricos de G. Temos: $\varphi(a + b) = \varphi(x + z, y + w) = 3(x + z) - 5(y + w) = (3x - 5y) + (3z - 5w) = \varphi(x, y) + \varphi(z, w) = \varphi(a) + \varphi(b)$. Isso mostra que φ é um homomorfismo de G em J.
- Suponhamos que (x, y) seja um elemento do núcleo de φ. Então, pela definição de núcleo de um homomorfismo, temos que $\varphi(x, y)$ = elemento neutro de $J = 0$ o que implica em $3x - 5y = 0 \Rightarrow y = \frac{3}{5}x \Rightarrow N(\varphi) = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = \frac{3}{5}x\} \Rightarrow N(\varphi) = \{(x, \frac{3}{5}x) \mid x \in \mathbb{R}\}$.

6) Sejam $G = (\mathbb{Z}_{10}, +)$ e $H = \{\bar{0}, \bar{5}\}$ um subgrupo de G. Construa a tábua do grupo-quociente $(G/H, +)$ e determine o inverso (aditivo) dos elementos $\bar{3} + H$ e $\bar{4} + H$.

Solução: Calculando as classes laterais à esquerda módulo H determinadas por elementos de G, temos:

- $\bar{0} + H = \{\bar{0} + \bar{0}, \bar{0} + \bar{5}\} = H$
- $\bar{1} + H = \{\bar{1} + \bar{0}, \bar{1} + \bar{5}\} = \{\bar{1}, \bar{6}\}$
- $\bar{2} + H = \{\bar{2} + \bar{0}, \bar{2} + \bar{5}\} = \{\bar{2}, \bar{7}\}$
- $\bar{3} + H = \{\bar{3} + \bar{0}, \bar{3} + \bar{5}\} = \{\bar{3}, \bar{8}\}$
- $\bar{4} + H = \{\bar{4} + \bar{0}, \bar{4} + \bar{5}\} = \{\bar{4}, \bar{9}\}$
- $\bar{5} + H = \{\bar{5} + \bar{0}, \bar{5} + \bar{5}\} = \{\bar{5}, \bar{0}\} = H$ e, a partir daqui, há apenas repetição de classes.

Portanto, $G/H = \{H, \bar{1} + H, \bar{2} + H, \bar{3} + H, \bar{4} + H\}$ e sua tábua é:

$+$	H	$\bar{1} + H$	$\bar{2} + H$	$\bar{3} + H$	$\bar{4} + H$
H	H	$\bar{1} + H$	$\bar{2} + H$	$\bar{3} + H$	$\bar{4} + H$
$\bar{1} + H$	$\bar{1} + H$	$\bar{2} + H$	$\bar{3} + H$	$\bar{4} + H$	H
$\bar{2} + H$	$\bar{2} + H$	$\bar{3} + H$	$\bar{4} + H$	H	$\bar{1} + H$
$\bar{3} + H$	$\bar{3} + H$	$\bar{4} + H$	H	$\bar{1} + H$	$\bar{2} + H$
$\bar{4} + H$	$\bar{4} + H$	H	$\bar{1} + H$	$\bar{2} + H$	$\bar{3} + H$

O elemento neutro de todo grupo-quociente é o elemento H. Assim, determinar o inverso de $\bar{3} + H$ é só verificar na tábua qual é o elemento que somado com ele dá como resultado o H. Chegamos à conclusão de que o inverso de $\bar{3} + H$ é o $\bar{2} + H$. Por um motivo semelhante, o inverso de $\bar{4} + H$ é o $\bar{1} + H$.
Observação: A adição de classes laterais é efetuada de acordo com a definição: $(\bar{a} + H) + (\bar{b} + H) = (\bar{a} + \bar{b}) + H = \overline{a + b} + H$.

7) Verifique se cada conjunto S a seguir é subanel de A (adição e multiplicação usuais).

a) $S = 5\mathbb{Z}, A = \mathbb{Z}$;

b) $S = \left\{ \begin{bmatrix} x & x & x \\ y & y & 0 \\ z & 0 & 0 \end{bmatrix} \mid x, y, z \in \mathbb{R} \right\}, A = M_{3\times 3}(\mathbb{R})$.

Solução:

a) S é o conjunto de todos os múltiplos de 5.

- É claro que S não é vazio porque $5 \in S$.
- Sejam $x, y \in S$. Então existem inteiros $m, n \in \mathbb{Z}$ tais que $x = 5m$ e $y = 5n$.
- $x - y = 5m - 5n = 5\underbrace{(m-n)}_{\in\mathbb{Z}} \in S$
- $x \cdot y = (5m)(5n) = 5\underbrace{(5mn)}_{\in\mathbb{Z}} \in S$

Fica mostrado dessa forma que S é um subanel de A

b) Consideremos os dois seguintes elementos de S (escolhidos aleatoriamente): $x = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 0 \\ 3 & 0 & 0 \end{bmatrix}$ e $y = \begin{bmatrix} 2 & 2 & 2 \\ -1 & -1 & 0 \\ 4 & 0 & 0 \end{bmatrix}$. Temos que seu produto é $xy = \begin{bmatrix} 5 & 1 & 2 \\ 2 & 2 & 4 \\ 6 & 6 & 6 \end{bmatrix} \notin S$. Logo, S não é subanel de A.

8) Verifique se $(I, +, \cdot)$ é um ideal do anel $(A, +, \cdot)$ em cada um dos seguintes casos:

a) $I = \{f : \mathbb{R} \longrightarrow \mathbb{R} \mid f(-1) = f(1) = 0\}$, $A = \mathbb{R}^{\mathbb{R}}$.

b) $I = \{f : \mathbb{R} \longrightarrow \mathbb{R} \mid f(-1) = f(1) = 2\}$, $A = \mathbb{R}^{\mathbb{R}}$.

Solução:

a)
- Seja f a função nula $f(x) = 0$. Então $f \in I \Rightarrow I \neq \emptyset$.
- Sejam $f, g \in I$. Então, $f(-1) = f(1) = g(-1) = g(1) = 0 \Rightarrow (f-g)(-1) = f(-1) - g(-1) = 0 - 0 = 0$ e $(f-g)(1) = f(1) - g(1) = 0 - 0 = 0$. Logo, $f - g \in I$.
- Se $f \in I$ e $h \in A$, então $(h \cdot f)(-1) = h(-1) \cdot f(-1) = h(-1) \cdot 0 = 0$ e $(h \cdot f)(1) = h(1) \cdot f(1) = h(1) \cdot 0 = 0$. Logo, $h \cdot f \in I$.

Pelo que foi mostrado, concluímos que I é um ideal de A.

b) Um exemplo de elemento de I pode ser dado por $f(x) = x^2 + 1$. Seja $g(x) = x \in A$. Temos que $h(x) = f(x) \cdot g(x)$ é tal que $h(x) = x^3 + x$, $h(-1) = -2$ e $h(1) = 2$. Logo, $h(x) \notin I$ de onde podemos concluir que I não é ideal de A.

9) Verifique se $(3\mathbb{Z}, +, \cdot)$ e $(5\mathbb{Z}, +, \cdot)$ são anéis isomorfos.

Solução: Suponhamos que exista um isomorfismo $f : 3\mathbb{Z} \longrightarrow 5\mathbb{Z}$. Então

$f(3) = 5n$ para algum $n \in \mathbb{Z}$. Como $f(0) = 0$ e f é injetora, temos que $n \neq 0$. Usando o fato de que f é um homomorfismo de anéis, temos:

- $f(9) = f(3 + 3 + 3) = f(3) + f(3) + f(3) = 5n + 5n + 5n = 15n$
- $f(9) = f(3 \cdot 3) = f(3) \cdot f(3) = (5n)(5n) = 25n^2$

o que implica em $15n = 25n^2 \Rightarrow 3 \cdot 5n = 5n \cdot 5n$. Como $5\mathbb{Z}$ é um anel de integridade e $5n \neq 0$, podemos cancelar o $5n$ nos dois membros da última igualdade de onde obtemos: $3 = 5n$. Essa última igualdade é um absurdo porque o segundo membro é um múltiplo de 5 e o primeiro membro não é. Portanto, não pode existir isomorfismo de $3\mathbb{Z}$ em $5\mathbb{Z}$.

10) Calcule $f(\sqrt{11})$ sabendo que $f : \mathbb{Q}[\sqrt{11}] \longrightarrow \mathbb{Q}[\sqrt{11}]$ é um isomorfismo de anéis e $\mathbb{Q}[\sqrt{11}] = \{a + b\sqrt{11} \mid a, b \in \mathbb{Q}\}$.

Solução: Se f for isomorfismo de anéis, então $f(1) = 1$ o que implica

- $f(2) = f(1 + 1) = f(1) + f(1) = 1 + 1 = 2$,
- $f(3) = f(1 + 2) = f(1) + f(2) = 1 + 2 = 3$,
- $f(4) = f(2 + 2) = f(2) + f(2) = 2 + 2 = 4$,
- $f(7) = f(3 + 4) = f(3) + f(4) = 3 + 4 = 7$,
- $f(11) = f(4 + 7) = f(4) + f(7) = 4 + 7 = 11$

e daí obtemos $11 = f(11) = f(\sqrt{11} \cdot \sqrt{11}) = f(\sqrt{11}) \cdot f(\sqrt{11}) \Rightarrow [f(\sqrt{11})]^2 = 11$, de onde concluímos que $f(\sqrt{11}) = \pm\sqrt{11}$.

11) Considere o anel $A = \mathbb{Z}$ e o ideal $I = 6\mathbb{Z}$ (adição e multiplicação usuais). Construa as tábuas de adição e multiplicação do anel-quociente A/I.

Solução: Temos que:

- $0 + I = I = \{\cdots, -18, -12, -6, 0, 6, 12, 18, \cdots\}$
- $1 + I = \{\cdots, -17, -11, -5, 1, 7, 13, 19, \cdots\}$

- $2 + I = \{\cdots, -16, -10, -4, 2, 8, 14, 20, \cdots\}$
- $3 + I = \{\cdots, -15, -9, -3, 3, 9, 15, 21, \cdots\}$
- $4 + I = \{\cdots, -14, -8, -2, 4, 10, 16, 22, \cdots\}$
- $5 + I = \{\cdots, -13, -7, -1, 5, 11, 17, 23, \cdots\}$
- $6 + I = \{\cdots, -12, -6, 0, 6, 12, 18, 24, \cdots\} = I$

Portanto, o anel-quociente de A por I é

$$A/I = \{I, 1 + I, 2 + I, 3 + I, 4 + I, 5 + I\}.$$

com as seguintes operações:

- $(a + I) + (b + I) = (a + b) + I$
- $(a + I) \cdot (b + I) = ab + I$

Todas as possíveis adições entre seus elementos podem ser observadas na seguinte tábua:

$+$	I	$1+I$	$2+I$	$3+I$	$4+I$	$5+I$
I	I	$1+I$	$2+I$	$3+I$	$4+I$	$5+I$
$1+I$	$1+I$	$2+I$	$3+I$	$4+I$	$5+I$	I
$2+I$	$2+I$	$3+I$	$4+I$	$5+I$	I	$1+I$
$3+I$	$3+I$	$4+I$	$5+I$	I	$1+I$	$2+I$
$4+I$	$4+I$	$5+I$	I	$1+I$	$2+I$	$3+I$
$5+I$	$5+I$	I	$1+I$	$2+I$	$3+I$	$4+I$

e todas as possíveis multiplicações na seguinte tábua:

$\cdot$	I	$1+I$	$2+I$	$3+I$	$4+I$	$5+I$
I	I	I	I	I	I	I
$1+I$	I	$1+I$	$2+I$	$3+I$	$4+I$	$5+I$
$2+I$	I	$2+I$	$4+I$	I	$2+I$	$4+I$
$3+I$	I	$3+I$	I	$3+I$	I	$3+I$
$4+I$	I	$4+I$	$2+I$	I	$4+I$	$2+I$
$5+I$	I	$5+I$	$4+I$	$3+I$	$2+I$	$1+I$

12) Determine o resto da divisão de $f(x) = \bar{2}x^5 - \bar{4}x^2 + \bar{3}x + \bar{5} \in \mathbb{Z}_{13}[x]$ por $g(x) = x - \bar{2} \in \mathbb{Z}_{13}[x]$.

Solução: O resto da divisão de $f(x)$ por $x - \bar{2}$ é igual a $f(\bar{2}) = \overline{64} - \overline{16} + \bar{6} + \bar{5}$

$= \overline{59} = \bar{4}$.

13) Verifique se os seguintes polinômios são irredutíveis sobre $\mathbb{Z}$:

a) $p(x) = x^3 + 4x^2 + 9x + 10$

b) $q(x) = x^3 + 6x^2 - 9x + 21$

Solução:

a) As possíveis raízes inteiras de $p(x)$ são os divisores de 10: ± 1, ± 2, ± 5, ± 10. Substituindo uma por uma em $p(x)$, obtemos que somente -2 é raiz: $p(-2) = 0$. Isso significa que $f(x)$ é divisível por $x - (-2) = x + 2$.

$$\begin{array}{r|l} x^3 + 4x^2 + 9x + 10 & x + 2 \\ \cline{2-2} -x^3 - 2x^2 & x^2 + 2x + 5 \\ \cline{1-1} \quad 2x^2 + 9x & \\ \quad -2x^2 - 4x & \\ \cline{1-1} \quad\quad 5x + 10 & \\ \quad\quad -5x - 10 & \\ \cline{1-1} \quad\quad\quad 0 & \end{array}$$

Dividindo-se $p(x)$ por $x + 2$ obtemos quociente igual a $x^2 + 2x + 5$ e resto nulo $\Rightarrow f(x) = (x + 2)(x^2 + 2x + 5)$ o que mostra que $f(x)$ é **redutível** sobre $\mathbb{Z}$.

b) Seja $p = 3$. Temos que $p \nmid 1$, $p|6$, $p|(-9)$, $p|21$ e $p^2 \nmid 21$. Logo, pelo Critério de Eisenstein, $q(x)$ é **irredutível** sobre $\mathbb{Z}$.

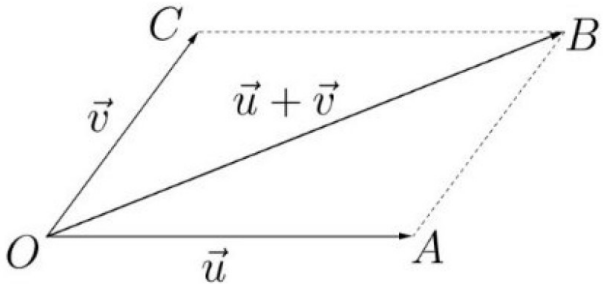
Capítulo 10

Testes

Neste capítulo, apresentamos testes do tipo objetivos e de múltipla escolha. São apresentadas várias alternativas A, B, C, ... entre as quais apenas uma deve ser correta.

10.1 Operações binárias

T1) Desde o início do Ensino Médio que é definida uma adição de vetores baseada principalmente em um diagrama formado por um paralelogramo:



Nesse tipo de diagrama, se os vetores forem determinados pelos segmentos orientados $\overrightarrow{OA}$ e $\overrightarrow{OC}$ do paralelogramo, então sua soma é definida como sendo determinada pelo segmento orientado $\overrightarrow{OB}$ da diagonal. A respeito da adição de vetores definida dessa forma podemos afirmar que ela

a) não é comutativa, não é associativa e não tem elemento neutro.

b) não é comutativa, não é associativa e tem elemento neutro.

c) não é comutativa, é associativa e não tem elemento neutro.

d) é comutativa, é associativa e não tem elemento neutro.

e) é comutativa, não é associativa e tem elemento neutro.

f) não é comutativa, é associativa e tem elemento neutro.

g) é comutativa, não é associativa e não tem elemento neutro.

h) é comutativa, é associativa e tem elemento neutro.

T2) Considere a seguinte resolução **detalhada** da equação do 1° grau $3x + 5 = 11$, onde o conjunto-universo é o dos números reais:

- $3x + 5 = 11$ (equação dada)
- $(3x + 5) + (-5) = 11 + (-5)$
- $3x + (5 + (-5)) = 6$
- $3x + 0 = 6$
- $3x = 6$
- $\frac{1}{3} \cdot (3x) = \frac{1}{3} \cdot 6$
- $(\frac{1}{3} \cdot 3) \cdot x = 2$
- $1 \cdot x = 2$
- $x = 2$. Logo, 2 é a única solução da equação.

Quais foram as propriedades da adição e da multiplicação de números reais utilizadas nessa resolução?

a) somente a comutatividade e associatividade da multiplicação

b) associatividade da adição, associatividade da multiplicação, elemento neutro da adição, elemento neutro da multiplicação, elemento inverso (simétrico) da adição, elemento inverso da multiplicação

c) somente a associatividade e comutatividade da adição

d) somente as propriedades do elemento neutro da multiplicação e da adição

e) somente o elemento inverso (simétrico) da adição e o elemento inverso da multiplicação.

T3) Se uma operação $\otimes$ definida em um conjunto $E \neq \emptyset$ for comutativa e associativa, então para quaisquer $x, y, z \in E$ temos que

a) $(x \otimes y) \otimes z = z \otimes (y \otimes x)$

b) $x \otimes x = y \otimes y$

c) $x \otimes y = z \otimes x$

d) $x \otimes (x \otimes y) = (y \otimes y) \otimes z$

e) $(x \otimes y) \otimes (y \otimes z) = y \otimes (x \otimes z)$

f) $(x \otimes y) \otimes (y \otimes z) = z \otimes (y \otimes x)$

T4) Selecione a única alternativa verdadeira entre as seguintes:

a) Toda operação associativa também é comutativa.

b) Se uma operação sobre um conjunto for associativa e comutativa, então esse conjunto tem que ser infinito.

c) Se uma operação sobre os números reais tem elemento neutro, então esse elemento neutro tem que ser o número 0 ou o número 1.

d) Existe operação que não é comutativa, nem associativa e nem tem elemento neutro.

e) Se uma operação tem elemento neutro, então todo elemento tem um inverso.

T5) Seja $*$ uma operação sobre um conjunto $E \neq \emptyset$. Definimos o quadrado de um elemento x, denotado por x^2, como sendo igual a $x*x$. Uma fórmula muito conhecida desde o Ensino Fundamental é $(a+b)(a-b) = a^2 - b^2$ que envolve as operações de adição, subtração e multiplicação de números reais. Uma demonstração dessa fórmula pode ser a seguinte:

$$\overbrace{(a+b)(a-b) = a(a-b) + b(a-b)}^{\text{igualdade 1}} = (a^2 - ab) + (ba - b^2) =$$

$$\overbrace{(a^2 - ab) + (ab - b^2) = ((a^2 - ab) + ab) - b^2}^{\text{igualdade 4}} = (a^2 + (-ab + ab)) - b^2 =$$

$$(a^2 + 0) - b^2 = a^2 - b^2$$

Quais são as propriedades utilizadas nas igualdades 1 e 4 dessa demonstração?

a) comutatividade e elemento neutro

b) distributividade e associatividade

c) associatividade e elemento inverso

d) distributividade e elemento neutro

e) comutatividade e associatividade

T6) Considere a operação $\odot$ definida no conjunto $A = \{1, 2, 3, 4\}$ cuja tábua é a seguinte:

$\odot$	1	2	3	4
1	3	4	1	2
2	4	3	2	1
3	1	2	3	4
4	2	1	4	3

Baseando-se nessa tábua, calcule o valor de $3 \odot (4^{-1} \odot 2)$.

a) 1

b) 2

c) 3

d) 4

e) Impossível de se efetuar tal operação.

T7) Sejam $M = \{1, 2, 3, 4, 6, 12\}$ e $*$ a operação sobre M definida por $x * y =$ mínimo múltiplo comum de x e y. Qual dos subconjuntos de M mostrados a seguir é fechado com relação a essa operação?

a) $A = \{3, 4, 12\}$

b) $B = \{1, 2, 3\}$

c) $C = \{2, 3, 4\}$

d) $D = \{3, 4, 6\}$

e) $E = \{1, 4, 6\}$

T8) Considerando as operações usuais de adição e potenciação sobre os números naturais positivos $\mathbb{N}^* = \{1, 2, 3, \dots\}$, qual das alternativas a seguir significa que *"a potenciação não é distributiva à esquerda com relação à adição"* ?

a) Existem $a, b, c \in \mathbb{N}^*$ tais que $(a + b)^c \neq a^c + b^c$

b) Existem $a, b, c \in \mathbb{N}^*$ tais que $a^{b+c} \neq a^b + a^c$

c) Existem $a, b, c \in \mathbb{N}^*$ tais que $a + b^c \neq a^c + b$

d) Existem $a, b, c \in \mathbb{N}^*$ tais que $a + b^c = a^c + b$

e) Existem $a, b, c \in \mathbb{N}^*$ tais que $a^{b+c} = a^b + a^c$

T9) Considere o conjunto $A = \{-5, -2, 0, 3, 5, 11, 19\}$ e a operação $x * y = \min(x, y) =$ menor entre x e y se $x \neq y$, ou x se $x = y$. Qual é o elemento neutro da operação $*$ definida sobre o conjunto A?

a) -5

b) -2

c) 0

d) 3

e) 5

f) 11

g) 19

h) a operação não tem elemento neutro

T10) Considere a operação $\oplus$ definida sobre o conjunto dos números reais $\mathbb{R}$: $x \oplus y = x + y + 3$. Qual é o elemento neutro dessa operação?

a) 0

b) 35

c) -35

d) -3

e) -29

f) 29

g) 3

T11) Considere a operação $\oplus$ definida sobre o conjunto dos números reais $\mathbb{R}$: $x \oplus y = x + y + 3$. Qual o elemento inverso de 29 com relação à operação $\oplus$?

a) 0

b) 35

c) -35

d) -3

e) -29

f) 29

g) 3

10.2 Grupos e subgrupos

T12) Considere as três definições mostradas a seguir:

[1] Um grupo é um conjunto G no qual está definida uma operação binária $*$ que satisfaz as seguintes propriedades:

- Existe $e \in G$ tal que $x * e = e * x = x$;
- Existe $x^{-1} \in G$ tal que $x * x^{-1} = e$;
- $x * (y * z) = (x * y) * z$ para quaisquer $x, y, z \in G$.

[2] Um grupo é um conjunto G no qual está definida uma operação binária $*$ que satisfaz as seguintes propriedades:

- $x * e = e * x = x$ para todo $x \in G$;
- Existem $x, x^{-1} \in G$ tal que $x * x^{-1} = e$;
- $x * (y * z) = (x * y) * z$ para quaisquer $x, y, z \in G$.

[3] Um grupo é um conjunto G no qual está definida uma operação binária $*$ que satisfaz as seguintes propriedades:

- Existe $x \in G$ tal que $x * e = e * x = x$;
- Para qualquer $x \in G$, existe $y \in G$ tal que $x * y = y * x = e$;
- Existem $x, y, z \in G$ tais que $x * (y * z) = (x * y) * z$.

Escolha uma resposta:

a) Todas as definições [1], [2], [3] estão corretas

b) Nenhuma das definições [1], [2], [3] está correta

c) Somente a definição [1] está correta

d) Somente a definição [2] está correta

e) Somente a definição [3] está correta

T13) Escolha a única alternativa verdadeira entre as seguintes:

a) Um grupo pode ter mais de um elemento neutro

b) O conjunto vazio pode ser um grupo, desde que se escolha uma operação conveniente

c) Se um grupo tem uma quantidade finita de elementos, então ele é abeliano (comutativo)

d) Uma equação da forma $a * x * b = c$ sempre tem uma única solução x em um grupo

e) O conjunto dos números inteiros $\mathbb{Z}$ é um grupo com a operação de multiplicação usual

T14) Associe cada item da primeira coluna com um item da segunda coluna mostradas a seguir:

[1] Conjunto dos números naturais $\mathbb{N}$ com a operação de adição de inteiros usual

[2] Conjunto de todos os pontos (x, y) do plano $\mathbb{R}^2$ com a operação de adição definida por $(a, b) + (c, d) = (a + c, b + d)$

[3] Conjunto de todas as matrizes 3×3 invertíveis com a operação de multiplicação de matrizes usual

[i] Grupo abeliano finito

[ii] Grupo não abeliano finito

[iii] Conjunto vazio

[iv] Conjunto unitário

[v] Grupo abeliano com uma infinidade de elementos

[vi] Não é um grupo

[vii] Grupo não abeliano com uma infinidade de elementos

A associação correta é:

a) 1-i, 2-ii, 3-iii

b) 1-iii, 2-iv, 3-i

c) 1-vii, 2-vi, 3-v

d) 1-v, 2-iv, 3-vi

e) 1-v, 2-iii, 3-vi

f) 1-vi, 2-v, 3-vii

T15) O conjunto $\mathbb{Q}[\sqrt{7}] = \{a + b\sqrt{7} \in \mathbb{R}^* \mid a, b \in \mathbb{Q}\}$ é um grupo com a operação de multiplicação usual dos números reais. Sendo $x = 2 - 5\sqrt{7} \in \mathbb{Q}[\sqrt{7}]$, qual é o inverso de x em $\mathbb{Q}[\sqrt{7}]$?

a) 0

b) $1 + \sqrt{7}$

c) $-\frac{2}{171} - \frac{5}{171}\sqrt{7}$

d) $\frac{2}{171} + \frac{5}{171}\sqrt{7}$

e) $2 + 5\sqrt{7}$

f) $-\frac{5}{171}$

g) $\sqrt{7}$

T16) Considerando $(G, *)$ um grupo e $a, b, c \in G$, qual é o elemento inverso de $a^{-1} * b * c^{-1}$?

a) $c^{-1} * b^{-1} * a$

b) $a * b * c$

c) $c * b^{-1} * a^{-1}$

d) $c * b^{-1} * a$

e) $c^{-1} * b^{-1} * a^{-1}$

T17) Considere as permutações $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ e $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ pertencentes ao grupo S_4. Determine o elemento desse grupo que corresponde ao resultado da operação $\sigma^{-1}\rho$ (que é o mesmo que $\sigma^{-1} \circ \rho$).

a) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$

b) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

c) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$

d) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

e) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

T18) Seja $G = \mathbb{R} - \{-1\}$ e a operação $*$ sobre G definida por $x * y = x + y + xy$. Então, temos que

a) $(G, *)$ é um grupo abeliano infinito

b) $(G, *)$ é um grupo abeliano finito

c) $(G, *)$ é um grupo não abeliano infinito

d) $(G, *)$ é um grupo não abeliano finito

e) $(G, *)$ não é um grupo

T19) Qual dos conjuntos H a seguir é um subgrupo de $\mathbb{Z}$ com a operação de adição usual dos inteiros?

a) $H = \{-1, 0, 1\}$

b) $H = \{2, 3, 5, 7, 11, 13, \dots\}$ = números primos positivos

c) $H = \{0, \pm 10, \pm 20, \pm 30, \pm 40, \dots\}$ = múltiplos de 10

d) $H = \{1, 2, 4, 8, 16, \dots\}$ = potências de 2 com expoentes não negativos

e) $H = \{\pm 1, \pm 3, \pm 5, \pm 7, \dots\}$ = inteiros ímpares

T20) Entre os conjuntos listados a seguir, qual é o único caso em que H é subgrupo do grupo G?

a) $H = [0, 2] = \{x \in \mathbb{R} \mid 0 \leq x \leq 2\}$, $G = \mathbb{R}$ com operação de adição usual

b) $H = \mathbb{R} - \mathbb{Q}$ = números irracionais, $G = \mathbb{R}$ com operação de adição usual

c) $H = \{e^n \mid n \in \mathbb{Z}\}$, $G = \mathbb{R}^*$ com operação de multiplicação usual, $e = 2,71828\ldots$

d) $H = \mathbb{R} - \mathbb{Q}$ = números irracionais, $G = \mathbb{R}^*$ com operação de multiplicação usual

e) $H = \{\pi^n \mid n \in \mathbb{N}\}$, $G = \mathbb{R}^*$ com operação de multiplicação usual, $\pi = 3,14159\ldots$

T21) Considere a seguinte demonstração:

"Seja $H = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} | a, b \in \mathbb{R}, a^2 + b^2 \neq 0 \right\} \subset GL_2(\mathbb{R})$ com a operação usual de multiplicação de matrizes quadradas 2×2. Escolhendo $a = 1$ e $b = 0$, temos que $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$. Logo, H não é o conjunto vazio.

Sejam $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ e $B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ dois elementos de H. Então $AB^{-1} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix}^{-1} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} \frac{c}{c^2+d^2} & \frac{-d}{c^2+d^2} \\ \frac{d}{c^2+d^2} & \frac{c}{c^2+d^2} \end{bmatrix} = \begin{bmatrix} \frac{ac+bd}{c^2+d^2} & \frac{-ad+bc}{c^2+d^2} \\ \frac{ad-bc}{c^2+d^2} & \frac{ac+bd}{c^2+d^2} \end{bmatrix} \in H$."

O que ficou assim demonstrado?

a) Que $H = GL_2(\mathbb{R})$

b) Que H é um subgrupo finito

c) Que H é um grupo abeliano que contém o $GL_2(\mathbb{R})$

d) Que H tem exatamente três elementos: I, A e B.

e) Que H é subgrupo de $GL_2(\mathbb{R})$

10.3 Homomorfismos, isomorfismos, grupos cíclicos

T22) Considerando $G = (\mathbb{R}^*, \cdot)$ o conjunto dos números reais não nulos com a operação de multiplicação usual, qual das funções $f : G \longrightarrow G$ a seguir é um homomorfismo?

a) $f(x) = \dfrac{1}{x}$

b) $f(x) = 4|x| + 2$

c) $f(x) = 1 + \cos^2 x$

d) $f(x) = 3x$

e) $f(x) = \log(1 + |x|)$

T23) Sejam $G = (\mathbb{R}^*, \cdot)$ e $f : G \longrightarrow G$ definida por $f(x) = \sqrt[3]{x}$. A respeito de f podemos afirmar que:

a) f não é homomorfismo de G em G e não possui inversa porque não é bijetora

b) f é um homomorfismo de G em G e sua inversa $f^{-1} : G \longrightarrow G$ também é.

c) f é um homomorfismo de G em G, mas sua inversa $f^{-1} : G \longrightarrow G$ não é.

d) f não é homomorfismo de G em G porque $\sqrt[3]{x+y} \neq \sqrt[3]{x} + \sqrt[3]{y} \Rightarrow f(x+y) \neq f(x) + f(y)$.

e) f não é homomorfismo de G em G, mas sua inversa $f^{-1} : G \longrightarrow G$ é.

T24) Considere a função exponencial $F : \mathbb{R} \longrightarrow \mathbb{R}_+^*$, $F(x) = e^x$. Considerando a adição usual de números reais no domínio e a multiplicação no contradomínio dessa função, qual das propriedades a seguir pode justificar que a exponencial é um homomorfismo de grupos?

a) $(e^x)^y = e^{xy}, \ \forall x, y \in \mathbb{R}$

b) Dado $a \in \mathbb{R}_+^*$, considerando $x = \log_e a$ temos $F(x) = e^{\log_e a} = a$

c) $e^x \cdot e^y = e^{x+y}, \ \forall x, y \in \mathbb{R}$

d) $e^0 = 1$ e $e^x > 0$ para todo $x \in \mathbb{R}$

e) Se existirem $x, y \in \mathbb{R}$ tais que $e^x = e^y$, então $x = y$

T25) Consideremos o seguinte homomorfismo $\varphi : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, $\varphi(x, y) = 2x - y$ definido entre os grupos aditivos $(\mathbb{Z} \times \mathbb{Z}, +)$ e $(\mathbb{Z}, +)$. Qual das alternativas a seguir contém apenas elementos do núcleo de φ?

a) $(0, 0)$, $(1, 1)$, $(2, 2)$

b) $(-1, 2)$, $(0, 0)$, $(1, -2)$

c) $(1, 2)$, $(2, 4)$, $(3, 6)$

d) $(-2,-1)$, $(0,1)$, $(1,0)$

e) $(-1,-1)$, $(0,0)$, $(1,1)$

T26) Qual é o núcleo do homomorfismo $f\ (\mathbb{R}^*,\cdot) \longrightarrow (\mathbb{R}^*,\cdot)$, $f(x) = \dfrac{1}{x^4}$?

a) $N(f) = \mathbb{R}^*$

b) $N(f) = \{1\}$

c) $N(f) = \{0\}$

d) $N(f) = \{\frac{1}{4},\ 4\}$

e) $N(f) = \{-1,\ 1\}$

T27) Escolha a alternativa correta entre as seguintes:

a) Existem inteiros $m > 2$ e $n > 2$ tais que o grupo de permutações $(S_m, \circ)$ é isomorfo ao grupo de classes de restos $(\mathbb{Z}_n, +)$.

b) O grupo de permutações $(S_5, \circ)$ é isomorfo ao grupo de classes de restos $(\mathbb{Z}_{120}, +)$.

c) Dados inteiros $m > 2$ e $n > 2$, o grupo de permutações $(S_m, \circ)$ não é isomorfo ao grupo de classes de restos $(\mathbb{Z}_n, +)$.

d) O grupo de permutações $(S_4, \circ)$ é isomorfo ao grupo de classes de restos $(\mathbb{Z}_4, +)$.

e) O grupo de permutações $(S_4, \circ)$ é isomorfo a algum subgrupo do grupo de classes de restos $(\mathbb{Z}_{24}, +)$.

T28) Qual é a ordem da permutação $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix} \in S_5$?

a) $o(\sigma) = 1$

b) $o(\sigma) = 2$

c) $o(\sigma) = 3$

d) $o(\sigma) = 4$

e) $o(\sigma) = 5$

T29) Considere as quatro afirmações a seguir a respeito do subgrupo $H = [4]$ do grupo multiplicativo $G = \mathbb{Q}^*$

1. $H \simeq (\mathbb{Z}, +)$
2. $H = [\frac{1}{4}]$
3. $1, 2, 4$ e 8 pertencem a H
4. $-4, 0$ e 4 pertencem a H

Escolha uma resposta:

a) Somente (1) e (3) são verdadeiras

b) Todas são falsas

c) Todas são verdadeiras

d) Somente (1) e (2) são verdadeiras

e) Somente (2) e (3) são verdadeiras

T30) Sejam $x = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in (GL_2(\mathbb{R}, \cdot)$ e $G = [x]$ = grupo cíclico gerado por x. Qual dos seguintes grupos J é isomorfo a G?

a) $J = (\mathbb{Z}_4, +)$

b) $J = (GL_4(\mathbb{R}), \cdot)$

c) $J = (\mathbb{Z}, +)$

d) $J = (\mathbb{R}_+^*, \cdot)$

e) $J = (S_4, \circ)$

T31) Sejam $y = \begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix} \in (GL_2(\mathbb{R}, \cdot)$ e $G = [y]$ = grupo cíclico gerado por y. Qual dos seguintes grupos J é isomorfo a G?

a) $J = (\mathbb{Z}_4, +)$

b) $J = (GL_4(\mathbb{R}), \cdot)$

c) $J = (\mathbb{Z}, +)$

d) $J = (\mathbb{R}_+^*, \cdot)$

e) $J = (S_4, \circ)$

10.4 Classes laterais, subgrupos normais, grupos quocientes

T32) Sejam $G = (\mathbb{Q}, +)$ e $H = \mathbb{Z}$ um subgrupo de G. Qual dos conjuntos listados a seguir corresponde a $\frac{1}{2} + H$, a classe lateral à esquerda, módulo H, definida pelo elemento $\frac{1}{2} \in G$?

a) $\{\ldots, -\frac{5}{2}, -\frac{3}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \ldots\}$

b) $\{\ldots, -\frac{5}{4}, -\frac{3}{4}, -\frac{1}{4}, \frac{1}{4}, \frac{3}{4}, \frac{5}{4}, \ldots\}$

c) $\{\ldots, -2, -\frac{3}{2}, -1, -\frac{1}{2}, 0, \frac{1}{2}, 1, \frac{3}{2}, 2, \ldots\}$

d) $\{-1, -\frac{1}{2}, 0, \frac{1}{2}, 1\}$

e) $\{\ldots, -7, -5, -3, -1, 1, 3, 5, 7, \ldots\}$

T33) Sejam $G = (\mathbb{Z}_9, +)$ e $H = \{\bar{0}, \bar{3}, \bar{6}\}$ subgrupo de G. Qual é a classe lateral, à direita, módulo H, determinada por $\bar{5} \in G$?

a) $\{\bar{0}, \bar{3}, \bar{6}\}$

b) $\{\bar{0}, \bar{1}, \bar{2}\}$

c) $\{\bar{1}, \bar{4}, \bar{7}\}$

d) $\{\bar{5}, \bar{6}, \bar{7}\}$

e) $\{\bar{2}, \bar{5}, \bar{8}\}$

T34) Sejam $G = (\mathbb{R}^*, \cdot)$ e $H = (\mathbb{Q}^*, \cdot)$. Existe uma infinidade de classes laterais à esquerda, módulo H, definidas por $x \in G$, e, entre elas, podemos afirmar que:

a) $2H \neq 3H$

b) $2H = \sqrt{2}H$

c) $3H = \sqrt{3}H$

d) $\sqrt{2}H \neq \sqrt{3}H$

e) $\sqrt{2}H \neq \sqrt{8}H$

T35) Sejam $G = (\mathbb{Z}_6, +)$ e $H = (\{\bar{0}, \bar{2}, \bar{4}\}, +)$. Entre as classes laterais à esquerda, módulo H, definidas por $x \in G$, podemos afirmar que:

a) $\bar{2} + H \neq \bar{4} + H$

b) $\bar{1} + H = \bar{3} + H$

c) $\bar{1} + H = \bar{0} + H$

d) $\bar{1} + H = \bar{4} + H$

e) $\bar{2} + H = \bar{3} + H$

T36) Um grupo G tem ordem 10. Se H for um subgrupo de G, quais as possibilidades para a ordem de H?

a) $o(H) = 100$

b) $o(H) = 4$ ou $o(H) = 8$

c) $o(H) = 4$ ou $o(H) = 6$ ou $o(H) = 9$

d) $o(H) = 3$ ou $o(H) = 7$ ou $o(H) = 8$

e) $o(H) = 1$ ou $o(H) = 2$ ou $o(H) = 5$ ou $o(H) = 10$

T37) Sejam G um grupo de ordem 120 e H um subgrupo de G de ordem 40. Quanto é o índice de H em G?

a) $(G : H) = 3$

b) $(G : H) = 60$

c) $(G : H) = 9$

d) $(G : H) = 80$

e) $(G : H) = 4$

T38) Sejam $G = (\mathbb{Z}_8, +)$ e H um subgrupo de G. Então podemos afirmar que:

a) A ordem de H é igual a 4, obrigatoriamente.

b) H pode ter ordem 6

c) Devemos ter $(G : H) = 4$, obrigatoriamente.

d) $\bar{0} \notin H$

e) $H \lhd G$

T39) Consideremos $x = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ e $y = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ dois elementos de $G = GL_2(\mathbb{R})$ e $H = [y]$ como sendo o grupo gerado pelo y:

$$H = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}, \right\}.$$

O que podemos afirmar a respeito de H e das classes xH e Hx?

a) Que $xH \neq Hx$ e, consequentemente, H é um subgrupo normal em G

b) Que $xH = Hx$ e, consequentemente, H não é um subgrupo normal em G

c) Que $xH \neq Hx$ e, consequentemente, H não é um subgrupo normal em G

d) Que $xH = Hx$ e, consequentemente, H é um subgrupo normal em G

e) Que $xH = Hx$ e, consequentemente, xH é um subgrupo normal em G

T40) Se $f : G \longrightarrow J$ for um homomorfismo de grupos e $N = N(f)$, então podemos afirmar que

a) $G/N = J/N$

b) $N \lhd G$

c) $N \lhd J$

d) $G/N \simeq J$

e) $J/N \simeq G$

T41) Sejam $G = GL_2(\mathbb{R})$ o conjunto de todas as matrizes reais 2×2 invertíveis e $S \subset G$ o conjunto de todas as matrizes reais 2×2 com determinante igual a 1. É possível mostrar que:

- $\varphi : (G, \cdot) \longrightarrow (\mathbb{R}^*, \cdot)$, $\varphi(X) = \det(X)$ é um homomorfismo de grupos;
- $N(f) = S$;
- φ é sobrejetora.

O que se pode concluir a partir daí?

a) $S \simeq G$

b) $\mathbb{R}^*/S \simeq G$

c) $G/S = \{0\}$

d) $G \simeq (\mathbb{R}^*, \cdot)$

e) $G/S \simeq (\mathbb{R}^*, \cdot)$

10.5 Anéis, subanéis, anéis de integridade, corpos

T42) Em todo anel comutativo A, para quaisquer $a, b, c \in A$, é sempre válido que:

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

b) $(a + b)^3 = a^3 + b^3$

c) $(a - b)^2 = a^2 - b^2$

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

e) $(a + b + c)^2 = a^2 + b^2 + c^2$

T43) Associe cada item da primeira coluna com um item da segunda coluna mostradas a seguir:

[1] Matrizes quadradas de ordem 3 com elementos reais $M_{3\times3}(\mathbb{R})$

[2] Conjunto de todas as funções de $\mathbb{R}$ em $\mathbb{R}$ com as operações $(f + g)(x) = f(x) + g(x)$ e $(f \cdot g)(x) = f(x) \cdot g(x)$

[3] Conjunto de todos os inteiros pares $(2\mathbb{Z}, +, \cdot)$

[i] Não é um anel

[ii] Anel comutativo, sem unidade

[iii] Anel comutativo, com unidade

[iv] Anel não comutativo, sem unidade

[v] Anel não comutativo, com unidade

A associação correta é:

a) 1-i, 2-ii, 3-iii

b) 1-iii, 2-iv, 3-i

c) 1-iii, 2-ii, 3-v

d) 1-v, 2-iv, 3-ii

e) 1-v, 2-iii, 3-ii

f) 1-ii, 2-v, 3-iv

T44) No anel $\mathbb{Z}_8$, qual é o conjunto S formado por todas as soluções da equação $x^2 = \bar{1}$?

a) $S = \{\bar{1}\}$

b) $S = \{\bar{0}\}$

c) $S = \{\bar{1}, -\bar{1}\}$

d) $S = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

e) $S = \{\bar{1}, \bar{3}\}$

T45) No anel $M_{2\times2}(\mathbb{R})$, sendo $x = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, quanto é o resultado da operação $x^0 + x^1 + x^2$?

a) $\begin{bmatrix} 8 & 12 \\ 18 & 26 \end{bmatrix}$

b) $\begin{bmatrix} 9 & 12 \\ 18 & 27 \end{bmatrix}$

c) $\begin{bmatrix} 9 & 9 \\ 27 & 18 \end{bmatrix}$

d) $\begin{bmatrix} 0 & 12 \\ 13 & 26 \end{bmatrix}$

e) $\begin{bmatrix} 8 & 18 \\ 9 & 27 \end{bmatrix}$

T46) Com a adição e multiplicação usuais, em qual dos casos a seguir temos que A é um subanel de B ?

a) $A = \mathbb{Z}_3$, $B = \mathbb{Z}_9$

b) $A =$ inteiros primos, $B = \mathbb{Z}$

c) $A = 2\mathbb{Z}$, $B = 8\mathbb{Z}$

d) $A = \mathbb{R} - \mathbb{Q}$, $B = \mathbb{R}$

e) $A = 4\mathbb{Z}$, $B = 2\mathbb{Z}$

T47) Qual dos seguintes conjuntos é um corpo com relação à adição $\bar{x} + \bar{y} = \overline{x + y}$ e multiplicação $\bar{x} \cdot \bar{y} = \overline{x \cdot y}$?

a) $\mathbb{Z}_9$

b) $\mathbb{Z}_{11}$

c) $\mathbb{Z}_{12}$

d) $\mathbb{Z}_{10}$

e) $\mathbb{Z}_8$

T48) Qual dos seguintes conjuntos é um anel de integridade? (adição e multiplicação são as usuais)

a) O conjunto $\mathbb{Q}$ dos números racionais

b) O conjunto $\mathbb{N}$ dos números naturais

c) $M_{2\times2}(\mathbb{Q})$

d) $\{f : \mathbb{Z} \longrightarrow \mathbb{Z} \mid f(1) = 1\}$

e) $\{f : \mathbb{Z} \longrightarrow \mathbb{Z} \mid f(0) = 0\}$

f) $M_{3\times3}(\mathbb{R})$

T49) Escolha a única alternativa verdadeira.

a) Existe um exemplo de corpo que não é anel de integridade

b) Existe um exemplo de corpo que tem apenas uma quantidade finita de elementos

c) Todo corpo tem que conter o conjunto dos números reais

d) Todo corpo que contiver os números racionais também terá que conter os números reais

e) Os conjuntos $\mathbb{Q}$ e $\mathbb{R}$ são exemplos de corpos e não existe outro corpo $\mathbb{K}$ diferente desses tal que $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{R}$.

T50) Qual dos seguintes conjuntos é um corpo com relação à adição e multiplicação usuais?

a) $\{a + b\sqrt{7} \mid a, b \in \mathbb{Z}\}$

b) $\{a + b\sqrt{7} \mid a, b \in \mathbb{R}, a > 0, b > 0\}$

c) $\{a + b\sqrt{7} \mid a, b \in \mathbb{Q}, a < 0, a < 0\}$

d) $\{a + b\sqrt{7} \mid a, b \in \mathbb{Q}\}$

e) $\{a + b\sqrt[3]{7} \mid a, b \in \mathbb{Q}\}$

10.6 Homomorfismos e isomorfismos de anéis

T51) Uma função $f : \mathbb{R} \longrightarrow \mathbb{R}$ possui as seguintes propriedades: $f(a + b) = f(a) + f(b)$ e $f(ab) = f(a)f(b)$ para quaisquer $a, b \in \mathbb{R}$. Como costuma ser denominada uma função como essa?

a) f é uma função contínua definida no anel $(\mathbb{R}, +, \cdot)$

b) f é uma transformação linear

c) f é uma função constante definida no anel $(\mathbb{R}, +, \cdot)$

d) f é uma função crescente definida no anel $(\mathbb{R}, +, \cdot)$

e) f é uma função monótona definida no anel $(\mathbb{R}, +, \cdot)$

f) f é um homomorfismo de anéis

T52) A função $g : \mathbb{Q} \longrightarrow \mathbb{Q}$ é um homomorfismo de anéis tal que $g(3) = 3$ e $g(5) = 5$. Podemos concluir que $g(8)$ e $g(9)$ são respectivamente iguais a:

a) 1 e 8

b) 8 e 9

c) 0 e 1

d) 0 e 0

e) 9 e 25

f) 64 e 81

T53) A função $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ é um homomorfismo do anel $(\mathbb{Z}, +, \cdot)$ no anel $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$. Nessas condições, quanto é $\varphi(0)$?

a) $(0, 0)$

b) $(1, 0)$

c) $(0, 1)$

d) $(1, 1)$

e) Impossível de se calcular

T54) Qual das funções a seguir é um homomorfismo de anéis?

a) $f : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R},\ f(x, y) = x^2 + y^2$

b) $g : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R},\ g(x, y) = x + y$

c) $h : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R},\ h(x, y) = 0$

d) $j : \mathbb{R} \longrightarrow \mathbb{R},\ j(x) = -x$

e) $p : \mathbb{R} \longrightarrow \mathbb{R},\ p(x) = x^2 - 5x + 6$

T55) A função $f : \mathbb{Z} \longrightarrow \mathbb{Z},\ f(x) = kx$, é um homomorfismo de anéis. Nessas condições, quais os possíveis valores para k ?

a) $k = 0$ ou $k = 1$

b) $k = 2$

c) $k = 1$ ou $k = 2$ ou $k = 3$

d) $k = -1$ ou $k = 1$

e) $k = -1$

T56) Considere as seguintes afirmações:

[1] Se A for um anel com unidade $1 \in A$ e $f : A \longrightarrow A$ um homomorfismo de anéis, então podemos concluir que $f(1) = 1$.

[2] Se A for um anel com unidade, $x \in A$ for invertível (com relação à multiplicação) e $f : A \longrightarrow A$ for um homomorfismo sobrejetor, então $f(x^{-1}) = [f(x)]^{-1}$.

[3] Sejam $f : A \longrightarrow B$ um homomorfismo de anéis e L um subanel de A. Então, a imagem direta de L pela f, $f(L)$, é um subanel de B.

Podemos afirmar que:

a) todas são verdadeiras

b) todas são falsas

c) somente [1] é verdadeira

d) somente [2] e [3] são verdadeiras

e) somente [3] é verdadeira

f) somente [2] é verdadeira

g) somente [1] e [2] são verdadeiras

h) somente [1] e [3] são verdadeiras

T57) Sendo $f : A \longrightarrow B$ um homomorfismo de anéis, que nome é dado a $f^{-1}(\{0\})$, a imagem inversa de $\{0\}$ pela função f ?

a) Domínio de f

b) Imagem de f

c) Valor mínimo de f

d) Núcleo de f

e) Função composta de f com a função constante nula

T58) Consideremos os anéis $A = (\mathbb{R}, +, \cdot)$ e $B = (M_{2\times2}(\mathbb{R}), +, \cdot)$ e o homomorfismo $f : A \longrightarrow B$ definido por $f(x) = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}$. O núcleo de f é:

a) $\{1\}$

b) $\{0\}$

c) $\{-1, 0, 1\}$

d) $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

e) $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

f) $(0, 0)$

g) $\{(1, 0),\ (0, 1)\}$

10.7 Ideais e anéis-quocientes

T59) Qual dos conjuntos I a seguir é um ideal de $\mathbb{R}$?

a) $I = \{0\}$

b) $I = \mathbb{Z}$

c) $I = \mathbb{Q}$

d) $I = \mathbb{R} - \mathbb{Q}$

e) $I = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$

T60) Qual dos conjuntos I a seguir é um ideal de $\mathbb{Z}$?

a) $I = \{-4m + 1 \,|\, m \in \mathbb{Z}\}$

b) $I = \{4m + 1 \,|\, m \in \mathbb{Z}\}$

c) $I = \{4m + 3 \,|\, m \in \mathbb{Z}\}$

d) $I = \{-4m \,|\, m \in \mathbb{Z}\}$

e) $I = \{4m \,|\, m \in \mathbb{Q}\}$

T61) Qual dos conjuntos I a seguir é um ideal de $\mathbb{R}^{\mathbb{R}}$, o conjunto de todas as funções de $\mathbb{R}$ em $\mathbb{R}$?

a) $I = \{f : \mathbb{R} \longrightarrow \mathbb{R} \,|\, f(-x) = f(x),\ \forall x \in \mathbb{R}\}$ = conjunto de todas as funções pares

b) $I = \{f : \mathbb{R} \longrightarrow \mathbb{R} \,|\, f(x) > 0,\ \forall x \in \mathbb{R}\}$ = conjunto de todas as funções positivas

c) $I = \{f : \mathbb{R} \longrightarrow \mathbb{R} \,|\, f(1) = 1\}$ = conjunto de todas as funções cujos gráficos passam pelo ponto $(1, 1)$

d) $I = \{f : \mathbb{R} \longrightarrow \mathbb{R} \,|\, f(-x) = -f(x),\ \forall x \in \mathbb{R}\}$ = conjunto de todas as funções ímpares

e) $I = \{f : \mathbb{R} \longrightarrow \mathbb{R} \,|\, f(0) = 0\}$ = conjunto de todas as funções cujos gráficos passam pela origem $(0, 0)$

T62) Selecione a única alternativa verdadeira:

a) Se I é um ideal de $\mathbb{Z}$, então I também é um ideal de $\mathbb{R}$

b) Se I é um ideal de $\mathbb{Z}$, então I também é um ideal de $\mathbb{Q}$

c) Todo subanel I de um anel comutativo A também é um ideal desse anel

d) Todo ideal I de um anel comutativo A também é um subanel desse anel

e) Existe um subconjunto finito com mais de 2 elementos que é ideal de $\mathbb{R}$

f) Existe um subconjunto finito com mais de 2 elementos que é ideal de $\mathbb{Q}$

T63) Sejam $A = \mathbb{Z}$ e $I = 7\mathbb{Z}$ com as operações usuais de adição e multiplicação e $x = 3 + I$, $y = 4 + I$ dois elementos do anel-quociente A/I. Calculando a soma $x + y$ e o produto $x \cdot y$ em A/I, obtemos respectivamente:

a) $4 + I$ e $5 + I$

b) $2 + I$ e $3 + I$

c) I e $5 + I$

d) $6 + I$ e $5 + I$

e) $2 + I$ e $1 + I$

T64) Seja J um ideal de um anel comutativo com unidade A. Os elementos neutros da adição e da multiplicação de A/J são respectivamente iguais a:

a) 1 e J

b) J e $1 + J$

c) 0 e J

d) $(-1)J$ e J

e) $-1 + J$ e $1 + J$

T65) Se p for um inteiro primo, o anel-quociente $\mathbb{Z}/p\mathbb{Z}$ é um corpo. Considerando $p = 11$, qual é o inverso multiplicativo de $x = 4 + 11\mathbb{Z} \in \mathbb{Z}/11\mathbb{Z}$?

a) $8 + 11\mathbb{Z}$

b) $5 + 11\mathbb{Z}$

c) $1 + 11\mathbb{Z}$

d) $9 + 11\mathbb{Z}$

e) $3 + 11\mathbb{Z}$

T66) A função $f : \mathbb{Z} \longrightarrow \mathbb{Z}_8$ definida por $f(x) = \bar{x}$ é sobrejetora e é um homomorfismo de anéis cujo núcleo é igual a $8\mathbb{Z}$, o conjunto dos inteiros múltiplos de 8. A partir dessas informações, podemos afirmar que:

a) $\frac{\mathbb{Z}}{\{0\}} \simeq \mathbb{Z}_8$

b) $\frac{\mathbb{Z}}{\{0\}} \simeq 8\mathbb{Z}$

c) $\mathbb{Z} \simeq 8\mathbb{Z}$

d) $\frac{\mathbb{Z}}{8\mathbb{Z}} \simeq \{0\}$

e) $\frac{\mathbb{Z}}{8\mathbb{Z}} \simeq \mathbb{Z}_8$

10.8 Polinômios

T67) Qual é o resto da divisão de $2x^5 + 3x^2 + 4x - 5$ por $x^3 + 2x^2 + 4$?

a) $21x^2 - 20x + 17$

b) $37x^2 - 21x + 11$

c) $-21x^2 + 20x - 37$

d) $21x^2 - 20x - 37$

e) $21x^2 + 20x - 17$

f) $-37x^2 - 20x + 17$

T68) Dividindo-se o polinômio $f(x)$ por $x^2 + 1$ obtém-se quociente $x - 2$ e resto $2x + 1$. Qual é o resto da divisão de $f(x)$ por $x - 3$?

a) 49

b) 19

c) 0

d) -13

e) 17

T69) Quando $p(x) = x^8 + x + 1 \in \mathbb{R}[x]$ é fatorado, um dos fatores é $x^2 + x + 1$. Sendo assim, podemos afirmar que:

a) $p(x) = (x^2 + x + 1)^4$

b) $p(x) = (x^2 + x + 1)(x^6 - x^5 + x^3 - x^2 + 1)$

c) $p(x) = (x^2 + x + 1)(x^2 + x - 1)(x^2 - x + 1)(x^2 - x - 1)$

d) $p(x) = (x^2 + x + 1)(x^6 + x^5 + x^3 + x^2 + x + 1)$

e) $p(x) = (x^2 + x + 1)(x^6 - x^5 + x^4 - x^3 + x^2 + 1)$

e) $p(x) = (x^2 + x + 1)(x^2 + x - 1)(x^4 - x^3 - x^2 - x - 1)$

T70) Determine os valores de A e B para que a igualdade

$$\frac{x}{x^2 - 9} = \frac{A}{x + 3} + \frac{B}{x - 3}$$

seja verificada para todo $x \in \mathbb{R} - \{-3, 3\}$.

a) $A = B = \frac{1}{2}$

b) $A = -2, B = 2$

c) $A = -\frac{1}{2}, B = 2$

d) $A = -2, B = \frac{1}{2}$

e) $A = B = 2$

T71) Se $f(x)$ for um polinômio de coeficientes reais de grau 3, qual é o grau do polinômio $g(x) = [f(x)]^3 + 10[f(x)]^2 - 4f(x) - 5$?

a) $\partial g = 6$

b) $\partial g = 8$

c) $\partial g = 5$

d) $\partial g = 7$

e) $\partial g = 9$

T72) Sendo $f(x) = \bar{2}x^2 - \bar{2}x + \bar{1} \in \mathbb{Z}_4[x]$, qual é o grau do polinômio $[f(x)]^2$?

a) 0

b) 1

c) 2

d) 3

e) 4

T73) Qual dos polinômios a seguir é irredutível sobre $\mathbb{Z}$?

a) $x^3 + 7x^2 + 14x - 21$

b) $x^4 - 5x^2 + 6$

c) $x^4 - 64$

d) $x^2 - 7x + 12$

e) $x^3 + 7x^2 + 14x$

T74) Quais são as raízes em $\mathbb{Z}_5$ do polinômio $p(x) = x^2 + \bar{4} \in \mathbb{Z}_5[x]$?

a) $\bar{3}$ e $\bar{4}$

b) $\bar{2}$ e $\bar{3}$

c) $\bar{1}$ e $\bar{2}$

d) $\bar{1}$ e $\bar{4}$

e) $\bar{2}$ e $\bar{4}$

T75) Qual é o conjunto S formado por todas as raízes da equação

$$10x^4 - 27x^3 - 110x^2 - 27x + 10 = 0 \text{ ?}$$

a) $\{-2, -\frac{1}{2}, \frac{1}{5}, 5\}$

b) $\{-5, -\frac{1}{2}, \frac{1}{5}, 2\}$

c) $\{-2, -\frac{1}{5}, \frac{1}{2}, 5\}$

d) $\{-4, -\frac{1}{2}, \frac{1}{3}, 2\}$

e) $\{-2, -\frac{1}{4}, \frac{1}{2}, 4\}$

T76) Escolha a única alternativa verdadeira.

a) Se A for um anel comutativo com unidade e $f(x), g(x) \in A[x]$ forem dois polinômios de graus 3 e 5, respectivamente, então seu produto $f(x) \cdot g(x)$ é um polinômio de grau 8

b) Se A for um anel comutativo com unidade e $f(x), g(x) \in A[x]$ forem dois polinômios de graus iguais a 4 , então seu produto $f(x) \cdot g(x)$ é um polinômio de grau 8

c) Se A for um anel comutativo com unidade e $f(x), g(x) \in A[x]$ forem dois polinômios de graus iguais a 4 , então sua soma $f(x) + g(x)$ é um polinômio de grau 4

d) Se A for um corpo e $f(x), g(x) \in A[x]$ forem dois polinômios de graus iguais a 4 , então seu produto $f(x) \cdot g(x)$ é um polinômio de grau 8

e) Se A for um corpo e $f(x), g(x) \in A[x]$ forem dois polinômios de graus iguais a 4 , então sua soma $f(x) + g(x)$ é um polinômio de grau 4

T77) O valor de k para que $p(x) = x^4 + kx^2 + 2x - 8$ seja divisível por $x + 2$ é:

a) -3

b) -1

c) 0

d) 1

e) 3

T78) O máximo divisor comum dos polinômios $x^4 + x^3 - 11x^2 + 20$ e $x^5 + 8x^4 + 23x^3 + 31x^2 + 20x + 5$ é

a) $x^2 - x + 5$

b) $x^2 - 5x + 1$

c) $x^2 + 5x + 5$

d) $x^2 + x + 5$

e) $x^3 + 5x - 1$

T79) As raízes racionais da equação $2x^5 + 23x^4 + 82x^3 + 98x^2 + 80x + 75 = 0$ estão contidas no conjunto

a) $\{1, 3, 5, 15, 25, 75, \frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \frac{15}{2}, \frac{25}{2}, \frac{75}{2}\}$

b) $\{\pm 1, \pm 3, \pm 5, \pm 15, \pm 25, \pm 75, \pm\frac{1}{2}, \pm\frac{3}{2}, \pm\frac{5}{2}, \pm\frac{15}{2}, \pm\frac{25}{2}, \pm\frac{75}{2}\}$

c) $\{\pm 1, \pm 3, \pm 6, \pm 15, \pm 25, \pm 60, \pm\frac{1}{2}, \pm\frac{3}{2}, \pm\frac{6}{2}, \pm\frac{15}{2}, \pm\frac{25}{2}, \pm\frac{60}{2}\}$

d) $\{\pm 1, \pm 3, \pm 5, \pm 15, \pm 25, \pm 75, \pm\frac{1}{4}, \pm\frac{3}{4}, \pm\frac{5}{4}, \pm\frac{15}{4}, \pm\frac{25}{4}, \pm\frac{75}{4}\}$

e) $\{\pm 1, \pm 3, \pm 5, \pm 15, \pm 25, \pm 75, \pm\frac{1}{8}, \pm\frac{3}{8}, \pm\frac{5}{8}, \pm\frac{15}{8}, \pm\frac{25}{8}, \pm\frac{75}{8}\}$

f) $\{-1, -3, -5, -15, -25, -5, -\frac{1}{2}, -\frac{3}{2}, -\frac{5}{2}, -\frac{15}{2}, -\frac{25}{2}, -\frac{75}{2}\}$

T80) Se $m = \sqrt[3]{45 - 29\sqrt{2}} + \sqrt[3]{45 + 29\sqrt{2}}$, então m é raiz da equação

a) $x^3 - 21x + 90 = 0$

b) $x^3 + 21x - 90 = 0$

c) $x^3 - 90x - 21 = 0$

d) $x^3 - 21x - 90 = 0$

e) $x^3 + 90x - 21 = 0$

Respostas dos testes

T1 - D	T2 - B	T3 - A	T4 - D	T5 - B
T6 - A	T7 - A	T8 - B	T9 - G	T10 - D
T11 - C	T12 - B	T13 - D	T14 - F	T15 - C
T16 - D	T17 - A	T18 - A	T19 - C	T20 - C
T21 - E	T22 - A	T23 - B	T24 - C	T25 - C
T26 - E	T27 - C	T28 - C	T29 - D	T30 - A
T31 - C	T32 - A	T33 - E	T34 - D	T35 - B
T36 - E	T37 - A	T38 - E	T39 - C	T40 - B
T41 - E	T42 - A	T43 - E	T44 - D	T45 - B
T46 - E	T47 - B	T48 - A	T49 - B	T50 - D
T51 - F	T52 - B	T53 - A	T54 - C	T55 - A
T56 - D	T57 - D	T58 - B	T59 - A	T60 - D
T61 - E	T62 - D	T63 - C	T64 - B	T65 - E
T66 - E	T67 - C	T68 - E	T69 - B	T70 - A
T71 - E	T72 - A	T73 - A	T74 - D	T75 - A
T76 - D	T77 - B	T78 - C	T79 - B	T80 - D

Referências Bibliográficas

[1] Domingues, H. H., Iezzi, G., *Álgebra Moderna*, Atual Editora Ltda., São Paulo, 1979.

[2] Gonçalves, A., *Introdução à Álgebra*, Projeto Euclides, Rio de Janeiro, 1979.

[3] Monteiro, L. H. J., *Elementos de Álgebra*, Ao Livro Técnico S. A., Rio de Janeiro, 1969.

[4] Fraleigh, J. B., *A first course in Abstract Algebra*, Addison–Wesley Publishing Company, Reading, 1966.

[5] Herstein, I. N., *Topics in Algebra*, Ginn and Company, Waltham, 1964.

[6] Ayres Jr, F., Jaisingh, L. R., *Theory and Problems of Abstract Algebra*, Schaum's Outline Series, 2nd. edition, McGraw Hill, New York, 2004.

Índice Remissivo

Lenimar Nunes de Andrade nasceu no sertão do Rio Grande do Norte no início da década de 60. Descobriu sua vocação para professor de Matemática aos 12 anos de idade quando dava aulas particulares a muitos colegas do colégio. Obteve o título de Bacharel em Matemática pela Universidade Federal da Paraíba em 1982, Mestre em Matemática pela Universidade Federal de Pernambuco em 1987 e de Doutor em Engenharia Elétrica pela UNICAMP em 1998. Em 1984, ingressou como professor de Matemática da Universidade Federal da Paraíba, em João Pessoa, e já teve oportunidade de ministrar mais de 25 disciplinas diferentes, algumas em nível de pós-graduação. Atualmente, é professor de Cálculo Numérico, Cálculo Diferencial e Integral, Cálculo Vetorial e Geometria Analítica para alunos de diversos cursos como Engenharia Civil, Engenharia Mecânica, Engenharia Elétrica, Engenharia da Computação, Bacharelado em Física, Bacharelado em Matemática, entre outros. Nos últimos 5 anos tem se dedicado também ao ensino a distância através da Universidade Aberta do Brasil.