Antonio Aparecido de Andrade é Professor do Departamento de Matemática do Instituto de Biociências, Letras e Ciências Exatas (Ibilce) da Universidade Estadual Paulista ``Júlio de Mesquita Filho" (Unesp), São José do Rio Preto - SP. Graduado em Matemática (Licenciatura) pelo Ibilce - Unesp. Mestre em Matemática pelo Instituto de Matemática e Computação Cientifica (Imecc) da Universidade Estadual de Campinas (Unicamp), Campinas - SP. Doutor em Engenharia Elétrica pela Faculdade de Engenharia Elétrica e de Computação (Feec) da Unicamp. Livre-docente pelo Ibilce - Unesp. Pós-doutorado pelo Departamento de Matemática do Imecc - Unicamp e pelo Departamento de Matemática e Estatistica da Universidade Estadual de San Diego, San Diego - California, EUA. Pesquisador na área de álgebra (teoria algébrica dos números), construções de reticulados, teoria da codificação, modulação e criptografia.

Antonio Aparecido de Andrade
Série Álgebra
Volume 5

Uma introdução às estruturas algébricas

Antonio Aparecido de Andrade

Uma introdução às estruturas algébricas

Volume 5

Antonio Aparecido de Andrade

UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
INSTITUTO DE BIOCIÊNCIAS, LETRAS E CIÊNCIAS EXATAS
CAMPUS DE SÃO JOSÉ DO RIO PRETO - SP
DEPARTAMENTO DE MATEMÁTICA

UMA INTRODUÇÃO ÀS

ESTRUTURAS ALGÉBRICAS

© 2022 - Antonio Aparecido de Andrade

Série Álgebra - Volume 5

Primeira Edição.

ISBN 979-85-35-49684-9

Antonio Aparecido de Andrade

São José do Rio Preto - SP
Janeiro - 2022

Sumário

Capítulo

1

Introdução

O presente texto foi elaborado em cima das disciplinas de álgebra ministradas nos Cursos de Graduação de Matemática (Licenciatura e Bacharelado) e Pós-graduação em Matemática do Instituto de Biociências, Letras e Ciências Exatas (Ibilce) da Universidade Estadual Paulista "Júlio de Mesquita Filho"(Unesp), Campus de São José do Rio Preto - SP.

Os conceitos de grupos, anéis e corpos são parte de uma área da matemática chamada álgebra abstrata ou álgebra moderna. Na álgebra abstrata a preocupação é em relação a conjuntos nas quais podemos operar algebricamente os elementos pertencentes a esse conjunto, ou seja, podemos combinar dois elementos a fim de obter um terceiro elemento com características dos dois primeiros. Nestas operações, são aplicadas regras que determinam a estrutura do conjunto.

O presente texto tem como objetivo de fazer uma breve introdução a álgebra abstrata introduzindo, no Capítulo 2, uma breve introdução á teoria dos conjuntos: definição, noção de conjuntos, relações de pertinência e inclusão, operações entre conjuntos. No Capítulo 3, apresentamos as relações binárias: definição, exemplos e representações, domínio, contradomínio, relação inversa, imagem direta e inversa de uma relação, composição de relações e propriedades de uma relação definida sobre um conjunto, relações de equivalência (definição e exemplos) e conjunto quociente, relações de ordem (definição e exemplos), conjuntos totalmente e parcialmente ordenados, elementos especiais em conjuntos parcialmente ordenados. No Capítulo 4, apresentamos as funções (definição e exemplos), funções injetoras, sobrejetoras e bijetoras, conjunto imagem direta e imagem inversa e suas propriedades em relação às operações entre conjuntos, aplicações monótonas, conjuntos equipotentes e conjuntos enumeráveis, exemplificando com alguns exemplos. No Capítulo 5, apresentamos os números naturais com suas principais operações, a aritmética dos números inteiros, axioma da boa

ordem, princípio de Indução finita, sistema de numeração decimal, divisibilidade, números primos, algoritmo da divisão de Euclides, Teorema Fundamental da Aritmética, máximo divisor comum, mínimo múltiplo comum, equações diofantinas lineares, aritmética modular, Pequeno Teorema de Fermat, Teorema de Euler e Teorema de Wilson. No Capítulo 6, apresentamos as operações binárias, também chamadas de operações de composição interna (definição e exemplos), propriedades de uma operação e tábua de uma operação definida sobre um conjunto finito. No Capítulo 7, apresentamos a teoria de grupos (definição e exemplos), subgrupos, principais propriedades, exemplos do grupo diedral e do grupo de permutações sobre um conjunto finito, e grupos cíclicos. No Capítulo 8, apresentamos as classes laterais, o Teorema de Lagrange, subgrupo normal e grupo quociente. No Capítulo 9, apresentamos os homomorfismos e isomorfismos de grupos e teoremas de isomorfismo. No Capítulo 10, apresentamos a teoria de grupos de permutações e o Teorema de Cayley. No Capítulo 11, apresentamos a teoria de anéis (definição e exemplos), anéis de integridade (domínios), subanéis e ideais, ideais principais, ideais primo e maximal, anel quociente, homomorfismo e isomorfismo de anéis e característica de um anel. No Capítulo 12, apresentamos a teoria de corpos (definição e exemplos), subcorpos, corpos de frações de um anel de integridade e corpos primos. No Capítulo 13, apresentamos a teoria de anel de polinômios em uma variável (definição e exemplos), grau de um polinômio, divisibilidade, algoritmo euclidiano, máximo divisor comum e mínimo múltiplo comum, raiz de um polinômio, algoritmo de Briot-Ruffini e relações de Girard. No Capítulo 14, apresentamos a teoria de anel de polinômios em uma variável sobre um corpo. Finalmente, apresentamos a fatoração e irredutibilidade de polinômios em uma variável e seus critérios. Finalmente, apresentamos a bibliografia utilizada ao longo do texto.

Capítulo

2

Teoria elementar dos conjuntos

A teoria dos conjuntos foi desenvolvida por Georg Ferdinand Ludwing Phillip Cantor (1845 - 1918) por volta de 1872. No início do século XX (1910 - 1913), a teoria de Cantor obteve um auxílio muito importante do matemático, filósofo e sociólogo Bertrand Russel (1872 - 1970). A ideia de conjunto é a mesma de coleção, classe de objetos, agrupamento, etc. Por exemplo, uma coleção de revistas é um conjunto e cada revista é um elemento desse conjunto. A grosso modo, um conjunto é qualquer coleção de objetos, os objetos que compoẽm um conjunto são chamados elementos e, neste caso, os elementos são distos que pertencem ao conjunto. No estudo da teoria dos conjuntos certas noções são consideradas primitivas, isto é, aceitas sem definição. Os conceitos primitivos da teoria dos conjuntos são: conjunto, elemento e relação de pertinência. A notação usada será:

1. para conjuntos são letras maiúsculas: A, B, C, $\cdots$, e
2. para elementos são letras minúsculas: a, b, c, $\cdots$

A relação de pertinência é entre elemento e conjunto, ou seja, se A é um conjunto e x um elemento, diz-se que $x \in A$ se x é um elemento do conjunto A e $x \notin A$ se x não é um elemento do conjunto A. As relações entre conjuntos são dadas por: contido ($\subset$), contido ou igual ($\subseteq$), contém ($\supset$), contém ou igual ($\supseteq$) e igualdade ($=$).

2.1 Conjuntos

O matemático inglês John Venn (1834 - 1923) adotou uma maneira de representar conjuntos que muito nos ajuda na visualização das operações entre conjuntos, onde os elementos de um

conjunto são representados por pontos interiores a uma região plana, limitada por uma linha fechada simples, isto é, uma linha que não se entrelaça, chamado diagrama de Euler-Venn. Basicamente, usamos três maneiras para representar os elementos de um conjunto.

1. Quando o conjunto é dado pela enumeração de seus elementos (mesmo quando possui infinitos elementos). Neste caso, escreve-se os elementos entre chaves e separados por vírgula. Por exemplo, $A = \{a_1, a_2, \ldots\}$.

2. Quando enuncia uma propriedade comum aos seus elementos, ou seja, o conjunto A é dado por $A = \{x : x \text{ possui}$
   $\text{tal propriedade}\}$.

3. Quando o conjunto é dado pelo diagrama de Euler-Venn.

Existem alguns tipos de conjuntos.

1. Conjunto vazio: é o conjunto que não possui elementos e denotado por $\{\}$ ou $\emptyset$. Por exemplo, $A = \{x \in \mathbb{R} : x^2 + 2 = 0\} = \emptyset$.

2. Conjunto unitário: é um conjunto que possui apenas um elemento. Por exemplo, o conjunto $A = \{x \in \mathbb{N} : 2 < x < 4\} = \{3\}$.

3. Conjunto finito: é o conjunto que possui um número finito de elementos. Por exemplo, $A = \{1, 3, 5, 7\}$.

4. Conjunto infinito: é o conjunto que possui um número infinito de elementos. Por exemplo, $A = \mathbb{N}$.

5. Conjunto universo U: é um conjunto ao qual pertencem todos os elementos de estudo.

Sejam A e B dois conjuntos.

1. Subconjunto $A \subseteq B$: se todo elemento x de A for também um elemento de B. Neste caso, A é chamado um subconjunto de B, ou seja,

   $$A \subseteq B \Longleftrightarrow (\forall x \in A \Longrightarrow x \in B).$$

   Quando $A \subseteq B$, diz-se que A está contido em B ou A é um subconjunto de B ou A é parte de B. O conjunto vazio é um conjunto sem elementos, e assim, $\emptyset$ é um subconjunto de qualquer conjunto A, inclusive dele mesmo, ou seja, $\emptyset \subseteq A$, para qualquer conjunto A. Além disso, o conjunto $\emptyset$ pode ser escrito como $\emptyset = \{x \in U : x \neq x\}$.

2. Conjuntos iguais: são conjuntos que possuem os mesmos elementos, ou seja,

   $$A = B \text{ se, e somente se, } A \subseteq B \text{ e } B \subseteq A,$$

   isto é, dois conjuntos são iguais quando têm os mesmos elementos.

3. Conjuntos distintos: dois conjuntos são distintos se não são iguais e denotado por $A \neq B$. Neste caso, existe um elemento $x \in A$ tal que $x \notin B$ ou existe um elemento $x \in B$ tal que $x \notin A$. Pode acontecer de $A \neq B$, mas $A \subset B$.

O conjunto das partes de um conjunto A é definido por

$$\mathcal{P}(A) = \{X : X \subseteq A\},$$

ou seja, $\mathcal{P}(A)$ é o conjunto formado por todos os subconjuntos de A. Neste caso, X é um subconjunto de A e X é um elemento de $\mathcal{P}(A)$, ou seja, $A \subseteq X$ e $X \in \mathcal{P}(A)$. Agora, se A tem n elementos, então $\mathcal{P}(A)$ tem 2^n elementos. Por exemplo,

1. se $A = \{a, b\}$, com $a \neq b$, então $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.
2. se $A = \emptyset$, então $\mathcal{P}(A) = \{\emptyset\}$.

As operações entre conjuntos são: união ($\cup$), interseção ($\cap$), diferença ou subtração ($-$) e complementar (c). Assim, em relação a dois conjuntos A e B temos as seguintes operações.

1. União: $A \cup B = \{x \in U : x \in A \text{ ou } x \in B\}$. Neste caso, vale as seguintes propriedades:
   - $A \cup B = B \cup A$ (comutativa).
   - $A \cup (B \cup C) = (A \cup B) \cup C$ (associativa).
   - $A \subseteq A \cup B$ e $B \subseteq A \cup B$.
   - $A \subseteq B$ se, e somente se, $A \cup B = B$.
   - $A = A \cup A$, $A = A \cup \emptyset$ e $U = A \cup U$.
2. Interseção: $A \cap B = \{x \in U : x \in A \text{ e } x \in B\}$. Neste caso, vale as seguintes propriedades:
   - $A \cap B = B \cap A$ (comutativa).
   - $A \cap (B \cap C) = (A \cap B) \cap C$ (associativa).
   - $A \cap B \subseteq A$ e $A \cap B \subseteq B$.
   - $A \cap A = A$, $A \cap \emptyset = \emptyset$ e $A \cap U = A$.
   - $A \subseteq B$ se, e somente se, $A \cap B = A$.
3. Subtração: $A - B = \{x \in U : x \in A \text{ e } x \notin B\}$. Neste caso, vale as seguintes propriedades
   - $A = B$ se, e somente se, $A - B = B - A = \emptyset$.
   - $A \neq B$ se, e somente se, $A - B \neq B - A$.
   - $A - A = \emptyset$, $A - B \subseteq A$, $A - \emptyset = A$ e $A - U = \emptyset$.
4. Complementar de A: $A^c = \{x \in U : x \notin A\}$.

5. Complementar de A em relação a B (neste caso, devemos ter $A \subseteq B$) é definido por $A_B^c = \{x \in U : x \in B \text{ e } x \notin A\} = B - A$. Se $B = U$, então $A_U^c = \{x \in U : x \notin A\}$. Nesse caso, vale as seguintes propriedades:

   - se $A \subseteq B$, se e somente se $B - A = A_B^c$, ou seja, quando A é um subconjunto de B, o conjunto diferença $B - A$ é chamado conjunto complementar de B em relação ao conjunto A.
   - $\emptyset_U^c = U$ e $U_U^c = \emptyset$.
   - $A_U^c \cap A = \emptyset$ e $A_U^c \cup A = U$.
   - $\emptyset_A^c = A$ e $\emptyset_\emptyset^c = \emptyset$.

6. Produto cartesiano: $A \times B = \{(x, y) : x \in A \text{ e } x \in B\}$. Nesse caso, vale as seguintes propriedades:

   - $A \times (B \times C) = (A \times B) \times C$ (associativa).
   - $A \times B \neq B \times A$.

Agora, se A, B e C são conjuntos, então

1. $A \subseteq A$ (reflexiva).
2. Se $A \subseteq B$ e $B \subseteq A$, então $A = B$ (anti-simétrica).
3. Se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$ (transitiva).
4. Leis de Morgan do matemático inglês Augustus de Morgan (1806 - 1871):

   - $(A \cup B)^c = A^c \cap B^c$ e
   - $(A \cap B)^c = A^c \cup B^c$.

5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ e $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (distributiva).

2.1.1 Exercícios

1. Sejam $A = \{x \in \mathbb{N} : x^2 + 1 \leq 2\}$ e $B = \{x \in \mathbb{Z} : -1 < x < 2\}$. Determine $A \cap B$, $A \cup B$, $A \times B$, $A - B$, A_B^c e B_A^c.
2. Se $A = \emptyset$, determine $\mathcal{P}(A)$.
3. Se $A = \{\emptyset\}$, determine $\mathcal{P}(A)$.
4. Se $A = \{1, 2, 3, 4, 5\}$, determine $\mathcal{P}(A)$.
5. Se $(A_i)_{i \in I}$ é uma família de subconjuntos de um conjunto E e se $(B_j)_{j \in J}$ é uma família de subconjuntos de um conjunto F, mostre que $(\bigcup_{i \in I} A_i) \times (\bigcup_{j \in J} B_j) = \bigcup_{(i,j) \in I \times J} (A_i \times B_j)$.

6. Considere a família de intervalos $(A_i)_{i\in\mathbb{N}}$, onde $A_i =]0, \frac{1}{i}[$. Mostre que $\bigcap_{i\in\mathbb{N}} A_i = \emptyset$.

7. Seja $A =]0, 1[$ e considere a família de intervalos $(A_i)_{i\geq 2}$, onde $A_i =]\frac{1}{i}, 1[$.

   (a) Mostre que $\bigcup_{i\geq 2} A_i = A$.

   (b) Mostre que $A_{i_1} \cup \cdots \cup A_{i_n} \neq A$, para quaisquer que sejam $i_1, \cdots, i_n$.

8. Sejam $A = \{x \in \mathbb{Z} - \{0\} : \frac{30}{x} = n, \text{ onde } n \in \mathbb{N}\}$ e $B = \{x \in \mathbb{R} : x = 3n, \text{ onde } n \in \mathbb{N}\}$. Determine $A \cap B$, $A \cup B$, $A \times B$, $A - B$, A^c_B e B^c_A.

2.2 Conjuntos numéricos

Os principais conjuntos formados por números são dados por:

1. $\mathbb{N} = \{0, 1, 2, \cdots\}$ é chamado conjunto dos números naturais.

2. $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ é chamado conjunto dos números inteiros.

3. $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z} \text{ e } b \neq 0\}$ é chamado conjunto dos números racionais. Um número racional é representado por uma razão entre dois inteiros, ou seja, é uma dízima periódica.

4. $\mathbb{I}$ é chamado o conjunto dos números irracionais. Um número irracional é um número com infinitas casas decimais e não periódica.

5. $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$ é chamado o conjunto dos números reais.

6. $\mathbb{C} = \{a + bi : a, b \in \mathbb{R} \text{ com } i^2 = -1\}$ é chamado o conjunto dos números complexos.

7. $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ij = k = -ji, jk = i = -kj, ki = j = -ik\}$ é chamado o conjunto dos números quatérnios de Hamilton.

Esses conjuntos, com exeção dos números irracionais, possuem as operações de adição (soma) e multiplicação (ou produto) muito bem definidas. Em relação a adição, considerando $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$, segue que

1. $a + b \in A$, para todo $a, b \in A$, chamada propriedade do fechamento.

2. $a + (b + c) = (a + b) + c$, para todo $a, b, c \in A$, chamada propriedade associativa.

3. $a + b = b + a$, para todo $a, b \in A$, chamada propriedade comutativa.

4. $a + 0 = a$, para todo $a \in A$, onde o 0 é chamado elemento neutro.

5. $a + (-a) = 0$, para todo $a \in A$, onde $-a$ é chamado elemento oposto (ou simétrico) de a.

Em relação a multiplicação (produto), considerando $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$, segue que

1. $ab \in A$, para todo $a, b \in A$, chamada propriedade do fechamento.

2. $a(bc) = (ab)c$, para todo $a, b, c \in A$, chamada propriedade associativa.

3. $a1 = a$, para todo $a \in A$, onde o elemento 1 é chamado elemento neutro.

4. Se $ab = 0$, então $a = 0$ ou $b = 0$, com $a, b \in A$, chamada *Lei do Anulamento do Produto.*

Além disso,

1. $ab = ba$, para todo $a, b \in A$, chamada propriedade comutativa, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.

2. Para todo $a \in A - \{0\}$, existe $a^{-1} \in A - \{0\}$ tal que $aa^{-1} = 1$, onde $A = \mathbb{Q}, \mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$. O elemento a^{-1} é chamado elemento inverso (ou simétrico) de a.

Em relação a adição e a multiplicação, segue que $a(b + c) = ab + ac$ e $(a + b)c = ac + bc$, para todo $a, b, c \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$, chamada operação distributiva em relação a adição) e a multiplicação. Existe uma operação de ordem, denotada por $\leq$, que satisfaz as seguintes propriedades básicas:

1. $a \leq a$, para todo $a \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$, chamada propriedade reflexiva.

2. Se $a \leq b$ e $b \leq a$, então $a = b$, com $a, b \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$, chamada propriedade anti-simétrica.

3. Se $a \leq b$ e $b \leq c$, então $a \leq c$, com $a, b, c \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$, chamada propriedade transitiva.

4. $a \leq b$ ou $b \leq a$, para todo $a, b \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$, chamada propriedade da totalidade.

5. Se $a \leq b$, então $a+c \leq b+c$, com $a, b, c \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$, chamada propriedade da compatibilidade com a adição.

6. Se $0 \leq a$ e $0 \leq b$, então $0 \leq ab$, com $a, b \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$, chamada propriedade da compatibilidade com a multiplicação.

Em relação a regra dos sinais, segue as seguintes propriedades:

1. Se $a > 0$ e $b > 0$, então $ab > 0$, com $a, b \in A$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$.

2. $a < 0$ e $b < 0$, então $ab > 0$, com $a, b \in A$, onde $A = \mathbb{Z}, \mathbb{Q}, \mathbb{I}$ ou $\mathbb{R}$.

3. Se $a > 0$ e $b < 0$, então $ab < 0$, com $a, b \in A$, onde $A = \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$.

Finalmente, as seguintes notações são usadas para denotarem os seguintes conjuntos:

1. $A^* = \{a \in A : \text{ existe } a^{-1} \in A \text{ tal que } aa^{-1} = 1\}$, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$, chamado conjunto dos elementos inversíveis de A.

2. $A_+ = \{x \in A : x \geq 0\}$ é chamado o conjunto dos elementos positivos de A, onde $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$.

3. $A_+ - \{0\} = \{x \in A : x > 0\}$ é chamado o conjunto dos elementos estritamente positivos de A.

4. $A_- = \{x \in A : x \leq 0\}$ é chamado o conjunto dos elementos negativos de A, onde $A = \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$.

5. $A_- - \{0\} = \{x \in A : x < 0\}$ é chamado o conjunto dos elementos estritamente negativos de A, onde $A = \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$.

2.2.1 Exercícios

1. Mostre que não existe um quadrado perfeito a^2 cujo último dígito é 2, 3, 7 ou 8.

2. Mostre que 44444444444444444443 não é um quadrado perfeito.

3. Mostre que $888\cdots882$ não é um quadrado perfeito.

4. Mostre que não existe um quadrado perfeito cujo os dois últimos dígitos são 85.

5. Mostre que $\sqrt{2}$ é irracional.

6. Mostre que $\sqrt{3}$ é irracional.

7. Mostre que $\sqrt[3]{4}$ é irracional.

8. Mostre que $\sqrt{6}$ é irracional.

9. Mostre que $\frac{1}{3}\sqrt{2} + 5$ é irracional.

10. Mostre que $log_5 2$ e $log_3 5$ são irracionais.

11. Mostre que $\sqrt{101}$ é irracional.

12. Mostre que $\sqrt{p}$ é irracional, onde p é um primo.

Capítulo

3

Relações binárias

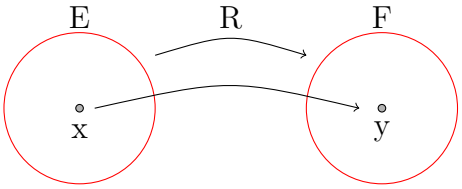
Conhecemos as operações fundamentais nos números naturais: a adição, a subtração, a multiplicação e a divisão. Mais explicitamente, dados dois números naturais, m e n, a adição associa o número $m + n$, chamado soma ou total de m com n; a subtração associa o número $m - n$, chamado de diferença entre m e n; a multiplicação, aos dois números, associa o número mn, chamado de produto de m por n; e a divisão associa o número m/n, chamado de quociente entre m e n. Observamos que a adição e a multiplicação de números naturais são sempre possíveis, isto é, dados dois números naturais é sempre possível encontrar um número natural que represente sua soma ou seu produto, o mesmo não ocorre quando se trata da subtração e da divisão. Este capítulo tem como propósito de abordar os conceitos básicos que serão fundamentais para o entendimento dos demais capítulos do presente texto. Os conteúdos abordados são algumas noções sobre relações binárias, relações de equivalência, classes de equivalência, conjunto quociente e relações de ordem. Deste modo, neste capítulo, apresentamos as relações binárias juntamente com domínio e imagem, relação inversa, relações e equivalências, classes de equivalências, conjunto quociente e partição de um conjunto, e em seguida, apresentamos as relações de ordens juntamente com os limites superiores de um conjunto, máximo de um conjunto, limites inferiores de um conjunto, mínimo de um conjunto, supremo e ínfimo de um conjunto, elementos maximais e elementos minimais de um conjunto.

3.1 Relações binárias

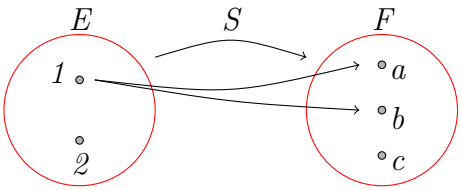
Sejam E e F dois conjuntos não vazios. O produto cartesiano de E por F, denotado por $E \times F$, é definido por $E \times F = \{(x, y) : x \in E \text{ e } y \in F\}$. Neste caso, $(a, b) = (c, d)$ se, e somente se, $a = c$ e $b = d$. Além disso, se $E = F$, então $E \times E = E^2$.

Definição 3.1.1. *Uma relação (binária) de E em F é um subconjunto R de $E \times F$. Se $E = F$, então R é chamada uma relação sobre E. De um modo geral, uma relação binária é qualquer conjunto de pares ordenados.*

Podemos representar E e F por meio do diagrama de Venn e indicamos cada par $(x, y) \in R$ por uma flecha com origem x e extremidade y, conforme a figura abaixo.



Exemplo 3.1.1. *Seja $E \times F = \{(1, x), (1, y), (1, z), (2, x), (2, y), (2, z)\}$, onde $E = \{1, 2\}$ e $F = \{a, b, c\}$. Assim, $R = \emptyset$, $S = \{(1, a); (1, b)\}$ e $T = E \times F$ são relações binárias. O diagrama de Venn da relação S é dada por:*



3.1.1 Domínio e imagem

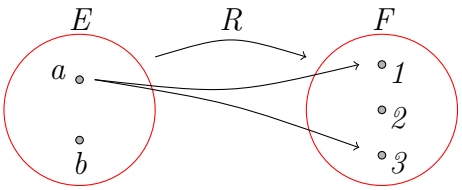
Sejam E e F conjuntos não vazios e R uma relação de E em F. Dados $a \in E$ e $b \in F$, se $(a, b) \in R$, dentotamos aRb, e se $(a, b) \notin R$, dentotamos aR_nb.

Exemplo 3.1.2. *Se $E = F = \{1, 2\}$ e $R = \{(1, 2), (2, 1)\}$, então $1R2$ e $2R1$. Mas, como $(1, 1), (2, 2) \notin R$, segue que $1R_n1$ e $2R_n2$.*

Definição 3.1.2. *Seja $R \subseteq E \times F$ uma relação.*

1. *O domínio de R é definido como $Dom(R) = \{x \in E :$ existe $y \in F$ tal que $(x, y) \in R\}$.*
2. *A imagem de R é definida como $Im(R) = \{y \in F :$ existe $x \in E$ tal que $(x, y) \in R\}$.*
3. *O contra-domínio de R é definido por $Cdom(R) = F$.*

Exemplo 3.1.3. *Se $E = \{a, b\}$, $F = \{1, 2, 3\}$ e $R = \{(a, 1), (a, 3)\}$, então $Dom(R) = \{a\}$, $Im(R) = \{1, 3\}$ e $Cdom(R) = \{1, 2, 3\}$. O diagrama de Venn é dado por:*



3.1.2 Relação inversa

Sejam E e F conjuntos não vazios e R uma relação de E em F.

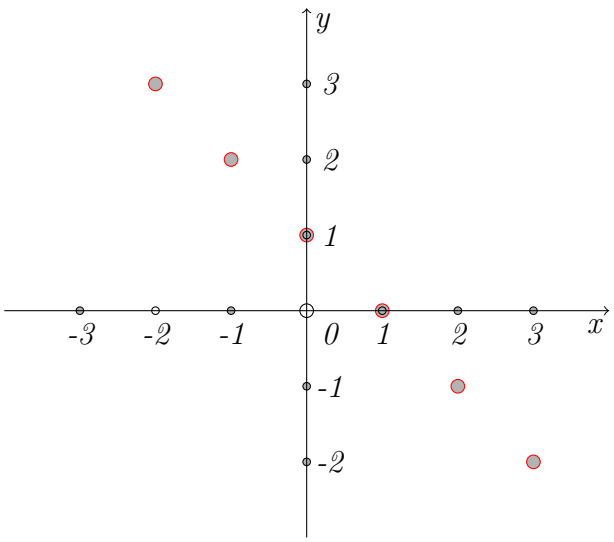
Definição 3.1.3. *A relação inversa de R é definida como* $R^{-1} = \{(y, x) \in F \times E : (x, y) \in R\}$.

Exemplo 3.1.4. *Se* $E = \{a, b\}$, $F = \{1, 2, 3\}$ *e* $R = \{(a, 1), (a, 2)\}$, *então* $R^{-1} = \{(1, a), (2, a)\}$. *Os diagramas de Venn de R e R^{-1} são dados, respectivamente, por:*

Exemplo 3.1.5. *Seja a relação* $R \subseteq \mathbb{Z}^2$ *definida por* $R = \{(x, y) \in \mathbb{Z}^2 : x + y = 1\}$. *Neste caso,*

1. $Dom(R) = \{x \in \mathbb{Z} :$ *existe* $y \in \mathbb{Z}$ *tal que* $x + y = 1\} = \mathbb{Z}$,
2. $Im(R) = \{y \in \mathbb{Z} :$ *existe* $x \in \mathbb{Z}$ *tal que* $x + y = 1\} = \mathbb{Z}$ *e*
3. $R^{-1} = \{(y, x) \in \mathbb{Z}^2 : (x, y) \in R\} = \{(y, x) \in \mathbb{R}^2 : x + y = 1\} = R$.

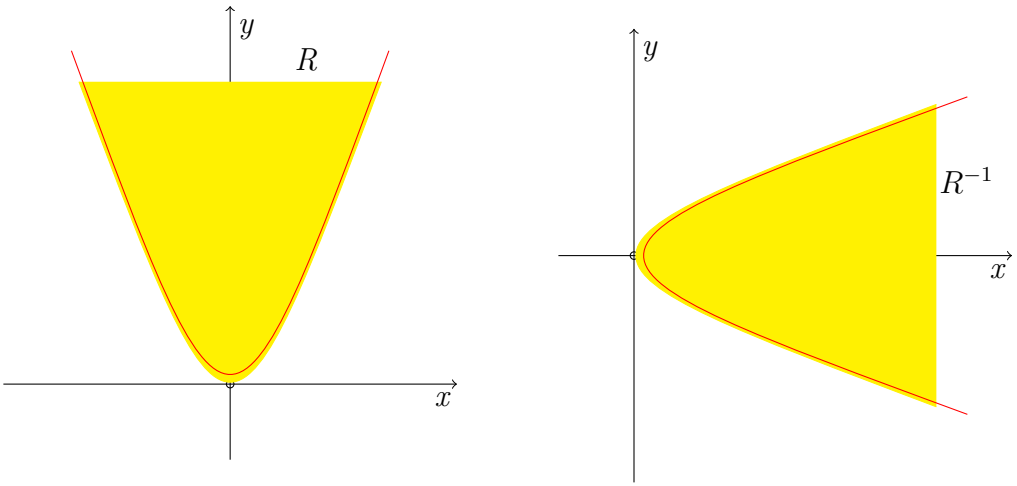
Graficamente, $R = R^{-1}$ *é dada por*



Exemplo 3.1.6. *Seja a relação* $R \subseteq \mathbb{R}^2$ *definida por* $R = \{(x, y) \in \mathbb{R}^2 : y \geq x^2\}$. *Neste caso,*

1. $Dom(R) = \{x \in \mathbb{R} :$ *existe* $y \in \mathbb{R}$ *tal que* $y \geq x^2\} = \mathbb{R}$,
2. $Im(R) = \{y \in \mathbb{R} :$ *existe* $x \in \mathbb{R}$ *tal que* $y \geq x^2\} = \mathbb{R}_+$ *e*
3. $R^{-1} = \{(y, x) \in \mathbb{R}^2 : (x, y) \in R\} = \{(y, x) \in \mathbb{R} : y \geq x^2\} = \{(x, y) \in \mathbb{R}^2 : x \geq y^2\}$.

Graficamente, R e R^{-1} são dadas, respectivamente, por



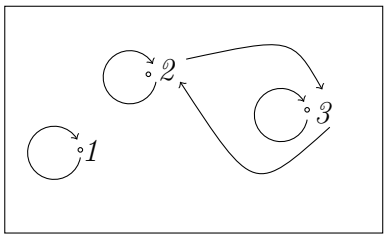
3.1.3 Relação de equivalência

O conceito de relação de equivalência é bastante intuitivo, mas de fundamental importância para o estudo de qualquer área da matemática. Para isso, sejam E um conjuntos não vazio e R uma relação sobre E.

Definição 3.1.4. *A relação R é chamada relação de equivalência se:*

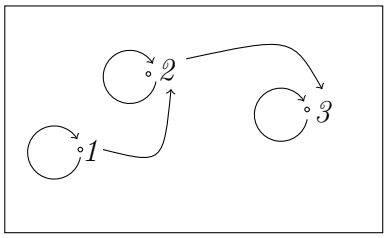
1. *xRx, para todo $x \in E$, ou seja, R é reflexiva.*
2. *Se xRy, então yRx, para todo $x, y \in E$, ou seja, R é simétrica.*
3. *Se xRy e yRz, então xRz, para todo $x, y \in E$, ou seja, R é transitiva.*

Exemplo 3.1.7. *Seja $E = \{1, 2, 3\}$. A relação $R = \{(1,1), (2,2), (3,3), (2,3), (3,2)\}$ é uma relação de equivalência, uma vez que é reflexiva, simétrica e transitiva.*



Exemplo 3.1.8. *Seja $E = \{1, 2, 3\}$. A relação $S = \{(1,1), (2,2), (3,3), (1,2), (2,3)\}$ não é uma*

relação de equivalência, pois S não é simétrica, uma vez que $(1,2) \in S$, mas $(2,1) \notin S$.

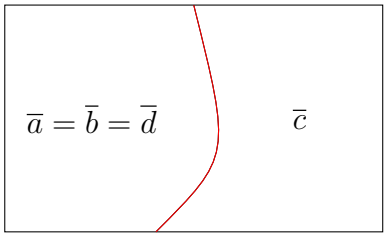


3.1.4 Classe de equivalência

A partir das relações de equivalência surgem as classes de equivalências que são de suma importância para gerar os conjuntos quocientes que veremos na próxima seção. Para isso, seja R uma relação de equivalência sobre um conjunto não vazio E.

Definição 3.1.5. *A classe de equivalência de um elemento $a \in E$, indicada por $\overline{a}$, é definida por $\overline{a} = \{x \in E : xRa\}$.*

Exemplo 3.1.9. *Seja $R = \{(a,a),(b,b),(c,c),(d,d),(a,b),(b,a),(b,d),(d,b),(a,d),(d,a)\}$ uma relação de equivalência sobre $E = \{a,b,c,d\}$. Neste caso, $\overline{a} = \{a,b,d\}$, $\overline{b} = \{a,b,d\}$, $\overline{c} = \{c\}$, $\overline{d} = \{a,b,d\}$, $\overline{a} \cap \overline{c} =$ e $\overline{a} \cup \overline{c} = E$. Graficamente, o conjunto E é dado por:*



Proposição 3.1.1. *Se R é uma relação de equivalência sobre E, então*

1. *$a \in \overline{a}$, para todo $a \in E$.*
2. *$E = \cup_{a \in E} \overline{a}$.*
3. *$\overline{a} \cap \overline{b} = \emptyset$ ou $\overline{a} = \overline{b}$, para todo $a, b \in E$.*

Demonstração. Para (1), como R é reflexiva, se $a \in E$, então aRa, ou seja, $a \in \overline{a}$. Para (2), por definição $\overline{a} \subseteq E$, e assim, $\cup_{a \in E} \overline{a} \subseteq E$. Por outro lado, se $a \in E$, então $a \in \overline{a}$, ou seja, $a \in \cup_{a \in E} \overline{a}$. Portanto, $E = \cup_{a \in E} \overline{a}$. Para (3), se $\overline{a} \cap \overline{b} \neq \emptyset$, então existe $x \in E$ tal que $x \in \overline{a} \cap \overline{b}$. Assim, $x \in \overline{a}$ e $x \in \overline{B}$, ou seja, xRa e xRb. Como R é simétrica e transitiva, segue que aRb. Agora, se $x \in \overline{a}$, então xRa. Como R é transitiva, segue que xRb, ou seja, $x \in \overline{b}$. Assim, $\overline{a} \subseteq \overline{b}$. De modo análogo, segue que $\overline{b} \subseteq \overline{a}$. Portanto, $\overline{a} = \overline{b}$. □

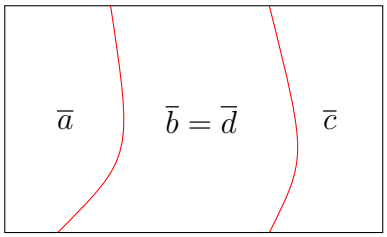
Observação 3.1.1. *As classes de equivalências determinam uma partição em E. Reciprocamente, se existe uma partição em E, então existe uma relação de equivalência R sobre E, de modo que, se aRb, então a e b pertencem ao mesmo conjunto.*

3.1.5 Conjunto quociente

Seja R uma relação de equivalência sobre um conjunto não vazio E.

Definição 3.1.6. *O conjunto quociente de E por R, indicado por E/R, é o conjunto de todas as classes de equivalências segundo a relação R, ou seja, $E/R = \{\overline{a} : a \in E\}$.*

Exemplo 3.1.10. *Seja R uma relação de equivalência sobre $E = \{a, b, c, d\}$ dada por $R = \{(a, a), (b, b), (c, c), (d, d), (b, d), (d, b)\}$. Neste caso, $\overline{a} = \{a\}$, $\overline{b} = \{b, d\}$, $\overline{c} = \{c\}$ e $\overline{d} = \{b, d\}$. Assim, $E/R = \{\{a\}, \{b, d\}, \{c\}\}$, ou seja, o conjunto quociente E/R é dado por*



3.1.6 Partição de um conjunto

Seja E um conjunto não vazio.

Definição 3.1.7. *Uma família $\mathcal{F}$ de subconjuntos não vazios de E é uma partição de E se:*

1. *$A, B \in \mathcal{F}$, então $A = B$ ou $A \cap B = \emptyset$, e*
2. *$\cup_{A \in \mathcal{F}} A = E$.*

Exemplo 3.1.11. *A família $\mathcal{F} = \{\{a\}, \{b, c\}, \{d\}\}$ é uma partição do conjunto $E = \{a, b, c, d\}$, uma vez que $E = \{a\} \cup \{b, c\} \cup \{d\}$ e $\{a\} \cap \{b, c\} = \{a\} \cap \{d\} = \{b, c\} \cap \{d\} = \emptyset$.*

Exemplo 3.1.12. *Se $P = \{x \in \mathbb{Z} : x \text{ é par}\}$ e $I = \{x \in \mathbb{Z} : x \text{ é impar}\}$, então $\mathcal{F} = \{P, I\}$ é uma partição de $\mathbb{Z}$, uma vez que $\mathbb{Z} = P \cup I$ e $P \cap I = \emptyset$.*

Exemplo 3.1.13. *A família $\mathcal{F} = \{]-\infty, -20],]-20, -5[, [-5, 23],]23, \infty[\}$ é uma partição de $\mathbb{R}$, uma vez que*

1. *$\mathbb{R} =]-\infty, -20] \cup]-20, -5[\cup [-5, 23] \cup]23, \infty[$ e*
2. *$]-\infty, -20] \cap]-20, -5[=]-\infty, -20] \cap [-5, 23] =]-\infty, -20] \cap]23, \infty[=]-20, -5[\cap [-5, 23] =]-20, -5[\cup]23, \infty[= [-5, 23] \cap]23, \infty[= \emptyset$.*

Veremos, a seguir, que via uma relação de equivalência sobre um conjunto não vazio E, fica determinada uma partição de E e vice-versa.

Proposição 3.1.2. *Se R é uma relação de equivalência sobre um conjunto E, então E/R é uma partição sobre E.*

Demonstração. Seja $\overline{a} \in E/R$. Como $a \in \overline{a}$, segue que $\overline{a} \neq \emptyset$, para todo $a \in E$. Se $\overline{a}, \overline{b} \in E/R$, então $\overline{a} \cap \overline{b} = \emptyset$ ou $\overline{a} = \overline{b}$. Finalmente, $\cap_{a \in E} \overline{a} = E$. Portanto, E/R é uma partição de E. □

Proposição 3.1.3. *Se $\mathcal{F}$ é uma partição de E, então existe uma relação de equivalência R sobre E tal que $E/R = \mathcal{F}$.*

Demonstração. Seja R uma relação sobre E definida como

$$xRy \text{ se, e somente se, existe } A \in \mathcal{F} : x, y \in A.$$

Mostramos que R é uma relação de equivalência sobre E. Assim, se $x \in E$, então existe $A \in \mathcal{F}$ tal que $x \in A$, ou seja, xRx. Agora, se $x, y \in E$ com xRy, então existe $A \in \mathcal{F}$ tal que $x, y \in A$. Logo, $y, x \in A$, ou seja, yRx. Finalmente, se $x, y, z \in E$ com xRy e yRz, então existem $A, B \in \mathcal{F}$ tal que $x, y \in A$ e $y, z \in B$. Como $A \cap B \neq \emptyset$, segue que $A = B$. Portanto, xRz, ou seja, R é uma relação de equivalência sobre E. □

3.1.7 Exercícios

1. Determine todas as relações sobre o conjunto $A = \{a, b\}$, com $a \neq b$.

2. Sejam A um conjunto de 5 elementos e $R = \{(0,1), (1,2), (2,3), (3,4)\}$ uma relação sobre A. Determine:

   (a) Os elementos de A.

   (b) Domínio e imagem de R.

   (c) Os elementos, domínio e imagem de R^{-1}.

   (d) Os gráficos de R e R^{-1}.

3. Seja A o conjunto das retas definidas pelos vértices de um paralelogramo. Seja a relação R sobre A definida por $xRy \iff x \parallel y$.

   (a) Determine os elementos de R.

   (b) Quais as propriedades que R satisfaz?

4. Sejam os conjuntos $A = \{0, 2, 4, 6, 8\}$ e $B = \{1, 3, 5, 7, 9\}$.

   (a) Determine os elementos de $R = \{(x, y) \in A \times B : y = x + 1\}$.

   (b) Determine os elementos de $S = \{(x, y) \in A \times B : x \leq y\}$.

   (c) Determine R^{-1} e S^{-1}.

5. Esboce o gráfico das seguintes relações sobre $\mathbb{R}$.

   (a) $R_1 = \{(x, y) \in \mathbb{R}^2 : x + y \leq 2\}$.

   (b) $R_2 = \{(x, y) \in \mathbb{R}^2 : y^2 = x\}$.

   (c) $R_3 = \{(x, y) \in \mathbb{R}^2 : 9x^2 + 4y^2 = 36\}$.

(d) $R_4 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 4\}$.

(e) $R_5 = \{(x, y) \in \mathbb{R} : x^2 + y^2 \geq 16\}$.

6. Seja A um conjunto com n elementos.

   (a) Quantas relações reflexivas existem sobre A?

   (b) Quantas relações simétricas existem sobre A?

   (c) Quantas relações transitivas existem sobre A?

7. Seja $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : 4x^2 + 9y^2 = 36\}$. Determine $Dom(R)$, $Im(R)$ e R^{-1}.

8. Sejam A e B conjuntos com m e n elementos, respectivamente. Determine o número de elementos de $A \times B$ e o número de relações de A em B.

9. Seja R uma relação sobre $A = \{1, 2, 3, 4, 5\}$ definida por $xRy \iff x - y = 2k$, para algum $k \in \mathbb{Z}$. Determine os elementos de R e quais propriedades que R satisfaz.

10. Seja R uma relação sobre $\mathbb{N} - \{0\}$ definida por $R = \{(x, y) : x, y \in \mathbb{N} - \{0\} \text{ e } 2x + y = 10\}$. Determine:

    (a) Domínio e imagem de R.

    (b) R^{-1} e domínio e imagem de R^{-1}.

11. Seja $E = \{x \in \mathbb{Z} :| x |\leq 5\}$ e R uma relação sobre E definida por $xRy \iff x^2 + 2x = y^2 + 2y$. Mostre que R é uma relação de equivalência e encontre E/R.

12. Mostre que $R = \{(x, y) \in \mathbb{R}^2 : x - y \in \mathbb{Q}\}$ é uma relação de equivalência sobre $\mathbb{R}$ e determine as classes de equivalências de $1/2$ e $\sqrt{2}$.

13. Seja R uma relação sobre $\mathbb{C}$ definida por $(x + yi)R(z + wi) \iff x^2 + y^2 = z^2 + w^2$.

    (a) Mostre que R é uma relação de equivalência.

    (b) Determine a classe $\overline{1 + i}$.

14. Construir sobre o conjunto $E = \{a, b, c, d\}$ relações binárias R_1, R_2 e R_3, onde R_1 seja apenas reflexiva, R_2 seja apenas simétrica e R_3 seja apenas transitiva.

15. Se R é uma relação de equivalência, mostre que R^{-1} é uma relação de equivalência.

16. Sejam R e S relações sobre um conjunto E.

    (a) Mostre que $R^{-1} \cup S^{-1} = (R \cap S)^{-1}$.

    (b) Mostre que $R^{-1} \cap S^{-1} = (R \cup S)^{-1}$.

    (c) Se R e S são transitivas, mostre que $R \cap S$ é transitiva.

    (d) Se R e S são simétricas, mostre que $R \cap S$ e $R \cup S$ são simétricas.

    (e) Se R e S são reflexivas, mostre que $R \cap S$ e $R \cup S$ são reflexivas.

(f) Mostre que $R \cup R^{-1}$ é simétrica.

(g) Se R é antisimétrica, mostre que R^{-1} também é.

17. Seja R uma relação sobre $\mathbb{C}$ definida por $(a+bi)R(c+di) \iff b = d$.

(a) Mostre que R é uma relação de equivalência.

(b) Determine o conjunto quociente $\mathbb{C}/R$.

18. Sejam $E = \mathbb{N}$ e R definida por $(a,b)R(c,d)$ se, e somente se, $a+b = c+d$. Mostre que R é uma relação de equivalência.

19. Seja S uma relação sobre $\mathbb{Z} \times \mathbb{Z}^*$ definida por $(a,b)S(c,d)$ se, e somente se, $ad = bc$. Mostre que S é uma relação de equivalência.

20. Sejam $E = \mathbb{C}$ e R definida por $(a+bi)R(c+di)$ se, e somente se, $a \leq c$ e $b \leq d$. Verifique se R é reflexiva, simétrica, antisimétrica e transitiva.

21. Seja R uma relação sobre $\mathbb{N}$ definida por $(a,b)R(c,b)$ se, e somente se, $a \mid c$ e $b \leq d$. Mostre que R é uma relação de equivalência.

22. Seja R uma relação sobr $A = \{x \in \mathbb{Z} : 0 \leq x \leq 10\}$ definida por $xRy \iff x - y = 4x$.

(a) Mostre que R é uma relação de equivalência.

(b) Determine o conjunto quociente A/R.

23. Sejam $E = \{-3,-2,-1,0,1,2,3\}$ e $R = \{(x,y) \in E^2 : x+ \mid x \mid = y+ \mid y \mid\}$. Mostre que R é uma relação de equivalência e determine E/R.

24. Seja R uma relação sobre $\mathbb{Q}$ definida por $xRy \longleftrightarrow x - y \in \mathbb{Z}$. Mostre que R é uma relação de equivalência e determine $\overline{1}$ e $\overline{1/2}$.

25. Mostre que $R = \{(a+bi, c+di) \in \mathbb{C}^2 : b = d\}$ é uma relação de equivalência e descreva $\mathbb{C}/R$.

26. Sejam E um conjunto não vazio e $A \subseteq E$.

(a) Mostre que $xRy \leftrightarrow x \cap A = y \cap A$ é uma relação de equivalência sobre $\mathcal{P}(E)$.

(b) Mostre que $xSy \leftrightarrow x \cup A = y \cup A$ é uma relação de equivalência sobre $\mathcal{P}(E)$.

27. Sejam $p(x_1, y_1)$ e $q(x_2, y_2)$ pontos de $\mathbb{R}^2$. Mostre que são relações de equivalências:

(a) $pRq \iff x_1 y_1 = x_2 y_2$.

(b) $pSq \iff y_2 - y_1 = x_2 - x_1$.

(c) $pTq \iff x_1^2 + y_1^2 = x_2^2 + y_2^2$.

3.2 Relação de ordem

Seja R uma relação sobre um conjunto não vazio E.

Definição 3.2.1. *A relação R é chamada uma relação de ordem (parcial) sobre E se:*

1. *aRa, para todo $a \in E$, ou seja, R é reflexiva.*
2. *Se aRb e bRa, então $a = b$, onde $a, b \in E$, ou seja, R é anti-simétrica.*
3. *Se aRb e bRc, então aRc, para todo $a, b, c \in E$, ou seja, R é transitiva.*

Neste caso, quando $a, b \in E$ e aRb, o elemento a é dito que precede b.

Um conjunto E com uma ordem parcial R é chamado um conjunto parcialmente ordenado mediante a ordem R. Uma ordem parcial R sobre E é chamada uma ordem total se para todo $x, y \in E$ tem-se que xRy ou yRx, ou seja, quaisquer dois elementos $x, y \in E$ são comparáveis mediante a relação de ordem R. Um conjunto E com uma ordem total é chamado conjunto totalmente ordenado mediante a ordem R.

Exemplo 3.2.1. *A relação R definida por $aRa \iff a \mid a$ é uma relação de ordem parcial sobre $\mathbb{N}$. De fato, como $a \mid a$, para todo $a \in \mathbb{N}$, segue que aRa. Agora, se aRb e bRa, onde $a, b \in \mathbb{N}$, então $a \mid b$ e $b \mid a$. Assim, $b = ac_1$ e $a = bc_2$, onde $c_1, c_2 \in \mathbb{N}$, e portanto, $a = bc_2 = a(c_1c_2)$. Como $c_1c_2 \neq 0$, segue que $a = b$. Finalmente, se aRb e bRc, com $a, b, c \in \mathbb{N}$, então $b = ac_1$ e $c = bc_2$, onde $c_1, c_2 \in \mathbb{N}$, e portanto, $c = bc_2 = a(c_1c_2)$. Como $c_1c_2 \neq 0$, segue que $a \mid c$, ou seja, aRc. Portanto, R é uma ordem parcial. A ordem não é total pois $4 \nmid 6$ e $6 \nmid 4$.*

Exemplo 3.2.2. *A relação R definida por $xRy \iff x \leq y$ é uma relação de ordem total sobre $\mathbb{R}$. De fato, como $a \leq a$, para todo $a \in \mathbb{R}$, segue que aRa. Agora, se aRb e bRa, onde $a, b \in \mathbb{R}$, então $a \leq b$ e $b \leq a$, e portanto, $a = b$. Agora, se aRb e bRc, com $a, b, c \in \mathbb{R}$, então $a \leq b$ e $b \leq c$, e portanto, $a \leq c$, ou seja, aRc. Finalmente, dados $a, b \in \mathbb{R}$, segue que $a \leq b$ ou $b \leq a$. Portanto, R é uma ordem total.*

Exemplo 3.2.3. *Sejam A um conjunto não vazio e $\mathcal{P}(A)$ o conjunto das partes de A. A relação R sobre $\mathcal{P}(A)$ definida por $xRy \iff x \subset y$ é uma relação de ordem parcial. De fato, como $a \subset a$, para todo $a \in \mathcal{P}(A)$, segue que aRa. Agora, se aRb e bRa, onde $a, b \in \mathcal{P}(A)$, então $a \subset b$ e $b \subset a$, ou seja, $a = b$. Finalmente, se aRb e bRc, com $a, b, c \in \mathcal{P}(A)$, então $a \subset b$ e $b \subset c$, e portanto, $a \subset c$, ou seja, aRc. Portanto, R é uma ordem parcial. A ordem não é total pois em $\mathcal{P}(A)$ existem conjuntos $\{a\}$ e $\{b\}$, com $a \neq b$, tal que $a \not\subset b$ e $b \not\subset a$.*

3.2.1 Limites superiores de um conjunto

Seja R uma relação de ordem sobre um conjunto não vazio E.

Definição 3.2.2. *Seja $A \subseteq E$ um subconjunto. Um elemento $a \in E$ é chamado um limite superior de A se todo elemento de A precede a, ou seja, xRa para todo $x \in A$.*

Exemplo 3.2.4. *Sejam a relação de ordem R sobre $\mathbb{Z}$ definida por $xRy \iff x \leq y$ e $A = \{0, 1, 2, 3\}$. Os limites superiores de A são todos os $a \in \mathbb{Z}$ tal que xRa, para todo $x \in A$, ou seja, $a = 3, 4, 5, 6, \cdots$*

Exemplo 3.2.5. *Sejam $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ e R a relação de ordem sobre E definida por $xRy \iff x \subset y$. Se $A = \{\{1\}, \{1, 3\}\}$, então os limites superiores de A são os subconjuntos a de E tal que xRa, para todo $x \in A$. Assim, $\{1, 3\}$ e $\{1, 2, 3\}$.*

3.2.2 Máximo de um conjunto

Sejam R uma relação de ordem sobre um conjunto não vazio E e $A \subseteq E$, onde $A \neq \emptyset$.

Definição 3.2.3. *O máximo de A, se existir, é um limite superior de A que pertence a A e denotado por $max(A)$.*

Exemplo 3.2.6. *O máximo de $A = \{0, 1, 2, 3\}$ com a relação de ordem R sobre $\mathbb{Z}$ definida por $xRy \leftrightarrow x \leq y$ é o elemento 3, pois é um limite superior que pertence a A.*

Exemplo 3.2.7. *O máximo do conjunto $A = \{\{1\}, \{1, 3\}\}$ com a relação de ordem R sobre o cojunto $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ definida por $xRy \iff x \subset y$ é o elemento $\{1, 3\}$, pois é um limite superior que pertence a A.*

Exemplo 3.2.8. *Os limites superiores do conjunto $A = \{\{1\}, \{2\}\}$ com a relação de ordem R sobre o conjunto $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ definida por $xRy \iff x \subset y$ são os elementos $\{1, 2\}$ e $\{1, 2, 3\}$. Como não pertencem a A, segue que A não tem máximo.*

3.2.3 Limites inferiores de um conjunto

Seja R uma relação de ordem sobre um conjunto não vazio E.

Definição 3.2.4. *Seja $A \subseteq E$ um subconjunto. Um elemento $a \in E$ é chamado um limite inferior de A se a precede todo elemento de A, ou seja, aRx para todo $x \in A$.*

Exemplo 3.2.9. *Sejam a relação de ordem R sobre $\mathbb{Z}$ definida por $xRy \iff x \leq y$ e $A = \{5, 10, 100\}$. Os limites inferiores de A são os elementos $a \in \mathbb{Z}$ tal que $a \leq 5$.*

Exemplo 3.2.10. *Sejam o conjunto $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ e R uma relação de ordem sobre E definida por $xRy \iff x \subset y$. Se $A = \{\{1, 2\}, \{1, 3\}\}$, então os limites inferiores de A são $\emptyset$ e $\{1\}$.*

3.2.4 Mínimo de um conjunto

Sejam R uma relação de ordem sobre um conjunto não vazio E e $A \subseteq E$, onde $A \neq \emptyset$.

Definição 3.2.5. *O mínimo de A, se existir, é um limite inferior de A que pertence a A e denotado por $min(A)$.*

Exemplo 3.2.11. *O mínimo do conjunto $A = \{5, 10, 100\}$ com a relação de ordem R sobre $\mathbb{Z}$ definida por $xRy \iff x \leq y$ é o elemento 5, pois é um limite inferior que pertence a A.*

Exemplo 3.2.12. *O mínimo do conjunto $A = \{\{1\}, \{1, 3\}\}$ com a relação de ordem R, definida por $xRy \iff x \subset y$, sobre $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ é o elemento $\{1\}$, pois é um limite inferior que pertence a A.*

Exemplo 3.2.13. *O conjunto $A = \{\{1, 2\}, \{1, 3\}\}$ com a relação de ordem R, definida por $xRy \iff x \subset y$, sobre $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ não possui mínimo.*

Proposição 3.2.1. *Se A é um subconjunto de um conjunto parcialmente ordenado E e existe máximo (mínimo) de A, então o máximo (mínimo) é único.*

Demonstração. Para o máximo, sejam M_1 e M_2 máximos de A. Assim, como M_1 é máximo de A e $M_2 \in A$, segue que M_2RM_1. De modo análogo, como M_2 é máximo de A e $M_1 \in A$, segue que M_1RM_2. Logo, $M_1 = M_2$. Para o mínimo, sejam m_1 e $_2$ mínimos de A. Assim, como m_1 é mínimo de A e $m_2 \in A$, segue que m_1Rm_2. De modo análogo, como m_2 é mínimo de A e $m_1 \in A$, segue que m_2Rm_1. Logo, $m_1 = m_2$. □

3.2.5 Supremo e ínfimo de um conjunto

Sejam R uma relação de ordem sobre um conjunto não vazio E e $A \subseteq E$, onde $A \neq \emptyset$.

Definição 3.2.6. *O supremo do conjunto A, denotado por $m = sup(A)$, é o mínimo do conjunto dos limites superiores de A, ou seja,*

1. *xRm, para todo $x \in A$, e*
2. *se $a \in E$ e xRa, para todo $x \in A$, então mRa.*

Exemplo 3.2.14. *O supremo do conjunto $A = \{\{1\}, \{1, 3\}\}$ com a relação de ordem R sobre o conjunto $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ definida por $xRy \iff x \subset y$ é o elemento $\{1, 3\}$. Agora, se $A = \{\{2\}, \{3\}\}$, então os limites superiores de A são $\{2, 3\}$ e $\{1, 2, 3\}$. O $sup(A) = \{2, 3\}$ e A não possui máximo.*

Exemplo 3.2.15. *Seja a relação de ordem $xRy \iff x \leq y$ sobre $\mathbb{R}$. Os limites superiores do conjunto $A = \{1/2, 2/3, 3/4, \cdots\}$ são $\{x \in \mathbb{R} : x \geq 1\}$. O supremo de A é o elemento 1 e não tem máximo.*

Definição 3.2.7. *O ínfimo de A, denotado por $m = inf(A)$, é o máximo do conjunto dos limites inferiores de A, ou seja,*

1. *mRx, para todo $x \in A$, e*
2. *se $a \in E$ e aRx, para todo $x \in A$, então aRm.*

Exemplo 3.2.16. *O ínfimo do conjunto* $A = \{\{1\}, \{1,3\}\}$ *com a relação de ordem* R *sobre o conjunto* $E = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$ *definida por* $xRy \iff x \subset y$ *é o elemento* $\{1\}$*. Agora, se* $A = \{\{2\}, \{3\}\}$*, então limites superiores de* A *são* $\{2,3\}$ *e* $\{1,2,3\}$*. O* $sup(A) = \{2,3\}$ *e* A *não possui máximo.*

Exemplo 3.2.17. *Seja a relação de ordem* R *sobre* $\mathbb{R}$ *definida por* $xRy \iff x \leq y$*. Os limites inferiores de* $A =]0,2[$ *são* $\{x \in \mathbb{R} : x \leq 0\}$*. O ínfimo é o elemento* 0 *e não possui mínimo.*

3.2.6 Elementos maximais e minimais de um conjunto

Os elementos maximais e minimais de um subconjunto não vazio de um conjunto parcialmente ordenado são definidos da seguinte maneira.

Definição 3.2.8. *Seja* A *um subconjunto não vazio de um conjunto parcialmente ordenado* E*.*

1. *Um elemento* $m_1 \in A$ *é um elemento maximal de* A *se não existe* $x \in A$ *tal que* $m_1 Rx$*, ou seja, quando o único elemento de* A *precedido por* m_1 *é ele próprio.*

2. *Um elemento* $m_o \in A$ *é um elemento minimal de* A *se não existe* $x \in A$ *tal que* xRm_o*, ou seja, quando o único elemento de* A *que precede* m_o *é ele próprio.*

Exemplo 3.2.18. *Em* $\mathbb{R}$ *não existem elementos maximais ou minimais com respeito a ordem usual.*

Exemplo 3.2.19. *Em* $D(36)$ *(divisores de 36), considere o subconjunto* $A = \{2,3,6,12,18\}$*. Os números* 2 *e* 3 *são elementos minimais, e os números* 12 *e* 18 *são elementos maximais em* A*, mas* A *não possui máximo e nem mínimo.*

3.2.7 Exercícios

1. Seja R um relação sobre $\mathbb{N}$ definida por $xRy \iff x \mid y$.

   (a) Mostre que R é uma relação de ordem parcial.

   (b) Se $A = \{3,4\}$, determine os limites superiores, limites inferiores, máximo, mínimo, supremo e ínfimo de A.

2. Seja a relação R sobre $\mathbb{C}$ definida por $(a+bi)R(c+di)$ se, e somente se, $a \leq c$ e $b \leq d$.

   (a) Mostre que R é uma ordem parcial sobre $\mathbb{C}$.

   (b) Determine os limites superiores, limites superiores, ínfimo, supremo, máximo, mínimo de $A = \{2+i; 1+2i\}$.

3. Se R é uma relação de ordem, mostre que R^{-1} também é uma relação de ordem parcial.

4. Seja a relação R sobre $\mathbb{N}$ definida por $(a,b)R(c,d)$ se, e somente se, $a|c$ e $b \leq d$.

   (a) Mostre que R é uma relaçao de ordem parcial.

(b) Determine os limites inferiores, limites superiores, ínfimo, supremo, máximo, mínimo de $A = \{(2,1);(1,2)\}$.

5. Seja a relação R sobre $\mathbb{N}$ definida por $(a,b)R(c,d)$ se, e somente se, $a \leq c$ e $b \mid d$.

   (a) Mostre que R é uma relaçao de ordem parcial.

   (b) Determine os limites inferiores, limites superiores, ínfimo, supremo, máximo e mínimo do conjunto $A = \{(3,1);(1,3)\}$.

6. Seja o conjunto $E = \{\{a\};\{b\};\{a,b,c\};\{a,b,d\};\{a,b,c,c\};\{a,b,c,d,e\}\}$. Determine os limites inferiores, limites superiores, ínfimo, supremo, máximo e mínimo do conjunto A, onde $A = \{\{a,b,c\};\{a,b,d\};\{a,b,c,d\}\}$.

7. Seja a relação sobre $\mathbb{N}$ definida por aRb se, e somente se, $a \mid b$.

   (a) Mostre que a relação R é uma relação de ordem parcial.

   (b) Quais dos seguintes conjuntos são totalmente ordenados $A = \{24,2,6\}$, $B = \{3,15,5\}$, $C = \{15,5,30\}$ e $D = \mathbb{N}$.

8. Determine os limites inferiores, limites superiores, ínfimo, supremo, máximo e mínimo do conjuto $A = \{x \in \mathbb{Q} : 0 \leq x^2 \leq 2\}$, em relação a relação de ordem de disigualdade.

9. Sejam $E = \{a,b,c,d\}$ e $\mathcal{P}(E)$ o conjunto das partes de E.

   (a) Mostre que a relação de inclusão é uma relação de ordem parcial em $\mathcal{P}(E)$.

   (b) Determine os limites superiores, limites superiores, ínfimo, supremo, máximo, mínimo de $A = \{\emptyset, \{a,d\}, \{c\}\}$.

10. Determine infimo, supremo, mínimo e máximo (se existirem) dos seguintes conjuntos:

    (a) $A = \left\{ \dfrac{(-1)^n + n}{n^2} : n \in \mathbb{N} \right\}$.

    (b) $B = \left\{ x \in \mathbb{R} : -1 \leq \dfrac{x-2}{x+3} \leq 0 \right\}$.

Capítulo

4

Aplicações ou funções

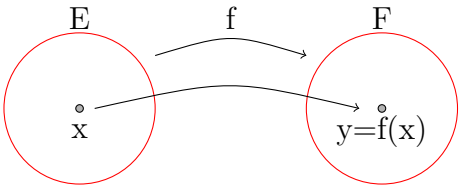
O conceito de função é um dos mais importantes da matemática de modo que toda vez que temos dois conjuntos e algum tipo de associação entre eles, que faça corresponder a todo elemento do primeiro conjunto um único elemento do segundo, obtemos uma função. O uso de funções pode ser encontrado em diversos fatos do nosso dia a dia. Por exemplo, na tabela de preços de uma fábrica, onde a cada produto corresponde um determinado preço; o valor pago numa conta da mensalidade escolar, que depende do valor associado a cada mês, enfim, existem diversos exemplos. Deste modo, neste capítulo, apresentamos o conceito de uma função (também conhecida com uma aplicação), funções injetoras, sobrejetoras e bijetoras, imagem direta e imagem inversa, aplicações monótonas, e finalmente, apresentamos as noções e propriedades dos conjuntos equipotentes e dos conjuntos enumeráveis.

4.1 Aplicações - funções

O conceito de função, assim como o de conjuntos, é essecial para todas as áreas da Matemática, onde esses dois conceitos são sempre a parte central para desenvolvimento de estudos nas áreas da Matemática. Assim, consideramos E e F dois conjuntos não vazios.

Definição 4.1.1. *Uma relação f de E em F é uma aplicação (ou função) de E em F se para todo $x \in E$, existe $!y \in F$ tal que xfy, ou seja, $xfy \iff (x, y) \in f$, para um único $y \in F$. Neste caso, indica-se tal fato por $f : E \to F$, e se xfy, então escreve-se $y = f(x)$ e lê-se y é a imagem de x por f.*

A função f também pode ser representada pelo conjunto $\{(x, f(x)) : x \in E\}$. O diagrama de Veen de uma função $f : E \to F$ é representado por:



Exemplo 4.1.1. *Se $E = \{a, b, c, d\}$ e $F = \{r, s, t, u, v\}$ e $f(c) = r$, $f(b) = s$, $f(a) = t$ e $f(d) = t$, então f é uma aplicação.*

Exemplo 4.1.2. *Se $E = \{a, b, c, \}$ e $F = \{r, s, t, u\}$ e $f(a) = r$ e $f(b) = s$, então f não é uma aplicação.*

Exemplo 4.1.3. *Se $E = \{a, b, c\}$ e $F = \{r, s, t, u, v\}$ e $f(a) = r$, $f(b) = s$, $f(a) = t$ e $f(d) = u$, então f não é uma aplicação.*

Definição 4.1.2. *Sejam $f : E \to F$ e $g : E \to F$ duas funções.*

1. *A função f é igual a função g, ou seja, as funções f e g são iguais, se $f(x) = g(x)$, para todo $x \in E$, ou seja, $f = g \iff f(x) = g(x)$, para todo $x \in E$.*
2. *O conjunto $D(f) = \{x \in E : \text{ existe } y \in F \text{ tal que } f(x) = y\}$ é definido como o domínio de uma função f.*
3. *O conjunto $Im(f) = \{y \in F : \text{ existe } x \in E \text{ tal que } f(x) = y\}$ é definido como a imagem de uma função f.*
4. *O contra-domínio de f é definido por $Cd(f) = F$.*

Exemplo 4.1.4. *Sejam $E = \{a, b, c, d\}$, $F = \{r, s, t, u, v\}$ e $f : E \to F$ uma aplicação definida por $f(c) = r$, $f(b) = s$, $f(a) = t$ e $f(d) = t$. Assim, $D(f) = \{a, b, c, d\}$, $Im(f) = \{r, s, t\}$ e $Cd(f) = \{r, s, t, u, v\}$.*

Exemplo 4.1.5. *Se $f : \mathbb{R} \to \mathbb{R}$ é uma função definida por $f(x) = x^2$, para todo $x \in \mathbb{R}$, então $D(f) = \mathbb{R}$, $Im(f) = \mathbb{R}_+$ e $Cd(f) = \mathbb{R}$.*

Definição 4.1.3. *Seja $X \subset E$, com $X \neq \emptyset$. A aplicação $i : X \to E$ tal que $f(x) = x$, para todo $x \in X$, é chamada aplicação inclusão de X em E. No caso de $X = E$, tem-se uma aplicação de E em E que é chamada aplicação idêntica de E.*

Exemplo 4.1.6. *Sejam $E = \{a, b, c, d, e\}$ e $X = \{b, c, d\}$. Neste caso, a aplicação inclusão $i : X \to E$ é dada por $i(b) = b$, $i(c) = c$ e $i(d) = d$. Agora, a aplicação idêntica de E é dada por $i(a) = a$, $i(b) = b$, $i(c) = c$, $i(d) = d$ e $i(e) = e$.*

Definição 4.1.4. *Sejam $f : E \to F$ uma aplicação e $A \subset E$, com $A \neq \emptyset$. A restrição de f ao conjunto A é a aplicação $f_A : A \to F$ definida por $(f_A)(x) = f(x)$, para todo $x \in A$.*

Exemplo 4.1.7. *Sejam $E = \{a, b, c, d, e\}$, $F = \{r, s, t, u, v\}$ e $f : E \to F$ definida por $f(a) = s$, $f(b) = u$, $f(c) = t$ e $f(d) = u$. Se $A = \{c, d\}$, então $f_A : A \to F$ é dada por $f(c) = t$ e $f(d) = u$.*

Exemplo 4.1.8. *Seja $f : \mathbb{Z} \to \mathbb{Z}$, onde $f = \{(x, x^2) : x \in \mathbb{Z}\}$. Se $A = \mathbb{N}$, então a restrição de f a $\mathbb{N}$ é dada por $f_{\mathbb{N}} = \{(x, x^2) : x \in \mathbb{N}\}$.*

4.1.1 Funções bijetoras

Sejam E, F, G e H conjuntos não vazios.

Definição 4.1.5. *Seja $f : E \to F$ uma aplicação. A aplicação f é chamada injetora sempre que $x_1 \neq x_2$ implicar que $f(x_1) \neq f(x_2)$, para todo $x_1, x_2 \in E$, ou seja, sempre que $f(x_1) = f(x_2)$ implicar que $x_1 = x_2$, para todo $x_1, x_2 \in E$.*

Exemplo 4.1.9. *Sejam $E = \{a, b, c\}$ e $F = \{r, s, t, u\}$. A função $f : E \to F$ definida por $f(a) = s$, $f(b) = t$ e $f(c) = u$ é injetora. Agora, se $f : E \to F$ é definida por $f(a) = r$, $f(b) = u$ e $f(c) = r$, então f não é injetora.*

Exemplo 4.1.10. *A função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = 2x + 5$, para todo $x \in \mathbb{R}$ é injetora, uma vez que se $f(x_1) = f(x_2)$, então $x_1 = x_2$. De modo análogo, a função $f : \mathbb{R} - \{0\} \to \mathbb{R}$ definida por $f(x) = \frac{x+1}{x}$, para todo $x \in \mathbb{R} - \{0\}$, é injetora.*

Definição 4.1.6. *Seja $f : E \to F$ uma função. Dizem que f é uma função sobrejetora se $Im(f) = F$, ou seja, para todo $y \in F$, existe $x \in E$ tal que $f(x) = y$.*

Exemplo 4.1.11. *Sejam $E = \{a, b, c, d\}$ e $F = \{r, s, t\}$. A função $f : E \to F$ definida por $f(a) = s$, $f(b) = t$, $f(c) = r$ e $f(d) = s$ é sobrejetora. Agora, se $f : E \to F$ é definida por $f(a) = r$, $f(b) = r$ e $f(c) = t$, então f não é sobrejetora.*

Definição 4.1.7. *Uma função $f : E \to F$ chamada de função bijetora se f é injetora e sobrejetora. Se f é bijetora, os conjuntos E e F são chamados equipotentes, ou seja, possuem a mesma cardinalidade.*

Exemplo 4.1.12. *A função $f : E \to F$, onde $E = \{a, b, c\}$ e $F = \{r, s, t\}$, definida por $f(a) = s$, $f(b) = r$ e $f(c) = t$, é bijetora, e neste caso, os conjuntos E e F são equipotentes.*

Exemplo 4.1.13. *Os conjuntos $\mathbb{N}$ e $\mathbb{N} - \{0\}$ são equipotentes, uma vez que a função $f : \mathbb{N} \to \mathbb{N} - \{0\}$ definida por $f(n) = n + 1$, para todo $n \in \mathbb{N}$, é bijetora. Também, os conjuntos $\mathbb{N}$ e $A = \{20, 21, 22, \cdots\}$ são equipotentes, uma vez que a função $f : \mathbb{N} \to A$ definida por $f(n) = n + 20$, para todo $n \in \mathbb{N}$, é bijetora.*

Definição 4.1.8. *Sejam E, F e G conjuntos não vazios, e sejam $f : E \to F$ e $g : F \to G$ funções. A composta de f e g é a aplicação $g \circ f : E \to G$ definida por $(g \circ f)(x) = g(f(x))$, para todo $x \in E$.*

Observe que para que exista a composta $g \circ f$, devemos ter que $Im(f) \subseteq D(g)$.

Exemplo 4.1.14. *Sejam $f : \mathbb{R} \to \mathbb{R}$ uma função, onde $f(x) = x + 1$, para todo $x \in \mathbb{R}$, e $g : \mathbb{R} \to \mathbb{R}_+$ uma função, onde $g(x) = x^2 + 1$, para todo $x \in \mathbb{R}$. Assim, $g \circ f : \mathbb{R} \to \mathbb{R}_+$ é dada por $(g \circ f)(x) = g(f(x)) = g(x + 1) = (x + 1)^2 + 1 = x^2 + 2x + 2$, para todo $x \in \mathbb{R}$. Também, $f \circ g : \mathbb{R}_+ \to \mathbb{R}$ e é definida por $(f \circ g)(x) = f(g(x)) = f(x^2 + 1) = (x^2 + 2) + 1 = x^2 + 2$, para todo $x \in \mathbb{R}_+$.*

Exemplo 4.1.15. *Sejam $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ uma função definida por $f(x, y) = (2x, x - y)$, para todo $(x, y) \in \mathbb{R} \times \mathbb{R}$, e $g : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ uma função definida por $f(x, y) = x + y$, para todo $(x, y) \in \mathbb{R} \times \mathbb{R}$. Assim, $g \circ f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ é definida por $(g \circ f)(x, y) = g(f(x, y)) = g(2x, x - y) = 2x + x - y = 3x - y$, para todo $(x, y) \in \mathbb{R} \times \mathbb{R}$. Neste caso, como $Im(g) \nsubseteq D(f)$, segue que não existe a $f \circ g$.*

Proposição 4.1.1. *Sejam E, F e G conjuntos não vazios, $f : E \to F$ e $g : F \to G$ funções.*

1. *Se f e g são injetoras, então $g \circ f$ é injetora.*
2. *Se f e g são sobrejetoras, então $g \circ f$ sobrejetora.*

Demonstração. Para (1), se $(g \circ f)(x_1) = (g \circ f)(x_2)$, com $x_1, x_2 \in E$, então $g(f(x_1)) = g(f(x_2))$. Como g é injetora, segue que $f(x_1) = f(x_2)$. Finalmente, como f é injetora, segue que $x_1 = x_2$, ou seja, $g \circ f$ é injetora. Para (2), seja $z \in G$. Como g é sobrejetora, segue que existe $y \in F$ tal que $g(y) = z$. Agora, como f é sobrejetora, segue que existe $x \in E$ tal que $f(x) = y$. Assim, $(g \circ f)(x) = g(f(x)) = f(y) = z$, e portanto, $g \circ f$ é sobrejetora. □

Corolário 4.1.1. *Se f e g são bijetoras, então $g \circ f$ é bijetora.*

Proposição 4.1.2. *Sejam E, F, G e H conjuntos não vazios. Se $f : E \to F$, $g : F \to G$ e $h : G \to H$ são funções, então $h \circ (g \circ f) = (h \circ g) \circ f$.*

Demonstração. Se $x \in E$, então $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)$. □

Exemplo 4.1.16. *Sejam $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x^2$, para todo $x \in \mathbb{R}$, $g : \mathbb{R} \to \mathbb{R}_+$ definida por $g(x) = sen(x)$, para todo $x \in \mathbb{R}$, e $h : \mathbb{R} \to \mathbb{R}_+$ definida por $h(x) = 2^x$, para todo $x \in \mathbb{R}$. Assim, $h \circ g \circ f : \mathbb{R} \to \mathbb{R}_+$ e é definida por $(h \circ g \circ h)(x) = h(g(f(x))) = h(g(x^2)) = h(sen(x^2)) = 2^{sen(x^2)}$, para todo $x \in \mathbb{R}$.*

Teorema 4.1.1. *Seja $f : E \to F$ uma função, onde E e F são conjuntos não vazios. A relação f^{-1} de F em E é uma função se, e somente se, f é bijetora.*

Demonstração. Suponhamos que f^{-1} é uma função. Se $f(x_1) = f(x_2) = y$, com $x_1, x_2 \in E$, então $x_1 f y$ e $x_2 f y$. Assim, $y f^{-1} x_1$ e $y f^{-1} x_2$. Como f^{-1} é uma função, segue que $x_1 = x_2$, ou seja, f é injetora. Para a sobrejetora, se $b \in F$, então $f^{-1}(b) = a \in E$. Assim, $b f^{-1} a$. Portanto, $a f b$ e $f(a) = b$, ou seja, f é sobrejetora. Portanto, f é bijetora. Reciprocamente, seja $y \in F$. Como f é sobrejetora, segue que existe $x \in E$ tal que $f(x) = y$. Assim, $y f^{-1} x$. Agora, se $x_1, x_2 \in E$ são tais que $y f^{-1} x_1$ e $y f^{-1} x_2$, então, $x_1 f y$ e $x_2 f y$, ou seja, $f(x_1) = f(x_2) = y$. Com f é injetora, segue que $x_1 = x_2$. Portanto, f^{-1} é uma função. □

Corolário 4.1.2. *Se f é bijetora, então $f^{-1} \circ f = id_E$ e $f \circ f^{-1} = id_F$.*

Demonstração. Se $x \in E$, então $f(x) = y \in F$. Assim, $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x = id_E(x)$. Portanto, $f^{-1} \circ f = id_E$. Agora, se $y \in F$, então $f^{-1}(y) = x \in E$. Assim, $(f \circ f^{-1})(y) = f(f^{-1}(y)) = f(x) = y = id_F(y)$. Portanto, $f \circ f^{-1} = id_F$. □

Corolário 4.1.3. *Se f é bijetora, então f^{-1} é bijetora.*

Demonstração. Se $f^{-1}(y_1) = f^{-1}(y_2)$, com $y_1, y_2 \in F$, então $f(f^{-1}(y_1)) = f(f^{-1}(y_2))$, ou seja, $(f \circ f^{-1})(y_1) = (f \circ f^{-1})(y_2)$. Assim, $id_F(y_1) = id_F(y_2)$, ou seja, $y_1 = y_2$. Portanto, f^{-1} é injetora. Para a sobrejetora, se $x \in E$, então $id_E(x) = x$, ou seja, $(f^{-1} \circ f)(x) = x$. Assim, $f^{-1}(f(x)) = x$, ou seja, f^{-1} é sobrejetora. Portanto, f^{-1} é bijetora. □

Teorema 4.1.2. *Se existe $g : F \to E$ tal que $g \circ f = id_E$ e $f \circ g = id_F$, então f e g são bijetoras, $g = f^{-1}$ e $f = g^{-1}$.*

Demonstração. Primeiro, vamos provar que f é bijetora. Para a injetora, se $f(x_1) = f(x_2)$, com $x_1, x_2 \in E$, então $g(f(x_1)) = g(f(x_2))$, ou seja, $(g \circ f)(x_1) = (g \circ f)(x_2)$. Como $g \circ f = id_E$ e $f \circ g = id_F$, segue que $x_1 = x_2$, ou seja, f é injetora. Para a sobrejetora, se $b \in F$, então $id_F(b) = b$. Assim, $(f \circ g)(b) = b$, isto é, $f(g(b)) = b$. Como $g(b) \in E$, segue que f é sobrejetora. Portanto, f é bijetora. Agora, vamos provar que g é bijetora. Para a injetora, se $g(y_1) = g(y_2)$, com $y_1, y_2 \in F$, então $f(g(y_1)) = f(g(y_2))$, ou seja, $y_1 = (f \circ g)(y_1) = (f \circ g)(y_2) = y_2$. Portanto, g é injetora. Agora, se $a \in E$, então $id_E(a) = a$. Assim, $(g \circ f)(a) = g(f(a)) = a$. Como $f(a) \in F$, segue que g é sobrejetora. Portanto, g é bijetora. Agora, vamos mostrar que $g = f^{-1}$. Se $(y, x) \in g$, então $g(y) = x$. Aplicando f, segue que $f(g(y)) = f(x)$. Como $f \circ g = id_F$, segue que $f(x) = y$. Assim, $(x, y) \in f$, e desse modo, $(y, x) \in f^{-1}$. Portanto, $g \subseteq f^{-1}$. Para a outra inclusão, se $(y, x) \in f^{-1}$, então $(x, y) \in f$, ou seja, $f(x) = y$. Aplicando g, segue que $g(y) = g(f(x)) = (g \circ f)(x) = id_E(x) = x$. Assim, $(y, x) \in g$, e desse modo, $f^{-1} \subseteq g$. Portanto, $g = f^{-1}$. Agora, mostramos que $f = g^{-1}$. Assim, se $(x, y) \in f$, então $y = f(x)$. Aplicando g, segue que $g(y) = g(f(x)) = (g \circ f)(x) = id_E(x) = x$. Assim, $(y, x) \in g$, e desse modo, $(x, y) \in g^{-1}$. Portanto, $f \subseteq g^{-1}$. Agora, se $(y, x) \in g^{-1}$, então $(x, y) \in g$, ou seja, $g(x) = y$. Aplicando f, segue que $f(y) = f(g(x)) = (f \circ g)(x) = id_F(x) = x$. Assim, $(y, x) \in f$, e deste modo, $g^{-1} \subseteq f$. Portanto, $f = g^{-1}$. □

4.1.2 Imagem direta e imagem inversa

Sejam E e F conjuntos não vazios e $f : E \to F$ uma função.

Definição 4.1.9. *A imagem direta de um subconjunto $A \subseteq E$ através da função f, indicada por $f(A)$, é definida por $f(A) = \{f(x) : x \in A\}$. Se $A = E$, então $f(E) = Im(f)$.*

Exemplo 4.1.17. *Sejam $E = \{a, b, c, d, e\}$, $F = \{r, s, u, v\}$ e $f : E \to F$ uma função definida por $f(a) = r$, $f(b) = s$, $f(c) = s$, $f(d) = u$ e $f(e) = v$. Se $A = \{b, c, d\}$, então $f(A) = \{s, u\}$.*

Exemplo 4.1.18. *Seja $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = -1$, para todo $x < 1$, e $f(x) = x + 1$, para todo $x \geq 1$. Se $A = [-2, 1[$, então $f(A) = \{-1, 2\}$.*

Definição 4.1.10. *A imagem inversa de um subconjunto $B \subseteq F$ através da função f, indicada por $f^{-1}(B)$, é definida por $f^{-1}(B) = \{x \in E : f(x) \in B\}$. Se $B = F$, então $f^{-1}(F) = E$.*

Exemplo 4.1.19. *Sejam $E = \{a, b, c, d, e\}$, $F = \{r, s, u, v\}$ e $f : E \to F$ uma função definida por $f(a) = s$, $f(b) = r$, $f(c) = u$, $f(d) = r$ e $f(e) = r$. Se $B = \{r, s, u\}$, então $f^{-1}(B) = \{a, b, c, d, e\}$.*

4.1.3 Aplicações monótonas

Sejam E e F conjuntos não vazios e $f : E \to F$ uma função, onde E e F são conjuntos parcialmente ordenados com uma relação de ordem que indicamos por R.

Definição 4.1.11. *Seja $f : E \to F$ uma função.*

1. *A função f é chamada uma função crescente se xRy implicar que $f(x)Rf(y)$.*
2. *A função f é chamada uma função decrescente se xRy implicar que $f(y)Rf(x)$.*
3. *A função f é uma função monótona se f é uma função crescente ou decrescente.*
4. *A função f é chamada uma função estritamente crescente se xRy, com $x \neq y$, implicar que $f(x)Rf(y)$, com $f(x) \neq f(y)$.*
5. *A função f é chamada uma função estritamente decrescente se xRy, com $x \neq y$, implicar que $f(y)Rf(x)$, com $f(x) \neq f(y)$.*

Exemplo 4.1.20. *A função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = x$ é estritamente crescente.*

Exemplo 4.1.21. *A função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = -x$ é estritamente decrescente.*

4.1.4 Exercícios

1. Determine todas as funções de $E = \{0, 1, 2\}$ em $F = \{3, 4\}$.
2. Determine todas as funções injetoras de $E = \{1, 2\}$ em $F = \{3, 4, 5\}$.
3. Determine todas as funções sobrejetoras de $E = \{1, 2, 3\}$ em $F = \{4, 5\}$.
4. Verifique se as funções $f : \mathbb{R} \to \mathbb{R}$ definidas por $f(x) = x^3$, $f(x) = x^2 - 5x + 6$, $f(x) = 2^x$, $f(x) =\mid sen(x) \mid$, $f(x) = x+ \mid x \mid$ e $f(x) = x + 3$, onde $x \in \mathbb{R}$, são bijetoras.
5. Determine uma função $fA \to B$, onde
   (a) $A = \mathbb{R}$, $B \subseteq \mathbb{R}$, f é injetora e não é sobrejetora.
   (b) $A \subseteq \mathbb{R}$, $B = \mathbb{R}$, f é injetora e não é sobrejetora.
   (c) $A = \mathbb{R}$, $B \subseteq \mathbb{R}$, f é sobrejetora e não é injetora.

(d) $A \subseteq \mathbb{R}$, $B = \mathbb{R}$, f é sobrejetora e não é injetora.

6. Sejam $A = \{1, 2, 3\}$, $B = \{4, 5, 6, 7\}$ e $C = \{8, 9, 0\}$. Sejam as funções $f : A \to B$ e $g : B \to C$ definidas por $f() = 4$, $f(2) = 5$, $f(3) = 6$, $g(4) = 8$, $g(5) = 8$, $g(6) = 9$ e $g(7) = 0$. Verifique se existem $f \circ g$ e $g \circ f$ e se são injetoras e sobrejetoras.

7. Mostre que a equipotência é uma relação de equivalência.

8. Mostre que a função $f : \mathbb{Z} \to \mathbb{N}$ definida por $f(n) = \begin{cases} 2n \text{ se } n \geq 0 \\ -2n - 1 \text{ se } k < 0 \end{cases}$ é uma bijeção.

9. Mostre que a função $f : [a, b] \to [0, 1]$ definida por $f(x) = \frac{x-a}{b-a}$ é uma bijeção.

10. Mostre que a função $f : (-1, 1) \to \mathbb{R}$ definida por $f(x) = \frac{x}{1+|x|}$ é uma bijeção e que $f^{-1} : \mathbb{R} \to (-1, 1)$ e definida por $f(x) = \frac{x}{1-|x|}$.

11. Sejam $f, g, h : \mathbb{R} \to \mathbb{R}$ definidas por $f(x) = x - 1$, $g(x) = x^2 + 2$ e $h(x) = x + 1$, onde $x \in \mathbb{R}$. Determine $f \circ g$, $f \circ h$, $g \circ h$, $g \circ f$, $h \circ f$, $h \circ g$, $(f \circ g) \circ h$ e $f \circ (g \circ h)$.

12. Sejam as funções $f, g : \mathbb{R} \to \mathbb{R}$ definidas por $f(x) = x^3 + 1$ e $g(x) = x^2 + 1$, onde $x \in \mathbb{R}$. Determine $f \circ f$, $g \circ g$, $f \circ g$ e $g \circ f$.

13. Determine $f \circ f$, $g \circ g$, $f \circ g$ e $g \circ f$, onde $f, g : \mathbb{R} \to \mathbb{R}$ são definidas por $f(x) = \begin{cases} x^2 \text{ se } x < 0 \\ 3x \text{ se } x \geq 0 \end{cases}$ e $g(x) = \begin{cases} 1 - x \text{ se } x < 1 \\ 1 + x \text{ se} x \geq 1. \end{cases}$

14. Determine $f \circ f$, $g \circ g$, $f \circ g$ e $g \circ f$, onde $f, g : \mathbb{R} \to \mathbb{R}$ são definidas por $f(x) = \begin{cases} x^2 + 1 \text{ se } x < 0 \\ 2x + 1 \text{ se } x \geq 0 \end{cases}$ e $g(x) = \begin{cases} 3x \text{ se } x < 1 \\ 7x + 1 \text{ se } 1 \leq x \leq 5 \\ 2 + x \text{ se } x > 5. \end{cases}$

15. Seja a função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = \begin{cases} 2x + 5 \text{ se } x < -1 \\ x^2 - 1 \text{ se } -1 \leq x \leq 1 \\ 5x \text{ se } x > 1. \end{cases}$
Esboce o gráfico e verifique se f é injetora e sobrejetora.

16. Seja a função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = cos(x)$, onde $x \in \mathbb{R}$. Determine $f([0, \pi/2])$, $f([0, \pi])$, $f(\mathbb{R})$, $f^{-1}(1/2)$, $f^{-1}([1/2, 1])$ e $f^{-1}(\mathbb{R})$.

17. Seja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por$f(x, y) = mdc(2, y)$. Verifique se f é injetora e sobrejetora.

18. Quais das funções abaixo são iguais.

(a) $f(x) = \frac{x^2-4x+3}{x-3}$ e $g(x) = x - 1$, com $x \in \mathbb{R} - \{3\}$.

(b) $f(x) = 1$ e $g(x) = x^4$, onde $x \in \{1, -1, i, -i\}$.

(c) $f(x) = x^3$, onde $x \in \mathbb{R}$, e $g(y) = y^3$, onde $y \in \mathbb{R}$.

19. Seja $f : \mathbb{R} \to \mathbb{R}$ uma função definida por $f(x) = \begin{cases} x + 1 \text{ se } x \leq 0 \\ 1 - 2x \text{ se } x > 0. \end{cases}$ Determine $f \circ f$.

20. Sejam f e g duas funções definidas por $f(x) = \begin{cases} x+1, \text{ se } x \geq 0 \\ -x+1, \text{ se } x < 0 \end{cases}$ e $g(x) = 3x - 2$.

    (a) Faça o gráfico da f e g.

    (b) Determine $D(f)$, $Im(f)$, $D(g)$ e $Im(g)$.

    (c) Verifique se f e g são injetoras e sobrejetoras.

    (d) Determine f^{-1} e g^{-1}.

    (e) Determine $f \circ g$, $g \circ f$, $D(f \circ g)$, $D(g \circ f)$, $Im(f \circ g)$ e $Im(g \circ f)$.

    (f) Faça o gráfico de $f \circ g$ e $g \circ f$.

    (g) Determine $f \circ f$, $D(f \circ f)$, $Im(f \circ f)$ e seu gráfico.

    (h) Determine $g \circ g$, $D(g \circ g)$, $Im(g \circ g)$ e seu gráfico.

21. Mostre que a função $f : \mathbb{Z}^2 \to \mathbb{Z}^2$ definida por $f(x, y) = (x+3, 2-y)$ é bijetora e determine f^{-1}.

22. Seja $f : \mathbb{R}^* \to \mathbb{R} - \{1\}$ definida por $f(x) = (x+2)/x$. Mostre que f é bijetora e determine f^{-1}.

23. Mostre que as funções $f :]-1, 1[\to \mathbb{R}$ e $g : \mathbb{R} \to]-1, 1[$ definidas por $f(x) = \frac{x}{1-|x|}$, onde $x \in]-1, 1[$, e $g(x) = \frac{x}{1+|x|}$, onde $x \in \mathbb{R}$, são bijetoras e determine $g \circ f$ e $f \circ g$.

24. Seja $f : \mathbb{R} \to \mathbb{R}$ uma função definida por $f(x) = ax^n$, onde $a \in \mathbb{R}$ e $n \in \mathbb{N}$. Determine a e n tal que $(f \circ f)(x) = 3x^4$.

25. Sejam as funções $f, g : \mathbb{R} \to \mathbb{R}$ definidas por $f(x) = \begin{cases} x^2 \text{ se } x \geq 0 \\ 1 + x \text{ se } x < 0 \end{cases}$ e $g(x) = 3x + 1$, onde $x \in \mathbb{R}$. Determine $g \circ f$ e $f \circ g$.

26. Sejam as funções $f : (-1, 1) \to \mathbb{R}$ definida por $f(x) = \frac{x}{1-|x|}$ e $g : \mathbb{R} \to (-1, 1)$ definida por $g(x) = \frac{x}{1+|x|}$. Mostre que f e g são bijetoras e calcule $f \circ g$ e $g \circ f$.

27. Sejam $f : E \to F$ uma função, $A \subseteq E$ e $B \subseteq F$. Mostre que:

    (a) $f(E) - f(A) \subseteq f(E - A)$.

    (b) $f^{-1}(F - B) = E - f^{-1}(B)$.

    (c) $f(A \cap f^{-1}(B)) = f(A) \cap B$.

28. Seja $f : E \to F$ uma função. Mostre que:

    (a) $A \neq \emptyset$ se, e somente se, $f(A) \neq \emptyset$.

    (b) Se $A \subseteq B \subseteq E$, então $f(A) \subseteq f(B)$.

    (c) $f(A \cup B) = f(A) \cup f(B)$.

    (d) $f(A \cap B) \subseteq f(A) \cap f(B)$.

(e) $A \subseteq f^{-1}(f(A))$ e $f(f^{-1}(B)) \subseteq B$.

(f) Mostre que f é injetora se, e somente se, $f(A \cap B) = f(A) \cap f(B)$.

(g) f é sobretora se, e somente se, $f(A^c) = (f(A))^c$.

29. Seja $f : E \to F$ uma função. Mostre que:

(a) Se $A \subseteq B \subseteq F$, mostre que $f^{-1}(A) \subseteq f^{-1}(B)$.

(b) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

(c) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$. Determine $f^{-1}(A^c) = (f^{-1}(A))^c$.

30. Mostre que a função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = ax + b$, com $a \neq 0$, é bijetora e determine f^{-1}.

31. Seja $F : \mathbb{R}^2 \to \mathbb{R}$ uma função definida por $f(x, y) = xy$.

(a) Verifique se f é injetora e sobrejetora.

(b) Determine $f^{-1}(\{0\})$ e $f([0, 1] \times [0, 1])$.

32. Sejam f e g funções.

(a) Se f e g são injetoras, mostre que $f \circ g$ é injetora.

(b) Se f e g são sobrejetoras, mostre que $f \circ g$ é sobrejetora.

(c) Se $g \circ f$ é injetora, mostre que f é injetora.

(d) Se $f \circ g$ é sobrejetora, mostre que f é sobrejetora.

33. Verifique se a função $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ definida por $f(x, y) = (2x + 3, 4y + 5)$ é injetora e sobrejetora.

34. Mostre que a função $f : \mathbb{R} - \{d/c\} \to \mathbb{R} - \{a/c\}$ definida por $f(x) = \frac{ax-b}{cx-d}$, onde $a, b, c, d \in \mathbb{R}$, $c \neq 0$ e $ad - bc \neq 0$, é bijetora e determine f^{-1}.

35. Seja a função $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = \begin{cases} x^2 & \text{se } x \leq 0 \\ \sqrt[3]{x} & \text{se } x > 0 \end{cases}$. Determinar $f([-1, 8])$, $f(\mathbb{R}_+)$, $f(\mathbb{R}_-)$, $f^{-1}(\{1, 16\})$, $f^{-1}([-1, 16])$ e $f^{-1}(\mathbb{R}_+^*)$.

36. Das funções de $\mathbb{R}$ em $\mathbb{R}$ abaixo, quais são injetoras e sobrejetoras: $f(x) = x^3 - 1$, $f(x) = x^2 - 5x + 6$, $f(x) = 2^x$, $f(x) = |sen(x)|$ e $f(x) = x + |x|$.

37. Sejam as funções reais $f(x) = 2x + 7$ e $(f \circ g)(x) = 4x^2 - 2x + 3$. Determinar g.

38. Seja $f : \mathbb{R} \to \mathbb{R}$ uma função definida por $f(x) =\mid x \mid$. Determine $f(\mathbb{R})$, $f([-1, 2])$, $f^{-1}([2, 5])$ e $f^{-1}(\{-7\})$.

39. Determine $D(f)$, $Im(f)$ e faça os gráficos das funções:

(a) $f(x) = \begin{cases} 3x - 2 & \text{se } x < 1 \\ x^2 & \text{se } x \geq 1 \end{cases}$

(b) $g(x) = \dfrac{x^2 - 9}{x - 3}$.

40. Determine $f \circ f$, $g \circ g$, $f \circ g$ e $g \circ f$ das seguintes funções

$$f(x) = \sqrt{3x - 4} \quad \text{e} \quad g(x) = \begin{cases} x^2 - 4 & \text{se } x < 3 \\ 2x - 1 & \text{se } x \geq 3. \end{cases}$$

4.2 Conjuntos equipotentes e enumeráveis

O infinito sempre assombrou os matemáticos e filósofos, estando relacionada aos maiores paradoxos e crises nos fundamentos da matemática, como é o caso dos famosos paradoxos de Zeno e de Eléia, que se baseiam em interpretações tortuosas do conceito de infinitude para provar a não existêencia de movimento.

No desenvolvimento da teoria dos conjuntos, o conceito de infinito desepenha um papel fundamental, sendo responsável por uma dos maiores problemas filosóficas na história da matemática. Como efeito desse problema, tivemos matemáticos e filosóficos sendo destruídos, novos questionamentos surgindo, divergências na própria concepção de verdade matemática, novas propostas de formalização da disciplina. Enfim, como aconteceu com as grandezas incomensuráveis e a história do quinto postulado de Euclides (esses dois também estão diretamente relacionados ao conceito de infinitude) os paradoxos da teoria dos conjuntos contribuíram enormemente para o enriquecimento do pensamento matemático.

Definição 4.2.1. *Dois conjuntos A e B são chamados equipotentes se existe uma bijeção f entre A e B.*

Sejam A, B e C conjuntos. A relação de equipotência é uma relação de equivalência, ou seja,

1. A é equipotente a A.
2. Se A é equipotente a B, então B é equipotente a A.
3. Se A é equipotente a B e B é equipotente a C, então A é equipotente a C.

Exemplo 4.2.1. *Os intervalos $[0, 1]$ e $[a, b]$, com $a < b$, são equipotentes, uma vez que a aplicação $f : [0, 1] \to [a, b]$ definida por $f(x) = (b - a)x + a$ é uma bijeção.*

Definição 4.2.2. *Seja A um conjunto.*

1. *O conjunto A é dito finito se é vazio ou se existe $n \in \mathbb{N}$ tal que A é equipotente a $\{1, 2, , 3, \ldots, n\}$. Caso contrário, A é dito infinito.*
2. *A cardinalidade do conjunto A é o número de elementos do conjunto A que pode ser finito ou infinito.*

O conjunto dos números naturais, o conjunto dos pontos de uma reta, o conjunto das retas em um plano, o conjunto das fraçõe e o conjunto dos números reais são exemplos de conjuntos infinitos. Observe que todos esses conjuntos são fomados por conceitos abstratos, e não por objetos concretos. Portanto, a idéia de infinitude não era fácil de assimilar.

Pergunta: será que a ordem que utilizamos para contar as coisas não afeta o resultado? Ninguém havia pensado nessa questão em conjuntos infinitos? Afinal, um conjunto infinito é infinito e não tem como contar os elementos de um conjunto infinito. Porém, algumas mentes mais aguçadas ousaram aprofundar-se nas questões filosóficas da infinitude. O cientista italiano Galileu Galilei (1564-1642) decidiu usar a noção de funções bijetoras para comparar conjuntos infinitos, chegando em um resultado bem curioso. Ele considerou a função que associa, a cada número natural, o seu dobro, conforme o seguinte diagrama:

$$\begin{array}{ccc} 0 & \longleftrightarrow & 0 \\ 1 & \longleftrightarrow & 2 \\ 2 & \longleftrightarrow & 4 \\ & \cdots & \end{array}$$

Com isso, Galilei mostrou que o conjunto dos números naturais tem a mesma cardinalidade que o conjunto dos nḿeros pares. Na época, isso parecia contradizer o axioma de Euclides que dizia que "o todo é sempre maior que a parte". O conjunto dos números pares é apenas uma parte do conjunto de todos os números naturais, e ainda assim, ambos os conjuntos têm a mesma cardinalidade, se utilizarmos essa noção de bijeções. Observe, que isso somente acontece com conjuntos infinitos. Em um conjunto finito, se tirarmos um único elemento não conseguimos associar biunivocamente os elementos do conjunto reduzido com os do conjunto todo.

O hotel de Hilbert: O matemático alemão David Hilbert (1862-1943) apresentou um exemplo parecido. Se chegamos em um hotel e todos os quartos estão ocupados, então sabemos que não existe vaga nesse hotel, a menos que um quarto seja desocupado. Agora, imaginamos um hotel com infinitos quartos, sendo um quarto para cada número natural, e que todos os quartos estão ocupados. Chega um novo hóspede querendo se hospedar e o dono não quer desalojar nenhum hóspede, mas também não quer perde clientes. Como existem infinitos quartos, mesmo que todos estejam ocupados, é possível resolver o problema. Para isso, é suficiente passar cada hóspede para o próximo quarto. Assim, quem está hospedado no quarto 0 vai para o quarto 1, e do quarto 1 para o 2, e assim, por diante, sobrando o quarto 0 para o novo hóspedes.

O problema do dono do hotel parece se complicar quando chega um ônibus com uma infinidade de hóspedes, um hóspede para cada número natural. Neste caso, o dono passa cada hóspede de um quarto para outro cujo número é o dobro do primeiro. Sobra, assim, todos os números ímpares para colocar os novos hóspedes. E se chegarem infinitos ônibus, cada ônibus marcado por um número natural diferente e com infinitos passageiros cada um, onde cada passageiro também marcado por um número? Nesse caso, o dono do hotel poderá ainda hospedar todo mundo de forma que não fique nenhum quarto vazio. Para isso, é suficiente colocar o n-ésimo passageiro do m-ésimo ônibus no quarto $2n(m+1)$, onde supomos que o hotel esteja vazio.

Aparentemente o paradoxo criado por Galilei não causou tanto impacto na matemática e na filosofia, nem foi devidamente explorado durante alguns séculos. Foi somente no século XIX que o assunto foi novamente estudado pelo matemático alemão Georg Cantor (1845-1918). Dessa vez, o impacto transformou totalmente o rumo da matemática moderna e deu início á teoria dos conjuntos que é vista hoje.

Cantor não só criou um paradoxo ou uma discussão filosófica através dessa idéia de comparar tamanho de conjuntos infinitos: ele de fato resolveu um problema matemático usando esse conceito. Enquanto outros matemáticos tiveram uma grande dificuldade para provar que números π e e são transcendentes (isto é, não são raízes de equações polinomiais de coeficientes inteiros), Cantor provou, de maneira relativamente simples, que existem muitos números transcendentes, mesmo sem exibir um sequer.

Definição 4.2.3. *Um conjunto A é dito enumerável se A é equipotente a um subconjunto dos números naturais $\mathbb{N}$. Caso contrário, o conjunto A é chamado não enumerável.*

Pela Definição 4.2.3, segue que todo comjunto finito e todo subconjunto de $\mathbb{N}$ são enumeráveis, e portanto, $\mathbb{N}$ é um conjunto enumerável. Agora, se A é um conjunto enumerável e $f : A \to B$ é uma bijeção, então B é enumerável.

Exemplo 4.2.2. *O conjunto $2\mathbb{N}$ é enumerável, uma vez que a aplicação $f : \mathbb{N} \to 2\mathbb{N}$ definida por $f(n) = 2n$, onde $n \in \mathbb{N}$, é uma bijeção.*

Exemplo 4.2.3. *O conjunto dos numeros inteiros $\mathbb{Z}$ é enumerável, uma vez que a aplicação $f : \mathbb{N} \to \mathbb{Z}$ definida por*

$$f(n) = \begin{cases} \frac{n-1}{2} & \text{se } n \text{ é impar} \\ -\frac{n}{2} & \text{se } n \text{ é par} \end{cases}$$

é uma bijeção.

Proposição 4.2.1. *Se A é um conjunto infinito, então A possui um subconjunto infinito enumerável.*

Demonstração. Vamos definir uma função $f : \mathbb{N} \to A$. Como A é infinito, segue que existe um elemento $x_0 \in A$. Assim, definimos $f(0) = x_0$. Como A é infinito, segue que $A_1 = A - \{x_0\}$ é não vazio, ou seja, existe $x_1 \in A_1$. Assim, definimos $f(1) = x_1$. De modo análogo, se $A_2 = A - A_1$, definimos $f(2) = x_2$, onde $x_2 \in A_2$. Por recorrência, definimos $f(n) = x_n$, onde $x_n \in A - \{x_0, x_1, x_2, \ldots, x_{n-1}\}$. A função f é injetora, uma vez que se $m, n \in \mathbb{N}$, com $m \neq n$, então $f(m) \in \{f(1), f(2), \ldots, f(n-1)\}$ e $f(n) \notin \{f(1), f(2), \ldots, f(n-1)\}$, ou seja, $f(m) \neq f(n)$. Assim, $f : \mathbb{N} \to Im(f) \subseteq A$ é uma bijeção, e portanto, A possui um subconjunto infinito enumerável. □

Proposição 4.2.2. *Sejam $A \subseteq B$ conjuntos. Se B é enumerável, então A é enumerável.*

Demonstração. Como B é enumerável, segue que B é equipotente a um subconjunto de $\mathbb{N}$, ou seja, existe uma aplicação bijetora $f : B \to C$, onde $C \subseteq \mathbb{N}$. Assim, a restrição de f ao conjunto A é uma bijeção na imagem, ou seja, $f_A :\to Im(f_A)$ é uma bijeção. Como $Im(f_A) \subseteq C \subseteq \mathbb{N}$, segue que A é enumerável. □

Proposição 4.2.3. *Sejam A e B conjuntos e $f : A \to B$ uma aplicação.*

1. *Se f é injetiva e B for enumerável, então A é enumerável.*
2. *Se f é sobrejetiva e A for enumerável, então B é enumerável.*

Demonstração. Para (1), como $f : A \to Im(f) \subseteq B$ é uma bijeção, pela Proposição 4.2.2, segue que $Im(f)$ é enumerável, e portanto, A é enumerável. Para (2), como f é sobrejetora, segue que para cada $b \in B$ existe $a \in A$ tal que $f(a) = b$. Com isso, obtemos a aplicação $g : B \to A$ tal que $f(g(b)) = b$, para todo $b \in B$. Assim, g é injetora, e pelo item (1), segue que B é enumerável. □

Lema 4.2.1. *O conjunto $\mathbb{N} \times \mathbb{N}$ é enumerável.*

Demonstração. A função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por $f(m, n) = 2^m 3^n$ é injetiva. Logo, $\mathbb{N} \times \mathbb{N} \to f(\mathbb{N} \times \mathbb{N}) \subseteq \mathbb{N}$ é uma bijeção. Portanto, $\mathbb{N} \times \mathbb{N}$ é enumerável. □

Proposição 4.2.4. *Sejam A e B conjuntos.*

1. *Se A e B são enumeráveis, então $A \times B$ é um conjunto enumerável.*
2. *Se $A \times B$ é enumerável, então A e B são enumeráveis.*

Demonstração. Para (1), como A e B são enumeráveis, segue que existem bijeções $f : A \to A_1$ e $g : B \to B_1$, onde A_1 e B_1 são subconjuntos de $\mathbb{N}$. Assim, aplicação $h : A \times B \to A_1 \times B_1$ definida por $h(a, b) = (f(a), g(b))$ é uma bijeção. Como $A_1 \times B_1 \subseteq \mathbb{N} \times \mathbb{N}$, segue que $A \times B$ é enumerável. □

Pela Proposição 4.2.4, segue que para uma quantidade finita de conjuntos enumeráveis, o produto cartesiano ainda será enumerável, entretanto para o caso infinito isso não ocorre, ou seja, dados infinitos conjuntos enumeráveis, não necessariamente o produto cartesiano será enumerável.

Corolário 4.2.1. *O conjunto dos números racionais é enumerável.*

Demonstração. Seja $\mathbb{Z}^*$ o conjunto dos inteiros não nulos. Como $\mathbb{Z}^* \subseteq \mathbb{Z}$, segue que $\mathbb{Z}^*$ é enumerável. Assim, pela Proposição 4.2.4, segue que $\mathbb{Z}^* \times \mathbb{Z}$ é enumerável. Agora, a aplicação $f : \mathbb{Z}^* \times \mathbb{Z} \to \mathbb{Q}$ definida por $f(m, n) = \frac{m}{n}$ é sobrjetororа. Pelo Lema 4.2.1, segue que $\mathbb{Q}$ é enumerável. □

Corolário 4.2.2. *A união de uma família enumerável de conjuntos enumeráveis é enumerável.*

Demonstração. Sejam $A_1, A_2, \ldots$ uma família enumerável de conjuntos enumeráveis. Assim, existem funções sobrejetoras $f_i : \mathbb{N} \to A_i$, para todo i. Sejam $A = \cup_{i=1}^{\infty} A_i$ e $f : \mathbb{N} \times \mathbb{N} \to A$ definida por $f(m, n) = f_n(m)$. Como f é sobrejetora, segue que A é enumerável. □

Teorema 4.2.1. *O intervalo $(0, 1)$ não é enumerável.*

Demonstração. Se $(0,1)$ for enumerável, então existe uma bijeção $f : \mathbb{N} \to (0,1)$. Assim, $f(i) = x_i$, para todo $i \in \mathbb{N}$, onde

$$\begin{aligned} x_1 &= 0, x_{11}x_{12}x_{13}\cdots \\ x_2 &= 0, x_{21}x_{22}x_{23}\cdots \\ x_3 &= 0, x_{31}x_{32}x_{33}\cdots \\ &\vdots \end{aligned}$$

Agora, seja $k \in (0,1)$ dado por $k = 0, k_1k_2k_3\ldots$, onde $k_i \neq x_{ii}$ para todo i. Desse modo, $k \in (0,1)$ e $k \neq x_i$, para todo i, o que é uma contradição. Portano, $(0,1)$ não é enumerável. □

Corolário 4.2.3. *O conjunto dos números reais $\mathbb{R}$ não é enumerável.*

Demonstração. Se $\mathbb{R}$ for enumumerável, então $(0,1)$ é enumerável, pois todo subconjunto de um conjunto enumerável é enumerável, o que é uma contradição. Portanto, $\mathbb{R}$ não é enumerável. □

Corolário 4.2.4. *O conjunto dos números irracionais não é enumerável.*

Demonstração. Se $\mathbb{R} - \mathbb{Q}$ for enumerável, segue que $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} - \mathbb{Q})$ é enumerável, o que é uma contradição. Portanto, o conjunto dos números irracionais não é enumerável. □

Definição 4.2.4. *Um número complexo α é chamado algébrico se existem inteiros $a_o, a_1, \cdots, a_n$, não todos nulos, tal que $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$. Caso, contrário, α é chamado transcendente.*

Lema 4.2.2. *O conjunto $P_n(\mathbb{Z})$ de todos os polinômios de coeficientes inteiros de grau máximo n é enumerável.*

Demonstração. A aplicação $f : \mathbb{Z}^{n+1} \to P_n(\mathbb{Z})$, definida por $f(a_o, a_1, \cdots, a_n) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, é bijetora. Portanto, $P_n(\mathbb{Z})$ é enumerável. □

Proposição 4.2.5. *O conjunto dos números algébricos é enumerável.*

Demonstração. Seja $P(\mathbb{Z})$ o conjunto dos polinômio de qualquer grau, ou seja, $P(\mathbb{Z}) = \cup_{n=1}^{\infty} P_n(\mathbb{Z})$. Como $P_n(\mathbb{Z})$ é enumerável, segue que $P(\mathbb{Z})$ é enumerável. Agora, seja R_p o conjunto das raízes de um polinômio $p(x) \in P(\mathbb{Z})$. A aplicação $f : P(\mathbb{Z}) \to \cup_{p\in P(\mathbb{Z})} R_p$ que associa cada polinômio $q \in P(\mathbb{Z})$ ao conjunto de suas raízes $R_q \in \cup R_p$ é sobrejetora. Portanto, $\cup_{p\in P(\mathbb{Z})} R_p$ é enumerável. □

Corolário 4.2.5. *O conjunto dos números transcendentes não é enumerável.*

Demonstração. Como $\mathbb{C}$ é a união dos números algébricos com os números transcendentes, segue que o conjunto dos números transcendentes não é enumerável. □

4.2.1 Exercícios

1. Mostre que a união e a interseção de dois conjuntos finitos é um conjunto finito.
2. Seja A um conjunto.
   (a) Mostre que A não é equipotente a $\mathcal{P}(A)$.
   (b) Mostre que A é finito se, e somente se, $\mathcal{P}(A)$ é finito.
3. Mostre que $\mathbb{Z}$ e $2\mathbb{Z}$ são equipotentes. Mostre que $\mathbb{Z}$ é equipotente a $n\mathbb{Z}$, onde $n > 1$.
4. Mostre que o conjunto dos naturais pares é equipotente ao conjunto dos naturais impares.
5. Mostre que os conjuntos $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$ são conjuntos enumeráveis e equipotentes.
6. Mostre que o intervalo aberto $]-1, 1[$ e $\mathbb{R}$ são equpotentes.
7. Sejam $a, b \in \mathbb{R}$, com $a < b$. Mostre que os intervalos $[-1, 1]$ e $[a, b]$ são equipotentes.
8. Mostre que $[0, 1]$ é equipotente a $]0, 2[$.
9. Mostre que $\mathbb{R}$ é equipotente a $[0, \infty[$.
10. Sejam A e B conjuntos enumeráveis. Mostre que $A \cup B$ e $\cap B$ são conjuntos enumeráveis.
11. Mostre que o conjunto $A = \{\frac{1}{n} : n \in \mathbb{Z} - \{0\}\}$ é enumerável.
12. Mostre que um conjunto A é enumerável se, e somente se, A é finito ou A é equipontente a $\mathbb{N}$.
13. Se A é enumerável, mostre que existe uma aplicação sobrejetora $f : \mathbb{N} \to A$.
14. Mostre que o conjunto $A = \{3^m 5^n : m, n \in \mathbb{N}\}$ é um conjunto enumerável.
15. Mostre que:
   (a) $\mathbb{N}^* \times \mathbb{N}$ é enumerável.
   (b) $\mathbb{Z}^* \times \mathbb{N}$ é enumerável.
   (c) $\mathbb{N}^* \times \mathbb{Q}$ é enumerável.
   (d) $\mathbb{Z}^* \times \mathbb{Q}^*$ é enumerável.

Capítulo

5

Números inteiros

Neste capítulo, apresentamos os números naturais, os números inteiros com as suas operações, princípio do menor inteiro, indução matemática, divisibilidade, algoritmo euclidiano, máximo múltiplo comum, mínimo múltiplo comum, números primos e compostos, e finalmente, congruência.

5.1 Números naturais

Nesta seção, veremos a construção lógica dos números naturais, com o objetivo de compreender através do conjunto dos naturais algumas propriedades, operações e relações do conjunto dos inteiros. Uma construção consistente do Conjunto dos Números Naturais foi desenvolvida no século XIX por Giuseppe Peano ($1858 - 1932$). Essa construção, comumente chamada de Axiomas de Peano, formulada em 1891, é uma estrutura simples e elegante, servindo como um bom exemplo, de construção de conjuntos numéricos. Peano usou três conceitos primitivos: o *zero*, o *número natural* e a relação *é sucessor de*, cujas notações são, respectivamente: 0, a e a^+. E, para caracterizá-los, formulou os seguintes axiomas, onde $\mathbb{N}$ é considerado como o conjunto dos números naturais.

P_1 : Zero é um número natural, ou seja, $0 \in \mathbb{N}$.

P_2 : Se a é natural, então a tem um único sucessor que também é natural, ou seja, se $a \in \mathbb{N}$, então $a^+ \in \mathbb{N}$. O elemento a^+ é chamado sucessor de a.

P_3 : O zero não é sucessor de nenhum número natural, ou seja, se $a \in \mathbb{N}$, então $a^+ \neq 0$, para todo $a \in \mathbb{N}$.

P_4 : Dois naturais que têm sucessores iguais são iguais, ou seja, se $a^+ = b^+$, então $a = b$.

P_5 : Seja S um conjunto de números naturais. Se S possui o zero e o sucessor de todo elemento de S, então esse conjunto possui todos os números naturais, ou seja, Se $S \subset \mathbb{N}$ e $0 \in S$, com $a \in S$, então $a^+ \in S$, então $S = \mathbb{N}$.

A Propriedade P_1 garante que o conjunto $\mathbb{N}$ é não vazio. Pela Propriedade P_4, segue que se $a \neq b$, então $a^+ \neq b^+$. A Propriedade P_5 é chamada princípio de indução completa.

Proposição 5.1.1. *Se $a \in \mathbb{N}$, então $a^+ \neq a$.*

Demonstração. Seja $S = \{a \in \mathbb{N} : a^+ \neq a\}$. Por (3), segue que $0 \in S$. Se $a \in S$, então $a^+ \in S$. Por (5), segue que $S = \mathbb{N}$, ou seja, para todo $a \in \mathbb{N}$, segue que $a^+ \neq a$. Pela Propriedade P_5, segue que $S = \mathbb{N}$. □

Proposição 5.1.2. *Se $b \in \mathbb{N}$, onde $b \neq 0$, então existe $a \in \mathbb{N}$ tal que $a^+ = b$.*

Demonstração. Seja $S = \{0\} \cup \{y \in \mathbb{N} : \ y \neq 0 \text{ e } x^+ = y\}$. Assim, $0 \in S$, e portanto, $0^+ \in S$. Agora, se $a \in S$ e $a \neq 0$, então $a^+ = (b^+)^+$. Pela Propriedade P_5, segue que $S = \mathbb{N}$. □

Proposição 5.1.3. *(Primeiro princípio de indução completa) Se para todo número natural n está associado uma afirmação $P(n)$ tal que*

1. *$P(0)$ é verdadeira, e*
2. *Se $P(k)$ é verdadeira, então $P(k^+)$ é verdadeira,*

então $P(n)$ é verdadeira, para todo $n \in \mathbb{N}$.

Demonstração. Seja $S = \{n \in \mathbb{N} : P(n) \text{ é verdadeira}\}$. Pela Propriedade P_5, segue que $S = \mathbb{N}$. □

5.1.1 Operações

Nesta seção, apresentamos as operações de adicão (soma) e de multiplicação (produto) dos números naturais.

Definição 5.1.1. *A adição em $\mathbb{N}$ é definida sob as seguintes condições:*

1. *$a + 0 = a$, para todo $a \in \mathbb{N}$.*
2. *$a + b^+ = (a + b)^+$, para todo $a, b \in \mathbb{N}$.*

Se $a + b = c$, então a e b são chamadas de parcelas e c a soma.

Agora, adotando, $0^+ = 1$, $1^+ = 2$, $\cdots$, segue que

$$\begin{aligned}
&1 + 1 = 1^+0^+ = (1 + 0)^+ = 1^+ = 2.\\
&1 + 2 = 1 + 1^+ = (1 + 1)^+ = 2^+ = 3.\\
&\vdots\\
&r + 1 = r + 0^+ = (r + 0)^+ = r^+, \text{ para todo } r \in \mathbb{N}.
\end{aligned}$$

Além disso, para todo $a, b \in \mathbb{N}$, obtemos as seguintes propriedades.

1. $0 + a = a$, para todo $a \in \mathbb{N}$. De fato: se $a = 0$, então $0 + 0 = 0$, por definição. Se $a \neq 0$, então existe $b \in \mathbb{N}$ tal que $0 + a = 0 + b^+ = (0 + b)^+ = b^+ = a$.

2. $a + 1 = a^+$, para todo $a \in \mathbb{N}$. De fato, $a + 1 = a + 0^+ = (a + 0)^+ = a^+$.

3. Se $a + b = 0$, então $a = b = 0$. De fato, se $b \neq 0$, então existe $u \in \mathbb{N}$ tal que $b = u^+$. Assim, $a + b = a + u^+ = (a + u)^+ = 0$, o que é um absurdo. Portanto, $b = 0$, e assim, $a = 0$.

Agora, para todo $a, b, c \in \mathbb{N}$, obtemos as seguintes propriedades.

1. $a + (b + c) = (a + b) + c$ (associativa). *Prova:* Por indução sobre c. Para $c = 0$, segue que $a + (b + c) = (a + b) + 0$. Agora. suponhamos que $(a + b) + r = a + (b + r)$. Assim, $(a + b) + r^+ = [(a + b) + r]^+ = [a + (b + r)]^+ = a + (b + r)^+ = a + (b + r^+)$, Assim, $(a + b) + c = a + (b + c)$, para todo $a, b, c \in \mathbb{N}$. o que prova o resultado.

2. $a + b = b + a$ (comutativa). *Prova:* Por indução sobre b. Para $b = 0$, segue que $a + 0 = a = 0 + a$. Agora, supondo que $a + r = r + a$, segue que $a + r^+ = (a + r)^+ = (r + a)^+$. Assim, $a + b = b + a$, para todo $a, b \in \mathbb{N}$, o que prova o resultado.

3. $a + 0 = a$ (0 é o elemento neutro da adição). *Prova:* Segue diretament da Definição 5.1.1.

4. Se $a + b = a + c$ (Lei do cancelamento). *Prova:* Por indução sobre a. Para $a = 0$, segue que $0 + b = 0 + c$, ou seja, $b = c$. Agora, suponhamos que $r + b = r + c$ implica que $b = c$. Assim, se $r^+ + b = r^+ + c$, então $b + r^+ = c + r^+$. Logo, $(b + r)^+ = (c + r)^+$. Por (4), segue que $b = c$, o que prova o resultado.

5. $a + 1 = 1 + a$. *Prova:* Por indução sobre a. Se $a = 0$, então $0 + 1 = 0 + 0^+ = (0 + 0)^+ = 0^+ = 1 = 1 + 0$. Agora, suponhamos que $1 + r = r + 1 = r^+$. Assim, $1 + r^+ = 1 + (r + 1) = (1 + r) + 1 = r^+ + 1$, o que prova o resultado.

Além disso,

1. O elemento 0 é único. De fato: suponhamos que existam dois elementos neutros 0_1 e 0_2. Assim, $a = a + 0_1 = a + 0_2$, para todo $a \in \mathbb{N}$. Pela Lei do Cancelamento, segue que $0_1 = 0_2$. Portanto, 0 é o único elemento neutro da adição.

2. Se $a + b = 1$, então $a = 0$ ou $b = 0$. De fato: se $b \neq 0$, então existe $u \in \mathbb{N}$ tal que $a + b = a + u^+ = (a + u)^+ = 1 = 0^+$. Assim, $a + u = 0$, e portanto, $a = u = 0$.

Definição 5.1.2. *A multiplicação (produto) em* $\mathbb{N}$ *é definida sob as seguintes condições:*

1. $a.0 = 0$, *para todo* $a \in \mathbb{N}$.

2. $a.b^+ = ab + a$, *para todo* $a, b \in \mathbb{N}$.

Se $ab = c$, *então* a *e* b *são os fatores e* c *o produto.*

Assim,

$$1.1 = 1.0^+ = 1.0 + 1 = 0 + 1 = 1$$
$$1.2 = 1.1^+ = 1.1 + 1 = 1 + 0^+ = (1 + 0)^+ = 1^+ = 2$$
$$2.2 = 2.1^+ = 2.1 + 2 = 2 + 2 = 2 + 1^+ = (2 + 1)^+ = 3^+ = 4.$$

Além disso, para todo $a \in \mathbb{N}$, segue que

1. $0.a = 0$. A prova é por indução sobre a. Se $a = 0$, por definição o resultado segue. Agora, suponhamos que $0.r = 0$. Assim, $0.r^+ = 0.r + 0 = 0 + 0 = 0$, o que prova o resultado.

2. $1.a = a$. A prova é por indução sobre a. Se a=0, por definição, segue que $1.0 = 0$. Agora, suponhamos que $1.r = r$. Assim, $1.r^{=}1.r + 1 = r + 1 = r^+$, o que prova o resultado.

Parra todo $a, b, c \in \mathbb{N}$, obtemos as seguintes propriedades.

1. $a(bc) = (ab)c$ (Associativa). A prova é por indução sobre c. Se $c = 0$, então $a(bc) = a(b.0) = 0 = (ab)0$. Agora, suponhamos que $a(br) = (ab)r$. Assim, $a(br^+) = a(br + b) = abr + ab = (ab)r^+$. Portanto, $a(bc) = (ab)c$, para todo $a, b, c \in \mathbb{N}$.

2. $ab = ba$ (Comutativa). A prova é por indução sobre b. Para $b = 0$, segue que $a0 = 0 = 0a$. Agora, suponhamos que $ar = ra$. Assim, $ar^+ = ar+a = ra+a = r^+a$. Portanto, $ab = ba$, para todo $a, b \in \mathbb{N}$.

3. $a.1 = a$ (1 é o elemento neutro). A prova é por indução sobre a. Para $a = 0$, segue que $0 = a.1 = a$. Agoa, suponhamos que $r.1 = r$. Assim, $r^+.1 = 1.r^+ = 1.r + r = r + 1 = r^+$. Portanto, $a.1 = 1.a$, para todo $a \in \mathbb{N}$.

4. Se $ab = 0$, então $a = 0$ ou $b = 0$ (Lei do anulamento do produto). De fato, se $b \neq 0$, então $b = r^+$, onde $r \in \mathbb{N}$. Logo, $0 = ab = ar^+ = ar + a$. Assim, $ar = a = 0$. De forma análoga procedemos com a.

5. Se $ac = bc$, com $c \neq 0$, então $a = b$ (Lei do cancelamento do produto). A prova é por indução sobre c. Se $c = 1$, então, por (3), segue que $ac = bc$ implica que $a = b$. Agora, suponhamos que $ar = br$. Assim, $ar^+ = br^+$, ou seja, $ar + a = br + b$. Como $ar = br$, segue que $ar + a = ar + b$. Assim, $a = b$.

6. Se $ab = 1$, então $a = 1$ ou $b = 1$. De fato, se $b \neq 1$, então $b = r^+$, onde $r \geq 1$ e $r \in \mathbb{N}$. Logo, $1 = ab = ar^+ = ar + a$. Como $ar + a = 1$ implica que $a(r + 1) = 1$. Assim, $a = 1$ e $r = 0$, o que é um absurdo.

7. $(a + b)c = ac + bc$ e $a(b + c) = ab + ac$ (Distributiva). A prova é por indução sobre c. Se $c = 0$, então $(a+b).0 = 0 = a.0+b.0$. Agora, suponhamos que $(a+b)r = ar+br$. Assim, $(a + b)r^+ = (a + b)r + (a + b) = (ar + br) + (a + b) = (ar + a) + (br + b) = ar^+ + br^+$. Portanto, $(a + b)c = ac + bc$, para todo $a, b, c \in \mathbb{N}$. O caso $a(b + c) = ab + ac$, para todo $a, b, c \in \mathbb{N}$, procedemos de modo análogo usando indução sobre a.

5.1.2 Relação de ordem

A relação $\leq$ sobre $\mathbb{N}$ é definida do seguinte modo. Sejam $a, b \in \mathbb{N}$.

1. Se $b = a + u$, com $u \in \mathbb{N}$, então $a \leq b$.

2. Se $b = a + v$, com $v \neq 0$, então $a < b$.

As relações $\geq$ e $>$ são definidas, respectivamente, por:

1. $a \geq b$ se, e somente se, $b \leq a$, e

2. $a > b$ se, e somente se, $b < a$.

Para todo $a, b, c \in \mathbb{N}$, obtemos as seguintes propriedades.

1. $a \leq a$ (reflexiva). *Prova:* Segue do fato que $a = a + 0$.

2. Se $a \leq b$ e $b \leq a$, então $a = b$ (anti-simétrica). *Prova:* Por hipótese, segue que $b = a + u$ e $a = b + v$, com $u, v \in \mathbb{N}$. Assim, $a = a + u + v$, ou seja, $u + v = 0$. Logo, $u = v = 0$, e portanto, $a = b$.

3. Se $a \leq b$ e $b \leq c$, então $a \leq c$ (transitiva). *Prova:* Por hipótese, $b = a + u$ e $c = b + v$, com $u, v \in \mathbb{N}$. Assim, $c = a + (u + v)$, ou seja, $a \leq c$.

4. Se $a \leq b$, então $a + c \leq b + c$. *Prova:* Por hipótese, segue que $b = a + u$, com $u \in \mathbb{N}$. Logo, $b + c = a + c + u$, e portanto, $a + c \leq b + c$.

5. Se $a \leq b$, então $ac \leq bc$. *Prova:* Por hipótese, segue que $b = a + u$, onde $u \in \mathbb{N}$. Assim, $bc = (a + u)c = ac + uc$, e portanto, $ac \leq bc$.

Teorema 5.1.1. *(Lei da Tricotomia) Se $a, b \in \mathbb{N}$, então vale uma e somente uma das relações: $a = b$, $a < b$ ou $a > b$.*

Demonstração. Supondo que $a \neq b$, segue que $a > b$ ou $a < b$, ou seja, $a = b + u$, com $u \neq 0$, ou $b = a + v$, com $v \neq 0$. Se ocorressem as duas possibilidades, segue que $a = a + (u + v)$, e assim, $u + v = 0$ implica que $u = v = 0$, o que é um absurdo. Portanto, $a = b$, $a > b$ ou $a < b$. de modo único. □

5.1.3 Sistema de numeração decimal

Ao escrevermos um número, precisamos reconhecer em que base de numeração estamos trabalhando. Embora seja usual o tratamento com a base decimal, outras bases podem ser consideradas. Na computação, é usada a base binária, na divisão da hora usamos a base sexagesimal (60 minutos), e na medida da circunferência em 360 graus.

Em um sistema posicional com base a, onde a é um natural maior que 1, todo número natural n pode ser escrito de modo único na forma

$$n = a_k a^k + a_{k-1} a^{k-1} + \ldots + a_1 a^1 + a_0 a^0,$$

onde $0 \leq a_i < n$, para todo i. Esse número é representado por

$$(a_n a_{n-1} \ldots a_1 a_0)_a.$$

Assim, são necessários a algarismos $\{0, 1, 2, \ldots, a-1\}$ para descrevermos os números na base a.

O sistema de numeração decimal, também chamado de sistema de numeração decimal posicional, é um conjunto de regras que são utilizadas para representar os números, sendo escritos na base 10.

A base é a quantidade de símbolos que servem para representar os números. Portanto, na base 10 são utilizados os 10 algarismos: $0, 1, 2, 3, 4, 5, 6, 7, 8$ e 9. A ordem é a posição na qual o algarismo ocupa em um número, sendo analisado da direita para a esquerda. Assim, dado um número natural n, podemos escrevê-lo na base 10 como

$$n = (a_n a_{n-1} \ldots a_1 a_0)_{10} = a_0 10^0 + a_1 10^1 + a_2 10^2 + \cdots + a_n 10^n,$$

onde $a_0, a_1, \ldots, a_n$ são números variando de $0, 1, 2, \ldots, 9$, e a_0 é chamado de unidade, a_1 é chamado de dezena, a_2 é chamado de centena, a_3 é chamado de unidade de milhar, a_4 é chamado de dezena de milhar, a_5 é chamado de centena de milhar, a_6 é chamado de unidade de milhão, a_7 é chamado de dezena de milhão, a_8 é chamado de centena de milhão, a_9 é chamado de unidade de bilhão, e assim, por diante. Por exemplo, o número 1235 é escrito como $1235 = 5.10^0 + 2.10^1 + 3.10^2 + 5.10^3$.

Um número n é par se $n = 2k$ e n é impar se $n = 2k + 1$, onde $k \in \mathbb{N}$.

5.1.4 Exercícios

1. Sejam os conjuntos $A = \{x \in \mathbb{N} : x = 24n, \text{ com } n \in \mathbb{N}\}$ e $B = \{n \in \mathbb{N} : 3n + 4 < 2n + 9\}$. Determine $A \cup B$ e $A \cap B$.

2. Representar analiticamente cada conjunto abaixo.

   (a) Conjunto $\mathbb{N}$ dos números naturais.

   (b) Conjunto P dos números naturais pares.

(c) Conjunto I dos números naturais ímpares.

(d) Conjunto E dos números naturais menores que 16.

(e) Conjunto L dos números naturais maiores que 11.

(f) Conjunto R dos números naturais maiores ou iguais a 28.

(g) Conjunto C dos números naturais que estão entre 6 e 10.

3. Um gavião viu um grupo de pombos, chegou perto deles e disse: Olá minhas 100 pombinhas. Uma delas respondeu: Não somos 100 não meu caro gavião, seremos 100, com nós, mais dois tantos de nós e mais você meu caro gavião. Quantos pombos há neste grupo?

4. Três homens querem atravessar um rio. O barco que eles possuem suporta no máximo 150 kg. Um deles pesa 50 kg, o segundo pesa 75 kg e o terceiro pesa 120 kg. Qual será o processo para eles atravessarem o rio sem afundar?

5. Forme um quadrado mágico com os números $1, 2, 3, 4, 5, 6, 7, 8$ e 9 tal que, a soma dos números de qualquer linha, qualquer coluna ou qualquer diagonal deverá ser sempre igual a 15.

6. Mostre que:

(a) a soma de dois números pares é um número par.

(b) a soma de dois números impares é um número par.

(c) a soma de um número par e um número impar é um número impar.

(d) o produto de dois números pares é um número par.

(e) o produto de dois números impares é um número impar.

7. Mostre que $(n-1)^3 - n^3$ é um número impar, para todo $n \in \mathbb{N}$.

8. Escrever:

(a) O número 25 na base 3

(b) O número 125 na base 2.

(c) O número 743 na base 8.

5.2 Princípio do menor inteiro ou axioma da boa ordem

Seja $S \subseteq \mathbb{Z}$ com $S \neq \emptyset$. O conjunto S é dito limitado inferiormente se existe $a \in \mathbb{Z}$ tal que $a \leq x$ para todo $x \in S$.

Definição 5.2.1. *O elemento a nestas condições é chamado limite inferior de S. O maior dos limites inferiores de A pertence a S e é chamado elemento mínimo de S.*

Exemplo 5.2.1. *Todo subconjunto de* $\mathbb{N}$ *é limitado inferiormente, o conjunto* $S = \{\cdots, -3, -2-1, 0, 1, 2\}$ *não é limitado inferiormente.*

O princípio da boa ordenação ou princípio da boa ordem diz que todo subconjunto não vazio formado por números naturais possui um menor elemento. Isso é o mesmo que dizer que todo subconjunto não vazio formado por números inteiros positivos possui um menor elemento. Em outras palavras, todo subconjunto $S \subseteq \mathbb{Z}$, com $S \neq \emptyset$, limitado inferiormente possui um elemento mínimo, ou seja, um elemento $a \in S$ tal que $a \leq x$, para todo $x \in S$ (isto é, a é um limite inferior de S).

Se $a \in \mathbb{Z}$ é um limite inferior de S, então todo elemento inteiro menor que a também é um limite inferior. Além disso, se S é limitado inferiormente, então o elemento mínimo do conjunto S é único.

Exemplo 5.2.2. *O mínimo do conjunto* $S = \{-6, -4, -2, 0, 3\}$ *é* -6*, o mínimo do conjunto* $S = \{2, 4, 6, \cdots\}$ *é* 2 *e o o conjunto* $S = \{1, \frac{1}{2}, \frac{1}{3}, \cdots\}$ *é limitado inferiormente e não possui elemento mínimo.*

5.2.1 Exercícios

1. Determine o menor inteiro do conjunto $A = \{\pm 1, \pm 10, \pm 2\}$.
2. Determine o menor inteiro do conjunto $A = \{0, 1, -1, -3\}$.
3. Determine o menor inteiro do conjunto $A = \{\frac{1}{1/n} : n \in \mathbb{N}\}$.

5.3 Indução matemática

Usando o princípio do menor inteiro, segue os resultados sobre indução matemática.

Teorema 5.3.1. *(Primeiro Princípio de Indução) Sejam* $a \in \mathbb{Z}$ *e* $P(n)$ *uma sentença associada a cada* $n \geq a$*, com* $n \in \mathbb{Z}$*. Se*

1. $P(a)$ *é verdadeira, e*
2. *Se* $P(k)$ *é verdadeira, com* $k \geq a$*, então* $P(k+1)$ *é verdadeira,*

então $P(n)$ *é verdadeira para todo* $n \geq a$*.*

Demonstração. Seja o conjunto $S = \{n \geq a : P(n) \text{ é falsa}\}$. Suponhamos que $S \neq \emptyset$. Como S é limitado inferiormente, segue que S possui um elemento mínimo s. Neste caso, $s \geq a$, $P(s)$ é falsa e $s - 1 \notin S$. Assim, $P(s-1)$ é verdadeira. Por (2), segue que $P(s)$ é verdadeira, o que é uma contradição. Portanto, $S = \emptyset$, ou seja, $P(n)$ é verdadeira para todo $n \geq a$. □

Exemplo 5.3.1. *Mostre que* $2^n > n$ *para todo* $n \geq 0$*. De fato, se* $n = 1$*, então* $2^0 = 1 > 0$*. Por hipótese de indução, suponhamos que* $P(k)$*, com* $k \geq 0$*, é verdadeiro, ou seja,* $2^k > k$*. Agora, vamos mostrar que* $P(k+1)$ *é verdadeiro. Como* $2^k > k$*, segue que* $2.2^k > 2k$*, ou seja,* $2^{k+1} > 2k$*. Como* $k < 2^k$*, segue que* $k + 1 \leq 2^k$*. Assim,* $k + 1 \leq 2^k < 2.2^k = 2^{k+1}$*. Portanto,* $2^n > n$ *para todo* $n > 0$*.*

Teorema 5.3.2. *(Segundo Princípio de Indução) Sejam $a \in \mathbb{Z}$ e $P(n)$ uma sentença associada a cada $n \geq a$, com $n \in \mathbb{Z}$. Se*

1. *$P(a)$ é verdadeira, e*
2. *$P(k)$ é verdadeira para todo k tal que $a \leq k < n$,*

então $P(n)$ é verdadeira para todo $n \geq a$.

Demonstração. Seja o conjunto $S = \{n \geq a : P(n) \text{ é falsa}\}$. Suponhamos que $S \neq \emptyset$. Como S é limitado inferiormente, segue que S possui um elemento mínimo s. Neste caso, $s \geq a$, $P(s)$ é falsa e $s - 1 \notin S$. Assim, $P(s-1)$ é verdadeira. Por (2), segue que $P(s)$ é verdadeira, o que é uma contradição. Portanto, $S = \emptyset$, ou seja, $P(n)$ é verdadeira para todo $n \geq a$. □

5.3.1 Exercícios

1. Mostre por indução que $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$, para todo $n \geq 1$.
2. Mostre por indução que $1.2 + 2.3 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$, para todo $n \geq 1$.
3. Mostre por indução que $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$, para todo $n \geq 1$.
4. Mostre por indução que $\frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$, para todo $n \in \mathbb{N}$.
5. Mostre por indução que $1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$, para todo $n \in \mathbb{N}$.
6. Mostre por indução que $1^3 + 2^3 + 3^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$, para todo $n \in \mathbb{N}$.
7. Mostre por indução que $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$, para todo $n \geq 1$.
8. Mostre por indução que $1 + 3 + 5 + \ldots + (2n-3) + (2n-1) = n^2$, para todo $n \geq 1$.
9. Mostre por indução que $1 + a + a^2 + a^3 + \ldots + a^{n-1} + a^n = \frac{a^{n+1}-1}{a-1}$, para todo $n \geq 0$ e $a \in \mathbb{R}$ com $a \neq 1$.
10. Mostre por indução que $2^n > n^2$, para todo $n \geq 5$.
11. Mostre por indução que $2^{n+1} \geq n + 2$, para todo $n \geq -1$.
12. Mostre por indução que $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2$.
13. Mostre por indução que $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$, para todo $a \geq 1$ e para todo $n \geq 1$.

5.4 Divisibilidade

Seja $a \in \mathbb{Z}$. O conjunto $S = \{0, \pm a, \pm 2a, \cdots\}$ é chamado conjunto dos múltiplos de a.

Definição 5.4.1. *Sejam $a, b \in \mathbb{Z}$. O elemento a é dito que divide b se existe $c \in \mathbb{Z}$ tal que $b = ac$, ou seja, b é um múltiplo de a. Neste caso, a notação usada é $a \mid b$, e se a não divide b, usamos a notação $a \nmid b$.*

Exemplo 5.4.1. $5 \mid 15$, *pois* $15 = 3.5$ *e* $0 \mid 0$, *uma vez que* $0 = 0.k$ *para todo* $k \in \mathbb{Z}$.

Propriedades 5.4.1. *Sejam $a, b, c \in \mathbb{Z}$.*

1. $a \mid 0$, *uma vez que* $0 = a0$.
2. $a \mid a$, *uma vez que* $a = a.1$, *chamada propriedade reflexiva.*
3. *Se $a \mid b$ e $b \mid c$, então $a \mid c$, pois existem $c_1, c_2 \in \mathbb{Z}$ tal que $b = ac_1$ e $c = bc_2$. Assim, $c = bc_2 = a(c_1c_2)$, ou seja, $a \mid c$. Essa propriedade é chamada propriedade transitiva. s*
4. *Se $a \mid b$, então $a \mid bx$, para todo $x \in \mathbb{Z}$. De fato, existe $c_1 \in \mathbb{Z}$ tal que $b = ac_1$. Assim, $bx = a(c_1x)$, para todo $x \in \mathbb{Z}$. Portanto, $a \mid bx$, para todo $x \in \mathbb{Z}$.*
5. *Se $a \mid b$ e $a \mid c$, então $a \mid (bx + by)$, para todo $x, y \in \mathbb{Z}$. De fato, existem $c_1, c_2 \in \mathbb{Z}$ tal que $b = ac_1$ e $c = ac_2$. Assim, $bx = a(c_1x)$ e $cy = a(c_2y)$ para todo $x, y \in \mathbb{Z}$. Logo, $bx + cy = a(c_1x + c_2y)$, e portanto, $a \mid (bx + cy)$.*
6. *Se $a \mid b$ e $b \mid a$, então $a = \pm b$. De fato, por hipórese, existem $c_1, c_2 \in \mathbb{Z}$ tal que $b = ac_1$ e $a = bc_2$. Assim, $a = bc_2 = a(c_1c_2$, ou seja, $a \mid a$ e $c_1c_2 = \pm 1$. Portanto, $c_1 = c_2 = \pm 1$, e portanto, $a = \pm b$.*
7. *Se $a \mid b$ e $a \mid c$, então $a \mid (b \pm c)$. De fato, por hipórese, existem $c_1, c_2 \in \mathbb{Z}$ tal que $b = ac_1$ e $c = ac_2$. Assim, $b \pm c = a(c_1 \pm c_2)$, ou seja, $a \mid (b \pm c)$.*

O algoritmo da divisão é também chamado algoritmo euclidiano em homenagem a Euclides.

Teorema 5.4.1. *(Algoritmo Euclidiano ou da Divisão) Se $a, b \in \mathbb{Z}$, com $b > 0$, então existem e são únicos $q, r \in \mathbb{Z}$ tal que $a = bq + r$, com $0 \leq r < b$.*

Demonstração. Seja $S = \{a - bx : x \in \mathbb{Z} \text{ e } a - bx \geq 0\}$. O conjunto $\neq \emptyset$, pois $b \geq 1$ e tomando $x = - \mid a \mid$, segue que $a - bx = a + b \mid a \mid \geq a + \mid a \mid \geq 0$. Pelo Princípio do Menor Inteiro, segue que existe $r \in S$, mínimo, tal que $r \geq 0$ e $r = a - bq$, com $q \in \mathbb{Z}$. Assim, $a = bq + r$, com $q, r \in \mathbb{Z}$. Além disso, $r < b$, pois se $r \geq b$, então $0 \leq r - b = a - bq - b = a - b(q + 1) < r$. Assim, r não é o mínimo de S. Portanto, $0 \leq r < b$. Para a unicidade, suponhamos que existam $q_1, r_1 \in \mathbb{Z}$ tal que $a = bq_1 + r_1$ com $0 \leq r_1 < b$. Assim, $bq + r = bq_1 + r_1$, ou seja, $b(q - q_1) = r_1 - r$. Portanto, $b \mid r_1 - r$. Como $-b < -r \leq 0$ e $0 \leq r_1 < b$, segue que $-b < r_1 - r < b$, ou seja, $\mid r_1 - r \mid < b$. Como $b \mid r_1 - r$ e $\mid r_1 - r \mid < b$, segue que $r_1 - r = 0$, ou seja, $r_1 = r$. Finalmente, como $r_1 = r$, segue que $bq = bq_1$. Como $b \neq 0$, segue que $q = q_1$. □

Corolário 5.4.1. *Se $a, b \in \mathbb{Z}$, com $b \neq 0$, então existem e são únicos $q, r \in \mathbb{Z}$ tal que $a = bq + r$, com $0 \leq r <\mid b \mid$.*

Demonstração. Se $b > 0$, o resultado segue do Teorema 5.4.1. Se $b < 0$, então $\mid b \mid > 0$. Pelo Teorema 5.4.1, segue que existem $q_1, r \in \mathbb{Z}$ únicos tal que $a =\mid b \mid q_1 + r$, com $0 \leq r <\mid b \mid$. Como $\mid b \mid = -b$, segue que $a = b(-q_1) + r$, com $0 \leq r <\mid b \mid$. Portanto, existem $q = -q_1, r \in \mathbb{Z}$ únicos tal que $a = bq + r$ com $0 \leq r <\mid b \mid$. □

Definição 5.4.2. *O inteiros q e r são chamados, respectivamente, quociente e resto da divisão de a por b.*

5.4.1 Máximo divisor comum e mínimo múltiplo comum

Seja $a \in \mathbb{Z}$. O conjunto dos divisores de a será denotado por $D(a)$. Intuitivamente, o máximo divisor comum de $a, b \in \mathbb{Z}$ é o maior elemento de $D(a) \cap D(b)$.

Proposição 5.4.1. *Se $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$, então existe um único $d \in \mathbb{Z}$ tal que $d > 0$, $d \in D(a) \cap D(b)$ e é o maior inteiro positivo com essa propriedade.*

Demonstração. Seja $S = \{ax + by : x, y \in \mathbb{Z}\}$. Tomando $x = a$ e $y = b$, segue que $a^2 + b^2 > 0$, ou seja, S possui números estritamente positivos. Pelo Princípio do Menor Inteiro, segue que existe $d \in S$ um elemento mínimo. Assim, $d = ax_0 + by_0 > 0$, com $x_0, y_0 \in \mathbb{Z}$. Pelo algoritmo da divisão, segue que existem $q, r \in \mathbb{Z}$ tal que $a = dq + r$ com $0 \leq r < d$. Assim, $r = a - dq = a - (ax_0 + by_0)q = a(1 - qx_0) + b(-qy_0) \in S$. Como $0 \leq r < d$ e d é o mínimo de S, segue que $r = 0$. Portanto, $a = dq$, ou seja, $d \mid a$. De modo análogo, segue que $d \mid b$. Agora, se $d' \mid a$ e $d' \mid b$, segue que $d' \mid (ax_0 + by_0)$, ou seja, $d' \mid d$. Portanto, existe único $d > 0$, onde $d \in D(a) \cap D(b)$ e é o maior com essa propriedade. □

Definição 5.4.3. *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$. Um número $d \in \mathbb{Z}$ é chamado máximo divisor comum de a e b se:*

1. *$d > 0$.*
2. *$d \mid a$ e $d \mid b$.*
3. *Se existe $d' \in \mathbb{Z}$ tal que $d' \mid a$ e $d' \mid b$, então $d' \mid d$.*

A notação usada é $d = mdc(a, b)$.

Exemplo 5.4.2. *Se $0, -2, 4 \in \mathbb{Z}$, então $mdc(4, 0) = 4$ e $mdc(-2, 4) = 2$.*

Além disso, se $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$, então $mdc(a, b) = mdc(\mid a \mid, \mid b \mid) = mdc(b, a) = mdc(\mid a \mid, b) = mdc(a, \mid b \mid)$.

Teorema 5.4.2. *(Identidade de Bezout) Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. Se $d = mdc(a, b)$, então existem $x_0, y_0 \in \mathbb{Z}$ tal que $d = ax_0 + by_0$.*

Demonstração. Pela Proposição 5.4.1, segue que existem $x_0, y_0 \in \mathbb{Z}$ tal que $ax_0 + by_0 = mdc(a, b)$. Portanto, $d = ax_0 + by_0$, para algum $x_0, y_0 \in \mathbb{Z}$. □

Definição 5.4.4. *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$. Um número $m \in \mathbb{Z}$ é chamado mínimo múltiplo comum de a e b se:*

1. *$m > 0$.*
2. *$a \mid m$ e $b \mid m$.*
3. *Se existe $m' \in \mathbb{Z}$ tal que $a \mid m'$ e $b \mid m'$, então $m \mid m'$.*

A notação usada é $m = mmc(a, b)$.

Se $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$, então

$$mmc(a, b) = mmc(\mid a \mid, \mid b \mid) = mmc(b, a) = mmc(\mid a \mid, b) = mmc(a, \mid b \mid).$$

Exemplo 5.4.3. *Se $0, -2, 4 \in \mathbb{Z}$, então $mmc(4, 0) = 4$ e $mmc(-2, 4) = 4$.*

5.4.2 Processo prático para encontrar o máximo divisor comum

O algoritmo euclidiano, como o próprio nome diz, foi descrito por Euclides nas proposições 1 e 2 do Livro 7 dos *Elementos*, mas acredita-se que sua origem seja muito anterior a Euclides. Dados a e b inteiros positivos e que $a \geq b$, o algoritmo de Euclides tem a finalidade de encontrar o máximo divisor comum entre a e b. Assim, dividindo a por b, encontramos o resto r_1. Se $r_1 \neq 0$, dividimos b por r_1, obtendo o resto r_2. Se $r_2 \neq 0$, dividimos r_1 por r_2, obtendo o resto r_3, e assim, por diante. O último resto diferente de zero desta sequência de divisões é o máximo divisor comum entre a e b. O algoritmo de Euclides também é usado para achar a expressão do $mdc(a, b)$ como combinação linear de a e b. Neste caso, faz-se uma tabela para se calcular o máximo divisor comum entre dois números.

Exemplo 5.4.4. *Cálculo do $mdc(963, 657)$ pelo algoritmo de Euclides e a sua expressão como combinação linear de 963 e 657. Neste caso, $963 = 657.1 + 306$; $657 = 306.2 + 45$; $306 = 45.6 + 36$; $45 = 36.1 + 9$ e $36 = 9.4 + 0$. Assim,*

	1	2	6	1	4
963	657	306	45	36	9
306	45	36	9	0	

Portanto, $mdc(963, 657) = 9$ e a sua expressão como combinação linear de 963 e 657 se obtém eliminando os restos $36, 45$ e 306 entre as quatro primeiras igualdades do seguinte modo: $9 = 45 - 36 = 45 - (306 - 45.6) = -306 + 7.45 = -306 + 7.(657 - 306.2) = 7.657 - 15.306 = 7.657 - 15.(963 - 657) = 963.(-15) + 657.22$, ou seja, $9 = mdc(963, 657) = 963x_0 + 657y_0$, onde $x_0 = -15$ e $y_0 = 22$.

Esta representação do inteiro $9 = mdc(963, 657)$ como combinação linear de 963 e 657 não é unica, pois somando e subtraindo o produto 963.657 ao segundo membro da igualdade $9 = 963.(-15) + 657.22$, segue que $9 = 963(-15 + 657) + 657(22 - 963) = 963.642 + 657(-941)$, ou seja, é uma outra representação do inteiro $9 = mdc(963, 657)$ como combinação linear de 963 e 657. Um outro exemplo um pouco diferente pode ser o seguinte.

Exemplo 5.4.5. *O máximo divisor comum de dois inteiros positivos a e b é 74 e na sua determinação pelo algoritmo de Euclides os quocientes obtidos foram $1, 2, 2, 5, 1$ e 3. Assim, os inteiros positivos a e b, são obtidos pela seguinte tabela*

	1	2	2	5	1	3
a	b	r	r_1	r_2	r_3	74
r	r_1	r_2	r_3	74	0	

Assim, $a = b+r$, $b = 2r+r_1$, $r = 2r_1+r_2$, $r_1 = 5r_2+r_3$, $r_2 = r_3+74$ e $r_3 = 74.3 = 222$. Portanto, $r_2 = 222+74 = 296$, $r_1 = 5.296+222 = 1702$, $r = 2.1702+296 = 3700$, $b = 2.3700+1702 = 9102$ e $a = 9102 + 3700 = 12802$.

Agora, perguntamos, porquê o resultado destas divisões é o máximo divisor comum? Outra dúvida, precisamos verificar que a sequência de divisões chega sempre a um resto zero, ou o algoritmo continuaria para sempre. Começamos tratando da segunda questão. Assim, vamos verificar onde o algoritmo pára. Digamos que, para calcular o máximo divisor comum entre dois inteiros a e b, com $b \geq 0$, fazemos uma sequência de divisões como: $a = bq_1 + r_1$, onde $0 \leq r_1 < b$; $b = r_1q_2 + r_2$, onde $0 \leq r_2 < r_1$; $r_1 = r_2q_3 + r_3$ onde $0 \leq r_3 < r_2$; $r_2 = r_3q_4 + r_4$, onde $0 \leq r_4 < r_3 < \cdots$. Esquecendo por um instante o que está acontecendo no primeiro membro das igualdades, no segundo membro das igualdades tem-se uma sequência de restos, e observamos que o seguinte é sempre menor que o anterior, mas todos são maiores ou iguais a zero. Seja a sequência das desigualdades dos restos

$$b > r_1 > r_2 > r_3 > r_4 > \cdots \geq 0. \tag{5.1}$$

Como entre b e 0 existe apenas uma quantidade finita de inteiros, segue que esta sequência não pode continuar indefinidamente. Mas ela só chega ao final se um dos restos for zero, e é isto que garante que o algoritmo sempre pára. Agora, falta verificar que o último resto não nulo coincide com o máximo divisor comum. Para entendermos isto, precisamos de um resultado auxiliar que é dado pelo seguinte lema.

Lema 5.4.1. *Sejam a e b números inteiros positivos. Se existem inteiros q e r tal que $a = bq+r$, então $mdc(a, b) = mdc(b, r)$.*

Demonstração. Suponhamos que $d_1 = mdc(a, b)$ e $d_2 = mdc(b, r)$, e mostremos que $d_1 = d_2$. Para isso, o raciocínio usado será de mostrar que $d_1 \leq d_2$ e $d_2 \leq d_1$. Provamos que $d_1 \leq d_2$ pois a outra desigualdade é verificada de maneira análoga. Como $d_1 = mdc(a, b)$, segue que d_1 divide a e b. Assim, existem inteiros q_1 e q_2 tal que $a = d_1q_1$ e $b = d_1q_2$. Por hipótese, $a = bq+r$, e assim, $d_1q_1 = d_1q_2q + r$, ou seja, $r = d_1q_1 - d_1q_2q = d_1(q_1 - q_2q)$. Deste modo, d_1 divide

r, e portanto, $d_1 = mdc(b, r)$. Mas, como $d_2 = mdc(b, r)$, segue que $d_1 \leq d_2$. Analogamente, $d_2 \leq d_1$. Portanto, $d_1 = d_2$. □

Finalmente, agora vamos usar o Lema 5.4.1 para justificar que o último resto não nulo da sequência de divisões é o máximo divisor comum. De fato, sejam a e b dois inteiros com $a \geq b$ e $b \neq 0$. Aplicando o algoritmo de Euclides para a e b e supondo que o resto nulo ocorre após n divisões, segue que $a = bq_1 + r_1$, onde $0 \leq r_1 < b$; $b = r_1q_2 + r_2$, onde $0 \leq r_2 < r_1$; $r_1 = r_2q_3 + r_3$, onde $0 \leq r_3 < r_2$; $r_2 = r_3q_4 + r_4$, onde $0 \leq r_4 < r_3$; $\cdots$; $r_{n-4} = r_{n-3}q_{n-2} + r_{n-2}$, onde $0 \leq r_{n-2} < r_{n-3}$; $r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}$, onde $0 \leq r_{n-1} < r_{n-2}$ e $r_{n-2} = r_{n-1}q_n$, onde $r_n = 0$. Agora, da última divisão, segue que r_{n-1} divide r_{n-2}. Logo, o maior divisor comum entre r_{n-1} e r_{n-2} é r_{n-1}. Portanto, $mdc(r_{n-2}, r_{n-1}) = r_{n-1}$. Pelo Lema 5.4.1, na penúltima divisão, segue que $mdc(r_{n-3}, r_{n-2}) = mdc(r_{n-2}, r_{n-1} =)r_{n-1}$. Novamente aplicando o Lema 5.4.1 na ante-penúltima divisão, segue que $mdc(r_{n-4}, r_{n-3}) = mdc(r_{n-3}, r_{n-2}) = r_{n-1}$. Fazendo este mesmo processo na igualdade anterior, segue que $mdc(a, b) = r_{n-1}$, que é o que queriamos provar.

5.4.3 Exercícios

1. Defina $mdc(a_1, a_2, \ldots, a_n)$ e $mmc(a_1, a_2, \ldots, a_n)$, onde $a_1, \cdots, a_n \in \mathbb{Z}$ são não nulos.
2. Mostre que $mdc(a, b, c) = mdc(a, mdc(b, c))$ e $mmc(a, b, c) = mmc(a, mmc(b, c))$, onde $a, b, c \in \mathbb{Z}$.
3. Mostre por indução que $80 \mid 3^{4n} - 1$, para todo $n \in \mathbb{N}$.
4. Mostre por indução que $9 \mid 4^n + 6n - 1$, para todo $n \in \mathbb{N}$.
5. Mostre por indução que $8 \mid 3^{2n} + 7$, para todo $n \in \mathbb{N}$.
6. Mostre por indução que 9 divide $n4^{n+1} - (n + 1)4^n + 1$, para todo $n \in \mathbb{N}$.
7. Mostre por indução que $8 \mid 3^{2n} - 1$, para todo $n \geq 0$.
8. Mostre por indução que $7 \mid n^7 - n$, para todo $n \geq 1$.
9. Mostre por indução que $3^{2n+1} + 2^{m+2}$ é divisível por 7, para todo $n \in \mathbb{N}$.
10. Mostre por indução que $2^{2n} + 15n - 1$ é divisível por 9, para todo $n \geq 0$.
11. Seja 7 o resto da divisão de um inteiro n por 12. Determine:
    (a) O resto da divisão de $2n$ por 12.
    (b) O resto da divisão de n por 4.
    (c) O resto da divisão de n por 8.
12. Mostre que n ou $n + 2$ ou $n + 4$ é divisível por 3.
13. Se n é impar, mostre que 8 divide $n^2 - 1$.

14. Se m e n são números impares, mostre que 8 divide $m^2 - n^2$.

15. Se $d = mdc(m, n)$, onde $m, n \in \mathbb{N}$, mostre que $mdc(m/d, n/d) = 1$.

5.5 Números primos

Nesta seção, apresentamos o conceito de número primo e veremos um importante resultado que os envolvem chamado Teorema Fundamental da Aritmética que é indispensável para os estudos que seguirá.

O estudo de métodos para determinar se um nuúmero é primo ocupou matemáticos como Fermat e Euler. Seja $a \in \mathbb{Z}$ com $a \neq 0$ e $a \neq \pm 1$. O número a tem pelo menos quatro divisores, ou seja, $\{1, -1, a, -a\} \subseteq D(a)$. Estes divisores são chamados divisores triviais de a.

Definição 5.5.1. *Um número $p \in \mathbb{Z}$, onde $p \neq 0$ e $p \neq \pm 1$, é chamado um número primo se os únicos divisores p são os divisores triviais. Um número $a \in \mathbb{Z}$, onde $a \neq 0$ e $a \neq \pm 1$, é chamado composto se não é um número primo, ou seja, se adimite outros divisores aém dos triviais.*

Em geral, usamos simplesmente os termos primos ou compostos. Por exemplo, os números $2, 3, 5$ e 7 são primos e os números $4, 6$ e 8 são compostos.

Exemplo 5.5.1. *Considerando o número 19 o conjunto $D(19) = \{\pm 1, \pm 19\}$ e, portanto, é primo. Para o número 20, segue que $D(20) = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20\}$, e assim, 20 é composto.*

Definição 5.5.2. *Dois números $a, b \in \mathbb{Z}$ são chamados relativamente primos (ou primos entre si) se $mdc(a, b) = 1$.*

Proposição 5.5.1. *Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid bc$ e se $mdc(a, b) = 1$, então $a \mid c$.*

Demonstração. Pela identidade de Bezout, segue que existem $x_0, y_0 \in \mathbb{Z}$ tal que $1 = ax_0 + by_0$. Multiplicando por c, segue que $c = a(cx_0) + (bc)y_0$. Portanto, $a \mid c$. □

Lema 5.5.1. *(Lema de Euclides) Se $p \in \mathbb{Z}$ é um número primo e $p \mid ab$, com $a, b \in \mathbb{Z}$, então $p \mid a$ ou $p \mid b$.*

Demonstração. Se $p \nmid a$, então $mdc(a, p) = 1$. Pelo Teorema 5.4.2, segue que existem $x_0, y_0 \in \mathbb{Z}$ tal que $1 = ax_0 + py_0$. Multiplicando por b em ambos os lados, segue que $b = (ab)x_0 + p(by_0)$. Como $p \mid ab$ e $p \mid p$, segue que $p \mid b$. □

Lema 5.5.2. *Se $a \in \mathbb{Z}$ e $a \geq 2$, então a admite um divisor primo p, onde $p > 0$.*

Demonstração. A demonstração é feita através do segundo princípio de indução com $a > 0$. Para $a = 2$ é suficiente tomar $p = 2$, uma vez que $2 \mid 2$. Agora, suponha que todo m tal que $2 \leq m < a$ tem um divisor primo. Temos que provar que a tem um divisor primo. Se a for primo, então $a \mid a$, e o resultado segue. Se a for composto, então a tem um divisor não trivial

$m > 1$. Assim, $a = mq$, para algum $q \in \mathbb{Z}$. Logo, $2 \leq m < a$. Por hipótese de indução, segue que existe um número primo p tal que $m = pq_1$, para algum $q_1 \in \mathbb{Z}$. Portanto, $a = pqq_1$, ou seja, a tem um fator primo p. Logo, $p \mid a$. Finalmente, se $a < 0$, segue que $-a > 0$, e o resultado segue de modo análogo. □

Teorema 5.5.1. *(Teorema Fundamental da Aritmética) Se $a \in \mathbb{Z}$, com $a \neq 0$ e $a \neq \pm 1$, então a é decomposto de modo único como o produto de números primos, ou seja, existem $p_1, p_2, \cdots, p_r$ primos tal que $a = \pm p_1 p_2 \cdots p_r$ e que a menos da ordem dos fatores a decomposição é única.*

Demonstração. A demonstração é feita através do segundo princípio de indução com $a > 0$. Se $a = 2$, como 2 é primo, o resultado segue. Suponhamos que $a > 2$ e que o resultado é verdadeiro para todo m tal que $2 \leq m < a$. Pelo Lema 5.5.2, segue que a admite um fator primo p_1, ou seja, $a = p_1 m$, para algum $m \in \mathbb{Z}$. Assim, se $m = 1$ ou m é primo, o resultado segue. Caso contrário, como $2 \leq m < a$, segue por hipótese de indução que existem $r - 1$ primos $p_2, p_3, \cdots, p_r$, com $r - 1 \geq 1$, tal que $m = p_2 p_3 \cdots p_r$. Portanto, $a = p_1 p_2 \cdots p_r$. Para a unicidade, se $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ são duas fatorações de a, então $p_1 \mid q_1 q_2 \cdots q_s$. Como p_1 é primo, pelo Lema 5.5.1 segue que $p_1 \mid q_j$, para algum $j = 1, 2, \cdots, s$. Sem perda de generalidade, suponhamos que $j = 1$. Assim, $q_1 = p_1$, e desse modo, cancelando p_1 segue que $p_2 \cdots p_r = q_2 q_3 \cdots q_s$. Repetindo esse procedimento o quanto for necessário, segue que $r = s$ e $p_i = q_i$ para todo $i = 1, 2, \cdots, r$. Finalmente, se $a < 0$, segue que $-a > 0$, e o resultado segue de modo análogo. □

Na decomposição $a = p_1 p_2 \cdots p_r$, segundo o Teorema 5.5.1, em geral, os fatores não são distintos. Assim, reunindo os fatores primos iguais, segue que $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, onde $1 \leq s \leq r$, $p_i \neq p_j$ sempre que $i \neq j$ e $\alpha_i \geq 1$ para todo $i = 1, 2, \cdots, s$. Além disso, muitas vezes é conveniente na fatoração de dois números tomar potências nulas para que a fatoração possua potências dos mesmos primos. Finalmente, se m é um divisor de $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, então $m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$, onde $0 \leq \beta_i \leq \alpha_i$ para todo $i = 1, 2, \cdots, s$. Além disso, $mdc(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}$, onde $\gamma_i = \min\{\alpha_i, \beta_i\}$, para $i = 1, 2, \cdots, s$ e $mmc(a, b) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_s^{\delta_s}$, onde $\delta_i = \max\{\alpha_i, \beta_i\}$, para $i = 1, 2, \cdots, s$. Desse modo, para fatorarmos um número a é preciso que dividamos n pelo menor primo divisor. O quociente q_1 deve ser dividido pelo menor primo divisor de q_1, e assim, por diante, até que q_n seja 1. Feito isso, todos os primos que foram divisores no processo dado acima, quando multiplicados, terão a como produto, ou seja, eles são os fatores de a.

Exemplo 5.5.2. *O número* 315 *possui a seguinte fatoração:* $3^2 \times 5 \times 7$.

Proposição 5.5.2. *Se $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ e $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$, então $b \mid a$ se, e somente se, $0 \leq \beta_i \leq \alpha_i$, para todo $i = 1, 2, \cdots, n$.*

Demonstração. Se $b \mid a$, então existe $q \in \mathbb{Z}$ tal que $a = bq$, ou seja, $p_1^{\alpha_1} \cdots p_n^{\alpha_n} = p_1^{\beta_1} \cdots p_n^{\beta_n} q$. Assim, $p_1^{\alpha_1 - \beta_1} \cdots p_n^{\alpha_n - \beta_n} = q$. Como $q \in \mathbb{Z}$, segue que $0 \leq \beta_1 \leq \beta_i$, para todo $i = 1, 2, \cdots, n$. Reciprocamente, se $0 \leq \beta_i \leq \alpha_i$, então $\beta_i = \alpha_i + x_i$, com x_i um inteiro positivo, para todo $i = 1, 2, \cdots, n$. Assim, $p_i^{\alpha_i} = p_i^{\beta_i + x_i} = p_i^{\beta_i} p_i^{x_i}$, ou seja, $p_i^{\beta_i}$ divide $p_i^{\alpha_i}$, para $i = 1, 2, \cdots, n$. Portanto, $b \mid a$. □

Exemplo 5.5.3. *As decomposições canônica dos números* $a = 42336$ *e* $b = 1270080$ *são dadas por* $a = 42336 = 2^5.3^3.7^2$ *e* $b = 1270080 = 2^6.3^4.5.7^2$. *O número* b *possui um fator* 2 *e um fator* 3 *a mais do que o número* a *e possui um fator* 5 *não presente em* a. *Multiplicando esses três fatores, obtemos o número* 30, *que é a divisão de* 1270080 *por* 42336.

Exemplo 5.5.4. *O número* $b = 17640$ *divide* $a = 13852800$, *uma vez que* $b = 17640 = 2^3.3^2.5.7^2$ *e* $a = 13582800 = 2^4.3^2.5^2.7^3.11$.

É possível descobrir quantos divisores positivos tem um número a partir da sua fatoração, ou seja, o número de divisores de $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ é dado por $D(a) = (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_n+1)$.

Exemplo 5.5.5. *O número de divisores* 1500 *é dado por* $D(1500) = (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_n+1) = (2+1)(1+1)(3+1) = 3.2.4 = 24$, *onde* $1500 = 2^2.3^1.5^3$. *Portanto, o número* 1500 *possui* 24 *divisores.*

Teorema 5.5.2. *Se Se* $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ *e* $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$ *e* $\gamma_i = min\{\alpha_i, \beta_i\}$, *para* $i = 1, 2, \cdots, n$, *então* $mdc(a, b) = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$.

Demonstração. Seja $d = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$. Como $\gamma_i = min\{\alpha_i, \beta_i\}$, para $i = 1, 2, \cdots, n$, segue que $\gamma_i \leq \alpha_i$ e $\gamma_i \leq \beta_i$. Pela Proposição 5.5.2, segue que $d \mid a$ e $d \mid b$. Agora, se d' é um divisor comum de a e b, então $d' = p_1^{\delta_1} \cdots p_n^{\delta_n}$, onde $\delta_i \leq \gamma_i$, para $i = 1, 2, \cdots, n$. Pela Proposição 5.5.2, segue que $d^{|'} \mid d$. Portanto, $d = mdc(a, b)$. □

Exemplo 5.5.6. *O máximo divisor* $a = 3896200 = 2^3.5^2.7.11^2.23$ *e* $b = 592480 = 2^5.5.7.23^2$ *é dado por* $d = mdc(a, b) = 2^3.5^1.7^1.11^0.23^1 = 6440$.

De modo análogo segue que o $m = mmc(a, b)$, onde $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ e $b = p_1^{\beta_1} \cdots p_n^{\beta_n}$ é dado por $m = p_1^{\gamma_1} \cdots p_n^{\gamma_n}$, onde $\gamma_i = max\{\alpha_i, \beta_i\}$, para todo $i = 1, 2, \cdots, n$.

Corolário 5.5.1. *Se* $a, b \in \mathbb{Z}$ *são ambos não nulo e diferente de* ± 1, *então* a/d *e* b/d *são primos entre si, onde* d *é um máximo divisor comum de* a *e* b.

Demonstração. Se $p_i^{\alpha_i}$ é um fator de a e $p_i^{\beta_i}$ é um fator de b, então $p_i^{\gamma_i}$ é um fator de d, onde $\gamma_i = \min\{\alpha_i, \beta_i\}$. Além disso, $p_i^{\alpha_i - \gamma_i}$ é um fator de a/d e $p_i^{\beta_i - \gamma_i}$ é um fator de b/d. Assim, $\alpha_i - \gamma_i = 0$ ou $\beta_i - \gamma_i = 0$, e portanto, $min\{\alpha_i - \gamma_i, \beta_i - \gamma_i\} = 0$. Como esse mínimo é o expoente de p_i em a/d e b/d, segue que não existem fatores comuns primos em a/d e em b/d. □

Teorema 5.5.3. *O conjunto de números primos é infinito.*

Demonstração. Suponhamos que o conjunto de números primos seja finito. Logo, existe p_n tal que p_n é o maior de todos os demais $p_1, p_2, \cdots, p_{n-1}$. Consideremos o inteiro $m > 1$ tal que:

$$m = p_1 p_2 \cdots p_n + 1.$$

Pelo Teorema Fundamental da Aritmética, segue que m admite pelo menos um divisor primo p. Mas, como $p_1, p_2, \cdots, p_n$ é conjunto de todos os primos, segue que $p = p_i$, para algum

$i = 1, 2, \cdots, n$. Assim, $p \mid m$ e $p \mid p_1 p_2 \cdots p_n$. Logo, $p \mid 1$, pois $1 = m - p_1 p_2 \cdots p_n$, o que é um absurdo. Portanto, o conjunto de primos é infinito. □

Teorema 5.5.4. *(Fermat) Se um inteiro $n > 1$ é composto, então n possui um divisor primo p tal que $p \leq \sqrt{n}$.*

Demonstração. Seja $n = ab$, com $1 < a \leq b < n$. Se $a < b$, então

$$n = ab \geq a^2$$

, ou seja, $a \leq \sqrt{n}$. Como $b > 1$, segue que b possui pelo menos um divisor primo p. Agora, como $p \mid a$, segue que $p^2 \mid a^2$, e assim, $p^2 \leq a^2$. Como $p \mid a$ e $a \mid n$, segue que $p \mid n$, ou seja, $p \leq \sqrt{n}$. □

Exemplo 5.5.7. *O número* 211 *é um número primo. Como* $\sqrt{211} \approx 15$*, segue que para sabermos se é composto é suficiente verificarmos se existe um inteiro entre* 2 *e* $\sqrt{211}$ *(inclusive) que divida* 211*. Sabendo que não existe esse divisor, segue pelo Teorema 5.5.4, segue que* 211 *é um número primo.*

Exemplo 5.5.8. *O método chamado Crivo de Eratóstenes é utilizado para determinar os números primos de* 1 *até um certo* n*. O método consiste em eliminar os múltiplos dos primos que são menores que* $\sqrt{n}$*. Por exemplo, encontremos os números primos menores que* 50*. Como* $7 < \sqrt{50}$*, é suficiente eliminar os múltiplos de* $2, 3, 5$ *e* 7*. Dessa forma,*

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~.

Assim, o números primos menores que 50 *são* $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$ *e* 47*.*

Um número da forma $F_k = 2^{2^k} + 1$ é chamado número de Fermat. Fermat observou que $F_0 = 2^{2^0} + 1 = 3$, $F_1 = 2^{2^1} + 1 = 5$, $F_2 = 2^{2^2} + 1 = 17$, $F_3 = 2^{2^3} + 1 = 257$ e $F_4 = 2^{2^4} + 1 = 65537$ são números primos. Com isso, Fermat acabou conjecturando que todos os inteiros da forma $F_k = 2^{2^k} + 1$ são números primos. Mas, Euler descobriu que $F_5 = 2^{2^5} + 1$ não é um número primo, mostrando que 641 é um fator de F_5, ou seja,

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 2^{28}(5^4 + 2^4) - (5.2^7)^4 + 1 = 2^{28}.641 - (640^4 - 1) = 641(2^{28} - 639(640^2 + 1)).$$

Os númeos da forma $M_k = 2^k - 1$, para $k \geq 2$, são chamados de números de Mersene. Se M_k for primo, então k é primo, mas a reciproca é falsa, uma vez que $M_{11} = 2047 = 23.89$. Se M_k for primo, M_k é chamado primo de Mersene.

5.5.1 Exercícios

1. Se $p \in \mathbb{Z}$ é um número primo tal que $p \mid a_1 \dots a_n$, mostre que $p \mid a_i$ para algum $i = 1, 2, \dots, n$.
2. Mostre que $6 \mid n(2n+7)(7n+1)$, para todo $n \in \mathbb{Z}$.
3. Mostre que 30 divide $n(n^2-49)(n^2+49)$, para todo $n \in \mathbb{Z}$.
4. Se p é primo e $p \mid ab$, mostre que $p \mid a$ ou $p \mid b$.
5. Se $a^k - 1$ for primo, mostre que $a = 2$ e k é primo.
6. Determine os primos menores que 50.
7. Verifique que 271 é primo ou composto.
8. Se abc é o maior número de 3 algarismos divisível por 3, determine $a + b + c$.
9. Determine o números de elementos entre 1 e 1000 que é divisível por 9.
10. Determine a tau que $mdc(a, 384) = 48$, onde $a < 384$.
11. Se $n > 4$ é composto, mostre que n divide $(n-1)!$.
12. Se $p > 1$ e p divide $(p-1)! + 1$, mostre que p é primo.
13. Mostre que $n! + 1$ adimite um fator primo $p > n$, para todo n.
14. Se $n > 2$, mostre que existe um primo p entre n e $n!$.
15. Se $2^n - 1$, com $n \geq 2$, é primo, mostre que n é primo.

5.6 Equações diofantinas lineares

O estudo das equações diofantinas lineares se deve a Diofanto de Alexandria, que viveu provavelmente no século III d.C., que foi um matemático grego e é considerado um dos fundadores da álgebra, onde escreveu uma obra sobre Aritmética em 13 volumes e dos quais apenas seis foram preservados. Tal estudo está relacionado com as equações do tipo $ax+by = c$, cujos coeficientes são inteiros. O objetivo desse estudo é dar condições para saber se uma equação diofantina possui ou não solução, e, caso exista, encontrá-las.

Definição 5.6.1. *Sejam $a, b, c \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. A equação $ax + by = c$, onde x e y são variáveis, é chamada equação diofantina linear.*

Exemplo 5.6.1. *A equação $2x+3y = 1$ possui soluções como $x = -1$ e $y = 1$, e $x = 5$ e $y = -3$. A equação $2x + 4y = 3$ não possui solução inteira.*

Proposição 5.6.1. *A equação $ax + by = c$ admite solução $x_0, y_0 \in \mathbb{Z}$ se, e somente se, d divide c, onde $d = mdc(a, b)$.*

Demonstração. Se x_0, y_0 é uma solução, então $ax_0 + by_0 = c$. Como $d \mid a$ e $d \mid b$, segue que $d \mid c$. Reciprocamente, se $d = mdc(a, b)$, então $d = ax_0 + by_0$, para algum $x_0, y_0 \in \mathbb{Z}$. Como $d \mid c$, segue que $c = dq$, onde $q \in \mathbb{Z}$. Assim, $c = dq = (ax_0 + by_0qr = a(x_0q) + b(y_0q)$, ou seja, ($x_0q$ e y_0q é uma solução da equação $ax + by = c$. □

Exemplo 5.6.2. *A equação $3x + 6y = 18$ possui solução, uma vez que $mdc(3, 6) = 3 \mid 18$, mas a equação $2x + 4y = 7$ não admite solução pois $mdc(2, 4) = 2 \nmid 7$.*

Proposição 5.6.2. *Se $x_0, y_0 \in \mathbb{Z}$ é uma solução de $ax + by = c$, com $a \neq 0$ e $b \neq 0$, e $d = mdc(a, b)$, então a equação admite infinitas soluções e o conjunto dessas soluções é dada por $S = \{(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t) : t \in \mathbb{Z}\}$.*

Demonstração. Se $x_1, y_1 \in \mathbb{Z}$ é uma solução de $ax + by = c$, então $c = ax_1 + by_1 = ax_0 + by_0$. Assim, $a(x_1 - x_0) = b(y_0 - y_1)$. Como $d = mdc(a, b)$, segue que $a = dq_1$ e $b = dq_2$, para algum $q_1, q_2 \in \mathbb{Z}$. Deste modo, $q_1(x_1 - x_0) = q_2(y_0 - y_1)$, e assim, $q_2 \mid q_1(x_1 - x_0)$. Mas, como $mdc(q_1, q_2) = 1$, segue que $q_2 \mid (x_1 - x_0)$, ou seja, $x_1 - x_0 = q_2q_3$, onde $q_3 \in \mathbb{Z}$. Assim, $x_1 = x_0 + \frac{b}{d}q_3$. Além disso, $q_1(x_1 - x_0) = q_2(y_0 - y_1) = q_1q_2q_3$, e assim, $y_1 = y_0 - q_1q_3$. Como $q_1 = \frac{a}{d}$, segue que $y_1 = y_0 - \frac{a}{d}q_3$, o que prova o resultado. □

Corolário 5.6.1. *Se $a \neq 0$, $b \neq 0$ e $mdc(a, b) = 1$, então o conjunto de solução da equação $ax+by = c$ é dado por $S = \{(x_0+bt, y_0-at) : t \in \mathbb{Z}\}$, onde $x_0, y_0 \in \mathbb{Z}$ é uma solução particular da equação.*

Exemplo 5.6.3. *Seja a equação diofantina $43x + 5y = 250$. Como $mdc(43, 5) = 1$ e $1 \mid 250$, segue que a equação possui solução. Agora, encontramos uma solução particular para a equação, que pode ser obtida do seguinte modo $43 = 5.8 + 3$, $5 = 3.1 + 2$ e $3 = 2.1 + 1$. Assim, $1 = 3 - 2.1 = 3 - (5 - 3.1) = 3.2 + 5.(-1) = (43 - 5.8).2 + 5.(-1) = 43.2 + 5.(-17)$, e portanto, o par $(2, -17)$ é uma solução particular da equação. Logo, a solução geral da equação é dada por $S = \{(2 + 5t, -17 - 43t);\ t \in \mathbb{Z}\}$.*

Exemplo 5.6.4. *Vamos determinar um par de inteiros positivos (x, y) de modo que o primeiro seja divisível por 7, o segundo seja divisível por 11 e a soma seja 100. Consideremos a seguinte equação diofantina linear $7x+11y = 100$, e primeiramente encontramos uma solução particular para essa equação diofantina linear. Como $mdc(7, 11) = 1$ e 1 divide 100, segue que a equação diofantina linear admite solução. Pelo algortmo de Euclides, segue que $11 = 7.1+4$, $7 = 4.1+3$, $4 = 3.1+1$ e $3 = 3.1$. Logo, $1 = 4-3.1 = 4-(7-4.1) = 4.2+7.(-1) = (11-7.1).2+7.(-1) = 11.2 + 7.(-2) + 7.(-1) = 11.2 + 7.(-3)$, e desse modo, o par $(-3, 2)$ não é solução da equação $7x + 11y = 100$. Mas, observando que $1 = 7.(-3) + 11.2$, e assim, $100 = 7.(-300) + 11.(200)$. Desse modo, o par $(-300, 200)$ é uma solução particular da equação diofantina em questão. Assim, $7.(-300) + 11.200 = 100$, ou seja, $-2100 + 2200 = 100$. Por outro lado, queremos dois inteiros positivos que satisfaça essa equação. Nesse raciocínio, sabemos que as soluções da equação diofantina $7x + 11y = 100$ são dadas pelos pares (x, y), onde $x = -300 + 11t$ e*

$y = 200 - 7t$, *onde* $t \in \mathbb{Z}$. *Assim, é suficiente determinar* t *para o qual* x *e* y *sejam positivos. Fazendo* $t = 27$, *segue que* $(x, y) = (-3, 11)$, *o que não nos interessa. Observe que para valores de* t *menores do que* 27, *o ponto de abscissa* x *será sempre negativo. Portanto, fazendo* $t = 28$, *segue que o par* $(8, 4)$ *é o primeiro par de inteiros positivos que satisfaz a equação diofantina* $7x + 11y = 100$.

Exemplo 5.6.5. *Vamos determinar os inteiros estritamente positivos de modo que quando divididos por* 11 *fornecem resto* 6 *e ao serem divididos por* 7 *fornecem resto* 3. *Seja* n *um inteiro tal que satisfaça as hipóteses, ou seja,* $n = 11x + 6 = 7y + 3$. *Assim, obtemos a seguinte equação diofantina linear* $11x - 7y = -3$. *Resolvendo essa equação diofantina, segue que* $(-6, -9)$ *é uma solução dessa equação. Assim, pela Proposição* $5.6.2$, *segue que a solução geral é dada por* $x = -6 - 7t$ *e* $y = -9 - 11t$, *onde* $t \in \mathbb{Z}$. *Como queremos os inteiros estritamento positivos, segue que devemos impor que* $n = 11(-6 - 7t) + 6 = -60 - 77t > 0$. *Logo,* $t = -1, -2, \cdots$, *e deste modo,* $x = 1, 8, 15, \cdots$. *Portanto, os inteiros procurados são* $n = 17, 94, 171, \cdots, 77r - 60, \cdots$.

Observação 5.6.1. *Se* (x_0, y_0) *é uma solução de* $ax + by = c$, *então os pares* $(-x_0, y_0)$, $(x_0, -y_0)$ *e* $(-x_0, -y_0)$ *são soluções das respectivas equações* $-ax + by = c$, $ax - by = c$ *e* $-ax - by = c$. *Por exemplo, sendo o par* $(2, -4)$ *solução da equação* $5x + 2y = 2$, *então* $(2, 4)$ *é uma solução de* $5x - 2y = 2$.

Observação 5.6.2. *A Proposicão 5.6.1 pode ser extendida para uma equação linear do tipo* $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$, *onde os* a_i, *para* $i = 1, 2, \cdots, n$, *são inteiros não nulos. A argumentação é mesma, ou seja, essa equação admite soluções se, e somente se,* $mdc(a_1, a_2, \cdots, a_n) = d \mid b$. *Com efeito, se* $(x_{1_0}, x_{2_0}, \cdots, x_{n_0})$ *é solução da equação diofantina* $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$, *então* $a_1x_{1_0} + a_2x_{2_0} + \cdots + a_nx_{n_0} = b$. *Se* $d = mdc(a_1, a_2, \cdots, a_n)$, *então* $d \mid a_i$, *para todo* $i = 1, 2, \cdots, n$. *Logo,* $d \mid a_1x_{1_0}$, $d \mid a_2x_{2_0}$, $\cdots$, $d \mid a_nx_{n_0}$. *Assim,* $d \mid (a_1x_{1_0} + a_2x_{2_0} + \cdots + a_nx_{n_0})$, *ou seja,* $d \mid b$. *Por outro lado, se* $d \mid b$, *e como* $d = mdc(a_1, a_2, \cdots, a_n)$, *segue que existem* $x_{1_0}, x_{2_0}, \cdots, x_{n_0}$ *tais que* $d = a_1x_{1_0} + a_2x_{2_0} + \cdots + a_nx_{n_0}$. *Além disso, como* $d \mid b$, *segue que* $d = bq$, *onde* $q \in \mathbb{Z}$. *Assim,* $b = dq = (a_1x_{1_0} + a_2x_{2_0} + \cdots + a_nx_{n_0})q = a_1(x_{1_0}r) + a_2(x_{2_0}r) + \cdots + a_n(x_{n_0}q)$. *Portanto,* $(x_{1_0}q, x_{2_0}q, \cdots, x_{n_0}q)$ *é solução da equação* $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$.

Exemplo 5.6.6. *Seja a equação diofantina* $100x + 72y + 90z = 6$. *Como* $mdc(100, 72, 90) = 2$ *e* $2 \mid 6$, *segue que essa equação admite soluções. Dividindo por* 2 *ambos lados da equação, segue que* $50x + 36y + 45z = 3$. *Deste modo,* $50 = 36.1 + 14$, $36 = 14.2 + 8$, $14 = 8.1 + 6$, $8 = 6.1 + 2$ *e* $6 = 2.3$. *Assim,* $2 = 8 - 6.1 = 8 - (14 - 8.1).1 = 8.2 + 14.(-1) = (36 - 14.2).2 + 14.(-1) = 14(-5) + 36.2 = (50 - 36.1).(-5) + 36.2 = 50.(-5) + 36.7$. *Além disso,* $45 = 2.22 + 1$, *ou seja,* $1 = 45.1 + 2.(-22)$. *Assim,* $1 = 45.1 + [50.(-5) + 36.7].(-22) = 50.110 + 36.(-154) + 45.1$. *Multiplicando por* 3, *segue que* $3 = 50.330 + 36.(-462) + 45.3$. *Assim, o terno* $(330, -462, 3)$ *é uma solução da equação* $50x + 36y + 45z = 3$. *Multiplicando ambos os lados equação* $3 = 50.330 + 36.(-462) + 45.3$ *por* 2, *segue que* $6 = 100.330 + 72.(-462) + 90.3$, *e portanto, o terno* $(330, -462, 3)$ *é uma solução da equação* $100x + 72y + 90z = 6$

5.6.1 Exercícios

1. Determine as soluções das equações diofantinas $7x + 3y = 2$, $3x + 2y = 493$, $4x + 6y = 9$ e $3x + 9y = 6$.

2. Quantas quadras de basquete e quantas quadras de vôlei são necessárias para que 60 alunos joguem simultaneamente qualquer um dos esportes?

3. Encontrar todos os números naturais n menores do que 20.000 tais que:o resto da divisão de n por 37 é 9 e o resto da divisão de n por 52 é 15.

4. Um trabalhador recebe 530 reais em tíquetes de alimentação, com valores de 30 reais ou 40 reais cada tíquete. De quantas formas pode ser formado o carnê de tíquetes desse trabalhador?

5. O custo de uma postagem é de 63 centavos e os valores dos selos são de 6 e 15 centavos. Como podemos combinar os selos para fazer essa postagem?

6. Um cinema possui dois preços de ingressos: 7 reais e 5 reais. Qual é o menor número de pessoas que podem assistir a um filme de modo que o valor arrecadado seja de 600 reais.?

7. Dois amigos compraram x e y quantidades de pares de sapatos. Considerando $3x + 4y = 61$, determine as possíveis quantidades de pares de sapatos que os amigos compraram juntos?

8. A soma do produto do dia de aniversário por 12 e o mês de aniversário por 31 de uma pessoa é 368.. Qual é o produto do dia de aniversário pelo mês de aniversário dessa pessoa?

9. Pedro deseja comprar filhotes de cães e de avestruzes, gastando um total de R$ 1.770,00. Um filhote de cão custa R$ 29,00 e um de avestruz custa R$ 21,00. Quantos cães e avestruzes Pedro poderá comprar?

5.7 Congruências

Apresentamos, nesta seção, o conceito da relação de congruência introduzido por Karl Friedrich Gauss $(1777 - 1855)$ em 1801, que é uma importante ferramenta para Teoria dos Números. Veremos ainda que desta relação segue uma partição de $\mathbb{Z}$ em classes de equivalência que facilita o trabalho com congruências. Se o Natal em 2015 foi numa sexta feira, em que dia da semana será o Natal em 2050?

Definição 5.7.1. *Sejam $a, b, m \in \mathbb{Z}$ tal que $m > 1$. O elemento a é dito côngruo a b módulo m se $m \mid a - b$. Neste caso, a notação usada é $a \equiv b (mod\ m)$. Se a não é côngruo a b módulo m, usamos a notação $a \not\equiv b (mod\ m)$.*

Exemplo 5.7.1. *Tem-se que $24 \equiv 3 (mod\ 7)$, uma vez que $7 \mid 24 - 3 = 21$, mas $16 \not\equiv 9 (mod\ 4)$, uma vez que $4 \nmid 16 - 9 = 5$.*

Segue diretamente das propriedades de divisibilidade que se $a, b, c, d, m \in \mathbb{Z}$ com $m > 1$, então

1. $a \equiv a(mod\ m)$, ou seja, é reflexiva. Segue do fato que $m \mid 0 = a - a$, para todo $a \in \mathbb{Z}$.

2. Se $a \equiv b(mod\ m)$, então $b \equiv a(mod\ m)$, ou seja, é simétrica. Com efeito, por hipótese, $m \mid (a - b)$, e assim, $a - b = mq$, onde $q \in \mathbb{Z}$. Assim, $b - a = m(-q)$. Logo, $m \mid (b - a)$, ou seja, $b \equiv a(mod\ m)$.

3. Se $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m)$, então $a \equiv c(mod\ m)$, ou seja, é transitiva. Com efeito, por hipótese, $m \mid (a-b)$ e $m \mid (b-c)$, ou seja, $a-b = mq_1$ e $b-c = mq_2$, onde $q_1, q_2 \in \mathbb{Z}$. Subtraindo, segue que $a - c = m(q_1 + q_2)$, ou seja, $a \equiv c(mod\ m)$.

Portanto, a relação de congruência é uma relação de equivalência.

Propriedades 5.7.1. *Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 1$.*

1. *$a \equiv b(mod\ m)$ se, e somente se, a e b fornecem o mesmo resto quando divididos por m. De fato, se $a \equiv b(mod\ m)$, então $m \mid a - b$, ou seja, $a - b = mq$, para algum $q \in \mathbb{Z}$. Na divisão euclidiana de b por m, segue que $b = mq_1 + r$, onde $q_1, r \in \mathbb{Z}$ com $0 \leq r < m$. Assim, $a = b + mq = m(q + q_1) + r$. Como $0 \leq r < m$, segue que r também é o resto da divisão de a por m. Reciprocamente, se $a = mq_1 + r$ e $b = mq_2 + r$, com $q_1, q_2, r \in \mathbb{Z}$ e $0 \leq r < m$, então $a - b = m(q_1 - q_2)$. Portanto, $a \equiv b(mod\ m)$.*

2. *Se $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então $a \pm c \equiv b \pm d(mod\ m)$. De fato, Por hipótese, $m \mid a-b$ e $m \mid c-d$. Assim, $m \mid (a-b) \pm (c-d)$, ou seja, $m \mid (a \pm c) - (b \pm d)$. Portanto, $a \pm c \equiv b \pm d(mod\ m)$.*

3. *Se $a \equiv b(mod\ m)$ e $c \equiv d(mod\ m)$, então $ac \equiv bd(mod\ m)$. De fato, por hipótese, $m \mid a-b$ e $m \mid c-d$. Assim, $m \mid (a-b)c$ e $m \mid b(c-d)$, ou seja, $m \mid ac-bc$ e $m \mid bc-bd$. Assim, $m \mid ac - bd$, e portanto, $ac \equiv bd(mod\ m)$.*

4. *Se $a \equiv b(mod\ m)$, então $a \pm c \equiv b \pm c(mod\ m)$ e $ac \equiv bc(mod\ m)$. De fato, por hipótese, $a - b = qm$, onde $q \in \mathbb{Z}$. Logo, $a = qm + b$, e assim, $a \pm c = qm + (b \pm c)$. Deste modo, $(a \pm c) - (b \pm c) = qm$, implicando que $a \pm c \equiv b \pm c(modm)$. Por outro lado, como $a - b = qm$, segue que $c(a-b) = cqm$. Assim, $ac - bc = (cq)m$, ou seja, $ac \equiv bc(mod\ m)$.*

5. *Se $a \equiv b(mod\ m)$, então $a^n \equiv b^n(mod\ m)$, para todo $n \geq 1$. De fato, a prova é feita por indução sobre n. Por hipótese, para $n = 1$ a afirmação é verdadeira. Agora, suponhamos verdadeira para $n = k$, ou seja, $a^k \equiv b^k(mod\ m)$. Para $n = k + 1$, como $a^{k+1} = a^k a$, $b^{k+1} = b^k b$, $a \equiv b(mod\ m)$ e $a^k \equiv b^k(mod\ m)$, segue que $a^{K+1} \equiv b^{k+1}(mod\ m)$.*

6. *Se $ca \equiv cb(mod\ m)$ e $mdc(m, c) = d$, então $a \equiv b(mod\ \frac{m}{d})$. De fato, por hipótese, $c(a - b) = qm$, onde $q \in \mathbb{Z}$. Logo, $\frac{c}{d}(a - b) = q\frac{m}{d}$ e como $mdc(\frac{c}{d}, \frac{m}{d}) = 1$, segue que $\frac{m}{d} \mid (a - b)$, ou seja, $a \equiv b(mod\ \frac{m}{d})$.*

7. *Se* $ca \equiv cb(mod\ m)$ *e* $mdc(m, c) = 1$*, então* $a \equiv b(mod\ m)$*. De fato, segue diretamente da propriedade anterior tomando* $d = 1$*.*

8. *Se* $ca \equiv cb(mod\ p)$*, onde* p *é primo e* $p \nmid c$*, então* $a \equiv b(mod\ p)$*. De fato, como* p *é primo e* $p \nmid c$*, segue que* $mdc(p, c) = 1$*. Assim, o resultado segue da propriedade anterior.*

9. *Se* $a + b \equiv c(mod\ m)$*, então* $a \equiv c - b(mod\ m)$*. De fato, como* $a + b \equiv c(mod\ m)$ *e* $-b \equiv -b(mod\ m)$*, segue que* $a \equiv c - b\ (mod\ m)$*.*

Exemplo 5.7.2. *Se* $27 \equiv 9\ (mod\ 9)$*, então* $27 = 9.3 + 0$ *e* $9 = 9.1 + 0$ *e, portanto,* 27 *e* 9 *deixam o mesmo resto quando divididos por* 9*. Além disso, como* $33 \equiv 15(mod\ 9)$*, ou seja,* $3.11 \equiv 3.5(mod\ 9)$ *e* $mdc(3, 9) = 3$*, segue que* $11 \equiv 5(mod\ 3)$*.*

Proposição 5.7.1. *Se* $a \equiv b(mod\ m_1)$*,* $a \equiv b(mod\ m_2)$ *e* $mdc(m_1, m_2) = 1$*, então* $a \equiv b(mod\ m_1m_2)$*.*

Demonstração. Como $a \equiv b(mod\ m_1)$, segue que $a - b = m_1q$, para algum $q \in \mathbb{Z}$. Além disso, como $a \equiv b(mod\ m_2)$, segue que $m_2 \mid a - b$, ou seja, $m_2 \mid m_1q$. Como $mdc(m_1, m_2) = 1$, segue que $m_2 \mid q$, ou seja, $q = m_2q_1$, com $q_1 \in \mathbb{Z}$. Assim, $a - b = m_1m_2q_1$, ou seja, $m_1m_2 \mid a - b$ e, portanto, $a \equiv b(mod\ m_1m_2)$. □

A relação de congruência é bastante útil para saber se um certo número divide outro, ou seja, para verificar se um número é divisível por outro. Por exemplo, será que 11 divide $10^{200} - 1$? Como $10 \equiv -1\ (mod\ 11)$, segue que $10^{200} \equiv (-1)^{200}(mod\ 11)$, ou seja, $10^{200} \equiv 1(mod\ 11)$. Portanto, $10^{200} - 1 \equiv 0\ (mod\ 11)$, e assim, 11 divide $10^{200} - 1$.

5.7.1 Exercícios

1. Mostre que a soma de dois números pares é um número par.
2. Mostre que a soma de dois números ímpares é um número par.
3. Mostre que a soma de um número par com um número impar é um número impar.
4. Mostre que a soma de dois números racionais é um número racional.
5. Mostre que o produto de dois números racionais é um número racional.
6. Mostre que o quadrado de um número impar é da forma $8n + 1$, onde $n \in \mathbb{Z}$.
7. Determine o resto da divisão de: 7^{12} por 4, 4^{15} por 7, 7^{30} por 11 e $2^{20} - 1$ por 41.
8. Determine o resto da divisão de 1073.640.2650 por 7.
9. Determine o último dígito dos números 345271^{79399} e 4321^{4321}.
10. Determine o resto da divisão de $531.31^2.2$ por 7.
11. Determine o algarismo das unidades de 9^{9^9} e 7^{7^7}.

12. Determine um critério de divisibilidade por 2.
13. Determine um critério de divisibilidade por 3.
14. Determine um critério de divisibilidade por 4.
15. Determine um critério de divisibilidade por 5.
16. Determine um critério de divisibilidade por 6.
17. Determine um critério de divisibilidade por 7.
18. Determine um critério de divisibilidade por 8.
19. Determine um critério de divisibilidade por 9.
20. Determine um critério de divisibilidade por 10.
21. Determine um critério de divisibilidade por 11.

5.8 Teoremas de Euler, Fermat e Wilson

O objetivo desta seção é o estudo dos teoremas de Euler, Fermat e Wilson que propõem informações importantes sobre primalidade e que auxiliam no trabalho das congruências. O resultado, conhecido por Pequeno Teorema de Fermat, foi proposto por Fermat em 1640, porém não deixou nenhuma demonstração do resultado. Assim, em 1736, Euler apresenta a primeira demonstração do teorema e alguns anos depois consegue uma generalização do resultado, que recebe o nome de Teorema de Euler. Para tanto, Euler precisou introduzir a função φ..

Teorema 5.8.1. *(Euler) Para todo inteiro $m > 1$ e para todo $a \in \mathbb{Z}$, primo com m, vale a congruência*

$$a^{\varphi(m)} \equiv 1 \ (mod\ m).$$

Demonstração. Consideremos o conjunto

$$S = \{s \in \mathbb{Z} : \ 1 \leq s \leq m \ e \ mdc(s, m) = 1\} = \left\{s_1, s_2, \cdots, s_{\varphi(m)}\right\}.$$

Para cada s_i, onde $i = 1, 2, \cdots, \varphi(m)$, façamos a divisão de as_i por m. Logo,

$$as_i = mq_i + r_i, \ onde \ q_i, r_i \in \mathbb{Z} \ e \ 0 \leq r_i < m.$$

Assim, $mdc(r_i, m) = 1$, para $i = 1, 2, \cdots, \varphi(m)$, pois se existisse $p \in \mathbb{Z}$ tal que $p \mid m$ e $p \mid r_i$, então $p \mid as_i$. Assim, $p \mid a$ ou $p \mid s_i$, o que é impossível, já que $mdc(a, m) = 1$ e $mdc(s_i, m) = 1$. Ainda, do conjunto $R = \left\{r_1, r_2, \cdots, r_{\varphi(m)}\right\}$ não existe elementos repetidos, pois se $r_i = r_j$, para $i \neq j$ com $0 \leq i, j < \varphi(m)$, então $as_i - mq_i = as_j - mq_j$, implicando em $a(s_i - s_j) = m(q_i - q_j)$. Como $mdc(m, a) = 1$, segue que $m \mid (s_i - s_j)$. Mas, $1 \leq s_i, s_j < m$, o que resultaria em

$s_i = s_j$, o que não é possível, pois $i \neq j$. Logo, $S = R$. Assim, multiplicando as congruências $as_i \equiv r_i \ (mod\ m)$, para $i = 1, 2, \cdots, \varphi(m)$, segue que

$$(as_1)(as_2)\cdots(as_{\varphi(m)}) = a^{\varphi(m)}s_1s_2\cdots s_{\varphi(m)} \equiv r_1r_2\cdots r_{\varphi(m)} \ (mod\ m).$$

Como m é primo com cada elemento do produto $s_1s_2\cdots s_{\varphi(m)}$ que é igual a $r_1r_2\cdots r_{\varphi(m)}$, segue que

$$a^{\varphi(m)} \equiv 1 \ (mod\ m),$$

o que prova o resultado. □

Exemplo 5.8.1. *Tomando $p = 8$ e $a = 5$, verifiquemos que o teorema é válido. Assim, $\varphi(8) = 4$ e $mdc(8, 5) = 1$, e desse modo, $5^4 = 5^2.5^2 = 25.25 \equiv 1.1 \ (mod\ 8)$.*

Teorema 5.8.2. *(Pequeno Teorema de Fermat) Se $p > 1$ é um inteiro primo e a um inteiro tal que $p \nmid a$, então*

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Demonstração. Como p é primo, segue, do Corolário 4.3 do relatório anterior, que $\varphi(p) = p-1$. Assim, sendo a primo com p, pelo Teorema de Euler, segue que

$$a^{\varphi(p)} = a^{p-1} \equiv 1 \ (mod\ p),$$

o que prova o resultado. □

Teorema 5.8.3. *(Fermat) $p > 1$ é um inteiro primo, então*

$$a^p \equiv a \ (mod\ p),$$

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

Demonstração. Se $p \mid a$, então $a \equiv 0 \ (mod\ p)$ e, daí, $a^p \equiv 0 \ (mod\ p)$. Desse modo, $a^p \equiv a \ (mod\ p)$. Se, ao invés, $p \nmid a$, então, pelo Pequeno Teorema de Fermat, $a^{p-1} \equiv 1 \ (mod\ p)$. Multiplicando a congruência por a segue que $a^p \equiv a \ (mod\ p)$. Portanto, $a^p \equiv a \ (mod\ p)$, para todo $a \in \mathbb{Z}$. □

Exemplo 5.8.2. *Mostremos que $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \ (mod\ p)$, para $p > 2$ primo. Como, pelo Teorema 5.8.3, $1^{p-1} \equiv 1 \ (mod\ p)$, $2^{p-1} \equiv 1 \ (mod\ p)$, $\cdots$, $(p-1)^{p-1} \equiv 1 \ (mod\ p)$, então somando todas as parcelas segue que $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv p - 1 \equiv -1 \ (mod\ p)$.*

Teorema 5.8.4. *Sejam p e q dois primos positivos distintos e $a \in \mathbb{Z}$. Se $a^p \equiv a \ (mod\ q)$ e $a^q \equiv a \ (mod\ p)$, então $a^{pq} \equiv a \ (mod\ pq)$.*

Demonstração. Do Teorema 5.8.3, segue que

$$(a^p)^q \equiv (a^p) \ (mod\ q) \ e \ (a^q)^p \equiv (a^q) \ (mod\ p).$$

Da hipótese, $a^p \equiv a \ (mod\ q)$ e $a^q \equiv a \ (mod\ p)$, logo, $a^{pq} \equiv a \ (mod\ q)$ e $a^{pq} \equiv a \ (mod\ p)$, ou seja, $q \mid (a^{pq} - a)$ e $p \mid (a^{pq} - a)$. Como $mdc(p, q) = 1$, segue que $pq \mid (a^{pq} - a)$, isto é, $a^{pq} \equiv a \ (mod\ pq)$, como queríamos. □

Exemplo 5.8.3. *Vamos verificar o Pequeno Teorema de Fermat com $a = 3$ e $p = 17$. O número 17 é um primo e não divide 3. Pelo Teorema 5.8.2, segue que $3^{17-1} = 3^{16} \equiv 1(mod\ 17)$. Sem usar o Teorema 5.8.2 também podemos chegar a esta conclusão facilmente, pois, como:*

$$3^3 = 27 \equiv 10(mod\ 17) \rightarrow 3^6 \equiv 100 \equiv -2(mod\ 17)$$

e

$$3^{12} \equiv 4(mod\ 17),$$

segue que

$$3^{17-1} = 3^{16} = 3^{12}.3^3.3 \equiv 4.10.3 \equiv 120 \equiv 1(mod\ 17).$$

Exemplo 5.8.4. *Mostramos que $5^{38} \equiv 4(mod\ 11)$. De fato, pelo Teorema 5.8.2:*

$$5^{10} \equiv 1(mod\ 11) rightarrow 5^{38} = 5^{10.3+8} = (5^{10})^3(5^2)^4 \equiv 1^3.3^4 \equiv 81 \equiv 4(mod\ 11).$$

Exemplo 5.8.5. *O número 117 é composto. Para mostrarmos essa afirmação, basta acharmos um inteiro a tal que a^{117} não seja côngruo à a módulo 117. Tomando $a = 2$, segue que*

$$2^{117} = 2^{7.16+5} = (2^7)^{16}.2^5$$

Por outro lado, observemos que

$$2^7 = 128 \equiv 11(mod\ 117).$$

Assim,

$$2^{117} \equiv 11^{16}.2^5 \equiv (121)^8.2^5 \equiv 4^8.2^5 \equiv 2^{21}(mod\ 117).$$

Ainda, $2^{21} = (2^7)^3$, o que nos dá que:

$$2^{21} \equiv 11^3 \equiv 121.11 \equiv 4.11 \equiv 44(mod\ 117).$$

Portanto,

$$2^{117} \equiv 44$$

e 44 não é côngruo a 2 módulo 117, e desse modo, o inteiro 117 é composto ($117 = 9.13$).

Vejamos agora um exemplo interessante, o qual mostra que a recíproca do Pequeno Teorema de Fermat, isto é: se $a^{n-1} \equiv 1(mod\ n)$, então n é primo, é falsa.

Exemplo 5.8.6. *O inteiro $2^{340} \equiv 1(mod\ 341)$. Com efeito, observe que:*

$$341 = 11.31 \quad e \quad 2^{10} = 1024 = 31.33 + 1 = 11.93 + 1.$$

Mas isto significa que

$$2^{10} \equiv 1(mod\ 31) \quad e \quad 2^{10} \equiv 1(mod\ 11).$$

Portanto,

$$2^{11} = 2.2^{10} \equiv 2.1 \equiv 2(mod\ 31) \ \ e \ \ 2^{31} = 2(2^{10})^3 \equiv 2.1^3 \equiv 2(mod\ 11).$$

Ainda, os inteiros 11 *e* 31 *são primos. Dai, que pelo Teorema 5.8.4, segue que*

$$2^{11.31} \equiv 2(mod\ 11.31) \quad ou \quad 2^{341} \equiv 2(mod\ 341)$$

de onde segue que $2^{340} \equiv 1(mod\ 341)$.

No que segue, veremos um resultado que foi enunciado pela primeira vez em *Meditationes Algebraicae* (1770) no trabalho do matemático inglês Edward Waring. A interessante propriedade informada por John Wilson (1741-1793) a Waring não foi provada, cabendo, em 1771, a Lagrange a demonstração do que hoje é conhecido como Teorema de Wilson.

Proposição 5.8.1. *Se* $p > 2$ *é um inteiro primo e* $2 \leq a \leq p-2$*, então existe um único* $b \in \{2, 3, \cdots, p-3, p-2\}$*, com* $b \neq a$*, tal que* $ab \equiv 1\ (mod\ p)$.

Demonstração. Considerando a congruência linear $ax \equiv 1\ (mod\ p)$, sendo $mdc(a, p) = 1$, pois $2 \leq a \leq p-2$, segue que a congruência admite uma única solução $b \in \{1, 2, \cdots, p-1\}$. De fato, $b \neq a$, pois se tivéssemos $b = a$, então $a^2 \equiv 1\ (mod\ p)$
$rightarrowa^2 - 1 = (a-1)(a+1) \equiv 0\ (mod\ p)$ e daí, $p \mid (a-1)$ ou $p \mid (a+1)$, o que não ocorre, já que $2 \leq a \leq p-2$. Ainda, $b \neq 1$ e $b \neq p-1$, pois caso $b = 1$ segue que $a \equiv 1\ (mod\ p)$, ou seja, $p \mid (a-1)$, o que já vimos anteriormente que não acontece. No caso $b = p-1$, segue que $a(p-1) = ap - a \equiv 1\ (mod\ p)$ e daí, $p \mid ap - (a+1)$, implicando em $p \mid (a+1)$, o que também não acontece. □

Teorema 5.8.5. *(Wilson) Se* $p > 1$ *é primo, então* $(p-1)! \equiv -1\ (mod\ p)$.

Demonstração. Sendo p um inteiro primo, consideremos o fatorial $(p-1)!$. Pela proposição anterior, segue que para todo $a \in \{2, 3, \cdots, p-2\}$, existe um único $b \in \{2, 3, \cdots, p-2\}$ tal que $ab \equiv 1\ (mod\ p)$. Desse modo, podemos agrupar dois a dois os inteiros $2, 3, \cdots, p-2$ de forma que $a_i b_i \equiv 1\ (mod\ p)$, para $i = 1, 2, \cdots, \frac{p-3}{2}$. e $a_i, b_i \in \{2, 3, \cdots, p-2\}$. Assim,

$$\begin{aligned}(p-1)! &= 1.2.\cdots(p-2)(p-1) = 1.a_1b_1.a_2b_2\cdots a_{\frac{p-3}{2}}b_{\frac{p-3}{2}}.(p-1)\\ &\equiv 1.1.1\cdots(p-1) \equiv p-1 \equiv -1\ (mod\ p).\end{aligned}$$

Portanto, para todo primo p positivo, segue que $(p-1)! \equiv -1\ (mod\ p)$. □

Exemplo 5.8.7. *Para* $p = 7$*, pelo Teorema de Wilson, segue que* $(7-1)!+1 = 6!+1 = 720+1 = 721 = 7.103$. *Assim,*

$$(7-1)! + 1 \equiv 0(mod\ 7), \quad ou\ seja, \quad (7-1)! \equiv -1(mod\ 7).$$

Veremos no próximo resultado que a recíproca do Teorema de Wilson também é válida.

Teorema 5.8.6. *Se* $(p-1)! \equiv -1 \ (mod\ p)$*, então* p *é primo.*

Demonstração. Se p não é primo, então existe um divisor q com $1 < q < p$. Como q é um fator de p, segue que q é um dos fatores de $(p-1)!$, ou seja, $q \mid (p-1)!$. Ainda, pela hipótese, segue que $(p-1)! \equiv -1 \ (mod\ p)$, ou seja, $(p-1)! = -1 + pk$, para algum $k \in \mathbb{Z}$. Assim, como $q \mid (p-1)!$ e $q \mid p$, segue que $q \mid 1$, o que é absurdo e, portanto, n é primo. □

Exemplo 5.8.8. *Utilizando a recíproca do Teorema de Wilson, vamos reconhecer se o inteiro 11 é primo. Mas isto é claro, pois observe que:*

$$(11-1)! + 1 = 10! + 1 = 1.2.3 \cdots 10 + 1 = 3628801 = 11.329891.$$

Portanto, $(11-1)! \equiv -1(mod\ 11)$*, o que nos leva a conclusão de que o inteiro* 11 *é primo.*

Exemplo 5.8.9. *Da mesma forma, o inteiro* 13 *é primo, uma vez que*

$$(13-1)! + 1 = 12! + 1 = 1.2.3 \cdots 12 + 1 = 479001601 = 13.36846277,$$

e portanto,

$$(13-1)! \equiv -1(mod\ 13).$$

5.8.1 Exercícios

1. Se p é um primo ímpar, mostre que $1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} (mod/p)$.
2. Mostre que as soluções de $x^2 + 1 \equiv 0(mod\ p)$, onde $p = 4m + 1$ é um primo, são $\pm 1 \cdot 2 \cdot \cdots \cdot 2m(mod\ p)$.
3. Seja p um número primo ímpar. Mostre que $1^2 \cdot 3^2 \cdots (p-2)^2 \equiv 2^2 \cdot 4^2 \cdots (p-1)^2 (mod\ p)$.
4. Mostre que $p > 1$ é primo se, e somente se, $(p-2)! \equiv 1(mod\ p)$.
5. Mostre que todo número elevado a quarta potência deixa resto 0 ou 1 quando dividido por 5.
6. Mostre que $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1(mod\ p)$, onde p é um primo impar.
7. Se $mdc(a, 5) = 1$, onde $a > 0$, mostre que $a^{8n} + 3a^{4n} + 1 \equiv 0(mod\ 5)$, para todo $n > 0$.
8. Seja p um primo impar. Mostre que a equação $x^2 + 1 \equiv 0(mod\ p)$ admite solução se, e somente se, $p \equiv 1(mod\ 4)$.
9. Mostre que $n > 1$ é um primo se, e somente se, $(n-2)! \equiv 1(mod\ n)$.
10. Se p e q são primos distintos tais que $a^p \equiv a(mod\ q)$ e $a^q \equiv a(mod\ p)$, mostre que $a^{pq} \equiv a(mod\ pq)$.

Capítulo

6

Leis de composição interna

Uma lei de composição interna é uma função que associa cada elemento do produto cartesiano de um conjunto a um elemento dese conjunto. A partir desse conceito obtemos várias propriedades, como veremos a seguir. Deste modo, no presente capítulo, apresentamos o conceito de operações sobre um conjunto (também conhecido como leis de composição interna), com a introdução das propriedades: associativa, comutativa, existência do elemento neutro, elementos simetrizáveis, e elementos regulares.

6.1 Operações - leis de composição interna

Seja E um conjunto não vazio.

Definição 6.1.1. *Uma aplicação $f : E \times E \to E$ é chamada operação sobre E (ou lei de composição interna em E) e denotada por $f(x, y) = x * y$, onde $x, y \in E$.*

Seja $*$ uma operação sobre um conjunto E e A um subconjunto não vazio de E. O conjunto A é chamado fechado em relação a operação $*$ ou que a operação é fechada sobre A se $a * b \in A$, para todo $a, b \in A$.

Exemplo 6.1.1.

1. *A relação $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida por $f(x, y) = x * y = mdc(x, y)$, onde $x, y \in \mathbb{N}$, é uma operação sobre $\mathbb{N}$.*

2. *O conjunto $m\mathbb{Z}$, onde $m \in \mathbb{Z}$, é fechado em relação a adição e a multiplicação.*

3. *O conjunto formado pelos números ímpares é fechado em relação a multiplicação, mas não é fechado em relação a adição.*

4. *A relação* $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *definida por* $f(x, y) = x - y$ *não define uma operação sobre* $\mathbb{N}$*, uma vez que* $(3, 5) \in \mathbb{N} \times \mathbb{N}e$ $f(3, 5) = 3 - 5 = -2$ *não pertence aos naturais.*

5. *A relação* $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *definida por* $f(x, y) = \frac{x}{y}$ *não define uma operação sobre* $\mathbb{Z}$*, uma vez que* $(3, 6) \in \mathbb{Z} \times \mathbb{Z}$ *e* $(3, 6) = \frac{3}{6} = \frac{1}{2}$ *não pertence aos inteiros.*

6. *A relação* $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *definida por* $f(x, y) = xy$ *define uma operação sobre* $\mathbb{N}$*, uma vez que para quaisquer* $x, y \in \mathbb{N}$*, segue que* xy *é um número natural.*

7. *A adição sobre* $\mathbb{N}$*,* $\mathbb{Z}$*,* $\mathbb{Q}$*,* $\mathbb{R}$ *ou* $\mathbb{C}$ *é uma operação binária.*

8. *A subtração sobre* $\mathbb{Z}$*,* $\mathbb{Q}$*,* $\mathbb{R}$ *ou* $\mathbb{C}$ *é uma operação binária.*

9. *A multiplicação sobre* $\mathbb{N}$*,* $\mathbb{Z}$*,* $\mathbb{Q}$*,* $\mathbb{R}$ *ou* $\mathbb{C}$ *é uma operação binária.*

10. *A adição e multiplicação de matrizes sobre o conjunto das matrizes quadradas* $M_n(A)$ *com coeficientes em* A*, onde* $A = \mathbb{N}$*,* $\mathbb{Z}$*,* $\mathbb{Q}$*,* $\mathbb{R}$ *ou* $\mathbb{C}$ *é uma operação binária.*

6.1.1 Associativa

A operação $*$ sobre E é associativa se $a * (b * c) = (a * b) * c$, para todo $a, b, c \in E$.

Exemplo 6.1.2. *Em* $\mathbb{R}$ *as operações de adição e muliplicação são associativas, uma vez que* $a + (b + c) = (a + b) + c$ *e* $a(bc) = (ab)c$*, para todo* $a, b, c \in \mathbb{R}$*. Em* $\mathbb{R}$ *a divisão e a subtração não são associativas, uma vez que* $2 = (8 : 2) : 2 \neq 8 : (2 : 2) = 8$ *e* $-1 = (8 - 4) - 5 \neq 8 - (4 - 5) = 9$*. Também, em* $\mathbb{N} - \{0\}$*, a potenciação* $a * b = a^b$ *não é associativa, uma vez que* $(2 * 3) * 2 = 2^3 * 2 = (2^3)^2 = 2^6$ *e* $2 * (3 * 2) = 2 * 3^2 = 2 * 9 = 2^9$*.*

Exemplo 6.1.3. *Em* $\mathbb{R}$ *a operação* $x * y = x + y + xy$ *é associativa, uma vez que* $x * (y * z) = x * (y + z + yz) = x + y + z + yz + x(y + z + yz) = x + y + z + yz + xy + xz + xyz$ *e* $(x * y) * z = (x + y + xy) * z = x + y + xy + z + (x + y + xy)z = x + y + z + xy + xz + yz + xyz$*, para todo* $x, y, z \in \mathbb{R}$*.*

6.1.2 Comutativa

A operação $*$ sobre E é comutativa se $a * b = b * a$, para todo $a, b \in E$.

Exemplo 6.1.4. *Em* $\mathbb{R}$ *as operações de adição e muliplicação comutativas, uma vez que* $a + b = b + a$ *e* $ab = ba$*, para todo* $a, b \in \mathbb{R}$*. Em* $\mathbb{R}$ *a divisão e a subtração não são comutativas, uma vez que* $2 = (8 : 4) \neq (4 : 8) = 0.5$ *e* $3 = 8 - 4 \neq 4 - 8 = -4$*. Também, em* $\mathbb{N} - \{0\}$*, a potenciação* $a * b = a^b$ *não é associativa, uma vez que* $2 * 3 = 2^3 = 8 \neq 3 * 2 = 9$*.*

Exemplo 6.1.5. *Em* $\mathbb{N} - \{0\}$ *a operação* $x * y = mdc(x, y)$*, com* $x, y \in \mathbb{N} - \{0\}$*, é comutativa, uma vez que* $mdc(x, y) = mdc(y, x)$*, para todo* $x, y \in \mathbb{N} - \{0\}$*.*

Exemplo 6.1.6. *Em* $\mathbb{R}$ *a operação* $x * y = x + y + xy$ *é comutativa, uma vez que* $x * y = x + y + xy = y * x$*, para todo* $x, y \in \mathbb{R}$*. Agora, sobre* $\mathbb{R}$*, a operação* $x * y = x + xy$*, com* $x, y \in \mathbb{R}$ *não é comutativa, uma vez que* $3 = 1 * 2 = 1 + 1.2 \neq 2 * 1 = 2 + 2.1 = 4$*.*

6.1.3 Elemento neutro

Um elemento $e \in E$ é chamado elemento neutro em relação a operação $*$ se $x*e = e*x = x$, para todo $x \in E$.

Exemplo 6.1.7. *Em $\mathbb{R}$ o 0 é o elemento neutro da adição, uma vez que $x+0 = 0+x = x$, para todo $x \in \mathbb{R}$. Em $\mathbb{R} - \{0\}$, o 1 é o elemento neutro da multiplicação, uma vez que $x.1 = 1.x$, para todo $x \in \mathbb{R} - \{0\}$.*

Exemplo 6.1.8. *No conjunto $M_2(\mathbb{R})$, das matrizes 2×2, a matriz nula $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ é o elemento neutro em relação a adição e a matriz identidade $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é o elemento neutro em relação ao produto.*

Exemplo 6.1.9. *Em $\mathbb{R} - \{-1\}$ a operação $x*y = x+y+xy$, com $x, y \in \mathbb{R}$, não possui elemento neutro, uma vez que se $x*e = x$, então $x+e+xe = x$, ou seja, $e(1+x) = 0$. Como $x \neq -1$, segue que $e = 0$, e portanto, 0 é o elemento neutro.*

Proposição 6.1.1. *O elemento neutro de uma operação $*$ sobre E é único (caso exista).*

Demonstração. Se e_1 e e_2 são elementos neutros da operação $*$, então $e_1 * x = x = x * e_1$ e $e_2 * x = x = x * e_2$, para todo $x \in E$. Em particular, tomando $x = e_2$ na primeira igualdade e $x = e_1$ na segunda igualdade, segue que $e_1 = e_1 * e_2 = e_2$, ou seja, o elemento neutro (caso exista) é único. □

6.1.4 Elementos simetrizáveis

Seja $*$ uma operação sobre E que admite um elemento neutro $e \in E$. Um elemento $a \in E$ é chamado elemento simetrizável em relação a operação $*$ se existe um elemento $b \in E$ tal que $a*b = b*a = e$. Neste caso, o elemento b é denotado por a' e é chamado de simétrico de a. O elemento neutro é sempre simetrizável e é o próprio simétrico.

No caso da adição o simétrico aditivo de a é denotado por $-a$ e no caso da multiplicação o simétrico multiplicativo de a é denotado por a^{-1}, caso existam.

Exemplo 6.1.10. *Em $\mathbb{N}$ a operação de adição, $x*y = x+y$, com $x, y \in \mathbb{N}$, tem como elemento neutro o 0. Neste caso, o 0 é o único elemento simetrizável de $\mathbb{N}$.*

Exemplo 6.1.11. *Em $\mathbb{Z}$ com a operação de adição, todos os elementos são simetrizáveis.*

Exemplo 6.1.12. *Em $\mathbb{Z}$ com a operação de multiplicação, os únicos elementos simetrizáveis são ± 1.*

Exemplo 6.1.13. *Em $\mathbb{R}$ com a operação de adição, todos os elementos são simetrizáveis.*

Exemplo 6.1.14. *Em $\mathbb{R}$ com a operação de multiplicação, os elementos simetrizáveis são $\mathbb{R} - \{0\}$.*

Proposição 6.1.2. *Seja $*$ uma operação associativa sobre E que admite um elemento neutro $e \in E$. Se $a \in E$ é simetrizável, então o simétrico de a é único.*

Demonstração. Se a' e a' são simétricos de a em relação a operação $*$, então $a * a' = a' * a = e$ e $a'' * a = a * a'' = e$. Assim, $a' * e = a' = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$, ou seja, o elemento simétrico de a é único. □

Proposição 6.1.3. *Seja $*$ uma operação associativa sobre E que admite um elemento neutro $e \in E$. Se $a, b \in E$ são simetrizáveis, então $a*b$ é simetrizável e seu simétrico é $(a*b)' = b'*a'$.*

Demonstração. Se a' e b' são os simétricos de a e b, respectivamente, em relação a operação $*$, então $(a * b) * (b' * a') = a * (b * b') * a' = a * a' = e$ e $(b' * a')(a * b) = b' * (a' * a) * b = b' * b = e$. Portanto, $b' * a'$ é o elemento simétrico de $a * b$. □

Corolário 6.1.1. *Seja $*$ uma operação associativa sobre E que admite um elemento neutro $e \in E$. Se $a \in E$ é simetrizável, então a' é simetrizável e $(a')' = a$.*

Demonstração. Se a é simetrizável, então existe o simétrico a' de a em E tal que $a*a' = a'*a = e$. Assim, por definição, a' é simetrizável, e desse modo, existe $(a')' \in E$ tal que $(a')' * a' = e$. Aplicando, a em ambos os lados, segue que $((a')') * a') * a = e * a$, ou seja, $(a')' * (a' * a) = a$. Assim, $(a')' * e = a$, e portanto, $(a')' = a$. □

Exemplo 6.1.15. *Todos os elementos de $\mathbb{R} - \{-1\}$ com a operação $x * y = x + y + xy$, onde $x, y \in \mathbb{R} - \{-1\}$, é simetrizável e o simétrico de $a \in \mathbb{R} - \{-1\}$ é dado por $a' = -\frac{a}{a+1}$, uma vez que se a' é o simétrico de a, então $a * a' = 0$. Assim, $a + a' + aa' = 0$, ou seja, $a' = -\frac{a}{a+1}$.*

6.1.5 Elementos regulares

Seja $*$ uma operação sobre E que é associativa. Um elemento $a \in E$ é chamado regular a esquerda se, para todo $x, y \in E$, $a * x = a * y$ e $x * a = y * a$ implicar que $x = y$, ou seja, vale a lei do cancelamento a esquerda. Um elemento $a \in E$ é chamado regular a direita se, para todo $x, y \in E$, $x * a = y * a$ implicar que $x = y$, ou seja, vale a lei do cancelamento a direita. Um elemento $a \in E$ é chamado regular se é regular a esquerda e regular a direita.

Exemplo 6.1.16. *Todos os elementos de $\mathbb{R}$, com relação a adição, são regulares e todos os elementos não nulos de $\mathbb{R}$, com relação ao produto, são regulares. Similarmente, todos os elementos de $\mathbb{Z}$, com relação a adição, são regulares e todos os elementos não nulos de $\mathbb{Z}$, com relação ao produto, são regulares.*

Exemplo 6.1.17. *Os elementos regulares de $\mathbb{R}$, com relação a operação $x * y = x + y + xy$, onde $x, y \in \mathbb{R}$, são os elementos $a \in \mathbb{R}$ tal que $a \neq -1$, uma vez que se $a * x = a * y$, então $a + x + ax = a + y + ay$, ou seja, $x + ax = y + ay$. Assim, $(x - y)(a + 1) = 0$, e $x = y$ sempre que $a \neq -1$.*

Exemplo 6.1.18. *Os elementos regulares de $\mathbb{R} - \{0, -1\}$, com relação a operação $x*y = x+xy$, onde $x, y \in \mathbb{R}$, são os elementos de $\mathbb{R}-\{0, -1\}$, uma vez que se $a*x = a*y$, então $a+ax = a+ay$, ou seja, $ax = ay$. Assim, $a(x-y) = 0$, e como $a \neq 0$, segue que $x = y$. Agora, se $x * a = y + a$, então $x + ax = y + ay$. Assim, $(x - y)(a + 1) = 0$. Como $a \neq -1$, segue que $x = y$.*

Proposição 6.1.4. *Seja $*$ uma operação sobre E que é associativa e tem elemento neutro. Se $a \in E$ é simetrizável, a é regular.*

Demonstração. Se $a \in E$ é simetrizável, então existe $a' \in E$ tal que $a' * a = a * a' = e$. Agora, sejam $x, y \in E$. Se $a * x = a * y$, então $a' * (a * x) = a' * (a * y)$. Assim, $(a' * a) * x = (a' * a) * y$, e portanto, $e * x = e * y$, ou seja, $x = y$. Similarmente, se $x * a = y * a$, então $(x * a) * a' = (y * a) * a'$. Assim, $x * (a * a') = y * (a * a')$, e portanto, $x * e = y * e$, ou seja, $x = y$. Portanto, a é regular. □

6.1.6 Tábua de operações

Sejam $E = \{a_1, a_2, \ldots, a_n\}$ um conjunto de n elementos e $\star$ uma operação sobre E. Considerando que a operação de dois elementos de E é dada por $a_i \star a_j = a_{ij}$, podemos dispor os elementos através da seguinte tábua, chamada tábua de uma operação.

$\star$	a_1	a_2	$\ldots$	a_i	$\ldots$	a_j	$\ldots$	a_n
a_1	a_{11}	a_{12}	$\ldots$	a_{1i}	$\ldots$	a_{1j}	$\ldots$	a_{1n}
a_2	a_{21}	a_{22}	$\ldots$	a_{2i}	$\ldots$	a_{2j}	$\ldots$	a_{2n}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
a_i	a_{i1}	a_{i2}	$\ldots$	a_{ii}	$\ldots$	a_{ij}	$\ldots$	a_{in}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
a_j	a_{j1}	a_{j2}	$\ldots$	a_{ji}	$\ldots$	a_{jj}	$\ldots$	a_{jn}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
a_n	a_{n1}	a_{n2}	$\ldots$	a_{ni}	$\ldots$	a_{nj}	$\ldots$	a_{nn}

Exemplo 6.1.19. *Sejam o conjunto $E = \{1, 3, 5, 9\}$ com a operação $a \star b = mdc(a, b)$. A tábua de operação é dada por*

$\star$	*1*	*3*	*5*	*9*
1	*1*	*1*	*1*	*1*
3	*1*	*3*	*1*	*3*
5	*1*	*1*	*5*	*1*
9	*1*	*3*	*1*	*9*

6.1.7 Exercícios

1. Em cada uma das operações abaixo verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares.

   (a) $E = \mathbb{R}_+$ e $x * y = \sqrt{x^2 + y^2}$

   (b) $E = \mathbb{R}$ e $x * y = \sqrt[3]{x^3 + y^3}$.

   (c) $E = \mathbb{Z}$ e $x * y = xy + 2x$

   (d) $E = \mathbb{Q}$ e $x * y = x + xy$

   (e) $E = \mathbb{Z} \times \mathbb{Z}$ e $(a, b) * (c, d) = (a + c, bd)$.

(f) $E = \mathbb{R}$ e $x * y = x^2 + y^2 + xy$.

(g) $E = \{a, b, c\}$ e $x * y = mdc(x, y)$

(h) $E = \mathcal{P}(\{a, b\})$ e $x * y = x \cup y$.

(i) $E = \mathcal{P}(\{0, 1\})$ e $x * y = (x \cup y) - (x \cap y)$

(j) $E = \mathbb{R}$ e $x * y = \frac{x+y}{2}$.

(k) $E = \mathbb{R}$ e $x* = x$.

(l) $E = \mathbb{R}^*$ e $x * y = x/y$.

(m) $E = \mathbb{R}_+$ e $x * y = \frac{x+y}{1+xy}$.

(n) $E = \mathbb{Z}$ e $x * y = x + y + xy$.

(o) $E = \mathbb{Z}$ e $x * y = x + xy$.

(p) $E = \mathbb{R}$ e $x * y = x^2 + y^2 + 2xy$.

(q) $E = \mathbb{N}$ e $x * y = min\{x, y\}$.

(r) $E = \mathbb{Z}$ e $x * y = mdc(, y)$.

(s) $E = \mathbb{Z}$ e $x * y = mmc(x, y)$.

2. Em cada uma das operações abaixo sobre $\mathbb{Z} \times \mathbb{Z}$, verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares.

(a) $(a, b) * (c, d) = (ac, 0)$.

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

(c) $(a, b) * (c, d) = (a + c, bd)$.

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

(e) $(a, b) * (c, d) = (a + c, b + d)$.

3. Verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares da operação $(a, b, c) * (d, e, f) = (ad, be, cf)$ sobre $\mathbb{Z}^3$.

4. Em cada uma das operações abaixo verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares, com a operação de adição.

(a) $E = \{x \in \mathbb{Z} : x \text{ é par}\} \subseteq \mathbb{Z}$

(b) $E = \{x \in \mathbb{Z} : x \text{ é impar}\} \subseteq \mathbb{Z}$

(c) $E = m\mathbb{Z} = \{x \in \mathbb{Z} : m \text{ divide } x\} \subseteq \mathbb{Z}$

(d) $E = \{\begin{pmatrix} cos(a) & sen(a) \\ -sen(a) & cos(a) \end{pmatrix} : a \in \mathbb{R}\} \subseteq M_2(\mathbb{R})$.

(e) $A = \{z \in \mathbb{C} : z = cos(\theta) + isen(\theta)\} \subseteq \mathbb{C}$.

5. Em cada uma das operações abaixo verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares, com a operação de multiplicação.

   (a) $E = \{x \in \mathbb{Z} : x \text{ é par}\} \subseteq \mathbb{Z}$

   (b) $E = \{x \in \mathbb{Z} : x \text{ é impar}\} \subseteq \mathbb{Z}$

   (c) $E = m\mathbb{Z} = \{x \in \mathbb{Z} : m \text{ divide } x\} \subseteq \mathbb{Z}$

   (d) $E = \left\{ \begin{pmatrix} cos(a) & sen(a) \\ -sen(a) & cos(a) \end{pmatrix} : a \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R})$.

   (e) $A = \{z \in \mathbb{C} : z = cos(\theta) + isen(\theta)\} \subseteq \mathbb{C}$.

6. Em cada uma das operações abaixo faça a tábua de operação e verifique se é fechada, associativa, comutativa, tem elemento neutro, encontre os elementos simetrizáveis e os elementos regulares, com a operação de multiplicação.

   (a) $E = \{1, 2, 3, 6\}$ e $x * y = mdc(x, y)$.

   (b) $E = \{1, 3, 9, 27\}$ e $x * y = mmc(x, y)$.

   (c) $E = \mathcal{P}(\{a, b\})$ e $x * y = x \cup y$.

   (d) $E = \mathcal{P}(\{a, b\})$ e $x * y = x \cap y$.

   (e) $E = \mathcal{P}(\{a, b\})$ e $x * y = (x \cup y) - (x \cap y)$.

   (f) $E = \{\sqrt{3/2}, \sqrt[3]{5/2}, \sqrt[4]{7/2}\}$ e $x * y = min\{x, y\}$.

   (g) $E = \{3\sqrt{2}, \pi, 7/2\}$ e $x * y = max\{x, y\}$.

   (h) $E = \{1, -1, i, -i\}$ e $x * y = xy$.

   (i) $E = \{1, 4, 5, 20\}$ e $x * y = max\{x, y\}$.

   (j) E é o conjunto das permutações de $A = \{1, 2, 3\}$ com a operação de composição de funções.

7. Determine $m, n \in \mathbb{Z}$ para que a operação $x * y = mx + ny$, sobre $\mathbb{Z}$, seja:

   (a) Associativa.

   (b) Comutativa.

   (c) Admita elemento neutro.

8. Seja a operação $*$ sobre $\mathbb{R}$ definida por $x * y = ax + by + cxy$, onde $a, b, c \in \mathbb{R}$. Determine a, b e c tal que a operação $*$ seja associativa e tenha elemento neutro.

9. Determine os elementos neutros a esquerda no conjunto $E = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}$ com a operação de multiplicação.

10. Construir a tábua de operação do conjunto $E = \{a, b\}$ com uma operação $*$.

11. Construir a tábua de operação do conjunto $E = \{a, b, c\}$ com uma operação $*$.

12. Construir as tábuas de operações do conjunto $E = \{a, b, c, d\}$ com uma operação $*$.

13. Construir a tábua da operação de composição das funções $f_1 = \{(a, a); (b, b); (c, c)\}$, $f_2 = (a, b); (b, c); (c, a)\}$ e $f_3 = \{(a, c); (b, a); (c, b)\}$.

14. Verifique se a operação dada por $(a, b) * (c, d) = (ac, ad + bc)$ é distributiva em relação a operação $(a, b)\triangle(c, d) = (a + c, b + d)$ sobre $\mathbb{Z} \times \mathbb{Z}$.

15. Ache $m \in \mathbb{R}$ tal que a operação $a * b = a + mb$ seja distributiva em relação a operação $x\triangle y = x + y + xy$.

16. Verifique se $G = \{z \in \mathbb{C} : z = cos(\theta) + isen(\theta)\} \subseteq \mathbb{C}$ com relação ao produto é fechada, comutativa e associativa. Determine o elemento neutro e os elementos simetrizáveis.

17. Determinar todas as operações sobre o conjunto $E = \{a, b\}$.

18. Seja A um conjunto não vazio e $\mathbb{R}^A$ o conjunto de todas as aplicações de A em $\mathbb{R}$. Seja as seguintes operações sobre $\mathbb{R}^A$, para todo $f, g \in \mathbb{R}^A$: $(f + g)(x) = f(x) + g(x)$, para todo $x \in A$, e $(fg)(x) = f(x)g(x)$, para todo $x \in A$.

    (a) Verifique que se $(\mathbb{R}^A, +)$ é fechada, comutativa e associativa. Determine o elemento neutro e os elementos simetrizáveis.

    (b) Verifique que se $(\mathbb{R}^A, \cdot)$ é fechada, associativa e comutativa. Determine o elemento neutro e os elementos simetrizáveis.

19. Se $(G, \star)$ é fechada, associativa, possui elemento neutro e todo elemento é simetrizável, para todo $x, y, z \in G$, mostre que $(x * y * z)^{-1} = z^{-1} * y^{-1} * x^{-1}$.

20. Seja $G = \mathbb{Z}_m$, onde $m \in \mathbb{N}$. Mostre que $g \in G$ é simetrizável em relação ao produto se, e somente se, $mdc(g, m) = 1$.

21. Determine uma operação sobre um conjunto E tal que todo elemento é regular, possui elemento neutro e e e é o único elemento simetrizável.

22. Encontro uma operação sobre um conjunto E que possui elemento neutro e todos os elementos de E, com excessão do elemento neutro, tem dois simétricos.

23. Determine uma operação sobre E tal que o composto de dois elementos simetrizáveis não é simetrizável.

24. Determine uma operação sobre um conjunto E que não é associativa, mas possui elemento regular.

25. Seja E um conjunto com uma operação $*$ que é associativa.

    (a) Mostre que $a \in E$ é regular se, e somente se, as aplicações $f : E \to E$ e $g : E \to E$ definidas por $g(x) = a * x$ e $g(x) = x * a$, onde $x \in E$, são injetoras.

(b) Se $a, b \in E$ são regulares, mostre que $a * b$ é regular.

(c) Se $a \in E$ é regular, mostre que o conjunto $a * E = \{a * x : x \in E\} = E$, quando E for finito.

Capítulo

7

Grupos e subgrupos

A teoria de grupos no século IX foi desenvolvida na teoria das equações algébricas, na teoria dos números e na geometria. Todas essas três áreas usaram métodos da teoria dos grupos, contudo os métodos foram mais explícitos na teoria das equações algébricas. Um dos temas centrais da geometria no seculo IX foi a busca por invariantes dentre os vários tipos de transformações geométricas. Gradualmente as atenções foram se focando nas transformações propriamente ditas, que em vários casos podem ser pensadas como elementos de grupos. Na teoria dos núumeros, no século XVIII Leonhard Euler considerou os restos das divisões de potências a^n por um número primo fixado, onde esses restos tem propriedades de grupos. Similarmente, C. F. Gauss em seu Disquisitiones Arithmeticae (1800) tratou extensivamente das formas quadráticas $ax^2+2bxy+cy^2$ e, em particular, mostrou que as classes de equivalências dessas formas, com relação a composição, tinham propriedades de grupos. Finalmente, a teoria das equações algébricas, trouxe o mais explícito conceito de grupo. Joseph-Louis Lagrange (1736-1813) iniciou o estudo das permutações das raízes de uma equação como uma ferramenta para resolvê-la. Essas permutações foram consideradas elementos de um grupo. Walter von Dick (1856-1934) e Heirich Weber (1842-1913) em 1882, independentemente, combinaram as essas raízes históricas e apresentaram definições claras da noção de um grupo (Fraleigh, J. B. A First Course in Abstract Algebra). Deste modo, neste capítulo, primeiramente, apresentamos o conceito de semi-grupo e monóide, o conceito de grupo e introduzimos suas principais propriedades, apresentamos uma classe especial de grupos através da introdução das operações de adição e multiplicação modular, e finalmente, apresentamos a estrutura de subgrupo de um grupo.

7.1 Grupos

O estudo da teoria dos grupos surgiu a partir de um trabalho publicado em 1770 pelo matemático Lagrange, onde nesse trabalho Lagrange considerava a resolubilidade das equações por meio das permutações de suas raízes. Posteriormente, os matemáticos Galois e Abel mostraram que é impossível resolver por meio de radicais as equações de grau maior do que quatro. O termo "grupo"foi usado, de maneira técnica, a primeira vez por Galois.

A presente seção, tem como objetivo uma recapitulação de alguns conceitos básicos de álgebra. Ao mesmo tempo, fixamos a terminologia e a notação adotadas nas demais seções, onde apresentamos uma estrutura algébrica que é muito útil para a álgebra abstrata, chamada grupo.

Definição 7.1.1. *Sejam G e F dois conjuntos não vazios.*

1. *O produto cartesiano de G por F é definido por $G \times F = \{(a, b) : a \in G, b \in F\}$.*
2. *Uma relação (binária) de G em F é um subconjunto de $G \times F$.*
3. *Uma aplicação de G em F, indicada por $f : G \to F$, é uma relação tal que para todo $a \in G$, existe um único $b \in F$ tal que $f(a) = b$.*
4. *Uma operação sobre G (ou lei de composição interna) é uma aplicação $f : G \times G \to G$, onde para quaisquer $x, y \in G$ usamos a notação $f(x, y) = x * y$.*

Sejam G um conjunto não vazio com uma operação $\star$ e $a \in G$. Relembramos que:

1. O elemento a é chamado regular à esquerda se $a \star x = a \star y$, com $x, y \in G$, implicar que $x = y$.
2. O elemento a é chamado regular à direita se $x \star a = y \star a$, com $x, y \in G$, implicar que $x = y$.
3. O elemento a é chamado regular se é regular à esquerda e á direita.

Por questão de simplicidade, daqui em diante, a notação usada para uma operção binária será denotada por ab em vez de $a \star b$.

Definição 7.1.2. *Seja G um conjunto não vazio munido de uma operação $\star$ (por simplicidade será considerada multiplicativa) sobre G. O conjunto G é chamado um grupo em relação a essa operação se as seguintes propriedades são satisfeitas:*

1. *associativa, isto é, $a(bc) = (ab)c$, para todo $a, b, c \in G$,*
2. *existe um elemento identidade ou neutro $e \in G$ tal que $ae = ea = a$, para todo $a \in G$, e*
3. *para todo $a \in G$ existe um elemento $a' \in G$ tal que $aa' = a'a = e$. O elemento a' (ou a^{-1}) é chamado elemento simétrico ou inverso do elemento a.*

Se, além disso, $ab = ba$ para todo $a, b \in G$, o grupo G é chamado um grupo comutativo ou abeliano.

Seja G um grupo.

1. O elemento neutro $e \in G$ é único. De fato, se $e_1, e_2 \in G$ são elementos neutros de G, então $e_1 = e_1e_2 = e_2$. Assim, $e_1 = e_2$, e portanto, o elemento neutro de G é único.

2. O simétrico de um elemento $a \in G$ é único. De fato, se a', a'' são simétricos de um elemento $a \in G$ e é o elemento neutro de G, então $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$. Assim, $a' = a''$, e poranto, o simétrico de a é único.

Seja G um conjunto não vazio munido de uma operação associativa. Um elemento $x \in G$ é chamado idempotente se $xx = x$. Se G é um grupo, então o único elemento idempotente de G é o elemento neutro.

Definição 7.1.3. *Seja G um grupo.*

1. *O grupo G é um chamado um grupo finito se G for um conjunto finito. Caso contrário, G é chamado um grupo infinito.*

2. *Se G for um grupo finito, o número de elementos de G é chamado de ordem de G e denotado por $\circ(G)$.*

Exemplo 7.1.1. *O conjunto dos números reais sob a operação de adição, o conjunto dos números reais não nulos sob a operação de multiplicação, o conjunto dos números inteiros sob a operação de adição, o conjunto dos números racionais sob a operação de adição, o conjunto dos números racionais não nulos sob a operação de multiplicação são exemplos de grupos infinitos.*

Exemplo 7.1.2. *O conjunto dos inteiros não nulos com a operação de multiplicação não é um grupo. Mas, considerando os números inteiros munido da operação subtração não é um grupo, uma vez que não existe um elemento neutro e tal que $e - x = x$, para todo $x \in \mathbb{Z}$.*

Exemplo 7.1.3. *O conjunto $\mathbb{Z}^*$ (respectivamente, $\mathbb{Q}^*$, $\mathbb{R}^*$ e $\mathbb{C}^*$) é um grupo com a operação de multiplicação usual.*

Exemplo 7.1.4. *O conjunto $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ forma um grupo com a multiplicação.*

Exemplo 7.1.5. *O conjunto $\mathbb{Q}^*$ munido com a operação de divisão ($\div$) não é um grupo, uma vez que $(48 \div 12) \div 4 = 4 \div 4 = 1 \neq 48 \div (12 \div 4) = 48 \div 3 = 16$.*

Exemplo 7.1.6. *O cojunto $G = \{-1, 1\}$ é um grupo com a operação de multiplicação.*

Exemplo 7.1.7. *O conjunto $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ com a operação multiplicação definida por $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $kj = -i$, $ik = -j$ e $ji = -k$ (ou $i^2 = j^2 = k^2 = ijk = -1$), forma um grupo, chamado grupo dos quatérnios . O grupo Q_8 também pode ser escrito como $Q_8 = \langle a, b : a^4 = e, a^2 = b^2 \text{ e } b^{-1}ab = a^3\rangle$, com $a = i$ e $b = j$.*

Exemplo 7.1.8. *O conjunto* $D_3 = \{e, \rho, \rho^2, \phi, \rho\phi, \rho^2\phi\}$, *onde* $\rho^3 = e$, $\phi^2 = e$ *e* $\phi\rho = \rho^2\phi$, *é um grupo chamado grupo diedral de ordem* 6.

Exemplo 7.1.9. *O conjunto* $D_4 = \{e, \rho, \rho^2, \rho^3, \phi, \rho\phi, \rho^2\phi, \rho^3\phi\}$, *onde* $\rho^4 = e$, $\phi^2 = e$ *e* $\phi\rho = \rho^3\phi$, *é um grupo chamado grupo diedral de ordem* 8.

Exemplo 7.1.10. *Seja* S *um conjunto não vazio. Uma permutação de* S *é uma bijeção de* S *em* S. *O conjunto* $B(S)$ *das bijeções de* S *em* S *munido da operação composição de funções é um grupo, chamado grupo das permutações de* S. *Em particular, se* $S = \{1, 2, \cdots, n\}$, *então* $B(S) = S_n$ *é um grupo chamado grupo simétrico de grau* n *(ou grupo de permutações de* n *elementos) cuja ordem é* $n!$. *Cada elemento* $\phi \in S_n$ *é chamado de permutação de* n *elementos e é representado por*

$$\phi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \phi(1) & \phi(2) & \cdots & \phi(n) \end{pmatrix}.$$

Assim, tomando $n = 5$, *segue que um elemento de* S_5 *é dado por*

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

Exemplo 7.1.11. *O conjunto* $M_n(\mathbb{A})$, *onde* $A = \mathbb{Q}$ *ou* $\mathbb{R}$, *das matrizes quadradas de ordem* n *munido com a operação de adição usual de matrizes é um grupo abeliano. Enquanto que se considerarmos* $M_n(\mathbb{R})$ *munido com a operação de multiplicação usual de matrizes não é um grupo, uma vez nem toda matriz* $A \in M_n(\mathbb{R})$ *é inversível. Agora, considrando o conjunto* $GL_n(\mathbb{A}) = \{X \in M_n(\mathbb{A}) : \det(X) \neq 0\}$ *com a operação de multiplicação usual é um grupo não comutativo, chamado grupo linear geral.*

Exemplo 7.1.12. *Se* $(G_i)_{\in I}$ *é uma família de grupos, então* $\prod_{i\in I} G_i$ *é um grupo com a operação* $(x_i)_{i\in I}(y_i)_{i\in I} = (x_i y_i)_{i\in I}$, *definida componente a componente, chamado grupo do produto direto externo dos grupos* G_i, *onde* $i \in I$. *Em particular, se* $i = 2$, *então* $G = G_1 \times G_2$ *com a operação* $(x_1, x_2) \triangle (y_1, y_2) = (x_1 * y_1, x_2 \star y_2)$, *onde* $*$ *é a operação do grupo* G_1 *e* $\star$ *é a operação do grupo* G_2, *é um grupo, onde o* (e_1, e_2) *é o elemento neutro (com* e_1 *o elemento neutro de* G_1 *e* e_2 *o elemento neutro de* G_2*) e* $(x_1, x_2)' = (x_1', x_2')$ *é o elemento simétrico do elemento* $(x_1, x_2) \in G_1 \times G_2$.

7.1.1 Exercícios

1. Mostre que os números naturais com a operação $a * b = a^b$ não é um grupo.
2. Mostre que $G = \{x \in \mathbb{R} : x \neq -1\}$ com a operação $x * y = x + y + xy$ é um grupo.
3. Mostre que S_n é um grupo comutativo se, e somente se, $\circ(S_n) = 1$ ou 2.
4. Mostre que todo grupo G tal que $\circ(G) \leq 5$ é abeliano.
5. Mostre que todo grupo G tal que $\circ(G) = p^2$, onde p é um número primo, é abeliano.
6. Se G é um grupo, mostre que:

(a) para todo $a \in G$, segue que $(a')' = a$,

(b) para todo $a, b \in G$, segue que $(ab)' = b'a'$, e

(c) se $ax = ay$ (ou $xa = ya$), então $x = y$, onde $a, x, y \in G$ (chamada lei do cancelamento).

7. Se G é um grupo abeliano, mostre que $(ab)^n = a^n b^n$, para todo $a, b \in G$ e $n \in \mathbb{N}$.

8. Seja G um grupo tal que $(ab)^2 = a^2 b^2$, para todo $a, b \in G$.

   (a) Mostre que G é um grupo abeliano.

   (b) Mostre que o resultado não vale para apenas dois inteiros consecutivos.

9. Seja G um grupo tal que $(ab)^n = a^n b^n$, para três inteiros consecutivos n, e para todo $a, b \in G$.

   (a) Mostre que G é abeliano.

   (b) Mostre que não vale para apenas dois inteiros consecutivos.

10. Se G é um grupo finito, mostre que existe $n \in \mathbb{N}$ tal que $a^n = e$ para todo $a \in G$.

11. Se todo elemento de um grupo G é seu próprio simétrico, mostre que G é abeliano.

12. Se G é um grupo de ordem par, mostre que G tem um elemento de ordem 2.

13. Seja G um conjunto finito que é fechado, associativo e que vale as leis do cancelamento. Mostre que G é um grupo.

14. Verifique se são grupos (e também grupos abelianos).

   (a) O conjunto de todos os racionais com denominador impar, com a soma usual dos racionais.

   (b) O conjunto de todos os racionais com denominador impar, com a multiplicação usual dos racionais.

   (c) $\{1, -1\}$ com a divisão.

   (d) O conjunto dos números inteiros com a subtração.

   (e) $\{2^m 3^n;\ m, n \in \mathbb{Z}\}$ com a multiplicação.

   (f) O conjunto de todas as aplicaçẽs $f : X \to G$, onde X é um conjunto e G é um grupo.

   (g) Um espaço vetorial V com a operação $+$.

   (h) O subconjunto das matrizes invertíveis de ordem $n \times n$, com a multiplicação usual de matrizes.

   (i) O conjunto de todas as funções pares com a adição de funções.

15. Seja G um grupo. Mostre que vale as leis do cancelamento (a direita e a esquerda).

16. Dado um grupo G, mostre que o elemento neutro é único. Mostre, também, que dado um elemento qualquer $a \in G$, o seu inverso é único.

17. Seja G um conjunto não vazio com uma operação binária tal que:

    (a) a operação é associativa;

    (b) existe um elemento identidade a esquerda e em G, isto é, $ex = x$, para todo $x \in G$;

    (c) para cada $a \in G$, existe um inverso a esquerda a' em G tal que $a'a = e$.

    Mostre que, e é também elemento neutro a direita e que a' é também elemento inverso a direita para cada a e conclua que tais axiomas definem G como um grupo. Veja que tais axiomas, aparentemente, parecem ser mais fracos que os de grupo, no entanto, são suficientes.

18. Prove que um conjunto não vazio G, com uma operação binária associativa tal que $ax = b$ e $ya = b$ tem soluções em G quaisquer que sejam $a, b \in G$, é um grupo.

19. Sejam $(G, *)$ e $(H, \circ)$ grupos com identidades e_G e e_H, respectivamente. Defina em $G \times H$ a operação: $(g_1, h_1) \triangle (g_2, h_2) = (g_1 * g_2, h_1 \star h_2)$.

    (a) Mostre que vale a lei associativa em $(G \times H, \triangle)$.

    (b) Determine o elemento neutro de $(G \times H, \triangle)$.

    (c) Para cada $(g, h) \in G \times H$, Determine seu inverso.

    (d) Mostre que se G e H são grupos abelianos, então $G \times H$ é um grupo abeliano.

20. Sejam G_1 e G_2 dois grupos quaisquer. Mostre que o produto cartesiano $G_1 \times G_2 = \{(x, y) : x \in G_1, y \in G_2\}$ munido com a operação componente a componente, induzida pelos grupos G_1 e G_2, é um grupo.

21. Verifique que se $(\mathbb{R}, \otimes)$ é um grupo abeliano com a operação $a \otimes b = a + b - 3$.

7.2 Adição e multiplicação modular

Seja $\mathbb{Z}_m = \{0, 1, 2, \cdots, m-1\}$, onde $m \in \mathbb{Z}$, com $m > 1$ e $r = 0, 1, \cdots, m-1$ é o resto da divisão de um número inteiro por m.

Definição 7.2.1. *(Adição módulo m) Sejam $a, b \in \mathbb{Z}_m$. A adição de a e b módulo m é definida por $a +_m b = r$, onde r é o resto da divisão euclidiana de $a + b$ por m.*

Exemplo 7.2.1. *Em $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, segue que $2 +_4 2 = 0$ e $1 +_4 3 = 0$.*

Propriedades 7.2.1. *Sejam $a, b, c \in \mathbb{Z}_m$. Em relação a operação de adição módulo m, segue as seguintes propriedades.*

1. *Associativa:* $a +_m (b +_m c) = (a +_m b) +_m c$. *De fato, se* $b +_m c = r_1$, *então* $b + c = mq + r_1$, *onde* $q, r_1 \in \mathbb{Z}$ *e* $0 \leq r_1 < m$. *Se* $a +_m r_1 = r$, *então* $a + r_1 = mq_1 + r$, *onde* $q_1, r \in \mathbb{Z}$ *e* $0 \leq r < m$. *Assim,* $b + c = mq + r_1 = mq + mq_1 + r - a$, *ou seja,* $a + b + c = m(q + q_1) + r$, *com* $0 \leq r < m$. *Logo,* r *é o resto da divisão de* $a+(b+c)$ *por* m, *ou seja,* $r = a +_m (b +_m c)$. *Analogamente,* $(a +_m b) +_m c$ *é o resto da divisão euclidiana de* $(a+b)+c$ *por* m. *Portanto,* $a +_m (b +_m c) = (a +_m b) +_m c$.

2. *Comutativa:* $a +_m b = b +_m a$. *De fato, se* $r = a +_m b$, *então* $a + b = mq + r$, *onde* $q, r \in \mathbb{Z}$ *e* $0 \leq r < m$. *Assim,* r *também é o resto da divisão de* $b + a$ *por* m, *ou seja,* $b +_m a = r$. *Portanto,* $a +_m b = b +_m a$.

3. *Elemento neutro:* $a +_m 0 = a$, *para todo* $a \in \mathbb{Z}_m$, *ou seja,* 0 *é o elemento neutro. De fato, segue diretamente do fato que* a *é o resto da divisão de* $a + 0 = a$ *por* m.

4. *Elementos simetrizáveis: Todo elemento* $a \in \mathbb{Z}_m$ *é simetrizável, ou seja, se* $a \in \mathbb{Z}_m$, *então existe* $m - a \in \mathbb{Z}_m$ *tal que* $a +_m (m - a) = 0$. *De fato, segue diretamente do fato que* 0 *é o resto da divisão de* $a + (m - a) = m$ *por* m.

Portanto, $(\mathbb{Z}_m, +_m)$, com $m > 1$, é um grupo comutativo.

Definição 7.2.2. *(Multiplicação módulo* m*) Sejam* $a, b \in \mathbb{Z}_m$. *A multiplicação de* a *e* b *módulo* m *é definida por* $a._m b = r$, *onde* r *é o resto da divisão de* ab *por* m.

Exemplo 7.2.2. *Em* $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, *segue que* $2._6 2 = 4$ *e* $2._6 3 = 0$.

Propriedades 7.2.2. *Sejam* $a, b, c \in \mathbb{Z}_m$. *Em relação a operação de multiplicação módulo* m, *segue as seguintes propriedades.*

1. *Associativa:* $a._m(b._m c) = (a._m b)._m c$. *De fato, se* $b._m c = r_1$, *então* $bc = mq + r_1$, *onde* $q, r_1 \in \mathbb{Z}$ *e* $0 \leq r_1 < m$. *Se* $a._m r_1 = r$, *então* $ar_1 = mq_1 + r$, *onde* $q_1, r \in \mathbb{Z}$ *e* $0 \leq r < m$. *Assim,* $abc = amq + ar_1 = amq + mq_1 + r$, *ou seja,* $abc = m(aq + q_1) + r$, *com* $0 \leq r < m$. *Logo,* r *é o resto da divisão de* $a(bc)$ *por* m, *ou seja,* $r = a._m(b._m c)$. *Analogamente,* $(a._m b)._m c$ *é o resto da divisão euclidiana de* $(ab)c$ *por* m. *Portanto,* $a._m(b._m c) = (a._m b)._m c$.

2. *Comutativa:* $a._m b = b._m a$. *De fato, se* $r = a._m b$, *então* $ab = mq + r$, *onde* $q, r \in \mathbb{Z}$ *e* $0 \leq r < m$. *Assim,* r *também é o resto da divisão de* ba *por* m, *ou seja,* $b._m a = r$. *Portanto,* $a._m b = b._m a$.

3. *Elemento neutro:* $a._m 1 = a$, *para todo* $a \in \mathbb{Z}_m$, *ou seja,* 1 *é o elemento neutro. De fato, segue diretamente do fato que* a *é o resto da divisão de* $a.1 = a$ *por* m.

4. *Elementos simetrizáveis:* $a \in \mathbb{Z}_m$ *é simetrizável, se e somente se,* $mdc(a, m) = 1$. *De fato, se* $a \in \mathbb{Z}_m$ *é simetrizável, então existe* $b \in \mathbb{Z}_m$ *tal que* $a._m b = 1$. *Assim,* $ab = mq + 1$, *onde* $q \in \mathbb{Z}$. *Desse modo,* $ab + m(-q) = 1$, *ou seja,* $mdc(a, m) = 1$. *Reciprocamente, se* $mdc(a, m) = 1$, *então existem* $x_0, y_0 \in \mathbb{Z}$ *tal que* $ax_0 + my_0 = 1$. *Assim,* $ax_0 = m(-y_0) + 1$, *ou seja,* 1 *é o resto da divisão de* ax_0 *por* m. *Portanto,* $a._m x_0 = 1$, *ou seja,* x_0 *é o simétrico de* a.

Portanto, $(\mathbb{Z}_p - \{0\}, .m)$, com p um número primo, é um grupo comutativo. Em geral, $\mathbb{Z}_m^*$, o conjunto dos elementos inversíveis de $\mathbb{Z}_m$, é um grupo comutativo.

Exemplo 7.2.3. *Se n não for um primo, então $\mathbb{Z}_n - \{0\} = \{1, 2, \cdots, n-1\}$ não forma um grupo multiplicativo sob a operação de multiplicação módulo n. Por exemplo, para $n = 4$, segue que $\mathbb{Z}_4 - \{0\} = \{1, 2, 3\}$ e $2 \times 2 = 0$. Mas, $\mathbb{Z}_4^* = \{1, 3\}$ forma um grupo abeliano multiplicativo. Agora, se p é um número primo, então o conjunto $\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\}$ é um grupo abelianos sob a operação de multiplicação módulo p.*

Exemplo 7.2.4. *Em relação a multiplicação, os elementos simetrizáveis de $\mathbb{Z}_6$ são $\{1, 5\}$ e os elementos simetrizávies de $\mathbb{Z}_5$ são $\{1, 2, 3, 4\}$.*

7.2.1 Exercícios

1. Em cada uma das operações abaixo faça a tábua da operação e verifique se é fechada, associativa, comutativa, tem elemento neutro, determine os elementos simetrizáveis e os elementos regulares.

   (a) $E = \{0, 1, 2, 3\}$ e $x * y$ é o resto da divisão em $\mathbb{Z}$ de $x + y$ por 4.

   (b) $E = \{1, 2, 3, 4\}$ e $x * y$ é o resto da divisão em $\mathbb{Z}$ de xy por 5.

   (c) $E = \mathbb{Z}_{24}$, onde $x * y$ é o resto da divisão de xy por 24.

2. Determine os elementos simetrizáveis e regulares de $\mathbb{Z}_6$ em relação ao produto.

3. Determine os elementos simetrizáveis e regulares de $\mathbb{Z}_{12}$ em relaç] ao ao produto.

4. Determine a ordem dos elementos de $(\mathbb{Z}_{12}, +_{12})$, $(\mathbb{Z}_7^*, .7)$ e $\mathbb{Z}_2 \times \mathbb{Z}_4$.

7.3 Subgrupos

Nesta seção, apresentamos uma estrutura algébrica que é um subconjunto não vazio de um grupo G.

Definição 7.3.1. *Sejam G um grupo e $H \subseteq G$ um subconjunto não vazio. O subconjunto H é chamado um subgrupo de G se as seguintes condições forem satisfeitas:*

1. *H é fechado em relação a operação do grupo G, isto é, para quaisquer $a, b \in H$, segue que $ab \in H$,*

2. *H é um grupo em relação a operação em H induzida por G.*

Um grupo G admite pelo menos os subgrupos G e $\{e\}$, ou seja, os chamados subgrupos triviais.

Exemplo 7.3.1. *O conjunto $\{2n : n \in \mathbb{Z}\}$, ou seja, o conjunto dos números pares é um subgrupo aditivo de $\mathbb{Z}$. O conjunto do inteiros $\mathbb{Z}$ é um subgrupo aditivo de $\mathbb{Q}$.*

Exemplo 7.3.2. *O conjunto* $S^1 = \{a+bi \in \mathbb{C} : a^2+b^2 = 1\}$ *é um subgrupo multiplicativo de* $\mathbb{C}^*$.

Exemplo 7.3.3. *O grupo linear especial* $SL_n(A) = \{M \in GL_n(A) : \det(M) = 1\}$, *onde* $A = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, *é um subgrupo de* $GL_n(A)$.

Sejam G um grupo e H um subgrupo de G.

1. Os elementos neutros de G e H são iguais. De fato, sejam e o elemento neutro de G e e_h o elemento neutro de H. Como $e_h e_h = e_h = e_h e$ e como todo elemento de G é regular, segue que $e_h = e$. Portanto, os elementos neutros de H e G são os mesmos.

2. O simétrico de um elemento $b \in H$ em H e G é único. De fato, sejam $b \in H$, b' o simétrico de b em G e b'_h o simétrico de b no subgrupo H. Assim, $b'_h b_h = e_h = e = b'b$, e deste modo, $b'_h = b'$. Portanto, o elemento inverso de b em H e em G é único.

Proposição 7.3.1. *Seja* G *um grupo. Um subconjunto não vazio* $H \subseteq G$ *é um subgrupo de* G *se, e somente se,* $a, b \in H$ *implicar que* $ab' \in H$, *onde* b' *é o simétrico de* b.

Demonstração. Suponhamos que H é um subgrupo de G. Portanto, se $a, b \in H$, então $ab'_h \in H$, ou seja, $ab' \in H$. Reciprocamente, como $H \neq \emptyset$, segue que existe $a \in H$ com $a \neq e$. Por hipótese, segue que $e = aa^{-1} \in H$. Dado $b \in H$, usando a hipótese e o fato de que $e \in H$, segue que $eb' = b' \in H$. Desse modo, se $a, b \in H$, então $b' \in H$, e assim, $a(b')' = ab \in H$ em consequência da hipótese, ou seja, H é fechado. Por último, se $a, b, c \in H$, então $a, b, c, \in G$, e portanto, $(ab)c = a(bc)$, ou seja, é associativa. □

Exemplo 7.3.4. *Consideremos o grupo aditivo dos reais* $(\mathbb{R}^\star, +)$. *O conjunto* $\mathbb{Z}$ *dos inteiros é um subgrupo de* $\mathbb{R}$ *uma vez que se* $a, b \in \mathbb{Z}$, *então* $a + (-b) = a - b \in \mathbb{Z}$.

7.3.1 Exercícios

1. Se $(H_i)_{i\in I}$ é uma família de subgrupos de um grupo G, mostre que $H = \cap_{i\in I} H_i$ é um subgrupo de G.

2. Sejam G um grupo, H e K subgrupos de G.

   (a) Mostre que $H \cup K$ é um subgrupo de G se, e somente se, $H \subseteq K$ ou $K \subseteq H$.

   (b) Dê um exemplo onde $H \cup K$ não é um subgrupo de G.

3. Sejam $S \subseteq G$ um subconjunto não vazio de um grupo e $(H_i)_{i\in I}$ a família de todos os subgrupos de G que contém S. Mostre que $\langle S\rangle = \cap_{i\in I} H_i$ é o menor (em relação a inclusão) subgrupo de G que contém S, chamado *subgrupo gerado por* S e o conjunto S é chamado *sistema de geradores do subgrupo* $\langle S\rangle$.

4. Sejam G um grupo e $Z(G) = \{g \in G; gx = xg, \text{ para todo } x \in G\}$.

   (a) Mostre $Z(G)$ é um subgrupo de G, chamado centro de G.

(b) Determine o centro do grupo $M_2(\mathbb{R})$.

(c) Determine o centro de S_3.

(d) Mostre que um grupo G é abeliano se, e somente se, $Z(G) = G$.

5. Sejam G um grupo e $a \in G$.

(a) Mostre que $N_G(a) = \{ag = ga : g \in G\}$ é um subgrupo de G, chamado normalizador de a em G.

(b) Mostre que $Z(G)$ é um subgrupo de $N_G(a)$.

(c) Mostre que G é abeliano se, e somente se, $G = N_G(a)$, para todo $a \in G$.

6. Se G é um grupo e H é um subgrupo de G, mostre que $gHg^{-1} = \{ghg^{-1} : h \in H\}$, onde $g \in G$, é um subgrupo de G.

7. Seja G o conjunto de todas as funções $f : \mathbb{R} \to \mathbb{R}$. Nos itens abaixo, verifique se os subconjuntos com a operação induzida é um subgrupo do grupo G com respeito a adição e com respeito a multiplicação.

(a) O subconjunto $H = \{f \in G : f(x) = 0\}$.

(b) O subconjunto de todas as funções $f \in G$ F tal que $f(1) = 0$.

(c) O subconjunto de todas as funções $f \in G$ tal que $f(1) = 1$.

(d) O subconjunto de todas as funções $f \in G$ tal que $f(0) = 1$.

(e) O subconjunto de todas as funções $f \in G$ tal que $f(0) = -1$.

(f) O subconjunto de todas as funções constantes de G.

8. Se G é um grupo abeliano com elemento identidade e, mostre $H = \{x \in G : x^2 = e\}$ é um subgrupo de G.

9. Seja G um grupo.

(a) Mostre que os elementos neutros de G e H são iguais.

(b) Seja $x \in H$. Se $x' \in H$ e $x'' \in G$ são simétricos de x, mostre que $x' = x''$.

(c) Mostre que se $x, y \in H$, então $xy \in H$.

10. Sejam G_1, G_2 e $G_1 \times G_2 = \{(x, y) : x \in G_1, y \in G_2\}$ o produto cartesiano dos grupos G_1 e G_2. Mostre que $G_1 \times G_2$ munido com a operação componente a componente, induzida pelos grupos G_1 e G_2, é um grupo.

11. Seja G um grupo.

(a) Se $a \in G$, mostre que $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ é um subgrupo de G.

(b) Seja $H \subseteq G$ um subgrupo. Se $a \in H$, mostre que $< a > \subseteq H$.

(c) Mostre que todo subgrupo H de $\mathbb{Z}$ é do tipo $H = [m]$, para algum $m \in \mathbb{Z}$.

(d) Sejam G um grupo e $a \in G$ tal que $\circ(a) = h$. Mostre que $a^m = e$ se, e somente se, h divide m.

12. Sejam G um grupo e $a \in G$ tal que $\circ(a) = n$.

(a) Mostre que $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.

(b) Mostre que $\circ(\langle a \rangle) = n$.

13. Mostre que:

(a) $H = \{a + bi : a, b \in \mathbb{R}\}$ é um subgrupo de $\mathbb{C}$ com a operação de adição.

(b) $H = \{a + bi \in \mathbb{C}^* : a, b \in \mathbb{R}\}$ é um subgrupo de $\mathbb{C}^*$ com a operação de multiplicação.

7.4 Grupos cíclicos

Sejam G um grupo, $a \in G$ e $n \in \mathbb{Z}$. A potência n-ésima de a é um elemento de G denotado por a^n e definida por:

1. $a^0 = e$, onde e é o elemento neutro de G.
2. $a^n = a^{n-1}a$ se $n \geq 1$.
3. $a^n = (a^{-n})^{-1}$ se $n < 0$.

Proposição 7.4.1. *Seja G um grupo. Se $a \in G$, então $H =< a >= \{a^m : m \in \mathbb{Z}\}$ é um subgrupo de G.*

Demonstração. Como $a^0 = e$, segue que $e \in H$. Por outro lado, se $x, y \in H$, então existem $m, n \in \mathbb{Z}$ de maneira que $x = a^m$ e $y = a^n$. Assim, $xy^{-1} = a^m a^{-n} = a^{m-n} \in H$. Portanto, H é um subgrupo de G. □

Definição 7.4.1. *Sejam G um grupo, $a \in G$ um elemento e $H =< a >= \{a^m : m \in \mathbb{Z}\}$.*

1. *O subgrupo $H =< a >$ de G é chamado subgrupo gerado por a e o elemento a é chamado o gerador de H.*
2. *Se $a^m \neq e$, para todo $m \in \mathbb{Z}$, então H é infinito.*
3. *Se $a^m = e$, para algum $m \in \mathbb{Z}$, então H é finito e o menor h positivo tal que $a^h = e$ é chamado a ordem de a e denotado por $\circ(a)$.*
4. *Um grupo G é chamado um grupo finito, se o número de elementos de G é finito e denotado por $\circ(G)$.*

Definição 7.4.2. *Um grupo G é chamado um grupo cíclico se existe um elemento $a \in G$ de maneira que $G = \langle a \rangle$. Neste caso, o elemento a é chamado de gerador de G.*

Observação 7.4.1. *Sejam G um grupo, $a \in G$, $m, n \in \mathbb{Z}$.*

1. *Se G é um grupo cíclico, então G é abeliano, uma vez que $a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$. Mas, a recíproca é falsa, ou seja, $\mathbb{Z}_2 \times \mathbb{Z}_2$ é um grupo abeliano mas não é cíclico.*

2. *Um mesmo grupo cíclico pode conter mais do que um gerador, por exemplo, o conjunto $G = \{1, -1, i, -1\}$ é um grupo multiplicativo cíclico com geradores i e $-i$.*

3. *Se G é um grupo aditivo cíclico gerado por a, então $G = \{ma : m \in \mathbb{Z}\}$.*

Exemplo 7.4.1. *O grupo multiplicativo $G = \{1, -1\}$ é cíclico, uma vez que $\{(-1)^m : m \in \mathbb{Z}\} = \{1, -1\} = G$.*

O grupo aditivo dos inteiros $\mathbb{Z}$ é um grupo cíclico gerado pelo número 1 ou -1.

Exemplo 7.4.2. *O grupo $\mathbb{Z}_n$, com $n > 0$, é cíclico gerado por $\overline{1}$. Em geral, $\mathbb{Z}_n = \langle k \rangle$ se, e somente se, $mdc(k, n) = 1$. Assim, $\mathbb{Z}_n$ possui $\phi(n)$ geradores distintos, onde ϕ é a função de Euler.*

Proposição 7.4.2. *Sejam G um grupo e $H \subseteq G$ um subgrupo. Se G é cíclico, então H é cíclico.*

Demonstração. Por hipótese, existe $a \in G$ tal que $G = \langle a \rangle$. Se $H = \{e\}$, então H é cíclico. Se $x \in H \subseteq G$, então $x = a^m \in H$ para algum $m \in \mathbb{Z}$. Seja $m_0 > 0$ o menor inteiro tal que $a^{m_0} \in H$. Claramente, $\langle a^{m_0} \rangle \subseteq H$. Agora, se $x \in H$, então $x = a^m$ para algum $m \in \mathbb{Z}$. Pelo algoritmo da divisão, segue que existem $q, r \in \mathbb{Z}$ únicos tal que $m = m_0 q + r$, onde $0 \leq r < m$. Assim, $x = a^m = a^{m_0 q + r} = a^{m_0 q} a^r$, e deste modo, $a^r = a^{-m_0 q} x \in H$. Pela minimalidade de m_0, segue que $r = 0$. Portanto, $x \in \langle a^{m_0} \rangle$. Assim, $H = \langle a^{m_0} \rangle$, ou seja, H é cíclico. □

Seja G um grupo finito cuja a ordem é pelo menos 2 e cujo elemento identidade é denotado por e. Se $h \neq e$ é um de seus elementos, então $H = \{h, h^2, h^3, \cdots\}$. Mas, esta sequência de elementos é finita uma vez que a ordem de G é finita. O primeiro elemento a se repetir deve ser o próprio h, uma vez que, se $h^i = h^j$ para $i \leq j$, então $h^{i-1} = h^{j-1}$. O elemento identidade deve estar em H, uma vez que se $h = h^k$, então $e = h^{k-1}$. Portanto, $H = \langle h \rangle$ é um subgrupo cíclico de G gerado por h.

Sejam G um grupo e $S = \{a_1, a_2, \cdots, a_n\} \subseteq G$ um subconjunto. O conjunto

$$[S] = [a_1, a_2, \cdots, a_n] = \{a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n} : k_i \in \mathbb{Z}, \text{ para } i = 1, 2, \ldots, n\}$$

é o menor subgrupo de G que contém S, onde o conjunto S é chamado conjunto de geradores do subgrupo $[S]$. Em particular, se $a \in G$, o subgrupo $[a]$ é chamado *subgrupo de G gerado por a*. O subgrupo $[S] \subseteq G$ é chamado *subgrupo de tipo finito* gerado por S, e o grupo G é chamado do tipo finito se $G = [S]$, para algum $S = \{a_1, a_2, \cdots, a_n\} \subseteq G$. Em particular, se $G = [a]$ para algum $a \in G$, o grupo G é chamado um *grupo cíclico* e a é chamado o gerador. Em geral, se $S \subseteq G$ é um subconjunto qualquer, então

$$[S] = \{a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n} : k_i \in \mathbb{Z}, \ a_1, a_2, \ldots, a_n \in S, \text{para } i = 1, 2, \ldots, n\}$$

é o menor subgrupo de G que contém S, onde o conjunto S é chamado conjunto de geradores do subgrupo $[S]$.

7.4.1 Exercícios

1. Mostre que:
   (a) Todo grupo de ordem 2 ou 3 é cíclico.
   (b) Todo grupo cíclico infinito tem dois e somente dois geradores.
   (c) Todo grupo cíclico é abeliano.
2. Se um subgrupo cíclico H de G é normal em G, mostre que todo subgrupo de H é normal em G.
3. Seja G um grupo. Se $m, n \in \mathbb{Z}$ e $a \in G$, mostre que
   (a) $a^m a^n = a^{m+n}$.
   (b) $a^{-m} = (a^m)^{-1}$.
   (c) $(a^m)^n = a^{mn}$.
4. Sejam G um grupo e $a \in G$.
   (a) Mostre que $\langle a \rangle$ é um subgrupo de G.
   (b) Se H é um subgrupo de G e $a \in H$, mostre que $\langle a \rangle \subseteq H$.
5. Determine todos os grupos de ordem 4.
6. Mostre que $(\mathbb{Z}_n, +)$ é cíclico.
7. Determinar o número de geradores de um grupo cíclico de ordem n.
8. Seja G um grupo abeliano finito. Se o número de soluções em G da equação $x^n = e$ é no máximo n, para todo $n \in \mathbb{N}$, mostre que G é cíclico.
9. Sejam G um grupo e $Z(G)$ o seu centro.
   (a) Se $G/Z(G)$ é um grupo cíclico, mostre que G é abeliano.
   (b) Mostre que $Z(S_3) = \{e\}$.
10. Seja G um grupo. Se $a \in G$, mostre que $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.
11. Seja $H \subseteq G$ um subgrupo. Se $a \in H$, mostre que $\langle a \rangle \subseteq H$.
12. Seja G um grupo. Se $a \in G$ é tal que $\circ(a) = h$, mostre que $a^m = e$ se, e somente se, h divide m.
13. Mostre que

(a) todo grupo cíclico é abeliano,

(b) todo subgrupo de um grupo cíclico é cíclico, e

(c) todo subgrupo H de $\mathbb{Z}$ é do tipo $H = \langle m \rangle$, para algum $m \in \mathbb{Z}$.

14. Se H é um subconjunto finito não vazio de um grupo G que é fechado em relação a operação do grupo, mostre que H é um subgrupo de G.

15. Sejam G um grupo e $a \in G$. Se $a^m = e$, mostre que $\circ(a) \mid m$.

Capítulo

8

Teorema de Lagrange

O Teorema de Lagrange, aplicado na teoria dos grupos, é um resultado importante da matemática que diz que se G é um grupo finito e H é subgrupo de G, então a ordem (quantidade de elementos) de H divide a ordem de G. O o matemático e físico Joseph Louis Lagrange nasceu em 25 de janeiro de 1736 na cidade de Turim (Itália), sendo considerado um dos matemáticos mais importantes do final do século XVIII, ao lado de Euler. Em 1795 Lagrange foi indicado para ser professor na Escola de Artilharia Real em Turim, no qual dois anos mais tarde contribuiu para a fundação da Academia Real de Ciência. Por volta de 1766 Lagrange foi convidado para substituir Euler na direção da seção matemática na Academia de Ciência de Berlim, onde permaneceu durante 20 anos. Em 1787 Lagrange tornou-se membro da Academia de Ciência de Paris onde ficou até final de sua carreira. Lagrange apresentou significativas contribuições para teoria das funções, teoria dos números, equações diferenciais, cálculo de probabilidades, dentre outras. Deste modo, no presente capítulo, apresentamos as classes laterais a direita e a esquerda, em seguida apresentamos o Teorema de Lagrange juntamente com suas principais consequências, e fiinalmente, apresentamos os subgrupos normais e o grupo quociente.

8.1 Classes laterais

Nesta seção, apresentamos as classes laterais de um subgrupo H em relação a um grupo G. Assim, dados dois subconjuntos A e B de um grupo G, usamos a notação AB para indicar o conjunto $AB = \{ab : a \in A,\ b \in B\}$ e usamos a notação A^{-1} para indicar o conjunto $A^{-1} = \{a^{-1} : a \in A\}$, onde a^{-1} é o elemento simétrico de a. Assim, $(AB)C = A(BC)$ e $(AB)^{-1} = B^{-1}A^{-1}$. Quando $A = \{a\}$, usamos simplesmente aB. Além disso,

1. $xA = yB$ se, e somente se, $y^{-1}xA = B$.

2. H é um subgrupo de G se, e somente se, $HH = H$ e $H^{-1} = H$.

3. Seja H um subgrupo de G. Assim, $xH = H$ se, e somente se, $x \in H$ se, e somente se, $Hx = H$.

Definição 8.1.1. *Seja H um subgrupo de G. Se $a, b \in G$, o elemento a é dito congruente a b módulo H se $ab^{-1} \in H$, e denotado por $a \equiv b(mod\ H)$.*

A relação da Definição 8.1.1 é uma relação de equivalência. Se $a \in G$, então sua classe de equivalência, denotada por $\overline{a}$, é dada por $\overline{a} = \{b \in G : a \equiv b(mod\ H)\}$.

Definição 8.1.2. *Dado $a \in G$ indicamos por aH (respectivamente, por Ha) e chamamos de classe lateral à esquerda (respectivamente, à direita), módulo H, definida por a, o seguinte subconjunto $aH = \{ax : x \in H\}$ (respectivamente, $Ha = \{xa : x \in H\}$).*

Exemplo 8.1.1. *Sejam o grupo aditivo $G = \mathbb{Z}_6$ e seu subgrupo $H = \{0, 3\}$. Segue que*

$$\overline{0} + H = \{\overline{0} + \overline{0},\ \overline{0} + \overline{3}\} = \{\overline{0},\ \overline{3}\} = H + \overline{0}, \quad \overline{1} + H = \{\overline{1} + \overline{0},\ \overline{1} + \overline{3}\} = \{\overline{1},\ \overline{4}\} = H + \overline{1},$$
$$\overline{2} + H = \{\overline{2} + \overline{0},\ \overline{2} + \overline{3}\} = \{\overline{2},\ \overline{5}\} = H + \overline{2}, \quad \overline{3} + H = \{\overline{3} + \overline{0},\ \overline{3} + \overline{3}\} = \{\overline{3},\ \overline{0}\} = H + \overline{3},$$
$$\overline{4} + H = \{\overline{4} + \overline{0},\ \overline{4} + \overline{3}\} = \{\overline{4}, \overline{1}\} = H + \overline{4}, \quad \overline{5} + H = \{\overline{5} + \overline{0},\ \overline{5} + \overline{3}\} = \{\overline{5},\ \overline{2}\} = H + \overline{5}.$$

Nos resultados a seguir, sem perda de generalidade, usamos a notação multiplicativa para indicar a lei de composição interna de um grupo. Trabalhamos, ademais, com classes laterais à esquerda, uma vez que as demonstrações são análogas com classes laterais à direita. Para isso, sejam G um grupo (que consideramos a operação multiplicativa) e H um subgrupo de G.

Proposição 8.1.1. *A união de todas as classes laterais módulo H é igual a G.*

Demonstração. Se e é o elemento neutro de G, então $e \in H$ e cada elemento $a \in G$ pertence à classe aH pois $a = ae$, o que prova o resultado. □

Proposição 8.1.2. *Se $a, b \in G$, então $aH = bH$ se, e somente se, $a^{-1}b \in H$.*

Demonstração. Pela Proposição 8.1.1, segue que $a \in aH$. Como $aH = bH$, segue que $a \in bH$. Logo, existe $h \in H$ de modo que $a = bh$, o que implica que $a^{-1}b = h^{-1} \in H$. Reciprocamente, se $a^{-1}b \in H$, então existe $h \in H$ tal que $a^{-1}b = h$, ou seja, $a = bh^{-1}$. Se $y \in aH$, então $y = ah_1$, onde h_1 é um elemento conveniente de H. Assim, $y = ah_1 = (bh^{-1})h_1 = b(h^{-1}h_1)$, o que mostra que $y \in bH$. Logo, $aH \subset bH$. De modo análogo, segue que $bH \subset aH$. Portanto, $aH = bH$. □

Proposição 8.1.3. *Se aH e bH são duas classes laterais módulo H, onde $a, b \in G$, então $aH \cap bH = \emptyset$ ou $aH = bH$.*

Demonstração. Se existe $x \in aH \cap bH$, então $x \in aH$ e $x \in bH$. Logo, existem $h_1, h_2 \in H$ de forma que $x = ah_1 = bh_2$. Assim, $a^{-1}b = h_1h_2^{-1} \in H$. Pela Proposição 8.1.2, segue que $aH = bH$. □

Proposição 8.1.4. *Se $a \in H$, então a classe lateral aH é equipotente a H, ou seja, aH e H possuem o mesmo número de de elementos.*

Demonstração. A aplicação $f : H \to aH$ definida por $f(h) = ah$, onde $h \in H$, é uma bijeção, uma vez que se $f(h_1) = f(h_2)$, então $ah_1 = ah_2$, e portanto, $h_1 = h_2$, ou seja f é injetora. Para a sobrejetora, se $ah \in aH$ então ah é a imagem de h pela aplicação f. Portanto, f é bijetora, ou seja, aH e H são equipotentes. □

Observação 8.1.1. *Sejam G um grupo e $H \subseteq G$ um subgrupo.*

1. *Se $a \in G$, então $aH \neq \emptyset$. Se $a, b \in G$, mostre que $aH = bH$ ou $aH \cap bH = \emptyset$.*
2. *Se G é comutativo e $a \in G$, então $aH = Ha$.*
3. *A aplicação $f : aH \to Ha^{-1}$ definida por $f(ah) = ha^{-1}$, para todo $a \in G$, é uma bijeção.*
4. *Duas classes laterais tem a mesma cardinalidade, ou seja que a aplicação $f : aH \to bH$, definida por $f(ah) = bh$, para todo $h \in H$, é uma bijeção, com $b \in G$.*

Assim, podemos afirmar que o conjunto das classes laterais à esquerda, módulo H, forma uma partição em G, com a peculiaridade de que aqui as classes são conjuntos equipotentes. Como existe uma bijeção entre aH e Ha^{-1}, segue que o conjunto das classes laterais à esquerda é equipotente ao conjunto das classes laterais à direita.

Se G é um grupo comutativo, então $aH = Ha$ para todo $a \in G$. O conjunto quociente de G, denotado por G/H, é o conjunto das classes laterais aH, com $a \in G$, ou seja, o conjunto $G/H = \{aH : a \in G\}$. O número de elementos de G/H é chamado de índice de H em G, e denotado por $[G : H]$, que é o mesmo para as classes laterais à esquerda e à direita.

Definição 8.1.3. *O conjunto quociente de G por H, denotado por G/H, é o conjunto das classes laterais à esquerda aH, com $a \in G$, ou seja, $G/H = \{aH : a \in G\}$. O número de elementos de G/H é chamado de índice de H em G, e denotado por $[G : H]$, que é o mesmo para as classes laterais à esquerda e à direita.*

Exemplo 8.1.2. *Sejam o grupo aditivo $\mathbb{Z}_6$ e o subgrupo $H = \{0, 2, 4\}$. As classes módulo H, à esquerda ou á direita (pois G é comutativo), são*

$$H = 0 + H = \{0, 2, 4\} \quad e \quad 1 + H = \{1, 3, 5\},$$

uma vez que as demais coincidem com uma dessas. Assim, a partição de $\mathbb{Z}_6$, neste caso, é dada por duas classes, cada uma com 3 elementos. Logo, $[\mathbb{Z}_6 : H] = 2$. Neste caso, o conjunto quociente é dado por $G/H = \{0 + H, 1 + H\}$ e o índice $[\mathbb{Z}_6 : H] = 2$.

Exemplo 8.1.3. *Considere o conjunto dos números inteiros $\mathbb{Z}$ sob a operação adição usual. O conjunto $4\mathbb{Z} = \{4n : n \in \mathbb{Z}\}$ forma um subgrupo de $\mathbb{Z}$. As classes laterais de $4\mathbb{Z}$ em $\mathbb{Z}$ são dadas por:*

$$\overline{0} = 0 + 4\mathbb{Z} = \{\cdots, -12, -8, -4, 0, 4, 8, 12, \cdots\},$$
$$\overline{1} = 1 + 4\mathbb{Z} = \{\cdots, -11, -7, -3, 1, 5, 9, 13, \cdots\},$$
$$\overline{2} = 2 + 4\mathbb{Z} = \{\cdots, -10, -6, -2, 2, 6, 10, 4, \cdots\} \text{ e}$$
$$\overline{3} = 3 + 4\mathbb{Z} = \{\cdots, -9, -5, -1, 3, 7, 11, 15, \cdots\}.$$

Neste caso, o conjunto quociente é dado por $G/H = \{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$ *e o índice* $[\mathbb{Z} : 4\mathbb{Z}] = 4$.

8.1.1 Exercícios

1. Sejam o grupo $\mathbb{Z}$ e o subgrupo $2\mathbb{Z}$.
   (a) Determine as classes lateriais de $2\mathbb{Z}$ em $\mathbb{Z}$.
   (b) Determine o índice $[\mathbb{Z} : 2\mathbb{Z}]$.
2. Sejam o grupo $\mathbb{Z}_8$ e o subgrupo $4\mathbb{Z}_8$.
   (a) Determine as classes lateriais de $4\mathbb{Z}_8$ em $\mathbb{Z}_8$.
   (b) Determine o índice $[\mathbb{Z}_8 : 4\mathbb{Z}_8]$.
3. Sejam o grupo $\mathbb{Q}$ e o subgrupo $\mathbb{Z}$.
   (a) Determine as classes lateriais de $\mathbb{Z}$ em $\mathbb{Q}$.
   (b) Determine o índice $[\mathbb{Q} : \mathbb{Z}]$.
4. Sejam o grupo $GL_n(A)$ e o subgrupo $SL_n(G) = \{M \in GL_n(A) : \det(M) = 1\}$, onde $A = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.
   (a) Determine as classes lateriais de $SL_n(A)$ em $GL_n(A)$.
   (b) Determine o índice $[GL_n(A) : SL_n(A)]$.
5. Sejam G um grupo, H um subgrupo de G e $a, b \in G$.
   (a) Mostre que a relação $a \equiv b(mod\ H)$ se, e somente se, $a^{-1}b \in H$ é uma relação de equivalência.
   (b) Determine $\overline{a}$, onde $a \in G$.
6. Sejam G um grupo, $H \subseteq G$ um subgrupo e $a \in G$.
   (a) Mostre que $aH = \{x \in G : a \equiv x(mod\ H)\}$.
   (b) Mostre que $aH \neq \emptyset$.
   (c) Se G é comutativo e $a \in G$, mostre que $aH = Ha$.
   (d) Mostre que a aplicação $f : aH \to Ha^{-1}$ definida por $f(ah) = ha^{-1}$, onde $a \in G$, é uma bijeção.

(e) Mostre que duas classes laterais tem a mesma cardinalidade, ou seja, que a aplicação $f : aH \to bH$, definida por $f(ah) = bh$, para todo $h \in H$, é uma bijeção, com $b \in G$.

(f) Mostre que H e aH são equipotentes.

(g) Mostre que a união de todas as classes laterais módulo H é igual a G.

7. Sejam G um grupo e H um subgrupo de G. Mostre que existe uma bijeção entre os conjunto das classes laterais a esquerda de H em G e o conjunto das classes laterais a direita de H em G.

8. Se G é um grupo, H e K são subgrupos de G de índices finitos em G, mostre que $H \cap K$ é de índice finito em G.

9. Sejam G um grupo finito, K um subgrupo de H e H um subgrupo de G. Mostre que $[G : K] = [G : H][H : K]$

8.2 Teorema de Lagrange

Nesta seção, apresentamos um famoso teorema, chamado Teorema de Lagrange , juntamente com suas principais propriedades. Esse teorema foi enunciado por Lagrange e sómente foi demonstrado 30 anos depois por Pietro Abbati (1768-1842). Esse teorema estuda a ordem de um grupo e através dele podemos simplificar algumas demonstrações de outros resultados que levaram vários anos para serem provados, como é o caso do Pequeno Teorema de Fermat que veremos mais adiante. A recíproca do Teorema de Lagrange nem sempre é válida, ou seja, se um número inteiro positivo m divide a ordem de um grupo G, não necessariamente existe um subgrupo de G com ordem m, onde os Teoremas de Cauchy e os Teoremas de Sylow apresentam uma resposta para esse caso.

Teorema 8.2.1. *(Lagrange) Se H é um subgrupo de um grupo finito de G, então $\circ(H)$ divide $\circ(G)$, ou seja, $\circ(G) = \circ(H)[G : H]$.*

Demonstração. Seja $[G : H] = r$. Se $\{a_1H, \cdots, a_rH\}$ é o conjunto das classes laterais à esquerda, módulo H, então $a_1H \cup \cdots \cup a_rH = G$. Como cada elemento de G pertence a uma e somente uma dessas classes e como o número de elementos de cada classe é $\circ(H)$, segue que $r \circ (H) = \circ(G)$, o que prova o teorema. □

Corolário 8.2.1. *Se $a \in G$ e $H = \langle a \rangle$, então a ordem de a divide a ordem de G e o quociente nessa divisão é $[G : H]$.*

Demonstração. Como $\circ(a) = \circ(H)$, pelo Teorema de Lagrange 8.2.1, segue que $\circ(G) = \circ(H)[G : H]$. □

Corolário 8.2.2. *Se $a \in G$, então $a^{\circ(G)} = e$.*

Demonstração. Se $H = \langle a \rangle$, então $\circ(G) = \circ(H)[G : H] = \circ(a)[G : H]$. Mas, como $a^{\circ(a)} = e$, segue que $a^{\circ(G)} = (a^{\circ(a)})^{[G:H]} = e^{[G:H]} = e$. □

Corolário 8.2.3. *Se G é um grupo finito cuja ordem é um número primo p, então G é cíclico e seus únicos subgrupos são os triviais, ou seja, G e $\{e\}$.*

Demonstração. Como $p > 1$, segue que existe $a \in G$ tal que $a \neq e$. Assim, $H = \langle a \rangle$ é um subgrupo de G de ordem no mínimo igual a 2. Logo, H possui e e a pelo menos. Como $\circ(H) \mid \circ(G)$ e $\circ(G)$ é um número primo, segue que $\circ(H) = p$. Assim, $H = G$ e, portanto, G é cíclico. Por outro lado, como os subgrupos de G devem ter ordem 1 ou p (devido ao Teorema de Lagrange), podemos afirmar que G possui apenas os subgrupos triviais. □

Observação 8.2.1. *O Teorema de Lagrange ajuda na determinação dos subgrupos de um grupo finito. Por exemplo, em S_3 os únicos subgrupos tem ordem $1, 2, 3, 6$. Os de ordem 1 e 6 são os triviais, e os de ordem 2 e 3 são cíclicos, uma vez que tem ordem prima.*

8.2.1 Exercícios

1. (Euler) Sejam n é um inteiro positivo e $a \in \mathbb{Z}$. Se $mdc(a, m) = 1$, mostre que $a^{\varphi(n)} \equiv 1(mod\ n)$.

2. (Fermat) Se p é um número primo e a é um inteiro, mostre que $a^p \equiv a(mod\ p)$.

3. Se G é um grupo de ordem par, mostre que G um número impar de elementos de ordem 2.

4. Seja H um subgrupo de um grupo G. Se $[G : H] = 2$, mostre que $a^2 \in H$, para todo $a \in G$.

5. Seja G um grupo. Se $a, b \in G$ comutam e $a^m = b^n = e$, mostre que $(ab)^k = e$, onde $k = mmc(m, n)$.

6. Sejam $G = M_2(\mathbb{Q})$ e $A, B \in G$ dadas por $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ e $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$. Mostre que $A^4 = B^3 = I$ e AB tem ordem infinita.

7. Sejam G um grupo e $a \in G$. Se a tem ordem $n = mk$, onde $m, k \geq 1$, mostre que a^k tem ordem m.

8.3 Grupo quociente

Nesta seção, apresentamos um subgrupo especial de um grupo G, onde será possível definir a estrutura de um grupo quociente.

Definição 8.3.1. *Seja H um subgrupo de um grupo G. O subgrupo H é um subgrupo normal de G se $aHbH = abH$ para todo $a, b \in G$, cuja notação é dada por $H \triangleleft G$.*

Exemplo 8.3.1. *Seja G um grupo. O conjunto $Z(G) = \{x \in G : xa = ax,\ para\ todo\ a \in G\}$, chamado centro de G, é um subgrupo normal de G, uma vez que $Z(G)$ é um subgrupo de G,*

pois $e \in Z(G)$, pois $ea = a = ae$, para todo $a \in G$. Se $x, y \in Z(G)$, então $a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$, para todo $a \in G$. Portanto, $xy \in Z(G)$. Agora, se $x \in G$ e $a \in G$, então $ax^{-1} = (xa^{-1})^{-1} = (a^{-1}x)^{-1} = x^{-1}a$, para todo $a \in G$. Portanto, $x^{-1} \in Z(G)$. Logo, $Z(G)$ é um subgrupo de G. Finalmente, mostremos que $Z(G) \triangleleft G$. Se $a \in G$ e $x \in Z(G)$, então $axa^{-1} = xaa^{-1} = x \in Z(G)$. Portanto, $Z(G) \triangleleft G$. Note que G é abeliano se, e somente se, $G = Z(G)$.

Sejam G um grupo e $H \subseteq G$ um subgrupo normal. As seguintes propriedades são verdadeiras, para todo $a, b \in G$,

1. $(aH)(bH) = abH$,
2. $[(aH)(bH)](cH) = (aH)[(bH)(cH)]$,
3. $(aN)(eH) = (eH)(aH)$,
4. $(aH)(a^{-1}H) = eH = (Ha)(Ha^{-1})$.

Assim, $G/H = \{aH : a \in G\}$ é um grupo chamado *grupo quociente* de G por H.

Proposição 8.3.1. *Sejam G um grupo e $H \subseteq G$ um subgrupo. Se G é cíclico, então G/H é cíclico.*

Demonstração. Por hipótese, existe $a \in G$ tal que $G = \langle a \rangle$. Se $H = \{e\}$, então $G/H = G$ é cíclico. Se $H \neq \{e\}$, então $a^m H \in G/H$, para todo $m \in \mathbb{Z}$, ou seja, $\langle aH \rangle \subseteq G/H$. Agora, se $x \in G/H$, então $x = a^m H$, para algum $m \in \mathbb{Z}$. Assim, $x \in \langle aH \rangle$, ou seja, $G/H \subseteq \langle aH \rangle$. Portanto, $G/H = \{a^m H : m \in \mathbb{Z}\}$, ou seja, G/H é cíclico. □

8.3.1 Exercícios

1. Sejam G um grupo e H um subgrupo de G.
   (a) Se G é abeliano, mostre que H é um subgrupo normal de G.
   (b) Mostre, através de um exemplo, que a recíproca é falsa.
   (c) Se $[G : H] = 2$, mostre que H é um subgrupo normal de G.
   (d) Se H é um subgrupo normal de G, mostre que $(aH)(bH) = abH$, para todo $a, b \in G$.
   (e) Mostre que H é um subgrupo normal de G se, e somente se, $a^{-1}Ha = H$, para todo $a \in G$.
2. Sejam H_1 e H_2 subgrupos de um grupo G.
   (a) Se H_1 e H_2 são subgrupos normais de G, mostre que $H_1 \cap H_2$ é um subgrupo normal de G.
   (b) Se H_1 é um subgrupo normal de G e H_2 é um subgrupo de G, mostre que $H_1 \cap H_2$ é um subgrupo normal de H_2.

3. Se G é um grupo finito e possui um único subgrupo H de cada ordem, mostre que todos os subgrupos de G são normais.

4. Mostre que todo subgrupo $H \neq \{e\}$ de um grupo infinito é infinito.

5. Se G é um grupo finito e possui um único subgrupo H de cada ordem, mostre que todos os subgrupos de G são normais.

6. Sejam G um grupo e $H \subseteq G$ um subgrupo. Mostre que as seguintes condições são equivalentes.

   (a) H é um subgrupo normal de G.

   (b) $aHa^{-1} = H$ para todo $a \in G$.

   (c) $aHa^{-1} \subset H$ para todo $a \in G$.

   (d) $aha^{-1} \in H$ para todo $a \in G$ e $h \in H$.

   (e) $HaHb = Hab$, para todo $a, b \in H$.

7. Seja G um grupo. Se H e K são dois subgrupos normais de G tal que $H \cap K = \{e\}$, mostre que se $a \in H$ e $b \in K$, então $ab = ba$.

8. Sejam G um grupo e H um subgrupo normal de G. Se $g \in G$, mostre que a ordem de gH em G/H é um divisor de $\circ(g)$.

9. Se G é um grupo abeliano e H é um subgrupo de G, mostre que G/H é um grupo abeliano.

Capítulo

9

Isomorfismo de grupos

Um homomorfismo de grupos é uma função entre dois grupos que preserva as operações binárias, ou seja, um homomorfismo é uma aplicação que têm como domínio e contradomínio estruturas algébricas de mesma natureza (mesma definição abstrata) e servem em geral para comparar tais estruturas. Deste modo, neste capítulo, apresentamos o conceito e propriedades de homomorfismo de grupos, os teoremas de isomorfismos de grupos e suas consequências, o conceito de automorfismos de grupos e suas principais prorpriedades.

9.1 Homomorfismo de grupos

Nesta seção, apresentamos o conceito de homomorfismos de grupos juntamente com suas principais propriedades.

Definição 9.1.1. *Sejam G_1 e G_2 dois grupos e $f : G_1 \to G_2$ uma aplicação. A aplicação f é chamada um homomorfismo de grupos se $f(xy) = f(x)f(y)$, para todo $x, y \in G_1$.*

Definição 9.1.2. *Seja $f : G_1 \to G_2$ um homomorfismo de grupos.*

1. *Se $G_1 = G_2$, a aplicação f é chamada um endomorfismo.*
2. *Se f é injetora, a aplicação f é chamada um monomorfismo.*
3. *Se f é sobrejetora, a aplicação f é chamada um epimorfismo.*
4. *Se f é bijetora, a aplicação f é chamada um isomorfismo e que os grupos G_1 e G_2 são isomorfos, onde denotamos por $G_1 \simeq G_2$.*

5. Se $G_1 = G_2$ e f é bijetora, a aplicação f é chamada um automorfismo.

Exemplo 9.1.1. *A função $f : \mathbb{Z} \to \mathbb{Z}$ dada por $f(x) = x$, para $x \in \mathbb{Z}$, é um homomorfismo de grupos.*

Exemplo 9.1.2. *A função $f : \mathbb{Z} \to \mathbb{Z}_2$ dada por $f(x) = \begin{cases} 0 & se \ \ x \ \ é \ par \\ 1 & se \ \ x \ \ é \ impar, \end{cases}$ é um homomorfismo de grupos.*

Definição 9.1.3. *Seja $f : G_1 \to G_2$ um homomorfismo de grupos. O kernel ou núcleo de f é definido por $\ker(f) = \{g \in G : f(g) = e_2\}$, onde e_2 é o elemento neutro de G_2, e a imagem de f é definida por $Im(f) = f(G_1) = \{f(g) : g \in G_1\} = \{h \in G_2 : \ \text{existe } g \in G_1 \text{ tal que } f(g) = h\}$.*

Sejam G um grupo e $H \subseteq G$ um subgrupo normal de G. A aplicação $f : G \to G/H$ definida por $f(x) = xH$, onde $x \in G$, é um homomorfismo de grupos, chamado homomorfismo canônico ou projeção. Além disso, f é sobrejetora. Também, se H é um subgrupo normal de grupo G, então H é o núcleo da projeção canônica $\pi : G \to G/H$, dada pr $\pi(g) = gH$. Além disso, se $H = \ker(f)$, então

$$xH = yH \text{ se, e somente se, } y^{-1}x \in H \text{ se, e somente se, } f(x) = f(y).$$

9.1.1 Exercícios

1. Seja $f : G_1 \to G_2$ um homomorfismo de grupos. Mostre que:
   (a) $f(e_1) = e_2$, onde e_i, para $i = 1, 2$ é o elemento de neutro de G_i.
   (b) $f(a^{-1}) = f(a)^{-1}$, para todo $a \in G_1$.
   (c) $f(a^n) = f(a)^n$, para todo $a \in G_1$ e $n \in \mathbb{Z}$.
2. Sejam $f : G_1 \to G_2$ e $g : G_2 \to G_3$ homomorfismos de grupos.
   (a) Mostre que f é bijetora se, e somente se, existe $f^{-1} : G_2 \to G_1$. Além disso, mostre que f^{-1} é um isomorfismo.
   (b) Mostre que $g \circ f : G_1 \to G_3$ é um homomorfismo.
   (c) Se f e g são injetoras, mostre que $g \circ f$ é injetora.
   (d) Se f e g são sobrejetoras, mostre que $g \circ f$ é sobrejetora.
3. Seja $f : G_1 \to G_2$ um homomorfismo de grupos.
   (a) Mostre que $\ker(f)$ é um subgrupo normal de G_1.
   (b) Mostre que $Im(f)$ é um subgrupo de de G_2.
   (c) Mostre que f é injetora se, e somente se, $\ker(f) = \{e_1\}$, onde e_1 é o elemento neutro de G_1.
   (d) Mostre que f é um isomorfismo se, e somente se, f^{-1} é um isomorfismo.

4. Seja $f : G_1 \to G_2$ um homomorfismo de grupos.

   (a) Se H é um subgrupo normal de G_1, mostre que $f(H)$ é um subgrupo normal de G_2.

   (b) Se K é um subgrupo normal de G_2, mostre que $f^{-1}(K)$ é um subgrupo normal de G_1.

   (c) Se f é sobrejetora e $H \subseteq G_1$ é um subgrupo normal, mostre que $f(H)$ é um subgrupo normal de G_2.

   (d) Se f é um isomorfismo e G_1 é abeliano, mostre que G_2 é abeliano.

5. Sejam G_1, G_2 e G_3 grupos.

   (a) Mostre que G_1 é isomorfo a G_1.

   (b) Mostre que se G_1 é isomorfo a G_2, então G_2 é isomorfo a G_1.

   (c) Se G_1 é isomorfo a G_2 e G_2 é isomorfo a G_3, mostre que G_1 é isomorfo a G_3.

6. Se G é um grupo finito, $f : G \to G$ um homomorfismo e $a \in G$, mostre que $\circ(a) = \circ(f(a))$.

7. Mostre que um grupo G é abeliano se, e somente se, a aplicação $\sigma : G \to G$ definida por $\sigma(x) = x^{-1}$, onde $x \in G$, é um homomorfismo.

8. Se $f : G_1 \to G_2$ é um homomorfismos sobrejetor de grupos, mostre que o conjunto das imagens inversas de $y \in G_2$ com relação a f é $(\ker(f))x$, onde $x = f^{-1}(y)$.

9. Sejam G um grupo finito e $n \in \mathbb{N}$. Se n e $\circ(G)$ são primos entre si, mostre que todo elemento $g \in G$ pode ser escrito como $g = x^n$, onde $x \in G$.

10. Seja a aplicação $f : \mathbb{R}_+^* \to \mathbb{R}$ definida por $f(x) = log(x)$, onde $\mathbb{R}_+^*$ é um grupo multiplicativo e $\mathbb{R}$ é um grupo aditivo. Mostre que f é um isomorfismo de grupos.

11. Seja a aplicação $f : \mathbb{R} \to \mathbb{R}_+ - \{0\}$ definida por $f(x) = 2^x$, onde $\mathbb{R}$ é um grupo aditivo e $\mathbb{R}_+ - \{0\}$ é um grupo multiplicativo. Mostre que f é um isomorfismo de grupos.

12. Mostre que f é um homomorfismo e determine $\ker(f)$ e $Im(f)$.

    (a) $f : \mathbb{Z} \to \mathbb{C}$ definida por $f(n) = i^n$.

    (b) $f : \mathbb{R}^* \to \mathbb{R}^*$ definida por $f(n) = |x|$.

    (c) $f : \mathbb{R} \to \mathbb{C}^*$ definida por $f(x) = e^{ix}$.

    (d) $f : \mathbb{Z}_6 \to \mathbb{Z}_3$ definida por $f(x) = x$.

9.2 Teoremas de isomorfismos de grupos

Nesta seção, apresentamos os teoremas de isomorfismos de grupos.

Proposição 9.2.1. *Sejam G um grupo e $H \subseteq G$ um subgrupo. Se H é um subgrupo normal de G, então a aplicação $\mu : G \to G/H$ definida por $\mu(g) = gH$, onde $g \in G$, é um homomorfismo sobrejetor com* $\ker(\mu) = H$.

Demonstração. Se $g_1 = g_2 \in G$, então $g_1 g_2^{-1} = e \in H$. Assim, $g_1 H = g_2 H$, e portanto, μ está bem definida. Agora, se $g_1, g_2 \in G$, então $\mu(g_1 g_2) = (g_1 g_2)H = (g_1 H)(g_2 H) = \mu(g_1)\mu(g_2)$, e portanto, μ é um homomorfismo. Para a sobrejetora, se $gH \in G/H$, onde $g \in G$, então $\mu(g) = gH$, e portanto, μ é sobrejetora. Finalmente, se $g \in \ker(\mu)$, então $\mu(g) = H = eH = gH$, ou seja, $g \in H$. Agora, se $g \in H$, então $\mu(g) = gH = H$, ou seja, $g \in \ker(\mu)$. Portanto, $\ker(\mu) = H$. □

Teorema 9.2.1. *(Primeiro teorema do isomorfismo) Se $\varphi : G_1 \to G_2$ é um homomorfismo sobrejetor de grupos, então $G_1/\ker(\varphi)$ é isomorfo a $Im(\varphi)$.*

Demonstração. Seja a aplicação $\phi : G_1/H \to Im(\varphi)$ definida por $\phi(gH) = \varphi(g)$, onde $g \in G_1$ e $H = \ker(\varphi)$. Assim, ϕ está bem definida, uma vez que se $g_1 H = g_2 H$, então $g_1 g_2^{-1} \in H$. Logo, $\varphi(g_1 g_2^{-1}) = e_2$, onde e_2 é o elemento neutro de G_2. Deste modo, $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1)(\varphi(g_2))^{-1} = e_2$, e deste modo, $\varphi(g_1) = \varphi(g_2)$, ou seja, ϕ está bem definida. Para a injetora, se $\phi(g_1 H) = \phi(g_2 H)$, então $\varphi(g_1) = \varphi(g_2)$. Assim, $e_2 = \varphi(g_1)(\varphi(g_2))^{-1} = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1 g_2^{-1})$, ou seja, $g_1 g_2^{-1} \in H$. Logo, $g_1 H = g_2 H$, e portanto, ϕ é injetora. Para a sobrejetora, se $g_2 \in Im(\varphi)$, então existe $g_1 \in G_1$ tal que $\varphi(g_1) = g_2$. Assim, existe $g_1 H \in G_1/H$ tal que $\phi(g_1 H) = \varphi(g_1) = g_2$, e portanto, ϕ é sobrejetora. □

Exemplo 9.2.1. *O núcleo do homomorfismo $f : \mathbb{R} \to S^1$, onde $S^1 = \{z \in \mathbb{C} : |z| = 1\}$, definido por $f(t) = e^{2\pi i t}$ é $\mathbb{Z}$. Como f é sobrejetora, segue que $\mathbb{R}/\mathbb{Z} \simeq S^1$. Da mesma forma, $\mathbb{R}^2/\mathbb{Z}^2 \simeq S^1 \times S^1$.*

Exemplo 9.2.2. *O determinante* $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$*, onde $GL_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) : \det(M) \neq 0\}$, é um homomorfismo sobrjetor cujo* $\ker(f) = SL_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) : \det(M) = 1\}$*. Assim, $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$.*

Proposição 9.2.2. *Se G é um grupo cíclico com m elementos, então G é isomorfo a $\mathbb{Z}_m$.*

Demonstração. Seja G um grupo cíclico com m elementos cujo gerador é g. Seja $\varphi : \mathbb{Z} \longrightarrow G$ definida por $\varphi(n) = g^n$, para todo $n \in \mathbb{Z}$. A aplicação φ é um homomorfismo sobrejetor de grupos. Além disso, $\varphi(n) = 0$ se, e somente se, $g^n = e$, se, e somente se, $m \mid n$ (pois g tem ordem m). Logo, $\ker(\varphi) = m\mathbb{Z}$. Pelo Teorema 9.2.1, segue que $G \simeq \mathbb{Z}/m\mathbb{Z}$. Por sua vez, a aplicação $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ definida por $\phi(n) = \overline{n}$, para todo $n \in \mathbb{Z}$, também é um homomorfismo sobrejetor de grupos aditivos. Agora, $\phi(n) = \overline{0}$ se, e somente se, $\overline{n} = \overline{0}$ se, e somente se, $m \mid n$. Assim, $\ker(\phi) = m\mathbb{Z}$. Pelo Teorema 9.2.1, segue que $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_m$. Portanto, $\mathbb{Z}_m \simeq G$. □

Proposição 9.2.3. *Seja G um grupo cíclico, ou seja, $G = \langle g \rangle$.*

1. *A aplicação $f : \mathbb{Z} \to G$ definida por $\varphi(k) = g^k$ é um homomorfismo sobrejetor.*
2. *Se G é infinito, então $G \simeq \mathbb{Z}$.*
3. *Se G é finito de ordem n e H é um subgrupo de G de ordem m, então $H = \langle g^{n/m} \rangle$.*
4. *Se G é finito de ordem n e $m|n$, então existe um único subgrupo de G de ordem m.*

Demonstração. (1) Se $k, l \in \mathbb{Z}$, então $\varphi(k+l) = g^{k+l} = g^k g^l = \varphi(k)\varphi(l)$, ou seja, φ é um homomorfismo. Agora, se $y \in G$, então existe $k \in \mathbb{Z}$ tal que $y = g^k$, e assim, $\varphi(k) = g^k$. Portanto, φ é um homomrfismo sobrejetor. Para (2), como G é infinito, segue que o núcleo $\ker(f)$ é um subgrupo de $\mathbb{Z}$, e assim, $\ker(f) = n\mathbb{Z}$, para algum n. Pelo Teorema 9.2.1, segue que $G \simeq \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$. Como G é infinito, segue que $n = 0$. Portanto, $G \simeq \mathbb{Z}$. Para (3), como $\circ(G) = n$ e H é um subgrupo de G, segue que $g^k \in H$, para algum $k \in \mathbb{Z}$. Assim, $g^{-k} \in H$. Logo, existe d o menor inteiro positivo tal que $g^d \in H$. Se $x \in H$, então $x = g^k$, para algum $k \in \mathbb{Z}$. Pelo algoritmo da divisão, segue que existem únicos $q, r \in \mathbb{Z}$ tal que $k = dq + r$, onde $0 \leq r < d$. Assim, $g^r = g^{k-qd} \in H$. Pela escolha de d, segue que $r = 0$, e portanto, $H = \langle g^d \rangle$. Como $\circ(H) = m$, segue que $d = n/m$. Finalmente, para (4), como o sugrupo $\langle g^{n/m} \rangle$ tem ordem m, pelo item (3), segue que é único com essa propriedade. □

Corolário 9.2.1. *Seja G um grupo cíclico gerado por g. Se $g^m \neq g^n$ sempre que $m \neq n$, então φ é injetora.*

Demonstração. Se $\varphi(m) = \varphi(n)$, então $g^m = g^n$. Assim, $g^{m-n} = e$, e por hipótese, segue que $m = n$. Portanto, φ é injetora. □

9.2.1 Exercícios

1. Mostre que dois grupos cíclicos de mesma ordem são isomorfos.
2. Sejam $f : G_1 \to G_2$ e $g : G_3 \to G_4$ isomorfismos de grupos. Mostre que $G_1 \times G_3$ é isomorfo a $G_2 \times G_4$.
3. Se G_1 e G_2 são grupos, mostre que $G_1 \times G_2$ é isomorfo a $G_2 \times G_1$.
4. Se G_1, G_2 e G_3 são grupos, mostre que $(G_1 \times G_2) \times G_3$ é isomorfo a $G_1 \times G_2 \times G_3$. Generalize.
5. Sejam G um grupo e $T = G \times G$.
   (a) Mostre que $H = \{(g, g) \in G \times G : g \in G\}$ é um grupo isomorfo a G.
   (b) Mostre que H é normal em T se, e somente se, G é abeliano.
6. Seja G um grupo. Se H e K são subgrupos normais de G, mostre que HK/K é isomorfo a $H/(H \cap K)$.
7. Se H e K são subgrupos normais de um grupo G, mostre que HK/K é isomorfo a $H/(H \cap K)$.
8. Seja $G = \{x^i y^j : i = 0, 1,\ j = 0, 1, \cdots, n-1, \text{ onde } x^2 = e,\ y^n = e,\ xy = y^{-1}x\}$ o grupo diedral.
   (a) Mostre que $H = \{e, y, y^2, \cdots, y^{n-1}\}$ é um subgrupo normal de G.
   (b) Mostre que G/H é isomorfo a H, onde $K = \{-1, 1\}$ é um grupo multiplicativo.

(c) Determine o centro de G.

9. Seja $f : \mathbb{R} \to S^1$ definida por $f(x) = e^{2\pi ix}$. Mostre que $\mathbb{R}/\mathbb{Z}$ é isomorfo a S^1 e que $\mathbb{R}^2/\mathbb{Z}^2$ é isomorfo a $S^1 \times S^1$.

10. Seja $f : GL_n(\mathbb{R}) \to \mathbb{R}^*$ definida por $f(A) = \det(A)$. Mostre que $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ é isomorfo a $\mathbb{R}^*$

Capítulo

10

Teorema de Cayley

Na teoria dos grupos, o teorema de Cayley, nomeado em homenagem a Arthur Cayley, afirma que todo grupo G é isomorfo a um subgrupo do grupo siméttrico agindo em G. Isso pode ser entendido como um exemplo da ação de grupo de G sobre os elementos de G. Uma permutação de um conjunto G é uma função bijetiva de um grupo G em G. O conjunto com todas as permutações formam um grupo com a composição de funções, chanadi de grupo simétrico de G. O Teorema de Cayley afirma que todo grupo pode ser visto como um subgrupo do grupo das permutações de um conjunto.

10.1 Grupo das Permutações

Seja E um conjunto não vazio. Uma permutação de E é uma bijeção de E em E. O conjunto $B(E)$ das bijeções de E em E munido da operação composição de funções é um grupo, chamado grupo das permutações de E. Quando E é finito, o grupo $B(E)$ é denotado por S_n também é chamado de grupo simétrico de grau n.

Seja $S = \{x_1, x_2, \cdots, x_n\}$ um conjunto finito com n elementos. Se $\phi \in B(S) = S_n$, então ϕ é uma bijeção, onde será representada por

$$\phi = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ x_{k_1} & x_{k_2} & x_{k_3} & \cdots & x_{k_n} \end{pmatrix},$$

isto é, $\phi(x_i) = x_{k_i}$, para $i = 1, 2, \cdots, n$. De uma maneira mais simples a permutação ϕ pode ser representada como

$$\phi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ k_1 & k_2 & k_3 & \cdots & k_n \end{pmatrix},$$

isto é, $\phi(i) = k_i$, para $i = 1, 2, \cdots, n$. Nesta notação não importa a ordem das colunas. Por exemplo, em S_3

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

Além disso, $\circ(S_n) = n(n-1)\cdots 2.1 = n!$, uma vez que para $\phi(1)$ existem n escolhas possíveis, para $\phi(2)$ existem $n-1$ escolhas, e assim, por diante.

Exemplo 10.1.1. *Sejam $S = \{x_1, x_2, x_3, x_4\}$ e $\phi \in S_4$. Se $\phi(x_1) = x_3$, $\phi(x_2) = x_4$, $\phi(x_3) = x_2$ e $\phi(x_4) = x_1$, então ϕ é representado por*

$$\phi = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_3 & x_4 & x_2 & x_1 \end{pmatrix},$$

e na representação simplificada ϕ é dada por

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

Se $\phi, \psi \in S_n$, então a composição (produto) $\psi \circ \phi$ é definida recursivamente da seguinte maneira: se $\phi(1) = i_1$ e $\psi(i_1) = k$, então $(\psi \circ \phi)(1) = k$, e assim, por diante, ou seja, se

$$\phi = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \quad \text{e} \quad \psi = \begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix},$$

então $\psi \circ \phi$ é dada por

$$\psi \circ \phi = \begin{pmatrix} 1 & \cdots & i_r & \cdots & n \\ j_1 & \cdots & j_{i_r} & \cdots & j_n \end{pmatrix} \circ \begin{pmatrix} 1 & \cdots & r & \cdots & n \\ i_1 & \cdots & i_r & \cdots & i_n \end{pmatrix} = \begin{pmatrix} \cdots & r & \cdots \\ \cdots & j_{i_r} & \cdots \end{pmatrix},$$

uma vez que $(\psi \circ \phi)(r) = \psi(\phi(r)) = \psi(i_r) = j_{i_r}$, onde $r = 1, 2, \cdots, n$. Também,

$$\phi^{-1} = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Exemplo 10.1.2. *Se $S = \{1, 2, 3, 4\}$,*

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \text{ e } \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

então a permutação $\phi \circ \psi$ é dada por

$$\phi \circ \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}.$$

Exemplo 10.1.3. *Os elementos do grupo S_3 são representados matricialmente por e =*

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\phi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\phi^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\psi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\phi \circ \psi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ *e* $\phi^2 \circ \psi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. *Note que* $\psi \circ \phi = \phi^2 \circ \psi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *e que* $\circ(S_3) = 6$.

Além da forma matricial, uma permutação pode ser expressa por uma forma mais conveniente através de uma notação cíclica. O conceito de um r-ciclo $(i_1, i_2, \cdots, i_r)$ para uma permutação $\phi \in S_n$ significa que $\phi(i_1) = i_2$, $\phi(i_2) = \phi^2(i_1) = i_3, \cdots$, $\phi(i_{r-1}) = \phi^{r-1}(i_1) = i_r$, $\phi(i_r) = \phi^r(i_1) = i_1$, e deixa os outros elementos de S fixo, ou seja, a permutação permuta ciclicamente os elementos de $S = \{i_1, i_2, \cdots, i_r\}$ e fixa os restantes. Além disso, $\phi^r(\phi^{i-1}(i_1)) = \phi^{i-1}(\phi^r(i_1))$, uma vez que

$$\phi^r(\phi^{i-1}(i_1)) = \phi(i_i) = i_i \quad \text{e} \quad \phi^{i-1}(\phi^r(i_1)) = \phi_{i-1}(i_1) = i_i.$$

Neste caso, a aplicação ϕ é chamada um ciclo de comprimento r (ou um r-ciclo) e que $\{i_1, i_2, \cdots, i_r\}$ é o suporte de ϕ. A notação usada é $\phi = (i_1 i_2 \cdots i_r)$. Se $r = 2$, a permutação ϕ é chamada uma transposição. Um r-ciclo possui ordem r. Mas, a recíproca é falsa. Em particular, se p é um primo, então uma permutação de ordem p em S_p é um p-ciclo.

Um mesmo r-ciclo pode ser representado de várias formas diferentes. Por exemplo, (5261), (2615) e (6152) representam o memo 4-ciclo dado por

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 4 & 2 & 1 \end{pmatrix}.$$

Além disso, nem toda permutação é um ciclo, como exemplo,

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

Exemplo 10.1.4. *Sejam* $S = \{1, 2, 3, 4\}$,

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \ \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \ e \ \phi \circ \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}.$$

As permutações ϕ, ψ *e* $\phi \circ \psi$ *na notação em ciclos são representadas como* $\phi = (1324)$, $\psi = (12)(34)$ *e* $\phi\psi = (1423)$. *Assim,* ϕ *e* $\phi\psi$ *possuem apenas um ciclo, e* ψ *possui dois ciclos. Agora, se*

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix},$$

então os ciclos de ϕ *são* (12), (3) *e* (456). *Assim, a permutação* ϕ *será representada apenas por* (12)(456).

Exemplo 10.1.5. *Seja* $\phi \in S_3$ *dada por* $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}$. *Assim,* $\phi(1) = 2$, $\phi(2) = 3$, $\phi(3) = 5$, $\phi(5) = 1$ *e* $\phi(4) = 4$. *Logo,* ϕ *é um ciclo de comprimento* 4, *ou seja,* $\phi = (1235)$.

Também, pode ser escrito como $\phi = (2351) = (5123) = (3512)$.

Proposição 10.1.1. *Se* $\phi = (i_1, i_2, \cdots, i_r)$ *é um ciclo de comprimento* r *de* S_n*, então* $\circ(\phi) = r$.

Demonstração. Pela definição de ciclo, segue que $\phi^{i-1}(i_1) = i_i$, para todo $i = 1, 2, \cdots, r$, e $\phi(i_1) = i_2$. Assim, $\phi^i \neq id$ sempre que $1 \leq i < r$, e portanto, $r \leq \circ(\phi)$. Agora, como $\phi^r(i_i) = \phi^r(\phi^{i-1}(i_1)) = \phi^{i-1}(\phi^r(i_1)) = \phi^{i-1}(i_1) = i_i$, para $1 \leq i \leq r$, segue que $\phi^r = id$, ou seja, $\circ(\phi) = r$. □

Definição 10.1.1. *Dois ciclos são disjuntos se os seus suportes são disjuntos.*

Proposição 10.1.2. *Dois ciclos disjuntos comutam.*

Demonstração. Sejam ϕ e ψ dois ciclos de S_n com suportes A e B, respectivamente. Se $x \in S$, então temos três casos a considerar:

1. se $x \in A$, então $(\phi \circ \psi)(x) = \phi(\psi(x)) = \phi(x)$ e $(\psi \circ \phi)(x) = \psi(\phi(x)) = \phi(x)$, pois $\phi(x) \in A$.
2. Se $x \in B$, o resultado segue de modo análogo.
3. Se $x \notin A$ e $x \notin B$, então $\phi(\psi(x)) = x = \psi(\phi(x))$.

Portanto, $\phi \circ \psi = \psi \circ \phi$. □

Proposição 10.1.3. *Toda permutação* $\phi \in S_n$ *é o produto de seus ciclos (disjuntos), onde é escrita de modo único, a menos da ordem em que os ciclos aparecem.*

Demonstração. Suponha que $\phi(1) \neq 1$, caso contrário trocamos a ordem do conjunto S_n. Seja a sequência $\phi^o(1) = 1, \phi(1), \phi^2(1), \phi^3(1), \cdots$. Como S_n é finito, segue que essa sequência é finita. Logo, existem inteiros positivos i, j com $i < j$ tal que $\phi^i(1) = \phi^j(1)$. Assim, $\phi^{j-i}(1) = 1$, e portanto, existe o menor inteiro positivo r tal que $\phi^r(1) = 1$ e que $\phi^\circ(1), \phi(1), \phi^2(1), \phi^3(1), \cdots, \phi^{r-1}(1)$ são disjuntos, uma vez que se $\phi^r(1) = \phi^j(1)$, para algum j tal que $0 < j < r$, então $\phi^{r-j}(1) = 1 = \phi^\circ(1)$, o que não ocorre pela escolha de r. Assim, obtemos o ciclo

$$\phi_1 = (1, \phi(1), \phi^2(1), \cdots, \phi^{r-1}(1))$$

o que coincide com a restrição de ϕ a seu conjunto suporte. Agora, suponha que exista $a \in S$ o menor inteiro de S que não aparece no suporte de ϕ_1 e que $\phi(a) \neq a$. Caso não existisse tal elemento, a demonstração estava terminada, ou seja, $\phi = \phi_1$. Agora, repetindo o mesmo argumento com a seguência

$$\phi^\circ(a) = a, \phi(a), \phi^2(a), \phi^3(a), \cdots$$

obtém-se um ciclo ϕ_2 que também coincide com a restrição de ϕ a seu conjunto suporte. Agora, mostremos que ϕ_1 e ϕ_2 são disjuntos. Para isso, suponhamos que b fosse um elemento comum aos suportes de ϕ_1 e ϕ_2. Assim, $b = \phi^t(1) = \phi^s(a)$, para algum $0 \leq s \leq t$. Logo, $\sigma^{t-s}(1) = \phi^{-s+t}(1) = \phi^{-s}(\phi^t(1)) = \phi^{-s}(\phi^s(a)) = a$, e assim, pertence ao suporte de ϕ_1 o que não ocorre

pela escolha de a. Finalmente, esse processo termina em um número finito de m passos, ou seja, repetindo o mesmo argumento chega-se que $\phi = \phi_1\phi_2\cdots\phi_m$ tem sobre os elementos de S o mesmo efeito que ϕ, segue que $\phi = \phi_1\phi_2\cdots\phi_m$. □

Toda vez que escrevemos uma permutação de S_n como um produto de ciclos disjuntos obtemos uma partição de n, ou seja, se os ciclos que aparecem tem comprimentos $n_1, n_2, \cdots, n_r$, onde $n_1 \leq n_2 \leq \cdots \leq n_r$, então $n = n_1 + n_2 + \cdots + n_r$.

Exemplo 10.1.6. *Seja a permutação $\phi \in S_8$ dada por*

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

Neste caso, $\phi(1) = 1$, $\phi^\circ(2) = 2, \phi(2) = 6, \phi^2(2) = \phi(\phi(2)) = \phi(6) = 5, \phi^3(2) = 7, \phi^4(2) = 2$ e $\phi^\circ(3) = 3, \phi(3) = 8, \phi^2(3) = 4, \phi^4(3) = 3$. Assim, $\phi_1 = (1)$, $\phi_2 = (2657)$ e $\phi_3 = (384)$, e portanto, $\phi = (1)(2657)(384)$.

Definição 10.1.2. *Um 2-ciclo é chamado de uma transposição.*

Um ciclo mais simples depois da identidade é um 2-ciclo. Um m-ciclo se escreve como um produto de $m-1$ transposições, uma vez que

$$(i_1 i_2 \ldots i_m) = (i_1 i_2)(i_2 i_3)\ldots(i_{m-1} i_m).$$

Além disso, $(im) = (2m)(12)(2m)$ e $(ij) = (j1)(i1)(j1)$, para todo $i, j, k \notin \{1, 2\}$.

Proposição 10.1.4. *Toda permutação em S_n é um produto de 2-ciclos.*

Demonstração. Temos que $id = (12)(12)$. Pela Proposição 10.1.3, é suficiente mostrar que todo ciclo é um produto de transposições. Seja o m-ciclo $(i_1, i_2, \cdots, i_m)$. Por um cálculo simples, segue a igualdade $(i_1, i_2, \cdots, i_m) = (i_1 i_2)(i_1 i_3)\cdots(i_1 i_m)$. □

Observação 10.1.1. *A decomposição de m-ciclo não é única, uma vez que se*

$$\phi = (i_1 i_2 \ldots i_m) = (i_1 i_m)(i_1 i_{m-1})\ldots(i_1 i_3)(i_1 i_2) = ((i_1 i_2)(i_2 i_3)\ldots(i_{m-2} i_{m-1})(i_{m-1} i_m).$$

Por exemplo, $(1234) = (12)(23)(34) = (14)(13)(12)$. Além disso, toda transposição (ij) pode ser escrita como $(ij) = (ai)(aj)(ai)$, para todo $a \in S$, com $a \neq i$ e $a \neq j$.

Exemplo 10.1.7. *Seja a permutação $\phi \in S_8$ dada por*

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

Assim, $\phi = (1)(2657)(384)$. Como $(2657) = (26)(25)(27)$ e $(384) = (38)(34)$, segue que $\phi = (26)(25)(27)(38)(34)$.

Definição 10.1.3. *Uma permutação $\phi \in S_n$ é chamada uma permutação par se pode ser representada como um produto de um número par de transpasições (ou 2-ciclos). Caso contrário, é chamada de permutação impar.*

Observação 10.1.2. *Seja S_n o grupo das permutações.*

1. *O produto de duas permutações pares é uma permutação par.*
2. *O produto de uma permutação par e uma permutação impar é uma permutação impar.*
3. *O produto de duas permutações impares é uma permutação par.*

Proposição 10.1.5. *Se A_n é o subconjunto de S_n consistindo de todas as permutações pares, então A_n é um subgrupo de S_n.*

Demonstração. Como o produto de duas permutações pares é uma permutação par, segue que A_n é um subgrupo de S_n. □

Definição 10.1.4. *O subgrupo A_n de S_n é chamado de grupo alternante de grau n.*

Corolário 10.1.1. *O subgrupo A_n é um subgrupo normal de S_n de índice 2 e $\circ(A_n) = \frac{1}{2}n!$.*

Demonstração. Seja aplicação $\varphi : S_n \to W$, onde $W = \{-1, 1\}$ é um grupo multiplicativo, definida por

$$\varphi(s) = \begin{cases} 1 & \text{se s é uma permutação par} \\ -1 & \text{se s é uma permutação impar.} \end{cases}$$

Pela Observação 10.1.2, segue que φ é um homomorfismo sobrejetor. Além disso, $\ker(\varphi) = A_n$, que é um subgrupo normal de G. Pelo Teorema 9.2.1, segue que S_n/A_n é isomorfo a W, e assim,

$$2 = \circ(W) = \circ(\frac{S_n}{A_n}) = \frac{\circ(S_n)}{A_n},$$

e como $\circ(S_n) = n!$, segue que $\circ(A_n) = \frac{1}{2}n!$. □

Proposição 10.1.6. *Se $n \geq 3$, então $A_n = \langle 3 - ciclos \rangle$.*

Demonstração. Se σ é um k-ciclo, então σ se escreve como o produto de $k-1$ transposições. Assim, todo 3-ciclo pertence a A_n. Por outro lado, se $\sigma \in A_n$, então σ se escreve como o produto de um número par de transposições. Assim, agrupando de par em par, segue dois casos: são disjuntas ou não, ou seja,

$$(ab)(cd) = (acb)(acd) \quad \text{e} \quad (ab)(bc) = (abc),$$

o que prova o resultado. □

10.1.1 Exercícios

1. Determine as órbitas e os ciclos das seguintes permutações, e escreva como um produto de ciclos disjuntos:

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

2. Expresse as seguintes permutações como um produto de ciclos disjuntos;

$$(1,2,3)(4,5)(1,6,7,8,9)(1,5) \text{ e } (1,2)(1,2,3)(1,2).$$

3. Mostre que $(1,2,\cdots,n)^{-1} = (n, n-1, \cdots, 2, 1)$.

4. Calcule $a^{-1}ba$, onde

   (a) $a = (1,3,5)(1,2)$ e $b = (1,5,7,9)$,
   (b) $a = (5,7,9)$ e $b = (1,2,3)$.

5. Mostre que

   (a) existe uma permutação a tal que$a^{-1}xa = y$, onde $x = (1,2)(3,4)$ e $y = (5,6)(1,2)$,
   (b) não existe uma permutação a tal que $a^{-1}(1,2,3) = (1,3)(5,7,8)$, e
   (c) não existe uma permutação a tal que $a^{-1}(1,2)a = (3,4)(1,5)$.

6. Determine

   (a) a ordem de um n-ciclo,
   (b) a ordem do produto de ciclos disjuntos de comprimento $m_1, m_2, \cdots, m_k$, e
   (c) a ordem de uma dada permutação.

7. Determine a estrutura de todas as potências de $(1,2,\cdots,8)$.

8. Determine para qual valor de m um m-ciclo é uma permutação par.

9. Determine qual das seguintes permutações são pares:

   (a) $(1,2,3)(1,2)$,
   (b) $(1,2,3,4,5)(1,2,3)(4,5)$, e
   (c) $(1,2)(1,3)(1,4)(2,5)$.

10. Mostre que o menor subgrupo de S_n contendo $(1,2)$ e $(1,2,\cdots,n)$ é S_n, ou seja, S_n é gerado por esses elementos.

11. Determine os subgrupos de S_n, para $n = 1,2,3,4$.

12. Determine os subgrupos normais de S_n, onde $n = 1,2,3,4$.

13. Mostre que $\{e\}$ e A_n são os únicos subgrupos normais de S_n, onde $n \geq 5$.

10.2 Teorema de Cayley

Nesta seção, veremos que apesar de existirem vários tipos de grupos, segue que todo grupo é isomorfo a um subgrupo conveniente das permutações. Ou seja, pelo Teorema de Cayley, segue que todo grupo pode ser representado como um subgrupo de $B(E)$ para algum conjunto E. Em particular, um grupo finito pode ser representado como um subgrupo de S_n, para algum n, onde S_n é o grupo simétrico de grau n.

Definição 10.2.1. *Sejam G um grupo e $g \in G$. A aplicação $T_g : G \to G$ definida por $T_g(x) = gx$, onde $x \in G$, é chamada de translação à esquerda definida por g. De modo análogo, definimos a translação à direita definida por g, ou seja, $T_g(x) = xg$, onde $x \in G$.*

Proposição 10.2.1. *A aplicação T_g é uma bijeção.*

Demonstração. Se $x, y \in G$ e $T_g(x) = T_g(y)$, então $gx = gy$, e deste modo $x = y$. Portanto, T_g é injetora. Agora, se $y \in G$, então existe $x = g^{-1}y \in G$ tal que $T_g(x) = gx = g(g^{-1}y) = y$, e portanto, T_g é sobrejetora. □

Proposição 10.2.2. *Seja G um grupo. Se $T(G)$ é o conjunto de todas as translações à esquerda de G, então $T(G)$ é um subgrupo de $B(G)$, o grupo das permutações de G.*

Demonstração. Como $T_e \in T(G)$, onde e é o elemento neutro de G, segue que $T(G) \neq \emptyset$. Agora, se $T_{g_1}, T_{g_2} \in T(G)$, onde $g_1, g_2 \in G$, então $(T_{g_1} \circ T_{g_2})(x) = T_{g_1}(T_{g_2}(x)) = T_{g_1}(g_2x) = g_1(g_2x) = (g_1g_2)x = T_{g_1g_2}(x)$, para todo $x \in G$. Assim, $T_{g_1} \circ T_{g_2} = T_{g_1g_2} \in T(G)$, ou seja, a operação composição é fechada. Também, se $T_g \in T(G)$, onde $g \in G$, então $T_g \circ T_{g^{-1}} = T_e$, onde e é o elemento neutro de G. Portanto, $(T_g)^{-1} = T_{g^{-1}} \in T(G)$. Finalmente, se $g_1, g_2 \in G$, então $T_{g_1} \circ T_{g_2^{-1}} = T_{g_1g_2^{-1}} \in T(G)$. Portanto, $T(G)$ é um subgrupo de $B(G)$. □

Teorema 10.2.1. *(Teorema de Cayley) Se G é um grupo, então a aplicação $\varphi : G \to T(G)$ definida por $\varphi(g) = T_g$, onde $g \in G$, é um isomorfismo.*

Demonstração. Como $\varphi(g_1g_2) = T_{g_1g_2} = T_{g_1} \circ T_{g_2} = \varphi(g_1) \circ \varphi(g_2)$, para todo $g_1, g_2 \in G$, segue que φ é um homomorfismo. Agora, se $g_1, g_2 \in G$ e $\varphi(g_1) = \varphi(g_2)$, então $T_{g_1} = T_{g_2}$ se, e somente se, $g_1g = g_2g$, para todo $g \in G$, e assim, pela lei do cancelamento, segue que $g_1 = g_2$. Portanto, φ é injetora. Finalmente, φ é sobrejetora, uma vez que todo elemento de $T(G)$ é do tipo T_g para algum $g \in G$. Deste modo, $\varphi(g) = T_g$, para todo $g \in G$, e portanto, φ é um isomorfismo. □

10.2.1 Exercícios

1. Seja S um conjunto não vazio. Mostre que $B(E)$ é um grupo em relação a composição.
2. Sejam G um grupo, $g \in G$ e $T_g : G \to G$ definida por $T_g(x) = gx$, onde $x \in G$, e seja $\varphi : G \to T(G)$ definida por $\varphi_g = T_g$, onde $g \in G$. Sejam $g_1, g_2 \in G$. Mostre que:
   (a) $T_{g_1g_2} = T_{g_1} \circ T_{g_2}$.
   (b) $T_{g_1} \circ \varphi_{g_2} = \varphi_{g_2} \circ T_{g_1}$.

3. Sejam G um grupo T_g como definida no exercício anterior. Se $\phi : G \to G$ é um automorfismo tal que $T_g \circ \phi = \phi \circ T_g$, mostre que $\phi = T_g$, para algum $g \in G$.

4. Sejam G um grupo, $T(G) = \{T_g : g \in G\}$ e $I(G) = \{I_g : g \in G\}$, onde $I_g : G \to G$ é definido por $I_g(x) = gxg^{-1}$. Determine $T(G) \cap I(G)$.

5. Mostre que $Z(G) = \{e\}$ se, e somente se, $I_g(G)$ é isomorfo a G.

6. Mostre que $Aut(\mathbb{Z})$ é isomorfo ao grupo $G = \{1, -1\}$.

Capítulo

11

Anéis e ideais

Um anel é uma estrutura algébrica que consiste em um conjunto associado a duas operaçõees binárias, normalmente chamadas de adição e multiplicação, onde cada operação combina dois elementos para formar um terceiro elemento. Além disso, o conjunto e suas duas operações devem satisfazer determinadas condições, ou seja, o conjunto deve ser um grupo abeliano sob adição e um monoide sob multiplicação de modo que a multiplicação distribui sobre a adição. Embora essas operações sejam familiares em muitas estruturas matemáticas, tais como sistemas de números ou números inteiros, também são muito gerais, tomando uma ampla variedade de outros conceitos matemáticos. Neste capítulo, apresentamos os conceitos de anéis, subanéis, ideais, ideais primos e maximais, anéis quocientes, nilradical e radical de Jacobson, homomorfismos de anéis, operações de ideais (soma e produto), característica de um anel e, finalmente, a divisibilidade de elementos de um anel.

11.1 Anel

A teoria de anéis é um assunto de importância fundamental na álgebra, que está totalmente conectada com outras grandes áreas como por exemplo: teoria de módulos, teoria de grupos, anéis de grupos, análise funcional, álgebra de operadores, etc. Nesta seção, apresentamos o conceito de anéis juntamente com suas principais propriedades.

Definição 11.1.1. *Seja A um conjunto diferente do vazio munido das leis de composição de adição $(x, y) \to x + y$ e de multiplicação $(x, y) \to xy$. O conjunto A é chamado um anel se:*

1. *$(A, +)$ é um grupo abeliano, ou seja:*

   (a) *Se $a, b, c \in A$ então $a + (b + c) = (a + b) + c$ (associativa);*

   (b) *Se $a, b \in A$ então $a + b = b + a$ (comutativa);*

   (c) *Existe o elemento neutro $0 \in A$ tal que, qualquer que seja $a \in A$, segue que, $a+0 = a$ (elemento neutro);*

   (d) *Qualquer que seja $a \in A$ existe um elemento em A, indicado genericamente por $-a$, tal que $a + (-a) = 0$ (simetria);*

2. *A multiplicação é distributiva em relação Ã adição, ou seja, se $a, b, c \in A$, então $a(b+c) = ab + ac$.*

3. *A multiplicação goza da propriedade associativa, ou seja, se $a, b, c \in A$, então $a(bc) = (ab)c$.*

Um anel não precisa ter elemento neutro da multiplicação, e também, os elementos não nulos de um anel não precisam ter inversos multiplicativos.

Observação 11.1.1. *Seja A um anel.*

1. *O elemento neutro é único.*

2. *O oposto $-a$ de um elemento A do anel é único.*

3. *Se $a_1, a_2, \ldots, a_n \in A$, então $-(a_1 + a_2 + \cdots + a_n) = (-a_1) + (-a_2) + \cdots + (-a_n)$.*

4. *Se $a \in A$, então $-(-a) = a$.*

5. *Se $a + x = a + y$, então $x = y$,* lei do cancelamento*, ou seja, todo elemento de A é regular em relação a adição.*

6. *A equação $a + x = b$ tem somente a solução $b + (-a)$.*

7. *Se $a \in A$, então $a0 = 0a = 0$.*

8. *Se $a, b \in A$, então $a(-b) = (-a)b = -(ab)$.*

9. *Se $a, b \in A$, então $(-a)(-b) = ab$.*

Definição 11.1.2. *Seja A um anel.*

1. *O anel A é chamado um anel comutativo se a sua multiplicação é comutativa, isto é, se $ab = ba$ para todo $a, b \in A$.*

2. *O anel A é chamado um anel com unidade se A possui o elemento neutro para a multiplicação. Esse elemento será indicado por 1_A ou apenas 1, se não houver possibilidade de confusão. Além disso, supomos sempre que $1 \neq 0$ (o elemento neutro aditivo de A). O elemento neutro da multiplicação do anel A é chamado unidade do anel.*

3. *O anel A é chamado um anel comutativo com unidade se a multiplicação é comutativa e para a qual existe o elemento neutro da multiplicação.*

Exemplo 11.1.1. *O conjunto dos números inteiros, o conjunto do números racionais, o conjunto dos números reais e o conjunto dos números complexos sob a adição e a multiplicação usuais são anéis comutativos com unidade.*

Exemplo 11.1.2. *O conjunto* $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ *sob as operações de soma e de produto módulo* n *são anéis comutativos com unidade, neste caso, o elemento* 1 *é o elemento unidade.*

Exemplo 11.1.3. *Os anéis* $n\mathbb{Z}$ *não admitem unidade, salvo quando* $n = 1$*, caso que se trata do próprio* $\mathbb{Z}$*.*

Exemplo 11.1.4. *O anel das matrizes* $M_n(\mathbb{K})$*, onde* $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *ou* $\mathbb{C}$*, não é comutativo, mas possui unidade.*

Exemplo 11.1.5. *Se* A *e* B *são anéis, então o produto direto* $A \times B = \{(a, b) : a \in A \text{ e } b \in B\}$*, onde as operações de soma e produto são definidas componente a componente, é um anel. Em geral, o produto direto de* n *anéis é um anel.*

Definição 11.1.3. *Seja* A *um anel.*

1. *Um elemento* a *não nulo de* A *é chamado divisor de zero se existe um elemento não nulo* $b \in A$ *tal que* $ab = 0$ *ou* $ba = 0$*.*
2. *Se* A *for um anel com unidade, um elemento* a *de* A *é denominado inversível (ou unidade) em* A *se existir* $b \in A$ *tal que* $ab = ba = 1$*, onde o elemento* b *será denotado por* a^{-1}*.*

O conjunto dos elementos inversíveis de A será denotado por A^* e é um grupo abeliano em relação a multiplicação. Além disso, é comum usarmos o termo unidade de A para um elemento inversível de A.

Definição 11.1.4. *Seja* A *um anel.*

1. *O anel* A *é chamado um anel com divisão, ou um quase corpo, se* $(A - \{0\}, \cdot)$ *é um grupo.*
2. *Um elemento* $a \in A$*,* $a \neq 0$*, é chamado um divisor de zero à esquerda de* A *se existe* $b \neq 0$ *em* A *tal que* $ab = 0$*. Analogamente,* $a \neq 0$ *é um divisor próprio de zero à direita se existe* $b \neq 0$ *tal que* $ba = 0$*.*
3. *Um anel comutativo com unidade* A *é chamado um anel de integridade (ou domínio) se para* $a, b \in A$ *tal que* $ab = 0$ *implicar que* $a = 0$ *ou* $b = 0$*, ou seja,* A *não possui divisores de zeros não nulos.*

A frase $ab = 0$ implica que $a = 0$ ou $b = 0$, onde $a, b \in A$, recebe o nome de *lei do anulamento do produto*. Assim, um anel de integridade é um anel comutativo com unidade em que vale a lei do anulamento do produto. Em outras palavras podemos dizer que A é um anel de integridade se o mesmo não contiver divisores de zero.

Exemplo 11.1.6. *Os anéis* $\mathbb{Z}$*,* $\mathbb{Q}$*,* $\mathbb{R}$ *e* $\mathbb{C}$ *são domínios.*

Exemplo 11.1.7. *No anel $\mathbb{Z}_6$ os elementos $\overline{2}$ e $\overline{3}$ são divisores de zero uma vez que são não nulos, e no entanto, $\overline{2}.\overline{3} = \overline{0}$. Assim, o anel $\mathbb{Z}_6$ não é um anel de integridade.*

Exemplo 11.1.8. *O anel $\mathbb{Z}_m$ é um domínio se, e somente se, m é primo. De fato, se m não for primo, então existem $r, s \in \mathbb{Z}$, de tal forma que $1 < r, s < m$ e $rs = m$. Assim, $\overline{0} = \overline{m} = \overline{rs}$. Desse modo, existem divisores de zero em $\mathbb{Z}_m$, o que é contra à hipótese. Reciprocamente, se existem $\overline{a}, \overline{b} \in \mathbb{Z}_m$ tal que $\overline{a}\overline{b} = \overline{0}$, então $m \mid ab$. Como m é primo, segue que $m \mid a$ ou $m \mid b$. Isto significa que $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$, ou seja, que $\mathbb{Z}_m$ é um domínio.*

Assim, $\mathbb{Z}_n$, com $n \neq p$, onde p é um primo, não é um anel de integridade.

Proposição 11.1.1. *Um anel comutativo com unidade A é um anel de integridade se, e somente se, todo elemento não nulo de A é regular quanto à multiplicação, isto é, se $a \neq 0$ e $ab = ac$ implicar que $b = c$, onde $a, b, c \in A$.*

Demonstração. Suponhamos que A é um anel de integridade e que $a \in A$ com $a \neq 0$. Se $ab = ac$, com $b, c \in A$, então $a(b - c) = 0$. Assim, pela hipótese e por termos tomado $a \neq 0$, segue que $b - c = 0$, ou seja, $b = c$. Reciprocamente, se existirem $a, b \in A$, ambos não nulos, de maneira que $ab = 0$, segue que $ab = a0$. Assim, por hipótese, segue que $b = 0$, o que é absurdo. □

11.1.1 Subanel

Nesta subseção, apresentamos o conceito e propriedades da estrutura de um subanel de um anel.

Definição 11.1.5. *Sejam A um anel e $N \subseteq A$ um subconjunto não vazio. O subconjunto N é chamado um subanel do anel A se N também é um anel com as operações de soma e de produto herdadas de A.*

Exemplo 11.1.9. *$\mathbb{Z} \subseteq \mathbb{Q}$, $\mathbb{Z} \subseteq \mathbb{R}$, $\mathbb{Z} \subseteq \mathbb{C}$, $\mathbb{Q} \subseteq \mathbb{R}$, $\mathbb{Q} \subseteq \mathbb{C}$ e $\mathbb{R} \subseteq \mathbb{C}$ são subanéis.*

Exemplo 11.1.10. *Se $A = M_2(\mathbb{R})$ e $L = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : \ a \in \mathbb{R} \right\}$, então L é um subanel de A.*

Exemplo 11.1.11. *O conjunto $L = \{a + b\sqrt{2} : a, b \in \mathbb{R}\}$ é um subanel de $\mathbb{R}$.*

Exemplo 11.1.12. *$L \subseteq \mathbb{Z}$ é um subanel se, e somente se, L é um subgrupo aditivo de $\mathbb{Z}$.*

Exemplo 11.1.13. *$M_n(\mathbb{Z})$ é um subanel de $M_n(\mathbb{Q})$.*

Exemplo 11.1.14. *Os únicos subanéis de $\mathbb{Z} \times \mathbb{Z}$ são da forma $n\mathbb{Z} \times \mathbb{Z}$, para algum $n \in \mathbb{N} - \{0\}$. De fato: claramente $n\mathbb{Z} \times \mathbb{Z}$ é um subanel de $\mathbb{Z} \times \mathbb{Z}$. Agora, sejam $M \subseteq \mathbb{Z} \times \mathbb{Z}$ um subanel e L o conjunto formado pelas primeiras coordenadas de M. Assim, se $a_1, a_2 \in L$, então $(a_1, b_1), (a_2, b_2) \in M$, para alguns b_1 e b_2. Logo, $(a_1, b_1) - (a_2, b_2) = (a_1 - a_2, b_1 - b_2) \in M$, e assim, $a_1 - a_2 \in L$. Desse modo, L é um subgrupo aditivo de $n\mathbb{Z}$, e portanto, $L = n\mathbb{Z}$, para algum $n \in \mathbb{N} - \{0\}$.*

Proposição 11.1.2. *Sejam A um anel e $N \subseteq A$ um subconjunto não vazio. Assim, N é um subanel de A se, e somente se, $a - b \in N$ e $ab \in N$ para todo $a, b \in N$, ou seja, N é fechado para a subtração e para a multiplicação de A.*

Demonstração. Se N é um subanel, então $(N, +)$ é um subgrupo do grupo $(A, +)$. Logo, $a-b \in N$, para todo $a, b \in N$. Ainda, pela hipótese, segue que N é fechado para a multiplicação de A, o que conclui a demonstração quanto a esta parte. Reciprocamente, como $a - b \in N$, para todo $a, b \in N$, segue que $(N, +)$ é um subgrupo de $(A, +)$. Assim, $(N, +)$ é um grupo abeliano. Por outro lado, como $N \subset A$ e N é fechado em relação à multiplicação de A, segue que $a(bc) = (ab)c$, para todo $a, b, c \in N$, e $a(b + c) = ab + ac$ e $(a + b)c = ac + bc)$ para todo $a, b, c \in N$. Portanto, N é um subanel de A. □

Definição 11.1.6. *Sejam A um anel comutativo com unidade e $L \subseteq A$ um subanel. O subanel L é chamado um subanel unitário se $1_A = 1_L$.*

Exemplo 11.1.15. *O anel $\mathbb{Z}$ tem unidade, $2\mathbb{Z} \subseteq \mathbb{Z}$ e $2\mathbb{Z}$ não possui unidade. Os anéis $\mathbb{Z} \subseteq \mathbb{Q}$ possuem a mesma unidade. O anel $\{0\} \times \mathbb{Z}$ possui $(0, 1)$ como unidade, $\{0\} \times \mathbb{Z} \subseteq \mathbb{Z} \times \mathbb{Z}$ e $\mathbb{Z} \times \mathbb{Z}$ possui $(1, 1)$ como unidade.*

Definição 11.1.7. *Seja A um anel.*

1. *Um elemento $a \in A$ é chamado nilpotente se $a^n = 0$, para algum $n \in \mathbb{N}$. O menor n tal que isso ocorra é chamado índice de nilpotência de a.*
2. *Um elemento $a \in A$ é chamado idempotente se $a^2 = a$.*

Um elemento nilpotente de um anel não nulo é um divisor de zero e a recíproca é falsa.

11.1.2 Exercícios

1. Seja $A = \{f : [0, 1] \to \mathbb{R} : f \text{ é contínua}\}$.
   (a) Verifique se A é um anel.
   (b) Verifique se $L = \{f \in A : f(1/2) = 0\}$ é um subanel de A.
2. Mostre que todo corpo $\mathbb{K}$ é um domínio de integridade.
3. Seja A um anel. Se $a^2 = a$, para todo $a \in A$, mostre que $a = -a$, para todo $a \in A$, e que A é comutativo.
4. Se L_1 e L_2 são subanéis de um anel A, mostre que $L_1 \cap L_2$ é um subanel de A.
5. Determine todos os subanéis de $\mathbb{Z}_6$.
6. Seja E um conjunto não vazio. Considere no conjunto das partes $\mathcal{P}(E)$ as seguintes operações $x \triangle y = (x \cup y) - (x \cap y)$ e $x * y = x \cap y$.
   (a) Mostre que $(\mathcal{P}(E), \triangle, *)$ é um anel comutativo com unidade.

(b) Mostre que os elementos de $\mathcal{P}(E)$ são idempotentes.

7. Mostre que os números racionais $\mathbb{Q}$ com as operações $a \oplus b = a+b-1$ e $a \odot b = a+b-ab$, onde $a, b \in \mathbb{Q}$, é um anel.

8. Sejam A um anel de integridade e $a \in A$. Se $a^2 = 1$, mostre que $a = 1$ ou $a = -1$.

9. Sejam A um anel de integridade e $a \in A$. Se $a^2 = a$, mostre que $x = 0$ ou $x = 1$.

10. Seja A um anel com unidade tal que $a^2 = a$ para todo $a \in A$. Mostre que A é um anel de integridade se, e somente se, $A = \{0, 1\}$.

11. Mostre que todo elemento não nulo de $\mathbb{Z}_n$ é uma unidade ou um divisor de zero.

12. Seja A um anel comutativo finito com unidade. Mostre que todo elemento não nulo de A é um divisor de zero ou uma unidade.

13. Seja a um elemento nilpotente de um anel comutativo com unidade A.

    (a) Mostre que $1 + a$ é uma unidade de A.

    (b) Mostre que a soma de um nilpotente com uma unidade é uma unidade de A.

14. Mostre que $A = \{f : \mathbb{R} \to \mathbb{R} : f \text{ é contínua}\}$ é um anel.

15. Sejam $A_1, A_2, \cdots, A_n$ anéis. Mostre que o produto direto $A_1 \times A_2 \times \cdots \times A_n$ é um anel, onde as operações de soma e produto são componente a componente.

16. Seja a relação $\sim$ sobre $A = \mathbb{N} \times \mathbb{N}$ definida por $(a, b) \sim (c, d) \leftrightarrow a + d = b + d$.

    (a) Mostre que $\sim$ é uma relação de equivalência sobre A.

    (b) Determine a classe de equivalência de $(a, b) \in A$.

17. Seja $A = \{f : [0, 1] \to \mathbb{R} : f \text{ é contínua}\}$.

    (a) Verifique se A é um anel.

    (b) Verifique se $L = \{f \in A : f(1/2) = 0\}$ é um subanel de A.

18. Seja A um anel tal que $x^2 = x$ para todo $x \in A$.

    (a) Mostre que $-x = x$, para todo $x \in A$.

    (b) Mostre que $xy = yx$, para todo $x, y \in A$.

19. Verifique se são subaníes.

    (a) $L = \left\{ \begin{pmatrix} 0 & a \\ b & c \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$ do anel $M_2(\mathbb{R})$.

    (b) $L = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ do anel $\mathbb{R}$.

20. Ache os elementos inversíveis dos anéis: $\mathbb{Z}_{18}$ e $\mathbb{C}$ e determine seus inversos.

21. Seja A um anel comutativo com unidade. Mostre que

    (a) Se $a, b \in A$ são inveríveis, mostre que $ab \in A$ é inversível.

    (b) Se $a \in A$ é inversível, mostre que $a^{-1} \in A$ é inversível.

22. Seja A um anel de integridade. Se $x \in A$ e $x^2 = x$, mostre que $x = 0$ ou $x = 1$.

23. Sejam os anéis $A = \mathbb{Z}[\sqrt{-11}] = \{a + b\sqrt{-11} : a, b \in \mathbb{Z}\}$ e $B = M_2(\mathbb{Q})$. Determine os elementos inversíveis de A e B.

24. Determine todos os subanéis de $\mathbb{Z}_{20}$.

25. Mostre que $L = \left\{ \begin{pmatrix} 0 & a \\ b & c \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$ é um subanel do anel $M_2(\mathbb{R})$.

26. Determine todos os subanéis de $\mathbb{Z}_{20}$.

11.2 Divisibilidade

O conceito de divisibilidade em um anel se extende naturalmente do conceito de divisibilidade sobre o anel dos números inteiros, com certa especibilidade para a existência de máximo divisor comum e mínimo múltiplo comum de elementos.

Definição 11.2.1. *Sejam A um anel comutativo com unidade e $a, b \in A$. O elemento a é dito que divide b se existe $c \in A$ tal que $b = ac$. Neste caso, usamos a notação $a \mid b$.*

Sejam A um anel comutativo com unidade e $a, b, c \in A$.

1. $a \mid 0$, uma vez que $0 = a0$.

2. $a \mid a$, uma vez que $a = a1$.

3. Se $a|b$, então $a|bx$, para todo $x \in A$. De fato, se $a|b$, então $b = ac$, para algum $c \in A$. Assim, $bx = a(cx)$, para todo $x \in A$. Portanto, $a|bx$.

4. Se $a \mid b$ e $b \mid c$, então $a \mid c$. De fato, se $a \mid b$ e $b \mid c$, então $b = ax$ e $c = by$, para algum $x, y \in A$. Assim, $c = ay = a(xy)$, ou seja, $a \mid c$.

5. Se $a \mid b$ e $a \mid c$, então $a \mid (bx \pm cy)$, para todo $x, y \in A$. De fato, se $a|b$ e $a|c$, então $b = ac_1$ e $c = ac_2$, para algum $c_1, c_2 \in A$. Assim, $bx = a(c_1x)$ e $cy = a(c_2y)$, para todo $x, y \in A$. Somando (ou subtraindo), segue que $bx \pm cy = a(c_1x \pm c_2y)$. Portanto, $a|(bx \pm cy)$.

Definição 11.2.2. *Sejam A um anel comutativo com unidade e $a, b \in A$. Um elemento $d \in A$ se diz um máximo divisor comum de a e b, denotado por $mdc(a, b)$, se*

1. *$d \mid a$ e $d \mid b$.*

2. *Para todo $d' \in A$ tal que $d' \mid a$ e $d' \mid b$ implica que $d' \mid d$.*

Neste caso, denotamos $d = mdc(a, b)$. Dois elementos $a, b \in A$ são chamados primos entre si se $mdc(a, b)$ é uma unidade. Em geral, sejam $a_1, a_2, \cdots, a_n$ elementos de A. Um elemento $d \in A$ é chamado um máximo divisor comum de $a_1, a_2, \cdots, a_n$, denotado por $d = mdc(a_1, a_2, \ldots, a_n)$, se:

1. *d divide a_i, para $i = 1, 2, \cdots, n$, e*
2. *se existe d' divide a_i, para $i = 1, 2, \cdots, n$, então d' divide d.*

Definição 11.2.3. *Sejam A um anel comutativo com unidade e $a, b \in A$. Um elemento $m \in A$ se diz um mínimo múltiplo comum de a e b, denotado por $mmc(a, b)$, se*

1. *$a \mid m$ e $b \mid m$.*
2. *Para todo $m' \in A$ tal que $a \mid m'$ e $b \mid m'$ implica que $m \mid m'$.*

Neste caso, denotamos $m = mmc(a, b)$. Em geral, sejam $a_1, a_2, \cdots, a_n$ elementos de A. Um elemento $m \in A$ é chamado um minimo múltiplo comum de $a_1, a_2, \cdots, a_n$ se:

1. *a_i divide m, para $i = 1, 2, \cdots, n$, e*
2. *se existe m' tal que a_i divide m', para $i = 1, 2, \cdots, n$, então m divide m'.*

Observamos que as definições dadas não garantem a existência de um máximo divisor comum e de um mínimo múltiplo comum de dois ou mais elementos de A.

Definição 11.2.4. *Dois elementos $a, b \in A$ são chamados associados se existe uma unidade $u \in A$ tal que $a = ub$, e denotado por $a \sim b$.*

Observação 11.2.1. *Sejam A um domínio comutativo com unidade e $a, b \in A$, com $a \neq 0$ e $b \neq 0$. Se $a|b$ e $b|a$, então $b = ac_1$ e $a = bc_2$, onde $c_1, c_2 \in A$. Assim, $a = bc_2 = a(c_1c_2)$. Com A é um domínio, segue que $c_1c_2 = 1$, Portanto, a e b são associados.*

Proposição 11.2.1. *Sejam A um domínio de integridade comutativo com unidade e $a, b \in A$. São equivalentes:*

1. *$a \sim b$.*
2. *$\langle a \rangle = \langle b \rangle$.*
3. *$a \mid b$ e $b \mid a$.*

Demonstração. (1) $\rightarrow$ (2) Suponhamos que $a \sim b$, ou seja, $a = bu$, onde $u \in A$ é uma unidade. Se $x \in \langle a \rangle$, então $x = ar$, para algum $r \in A$. Assim, $x = ar = b(ru)$, ou seja, $x \in \langle b \rangle$. Portanto, $\langle a \rangle \subseteq \langle b \rangle$. De modo análogo, segue que $\langle b \rangle \subseteq \langle a \rangle$, ou seja, $\langle a \rangle = \langle b \rangle$. Para (2) $\rightarrow$ (3), como $a \in \langle a \rangle = \langle b \rangle$, segue que $a = br$, para algum $r \in A$. De modo análogo, segue que $b = as$, para algum $s \in A$. Portanto, $a \mid b$ e $b \mid a$. Finalmente, para (3) $\rightarrow$ (1), por hipótese $b = ar$ e $a = bs$, onde $r, s \in A$. Assim, $a = br = a(rs)$. Se $a = 0$, então $b = 0$ e $0 = 0.1$. Se $a \neq 0$, então $rs = 1$, ou seja, r e s são unidades. Portanto, $a \sim b$. □

Proposição 11.2.2. *Sejam A um anel de integridade e $a, b \in A$.*

1. *Se $d, d_1 \in A$ são máximos divisores comuns de a e b, então d e d_1 são associados.*
2. *Se $d = mdc(a, b)$, então todo associado de d também é $mdc(a, b)$.*

Demonstração. Para (1), por hipótese, existem $x, y \in A$ tal que $d_1 = dx$ e $d = d_1 y$. Assim, $d = d(xy)$, e deste modo, $xy = 1$. Portanto, x e y são unidades, ou seja, d e d_1 são associados. Para (2), se $d_1 \in A$ é tal que $d_1 \sim d$, então $d_1 \mid d$. Como $d \mid a$ e $d \mid b$, segue que $d_1 \mid a$ e $d_1 \mid b$. Agora, se existe $d' \in A$ tal que $d' \mid a$ e $d' \mid b$, então $d' \mid d$. Como $d \mid d_1$, segue que $d' \mid d_1$. Portanto, d_1 é um $mdc(a, b)$. □

11.2.1 Exercícios

1. Sejam a e b elementos de um anel comutativo com unidade.
   (a) Mostre que $a \mid b$ se, e somente se, $\langle b \rangle \subseteq \langle a \rangle$.
   (b) Mostre que $a \mid b$ e $b \mid a$ se, e somente se, $\langle a \rangle = \langle b \rangle$.
2. Mostre que a relação de ser associados é de equivalência.
3. Seja A um anel de integridade.
   (a) Mostre que o zero do anel possui somente um associado (o próprio zero).
   (b) Se $u \in A$ é inversível, mostre que o conjunto dos elementos associados a u é A^*, o conjunto das unidades de A.
4. Sejam a e b elementos associados de um anel de integridade e $c \in A$. Mostre que $c \mid a$ se, e somente se, $c \mid b$.
5. Defina $mdc(a_1, a_2, \cdots, a_n)$, onde $a_1, \cdots, a_n \in A$ são não nulos e A é um domínio. Mostre que dois $mdc(a_1, a_2, \cdots, a_n)$ em A são associados.
6. Sejam A um domínio e $a_1, a_2, \cdots, a_n$ elementos de A tal que $\langle a_1, a_2, \cdots, a_n \rangle = \langle d \rangle$ para algum $d \in A$. Mostre que d é um $mdc(a_1, a_2, \cdots, a_n)$.
7. Sejam A um domínio e $a_1, a_2, \cdots, a_n \in A$ tal que $\langle a_1, a_2, \cdots, a_n \rangle = \langle d \rangle$. Mostre que existe $mdc(a_1, a_2, \cdots, a_n)$ e é igual a d.
8. Detemine o conjunto das unidades dos anéis $\mathbb{Z}$ e $\mathbb{Q}$.
9. Determine o conjunto das unidades do anel $M_2(\mathbb{Z})$.
10. Dê exemplo de um anel, onde o conjunto das unidade de um anel A é vazio.
11. Verdadeiro ou falso. Sejam A um domínio, a, b e c em A.
    (a) Se a divide b e a divide c, então a divide $b + c$.
    (b) Se a divide $b + c$ e a divide b, então a divide c.
    (c) Se a e b são unidades, então a e b são associados.

11.3 Ideal

Vamos ver agora uma classe de subanéis que é muito importante na teoria dos anéis, que é a classe dos ideais de um anel. Em teoria dos anéis um ideal é um subconjunto especial de um anel. O conceito generaliza de uma maneira apropriada algumas importantes propriedades dos inteiros como número par e múltiplo de 3.

O conceito de ideais foi propostos primeiramente por Dedekind em 1876 na terceira edição do seu livro Vorlesungen über Zahlentheorie (Seminários em Teoria dos Números). Foram uma generalização para o conceito de número ideal desenvolvido por Ernst Eduard Kummer. Mais tarde o conceito foi expandido por David Hilbert, e especialmente, por Emmy Noether.

Definição 11.3.1. *Sejam A um anel e I um subanel de A. O subanel I é chamado um ideal de A se $ax, xa \in A$ para todo $a \in A$ e $x \in I$. Um ideal I de A é próprio se $I \neq A$.*

Exemplo 11.3.1. *Os conjuntos $\{0\}$ e A são ideais de A. Esses ideais são chamados de ideais triviais de A, enquanto que os ideais não triviais de A são chamados ideais próprios de A.*

Exemplo 11.3.2. *Todo ideal em um anel A é, por definição, um subanel de A. Contudo, a recíproca não vale. Por exemplo, $\mathbb{Z}$ é um subanel de $\mathbb{Q}$ mas não é um ideal em $\mathbb{Q}$, uma vez que $1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$, mas $\frac{1}{2}.1 = \frac{1}{2} \notin \mathbb{Z}$.*

Exemplo 11.3.3. *No anel $\mathbb{Z}$ os subconjuntos $n\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\}$, onde n é um número inteiro, são ideais, uma vez que*

1. *$0 \in n\mathbb{Z}$, pois $0 = n0$.*
2. *$nq_1 - nq_2 = n(q_1 - q_2) \in n\mathbb{Z}$, para todo $q_1, q_2 \in \mathbb{Z}$.*
3. *$a(nq) = n(aq) \in n\mathbb{Z}$, para todo $a \in \mathbb{Z}$.*

Definição 11.3.2. *Um anel A é chamado simples se seus únicos ideais são os triviais.*

Proposição 11.3.1. *Se I é um ideal de um anel A, então*

1. *$0 \in I$, ou seja, o zero (elemento neutro) de A pertence a I.*
2. *Se $a \in I$, então $-a \in I$.*
3. *Se $a, b \in I$, então $a + b \in I$.*
4. *Se o anel A possui unidade e se existe um elemento inversível $b \in A$ tal que $b \in I$, então $I = A$.*

Demonstração. Para (1), como $I \neq \emptyset$, segue que existe $a \in I$. Assim, $0 = a - a \in I$. Para (2), seja $a \in I$. Como $0 \in I$ (devido à parte (1)), segue que $0 - a = -a \in I$. Para (3), se $a, b \in I$ então $a, -b \in I$, pela parte (2). Assim, $a - (-b) = a + b \in I$. Para (3), se $a \in A$, então $a = a.1$. Como b é inversível, segue que existe um elemento $c \in A$ tal que $bc = 1$. Assim, $a = (ab)c$ e, pela definição de ideal, segue que $ab \in I$, e consequentemente, que $(ab)c \in I$, o que implica que $a \in I$. Provamos, assim, que $A \subset I$. Como $I \subset A$, pois I é ideal de A, segue que $A = I$. □

Corolário 11.3.1. *Um subconjunto não vazio I de um anel A é um ideal de A se, e somente se, $a - b \in I$, para todo $a, b \in I$, e xa e ax pertencem a I, para todo $a \in A$ e $x \in I$.*

Sejam A um anel comutativo e $a_1, a_2, \cdots, a_n \in A$, com $n \geq 1$. O conjunto $\langle a_1, a_2, \cdots, a_n\rangle = \{x_1a_1 + x_2a_2 + \cdots + x_na_n \mid x_1, x_2, \cdots, x_n \in A\}$ é um ideal em A, uma vez que

1. $0 = 0a_1 + 0a_2 + \ldots + 0a_n \in \langle a_1, a_2, \cdots, a_n\rangle$.

2. Se $a, b \in \langle a_1, a_2, \cdots, a_n\rangle$ então existem $x_1, \cdots, x_n \in A$ tal que $a = x_1a_1 + \cdots + x_na_n$ e existem $y_1, \cdots, y_n \in A$ tal que $b = y_1a_1 + \cdots + y_na_n$. Assim, $a - b = (x_1 - y_1)a_1 + \cdots + (x_n - y_n)a_n \in \langle a_1, a_2, \cdots, a_n\rangle$.

3. Se $a \in A$ e $b \in \langle a_1, a_2, \ldots, a_n\rangle$, então existem $x_1, \cdots, x_n \in A$ tal que $b = x_1a_1 + \cdots + x_na_n$. Assim, $ab = a(x_1a_1 + \cdots + x_na_n) = (ax_1)a_1 + \cdots + (ax_n)a_n \in \langle a_1, a_2, \cdots, a_n\rangle$.

Portanto, $\langle a_1, a_2, \cdots, a_n\rangle$ é um ideal de A. Em particular, $\langle a\rangle = \{ax : x \in A\}$, onde $a \in A$, é um ideal.

Definição 11.3.3. *O ideal $\langle a_1, a_2, \cdots, a_n\rangle$ é chamado ideal gerado por $a_1, a_2, \cdots, a_n$. Um ideal gerado por um só elemento $a \in A$ recebe o nome de ideal principal gerado por a. Neste caso, além da notação $\langle a\rangle$, também é comum usar a notação aA. Se todos os ideais de um anel são principais, então este anel é chamado de anel principal.*

Exemplo 11.3.4. *Se I é um ideal em $\mathbb{Z}$, então existe $n \in \mathbb{Z}$ de tal modo que $I = n\mathbb{Z}$, ou seja, $\mathbb{Z}$ é um anel principal. De fato, seja I um ideal em $\mathbb{Z}$. Se I tem apenas o elemento zero de $\mathbb{Z}$, ou seja, $I = \{0\}$, segue que I é principal pois $\langle 0\rangle = \{0\}$. Agora, se $I \neq \{0\}$ então, pelo princípio do menor inteiro, segue que existe $b \in I$, sendo o menor dos elementos de I que são estritamente positivos. O fato de $x \in I$ implica que $-x \in I$, o que garante a existência de um elemento estritamente positivo em I. Agora, se $a \in I$, pelo algoritmo da divisão, segue que existem $q, r \in \mathbb{Z}$ tal que $a = bq + r$, onde $0 \leq r < b$. Assim, $r = a - bq$, o que implica que $r \in I$, uma vez que $a, b \in I$. Como b é o menor elemento estritamente positivo de I, segue que não é possível que $0 < r < b$. Portanto, $r = 0$ e, assim, $a = bq$, ou seja, $a \in \langle b\rangle$. Com isso provamos que $I \subset \langle b\rangle$. Como naturalmente $\langle b\rangle \subset I$, uma vez que $b \in I$, segue que $I = \langle b\rangle$.*

Proposição 11.3.2. *Seja A um domínio principal. Se $a, b \in A$, então existem $h_1, h_2 \in A$ de maneira que o elemento $d = ah_1 + bh_2$ é um máximo divisor de a e b.*

Demonstração. Seja o ideal $I =< a, b >= \{am_1 + bm_2 : m_1, m_2 \in A\}$. Como todo ideal em A é principal, segue que existe $d \in I$ de maneira que $I =< d >$. Mostremos que d é um máximo divisor comum de a e b. Como $a \in I$, segue que existe $q_1 \in A$ tal que $a = dq_1$, ou seja, $d \mid a$. Como $b \in I$, segue que existe $q_2 \in A$ tal que $b = dq_2$, ou seja, $d \mid b$. Agora, como $d \in I$, segue que existem $h_1, h_2 \in A$ de modo que $d = ah_1 + bh_2$. Finalmente, se $d' \in A$ divide a e divide b, então $d' \mid d$. □

11.3.1 Operações de ideais

Sejam A um anel comutativo com unidade, I e J ideais de A. Sejam I e J ideais de um anel comutativo com unidade A. A soma $I + J = \{x + y : x \in I \text{ e } y \in J\}$ é um ideal de A, sendo o menor ideal de A que contém I e J. Em geral, a soma $\sum_{i\in I} I_i$ (possivelmente infinita) de ideais $(I_i)_{i\in I}$ de A é um ideal de A, sendo o menor ideal de A que contém todos os I_i, onde os elementos são somas $\sum_{i\in I} a_i$, onde $a_i \in I_i$ para todo $i \in I$ e quase todos os a_i são nulos.

A interseção de uma família $(I_i)_{i\in I}$ de ideais de A é um ideal de A e é o maior ideal de A contido em todos os ideais I_i, onde $i \in I$. A união $I \cap J$ de ideais é um ideal de A se, e somente se, $I \subseteq J$ ou $J \subseteq I$.

O produto de dois ideais I e J de A é definido como $IJ = \langle xy : x \in I \text{ e } y \in J\rangle = \{a_1b_1 + \cdots + a_nb_n \,|\, a_i \in I \text{ e } b_i \in J, i = 1, 2, \cdots, n; \text{ para } n = 1, 2, \cdots\}$. Analogamente, definimos o produto de qualquer família finita de ideais. Em particular, as potências I^n de um ideal I de A são definidos de modo análogo, onde $I^0 = A$. Assim, I^n, com $n > 0$, é o ideal gerado por todos os produtos $x_1x_2 \cdots x_n$, onde cada $x_i \in I$.

Agora, se I, J e K são ideais de um anel A, então $I(J + K) = IJ + IK$. Se $I \supseteq J$ ou $I \supseteq K$, então $I \cap (J + K) = I \cap J + I \cap K$. Em $\mathbb{Z}$ é verdadeiro para todo I, J e K. Além disso, em $\mathbb{Z}$, segue que $(I + J)(I \cap J) = IJ$, mas em geral, segue que $(I + J)(I \cap J) \subseteq IJ$. Também, $IJ \subseteq I \cap J$, e a igualdade é verdadeira quando $I + J = A$, ou seja, quando I e J são coprimos. Assim, I e J são coprimos se, e somente se, $x + y = 1$ para algum $x \in I$ e $y \in J$.

11.3.2 Exercícios

1. Mostre que $\mathbb{Z}$ é um anel principal.

2. Mostre que $\mathbb{Z}_m$ é um anel principal para todo $m > 1$.

3. Sejam A um anel comutativo com unidade, I e J ideais de A.

   (a) Mostre que $I + J$ é um ideal de A e que $I + J$ é o menor ideal de A que contém I e J.

   (b) Mostre que $I \cap J$ é um ideal de A e que $I \cap J$ é o maior ideal A que está contido em I e em J.

   (c) Mostre $I \cup J$ é um ideal de A se, e somente se, $I \subseteq J$ ou $J \subseteq I$.

   (d) Se $I + J = A$, mostre que $IJ = I \cap J$.

   (e) Se $I \cap J = \{0\}$, mostre que $xy = 0$, para todo $x \in I$ e $y \in J$.

   (f) Mostre que o produto IJ é um ideal de A.

   (g) Mostre que $IJ \subseteq I \cap J$.

4. Seja A um anel comutativo com unidade. Mostre que A é um corpo se, e somente se, os únicos ideais de A são os triviais.

5. Mostre que o conjunto dos elementos nilpotentes de um anel comutativo é um ideal.

6. Sejam A um anel e (I_i) uma família de ideais de A.
   (a) Mostre que $\cap_i I_i$ é um ideal de A.
   (b) Se $I_1 \subseteq I_2 \subseteq \cdots$, mostre que $\cup_i^{\infty} I_i$ é um ideal de A.
7. Sejam A um anel comutativo com unidade e $a_1, a_2, \cdots, a_n$ elementos de A. Mostre que $\langle a_1, a_2, \cdots, a_n\rangle$ é o menor ideal de A que contém $\{a_1, a_2, \cdots, a_n\}$.
8. Mostre que todo ideal não nulo de $\mathbb{Z}_n$ é da forma $\langle \overline{d}\rangle$, onde d é um divisor de n, ou seja, $\mathbb{Z}_n$ é um anel de ideais principais.
9. Mostre que o anel $M_2(\mathbb{K})$ das matrizes 2×2 com coeficientes em um corpo $\mathbb{K}$ é um anel simples.
10. Todo subanel de um anel simples é simples?
11. Mostre que todo anel comutativo simples é um corpo.
12. Verifique se $I = \{(2m, 3n) : m, n \in \mathbb{Z}\}$ é um ideal principal de $\mathbb{Z} \times \mathbb{Z}$.
13. Mostre que $\mathbb{Z}_n$, onde $n > 1$, é um anel de ideais principais.
14. Seja $(I_i)_{i\in J}$, onde $J \subseteq \mathbb{N}$, ideais de um anel A. Mostre que $\cap_{i\in I} I_i$ é um ideal de A.
15. Mostre que $K = \{x \in A \mid x^n = 0, \text{ para algum } n \in \mathbb{N}\}$ é um ideal de um anel A.
16. Verifique se $J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in A \right\}$ é um ideal de $M_2(A)$, onde A é um anel.

11.4 Ideal primo e ideal maximal

Nesta seção, apresentamos os conceitos de ideais primos e maximais, elementos primos e irredutíveis, e também, apresentamos algumas de suas propriedades, que serão utilizadas posteriormente.

Definição 11.4.1. *Seja P um ideal num anel comutativo A. O ideal P é chamado um ideal primo se $P \neq A$ e se $ab \in P$ implicar que $a \in P$ ou $b \in P$, para todo $a, b \in A$.*

Exemplo 11.4.1. *O ideal $\{0\}$ em $\mathbb{Z}$ é um ideal primo pois $\{0\} \neq \mathbb{Z}$, e se $ab \in \{0\}$, então $a \in \{0\}$ ou $b \in \{0\}$, uma vez que $\mathbb{Z}$ é um anel de integridade.*

Exemplo 11.4.2. *Os ideais primos não nulos de $\mathbb{Z}$ são os $p\mathbb{Z}$, onde p é um primo de $\mathbb{Z}$. De fato, seja $n\mathbb{Z}$ um ideal de $\mathbb{Z}$ e suponha que $n\mathbb{Z}$ é um ideal primo. Se n não for primo, então existem $a, b \in \mathbb{Z}$ tal que $n = ab$, onde $1 < a, b < n$. Como, por hipótese, estamos supondo que $n\mathbb{Z}$ é primo, segue que a ou b pertencem a $n\mathbb{Z}$. Suponha que $a = kn$ com $k \in \mathbb{Z}$. Assim, $n = knb$ ou $n(1 - kb) = 0$, e como estamos no domínio $\mathbb{Z}$, segue que $n = 0$ ou $1 - kb = 0$, isto é, $n = 0$ ou $b = 1$. Como $n \neq 0$ e $b \neq 1$, segue que n é primo. Por outro lado, suponha que p é primo e $xy \in p\mathbb{Z}$. Logo, p divide xy, e pelo Algoritmo de Euclides, segue que p divide x ou p divide y, isto é, $x \in p\mathbb{Z}$ ou $y \in p\mathbb{Z}$. Portanto, $p\mathbb{Z}$ é um ideal primo.*

Seja $A = \mathbb{Z}$ e p um número primo. O ideal $\langle p\rangle$ é um ideal primo, uma vez que que $1 \notin \langle p\rangle$, pois $p \neq \pm 1$. Assim, $\langle p\rangle \neq \mathbb{Z}$. Por outro lado, se $ab \in \langle p\rangle$, com $a, b \in \mathbb{Z}$, então p divide ab, e assim, p divide a ou p divide b. Portanto, $a \in \langle p\rangle$ ou $b \in \langle p\rangle$, o que prova que $\langle p\rangle$ é um ideal primo de $\mathbb{Z}$. Reciprocamente, se $\langle p\rangle$ é um ideal primo, então p é um número primo.

Exemplo 11.4.3. *$\{0\} \times \mathbb{Z} \subseteq \mathbb{Z} \times \mathbb{Z}$ é um ideal primo.*

Definição 11.4.2. *Sejam A um anel comutativo e $M \subseteq A$ um ideal. O ideal M é chamado um ideal maximal de A se $M \neq A$ e se o único ideal de A que contém M, e que é diferente de M, é o próprio anel A. Ou seja, M é um elemento maximal, em relação à inclusão, no conjunto dos ideais de A que são diferentes de A, ou ainda, se existir um ideal J do anel A tal que $M \subset J \subset A$, então $M = J$ ou $J = A$.*

Definição 11.4.3. *Sejam A um anel comutativo e $m \subseteq A$ um ideal. O ideal m é chamado um ideal minimal de A se $m \neq \{0\}$ e se o único ideal de A que está contido em m, e que é diferente de m, é o ideal $\{0\}$. Ou seja, m é um elemento minimal, em relação à inclusão, no conjunto dos ideais de A que são diferentes de $\{0\}$, ou ainda, se existir um ideal J do anel A tal que $\{0\} \subset J \subset m$, então $m = J$ ou $J = \{0\}$.*

Exemplo 11.4.4. *Se $M = \langle p\rangle$, onde p é um número primo, então M é um ideal maximal de $\mathbb{Z}$. De fato, suponhamos que J é um ideal de $\mathbb{Z}$ tal que $\langle p\rangle \subset J \subset \mathbb{Z}$. Como $\mathbb{Z}$ é um domínio principal, segue que existe $a \in \mathbb{Z}$ tal que $J = \langle a\rangle$. Logo, $p \in \langle p\rangle \subset \langle a\rangle \subset \mathbb{Z}$. Assim, $p \in \langle p\rangle$, e deste modo, $p \in \langle a\rangle$, o que implica que a divide p. Logo, $a = \pm 1$ ou $a = \pm p$, uma vez que p é primo. Portanto, $J = \mathbb{Z}$ ou $J = \langle p\rangle$, que mostra que $\langle p\rangle$ é um ideal maximal de $\mathbb{Z}$.*

Exemplo 11.4.5. *O ideal $2\mathbb{Z} \times \mathbb{Z} \subseteq \mathbb{Z} \times \mathbb{Z}$ é um ideal maximal. De fato: se $2\mathbb{Z} \times \mathbb{Z} \subsetneq I$, então o elemento $(2r + 1, s) \in I$, para algum $r, s \in \mathbb{Z}$. Como $(2r, s - 1) \in I$, pois $(2r, s - 1) \in 2\mathbb{Z} \times \mathbb{Z}$, segue que $(1, 1) \in I$. Assim, $I = \mathbb{Z} \times \mathbb{Z}$.*

Teorema 11.4.1. *Todo ideal maximal M de um anel comutativo com unidade A é um ideal primo.*

Demonstração. Sejam $a, b \in A$ com $ab \in M$. Suponhamos que a não pertença a M. Seja o conjunto $\langle a\rangle + M \subset A$. Como a não pertence a M, segue que $M \subsetneq \langle a\rangle + M$. Logo, $\langle a\rangle + M = A$, pois M é um ideal maximal. Desta forma, $1 = ax + m$, para algum $x \in A$ e para algum $m \in M$. Assim, $b = (ab)x + bm \in M$ e portanto, M é primo. □

A recíproca do Teorema 11.4.1, em geral, não é verdadeira. O próximo teorema fornece uma condição para que a recíproca seja verdadeira.

Teorema 11.4.2. *Se A for um domínio principal, então todo ideal primo não nulo de A é maximal.*

Demonstração. Seja P um ideal primo de A tal que $P \neq A$. Seja J um ideal de A tal que $P \subset J \subset A$. Como P e J são ideais de A, segue que existem $a, b \in A$ tal que $P = \langle a\rangle$ e $J = \langle b\rangle$. Como $P \subset J$, segue que $\langle a\rangle \subset \langle b\rangle$. Assim, $a \in \langle b\rangle$, ou seja, existe $q \in A$ tal que $a = bq \in P$.

Como P é primo, segue que $b \in P$ ou $q \in P$. Analisemos os casos. Se $b \in P = \langle a \rangle$, então existe $s \in A$ tal que $b = as$. Assim, $b \in \langle a \rangle$. Como $a = bq$ e $b = as$, segue que $\langle a \rangle = \langle b \rangle = P = J$. Por outro lado, se $q \in P = \langle a \rangle$, então existe $t \in A$ tal que $q = at$. Assim, $a = bq = bat$, e deste modo, $1 = bt$. Logo, b é inversível, e assim, $J = A$. Portanto, P é um ideal maximal. □

11.4.1 Exercícios

1. Determinar todos os ideais de $\mathbb{Z}_8$.
2. Seja A um anel comutativo com unidade. Mostre que $\langle 0 \rangle$ é primo se, e somente se, A é um anel de integridade.
3. Seja A um anel comutativo com unidade.
   (a) Mostre que $\langle 0 \rangle$ é primo se, e somente se, A é um anel de integridade.
   (b) Mostre que A é um anel de integridade se, e somente se, todo elemento de A é regular em relação a multiplicação.
4. Mostre que $\mathbb{Z}_m$ é um anel de integridade se, e somente se, m é primo.
5. Seja A um anel comutativo com unidade.
   (a) Mostre que A possui um ideal maximal.
   (b) Se I é um ideal de A, mostre que A possui um ideal maximal que contém I.
   (c) Mostre que as unidades de A estão contidas em um ideal maximal.
6. Dê exemplo de ideais primos que não são maximais.
7. Sejam A um anel comutativo com unidade e $I \subseteq A$ um ideal de A.
   (a) Se $a \in A$, mostre que $a + I$ é inversível se, e somente se, existe $x \in A$ tal que $ax - 1 \in I$, onde $a + I = \{a + x : x \in I\}$.
   (b) Mostre que $\langle 0 \rangle$ é primo se, e somente se, A é um anel de integridade.
8. Mostre que num anel finito todo ideal primo é maximal.
9. Seja $A = \{f : [0, 1] \to \mathbb{R} : f \text{ é contínua}\}$.
   (a) Mostre que A é um anel.
   (b) Mostre que $I = \{f \in A : f(1/2) = 0\}$ é um ideal.
   (c) Mostre que I é maximal.
10. Se $\mathbb{K}$ é um anel comutativo com unidade, então as seguintes condições são equivalentes:
    (a) $\mathbb{K}$ é um corpo.
    (b) $\{0\}$ é um ideal maximal em $\mathbb{K}$.

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

11. Sejam A um anel comutativo com unidade e I, J e P ideais de A.

(a) Se P é primo e $IJ \subseteq P$, mostre que $I \subseteq P$ ou $J \subseteq P$.

(b) Se $IJ \subseteq P$ implica que $I \subseteq P$ ou $J \subseteq P$, mostre que P é um ideal primo de A.

12. Mostre que $I = \langle 2 + 2i \rangle$ não é um ideal primo de $\mathbb{Z}[i]$.

13. Seja A um anel.

(a) Sejam $P_1, P_2, \cdots, P_n$ ideais primos de A e I um ideal de A. Se $I \subseteq \cup_{i=1}^{n} P_i$, mostre que $I \subseteq P_i$, para algum i.

(b) Sejam $I_1, I_2, \cdots, I_n$ ideais de A e P um ideal primo de A. Se $P \subseteq \cap_{i=1}^{n} I_i$, mostre que $P \subseteq I_i$, para algum i. Se $P = \cap_{i=1}^{n} I_i$, mostre que $P = I_i$, para algum i.

14. Se A é o anel das funções contínuas de $\mathbb{R}$ em $\mathbb{R}$, mostre que $I = \{f \in A : f(0) = 0\}$ é um ideal maximal de A.

15. Se A é o anel das funções contínuas de $\mathbb{R}$ em $\mathbb{R}$, mostre que $I = \{f \in A : f(0) = 0\}$ é um ideal maximal de A.

16. Seja $A = \{f : [0, 1] \to \mathbb{R} : f \text{ é contínua}\}$.

(a) Mostre que A é um anel.

(b) Mostre que $I = \{f \in A : f(1/2) = 0\}$ é um ideal maximal de A.

11.5 Anel quociente

Sejam A um anel comutativo com unidade e $I \subseteq A$ um ideal. Consideremos a relação $\sim$ sobre A, em relação a I, definida por $x \sim y \iff x - y \in I$, para todo $x, y \in A$. Trata-se de uma relação de equivalência sobre A pois,

1. Como $0 \in I$, segue que $x - x \in I$, para todo $x \in A$. Portanto, $x \sim x$, para todo $x \in A$.

2. Se $x \sim y$ então $x - y \in I$, e assim, $-(x - y) \in I$. Logo, $y - x \in I$, e portanto, $y \sim x$.

3. Se $x \sim y$ e $y \sim z$, então $x - y \in I$ e $y - z \in I$. Assim, $(x - y) + (y - z) \in I$, ou seja, $x - z \in I$. Portanto, $x \sim z$.

O conjunto das classes de equivalências será denotado por A/I.

Proposição 11.5.1. *Se a classe de equivalência de um elemento $a \in A$ é indicado por $\overline{a}$, então $\overline{a} = \{a + i : i \in I\}$.*

Demonstração. Indiquemos num primeiro momento o conjunto $\{a+i \mid i \in I\}$ por E e provamos que $\overline{a} \subset E$ e $E \subset \overline{a}$. Seja $x \in A$. Se $x \in \overline{a}$ então $x \sim a$, ou seja, $x - a \in I$. Logo, existe $i_1 \in I$ tal que $x - a = i_1$, ou seja, existe $i_1 \in I$ tal que $x = a + i_1$. Assim, $x \in E$, e portanto, $\overline{a} \subset E$. Agora, para a outra inclusão, se $x \in E$, então existe $i_1 \in I$ tal que $x = a + i_1$, ou seja, existe $i_1 \in I$ tal que $x - a = i_1$. Assim, $x - a \in I$, ou seja, $x \sim a$. Logo, $x \in \overline{a}$, e deste modo, $E \subset \overline{a}$. Portanto, $\overline{a} = \{a + i \mid i \in I\}$. □

Com base na Proposição 11.5.1 indicamos por $a + I$ a classe de equivalência $\overline{a}$, a qual é chamada classe lateral determinada por a módulo I em A. Assim, para $a, b \in A$, segue que $a \sim b \Leftrightarrow a + I = b + I$, conforme a próxima proposição.

Proposição 11.5.2. *Sejam $a, b \in A$. Assim, $a - b \in I$ se, somente se, $a + I = b + I$.*

Demonstração. Sejam $a, b \in A$ tal que $a - b \in I$. Se $y \in a + I$, então existe $x \in I$ tal que $y = a+x$, e deste modo, $y = b+(-b)+a+x = b+(a-b)+x$. Logo, existe $x_1 = (a-b)+x \in I$ tal que $y = b + x_1$. Assim, $y \in b + I$, e portanto, $a + I \subset b + I$. De modo análogo, segue que $b + I \subset a + I$, e portanto, $a + I = b + I$. Reciprocamente, como $a \in a + I$, segue que $a \in a + I = b + I$. Assim, existe $x \in I$ tal que $a = b + x$. Logo, $a - b = x \in I$, e portanto, $a - b \in I$. □

Agora, definimos as operações de adição e multiplicação no conjunto quociente A/I. Para a *adição* em A/I, segue que a operação $(a + I) + (b + I) = (a + b) + I$, para todo $a, b \in A$, define uma lei de composição interna em A/I, uma vez que se $a + I = a' + I$ e $b + I = b' + I$, então $a - a' \in I$ e $b - b' \in I$. Assim, $(a - a') + (b - b') = (a + b) - (a' + b') \in I$, ou seja, $(a + b) + I = (a' + b') + I$. Essa lei de composição interna é a adição em A/I. Relativamente a essa adição, segue que A/I é um grupo abeliano, uma vez que para todo $a, b, c \in A$, segue que

1. $(a+I)+[(b+I)+(c+I)] = (a+I)+[(b+c)+I] = [a+(b+c)]+I = [(a+b)+c]+I = [(a+b)+I]+(c+I) = [(a+I)+(b+I)]+(c+I)$. Portanto, a operação é associativa.

2. $(a + I) + (b + I) = (a + b) + I = (b + a) + I = (b + I) + (a + I)$. Portanto, a operação é comutativa.

3. O elemento neutro é a classe $0 + I = I$, ou seja, o próprio ideal I, onde 0 é o elemento neutro de A.

4. Se $a \in A$, então para cada classe $a + I$, a classe $(-a) + I$ é o seu elemento oposto, pois $(a + I) + (-a + I) = (a - a) + I = 0 + I = I$. Logo, $-(a + I) = (-a) + I$.

Assim, $\overline{a} = \overline{b}$ se, e somente se, $a - b \in I$ e $\overline{a} = \overline{0}$ se, e somente se, $a \in I$.

Para a *multiplicação* em A/I, segue que a operação $(a + I)(b + I) = ab + I$ para todo $a, b \in I$, define uma lei de composição interna em A/I, uma vez que se $a + I = a' + I$ e $b + I = b' + I$, então $a - a' \in$ e $b - b' \in I$. Assim, $b(a - a') \in I$ e $a'(b - b') \in I$. Logo, $b(a - a') + a'(b - b') = ba - ba' + a'b - a'b' = ba - b'a' \in I$. Isto significa que $ba + I = b'a' + I$. Esta multiplicação apresenta as seguintes propriedades, para todo $a, b, c \in A$,

1. $(a+I)[(b+I)(c+I)] = (a+I)[(bc)+I] = [a(bc)]+I = [(ab)c]+I = [(ab)+I](c+I) = [(a+I)(b+I)](c+I)$, isto é, é associativa.

2. $(a+I)(b+I) = (ab)+I = (ba)+I = (b+I)(a+I)$, isto é, é comutativa.

3. $(a+I)[(b+I)+(c+I)] = (a+I)[(b+c)+I] = [a(b+c)]+I = [ab+ac]+I = (ab+I)+(ac+I) = (a+I)(b+I)+(a+I)(c+I)$, isto é, é distributiva em relação à adição.

Definição 11.5.1. *Sejam A um anel comutativo e I um ideal em A. O anel $(A/I, +, .)$ é chamado anel quociente de A por I.*

Além disso, se o anel A possui unidade, então o anel A/I também possui unidade dada pela classe $1+I$, onde 1 indica a unidade do anel A. Portanto, neste caso, $(A/I, +, .)$ é também um anel comutativo com unidade se A for anel comutativo com unidade. Agora, se A é um domínio $I \subseteq A$ é um ideal, não implica que A/I é um domínio, uma vez que $\mathbb{Z}$ é um domínio, mas $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}_6$ não é um domínio porque $2.3 = 0$.

11.5.1 Exercícios

1. Seja $\mathbb{Z}$ o anel dos inteiros.

   (a) Mostre que $\mathbb{Z}$ é um anel principal.

   (b) Mostre que $P =< m >\subseteq \mathbb{Z}$ é um ideal primo se, e somente se, $m \in \mathbb{Z}$ é primo.

   (c) Mostre que todo ideal primo de $\mathbb{Z}$ é um ideal maximal.

   (d) Mostre que $\mathbb{Z}_m$ é um anel de integridade se, e somente se, m é primo.

   (e) Mostre que todos os ideais de $\mathbb{Z}_m$ são principais.

2. Seja A um anel comutativo com unidade e I um ideal de A.

3. Mostre que todo ideal maximal de A é um ideal primo. E a recíproca vale?

4. Sejam A um anel comutativo com unidade e $I \subseteq A$ um ideal.

   (a) Mostre que I é um ideal primo se, e somente se, A/I é um domínio.

   (b) Mostre que I é um ideal maximal se, e somente se, A/I é um corpo.

5. Sejam A um anel comutativo com unidade e $I \subseteq A$ um ideal. Mostre que existe uma bijeção entre os ideais de A que contém I e os ideais de A/I.

6. Dê exemplo de uma anel de integridade A e de um ideal I de A, onde A/I não é de integridade.

7. Sejam A um anel e I o ideal dos elementos nilpotentes de A. Mostre que I é o único elemento nilpotente de A/I.

8. Seja A um domínio principal. Se I é um ideal de A, mostre que A/I é um anel principal.

9. Sejam A um anel, I e J ideais de A. Mostre que $I \cap J$ é o maior ideal de A que está contido em I e em J.

10. Sejam A um anel comutativo com unidade e I, J ideais de A.

    (a) Mostre que $K = \{x \in A \mid xy \in I, \ \forall y \in J\}$ é um ideal de A.

    (b) Mostre que $a + I$ é inversível se, e somente se, existe $x \in A$ tal que $ax - 1 \in I$.

    (c) Mostre que $I \cup J$ é um ideal se, e somente se, $I \subseteq J$ ou $J \subseteq I$.

    (d) Mostre que $I \cap J$ é o maior ideal que está contido em I e em J.

    (e) Mostre que $I + J$ é o menor ideal que contém I e J.

11. Seja A um anel comutativo com unidade.

    (a) Se A é finito, mostre que todo ideal primo de A é maximal.

    (b) Se A é um corpo, mostre que A é um anel de integridade.

    (c) Se A é um anel de integridade e finito, mostre que A é um corpo.

12. Seja A um anel comutativo com unidade e I um ideal de A.

    (a) Mostre que todo ideal maximal de A é um ideal primo. E a recíproca vale?

    (b) Mostre que I é um ideal maximal se, e somente se, A/I é um corpo.

    (c) Mostre que I é um ideal primo se, e somente se, A/I é um domínio.

    (d) Seja $(I_i)_{i \in J}$, onde $J \subseteq \mathbb{N}$, ideais de A. Mostre que $\cap_{i \in I} I_i$ é um ideal de A.

    (e) Mostre que $K = \{x \in A \mid x^n = 0, \text{ para algum } n \in \mathbb{N}\}$ é um ideal de A.

    (f) Verifique se $J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in A \right\}$ é um ideal de $M_2(A)$.

13. Sejam A um anel comutativo com identidade e $I \subseteq A$ um ideal de A.

    (a) Se $a \in A$, mostre que $a + I$ é inversível se, e somente se, existe $x \in A$ tal que $ax - 1 \in I$, onde $a + I = \{a + x : x \in I\}$.

14. Mostre que num anel finito todo ideal primo é maximal.

15. Seja A um domínio principal. Se I é um ideal de A, mostre que A/I é um anel principal.

11.6 Homomorfismo de anéis

O conceito de homomorfismo de anéis é bastante similar ao conceito de homomorfismo de grupos, com a diferença que um anel possui duas operações.

Definição 11.6.1. *Sejam A e B anéis comutativos com unidade.*

1. *Uma aplicação $f : A \longrightarrow B$ é chamada um homomorfismo de anéis se, para todo $x, y \in A$, segue que $f(x + y) = f(x) + f(y)$ e $f(xy) = f(x)f(y)$.*

2. *Se, além disso, f for bijetora, a aplicação f é denominada de isomorfismo, e que os anéis A e B são ditos isomorfos, e neste caso, usamos notação $A \simeq B$.*

3. *Se f é um isomorfismo e $A = B$, a aplicação f é chamada um automorfismo.*

Pela Definição 11.6.1, segue que

1. $f(-a) = -f(a)$, para todo $a \in A$,

2. $f(0_A) = 0_B$, onde 0_A e 0_B são os elementos neutros de A e B, respectivamente, pois $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A)$, o que implica, por cancelamento, que $f(0_A) = 0_B$.

3. $f(na) = nf(a)$, para todo $n \in \mathbb{Z}$ e $a \in A$.

4. $f(-a) = -f(a)$, para todo $a \in A$.

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

Exemplo 11.6.1.

1. *Seja $A = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. A aplicaão $f : A \to A$ definida por $f(a + b\sqrt{2}) = a - b\sqrt{2}$ é um isomorfismo.*

2. *A aplicação $f : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ definida por $f(a) = (\overline{a}, \overline{a})$ é um isomorfismo.*

3. *$\mathbb{Z}_4$ não é isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. De fato: se $f : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ é um isomorfismo, então $f(0) = (0, 0)$ e $f(1) = (1, 1)$. Mas $f(2) = f)(1+1) = f(1)+f(1) = (1, 1)+(1, 1) = (0, 0)$. Portanto, f não é injetora.*

4. *Se $f : A \to B$ e $g : B \to C$ são isomorfismos de anéis, então $g \circ f : A \to C$ é um isomorfismo.*

Definição 11.6.2. *Seja $f : A \longrightarrow B$ um homomorfismo de anéis comutativos com unidade. O núcleo (ou kernel) da aplicação f é definido por* $\ker(f) = \{x \in A : f(x) = 0_B\}$ *e a imagem da aplicação f é definida por $Im(f) = \{f(x) : x \in A\}$.*

Proposição 11.6.1. *Se $f : A \longrightarrow B$ é um homomorfismo de anéis, então* $\ker(f)$ *é um ideal do anel A.*

Demonstração. Como $f(0_A) = 0_B$, segue que $0_A \in Ker(f)$. Agora, se $x, y \in Ker(f)$, então $f(x) = f(y) = 0$. Assim, $f(x - y) = f(x) - f(y) = 0 - 0 = 0$, ou seja, $x - y \in Ker(f)$. Finalmente, se $x \in Ker(f)$ e $a \in A$, então $f(ax) = f(a)f(x) = f(a)0 = 0$, ou seja, $ax \in Ker(f)$. Portanto, $Ker(f)$ é um ideal em A. □

Seja $f : A \longrightarrow B$ um homomorfismo de anéis.

1. f é injetora se, e somente se, $\ker(f) = \{0\}$.

2. f é um isomorfismo se, e somente se, f^{-1} é um isomorfismo.

Proposição 11.6.2. *Seja $f : A \longrightarrow B$ é um homomorfismo de anéis comutativos com unidade. Se J é um ideal de B, então $f^{-1}(J)$ é um ideal em A.*

Demonstração. Como $f(0_A) = 0_B \in J$, segue que $0_A \in f^{-1}(J)$. Agora, se $x, y \in f^{-1}(J)$ então $f(x), f(y) \in J$, e assim, $f(x) - f(y) \in J$. Logo, $f(x - y) \in J$, ou seja, $x - y \in f^{-1}(J)$. Finalmente, se $a \in A$ e $x \in f^{-1}(J)$, então $f(x) \in J$, e assim, $f(ax) = f(a)f(x) \in J$. Logo, $ax \in f^{-1}(J)$. Portanto, $f^{-1}(J)$ é um ideal em a. □

Teorema 11.6.1. *(Teorema do Isomorfismo para Anéis) Se $f : A \longrightarrow B$ é um homomorfismo de anéis, então $A/\ker(f) \simeq Im(f)$.*

Demonstração. Seja a aplicação $\varphi : A/\ker(f) \longrightarrow Im(f)$ definida por $\varphi(a + \ker(f)) = f(a)$, onde $\overline{a} = a + \ker(f) \in A/\ker(f)$. Mostramos que φ é um homomorfismo bijetor, ou seja, um isomorfismo. Se $a, b \in A$, então $\varphi(\overline{a} + \overline{b}) = \varphi(\overline{a + b}) = f(a + b) = f(a) + f(b) = \varphi(\overline{a}) + \varphi(\overline{b})$ e $\varphi(\overline{a}\overline{b}) = \varphi(\overline{ab}) = f(ab) = f(a)f(b) = \varphi(\overline{a})\varphi(\overline{b})$. Portanto, φ é um homomorfismo. Agora, se $\overline{a} \in \ker(\varphi)$ então $\varphi(\overline{a}) = 0_B$. Assim, $f(a) = 0_B$, ou seja, $a \in \ker(f)$, e deste modo, $\overline{a} = \overline{0}$. Portanto, $\ker(\varphi) = \{\overline{0}\}$, ou seja, φ é injetora. Para a sobrejetora, se $y \in \mathrm{Im}(f)$, então existe $x \in A$ tal que $f(x) = y$. Logo, existe $\overline{x} \in A/\ker(f)$ tal que $\varphi(\overline{x}) = f(x) = y$, e portanto, φ é sobrejetora. Assim, concluímos que φ é um isomorfismo e que $A/\ker(f)$ é isomorfo a $Im(f)$. □

Teorema 11.6.2. *Seja A um anel comutativo com unidade e P um ideal de A, com $P \neq A$. Assim, P é um ideal primo se, e somente se, A/P é um domínio.*

Demonstração. Como A é um anel comutativo com unidade, segue que A/P é um anel comutativo com unidade. Sejam $a, b \in A$. Se $\overline{a}\overline{b} = \overline{0}$, então $ab \in P$. Como P é primo, segue que $a \in P$ ou $b \in P$. Assim, $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$, e portanto, A/P é um domínio. Reciprocamente, se $ab \in P$, então $\overline{a}\overline{b} = \overline{0}$. Como A/P é um domínio, segue que $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. Assim, $a \in P$ ou $b \in P$, e portanto, P é um ideal primo. □

Exemplo 11.6.2. *O ideal $P = \langle p \rangle$ é um ideal primo de $\mathbb{Z}$, uma vez que $\mathbb{Z}/\langle p \rangle \simeq \mathbb{Z}_p$, e como $\mathbb{Z}_p$ é um domínio, segue que $\langle p \rangle$ é um ideal primo de $\mathbb{Z}$.*

Sejam A um anel comutativo com unidade e $I \subseteq A$ um ideal. A aplicação $f : A \to A/I$ definida por $f(a) = a + I$, onde $a \in A$, é um homomorfismo sobrejetor, chamado homomorfismo canônico.

Proposição 11.6.3. *Se A é um anel, B um subanel de A e P um ideal primo de A, então $P \cap B$ é um ideal primo de B.*

Demonstração. Consideremos os seguintes homomorfismos

$$B \xrightarrow{i} A \xrightarrow{\pi} \frac{A}{P},$$

sendo i a inclusão e π a projeção, isto é, $i(b) = b$, onde $b \in B$ e $\pi(a) = a + P$, onde $a \in A$. Seja $\theta = \pi \circ i : \ B \to A/P$ tal que $\theta(b) = b + P$, onde $b \in B$. A aplicação θ é um homomorfismo, pois é composição de homomorfismos. Além disso, $\ker(\theta) = P \cap B$. De fato, se $x \in \ker(\theta)$ então $x \in B$ e $\theta(x) =) + P$, o que implica que $x \in B$ e $x + P = x + 0$, ou seja, $x \in P$. Portanto, $x \in P \cap B$. Logo, $\ker(\theta) \subset P \cap B$. Por outro lado, se $y \in P \cap B$, então $\theta(y) = (\pi \circ i)(y) = \pi(i(y)) = \pi(y) = y + P \overset{y \in P}{=} 0 + P$, e assim, $y \in \ker(\theta)$, ou seja, $P \cap B \subset \ker(\theta)$. Portanto, $\ker(\theta) = P \cap B$. Logo, pelo Teorema 11.6.1, segue que $B/\ker(\theta) \simeq Im(\theta)$. Assim, $B/P \cap B \simeq Im(\theta) \subset A/P$. Mas, como A/P é um domínio, segue que $Im(\theta)$ é um domínio, pois é um subanel de A/P. Assim, $B/(B \cap P)$ é um domínio, o que implica que $B \cap P$ é um ideal primo. □

11.6.1 Exercícios

1. Seja $f : A \to B$ um homomorfismo de anéis.
   (a) Se L é um subanel de A, mostre que $f(L)$ é um subanel de B.
   (b) Se f é sobrejetora, mostre que $f(1) = 1$.
   (c) Se f é sobrejetora e $a \in A$ é inversível, mostre que $f(a)$ é inversível.
   (d) Se $J \subseteq B$ é um ideal, mostre que $f^{-1}(J)$ é um ideal de A.
2. Determine todos os homomorfismos de $\mathbb{Z}$ em $\mathbb{Z}$.
3. Determine todos os homomorfismos de $\mathbb{Q}$ em $\mathbb{Q}$.
4. Sejam $f : A \to B$ um homomorfismo sobrejetor de anéis comutativos com unidade e I um ideal de B.
   (a) Se I é um ideal primo em B, mostre que $f^{-1}(I)$ é um ideal primo de A.
   (b) Se I é um maximal em B, mostre que $f^{-1}(I)$ é um ideal maximal de A.
5. Mostre que a imagem por homomorfismo de um anel de ideais principais é um anel de ideais principais.
6. Sejam A um anel e I um ideal de A. Mostre que existe uma correspondência biunívoca entre os ideais de A que contém I e os ideais do anel quociente A/I.
7. Seja A um anel não nulo. Mostre que A é um corpo se, e somente se, todo homomorfismo não nulo de A em um anel não nulo B é injetor.
8. Sejam A um anel, I e J ideais de A tal que $I + J = A$. Mostre que existe um isomorfismo de A/IJ em $A/I \times A/J$.
9. Sejam A um anel e $I_1, I_2, \cdots, I_n$ ideais de A tal que $I_i + I_j = A$, para todo $i \neq j$. Mostre que existe um isomorfismo de $A/I_1 I_2 \cdots I_n$ em $A/I_1 \times \cdots \times A/I_n$.
10. Sejam $m, n \in \mathbb{N}$. Mostre que $\mathbb{Z}_{mn}$ e $\mathbb{Z}_m \times \mathbb{Z}_n$ são isomorfos se, e somente se, $mdc(m, n) = 1$.

11. Sejam A um anel e $I_1, I_2, \cdots, I_n$ ideais de A. Seja a aplicação $\phi : A \to A/I_1 \times \cdots \times A/I_n$ definida por $\phi(a) = (a + I_1, \cdots, a + I_n)$, onde $a \in A$.

    (a) Mostre que ϕ é um homomorfismo de anéis.

    (b) Se I_i e I_j, para $i \neq j$, são coprimos, mostre que $\prod_{i=1}^{n} I_i = \cap_{i=1}^{n} I_i$.

    (c) Mostre que ϕ é injetora se, e somente se, $\cap_{i=1}^{n} I_i = \{0\}$.

    (d) Mostre que ϕ é sobrejetiva se, e somente se, I_i e I_j são coprimos para todo $i \neq j$.

12. Seja a relação $\sim$ sobre $A = \mathbb{N} \times \mathbb{N}$ definida por $(a, b) \sim (c, d) \leftrightarrow a + d = b + d$. Seja E o conjunto das classes de equivalência. Defina as operações $\oplus$ e $\otimes$ em E por $\overline{(a,b)} \oplus \overline{(c,d)} = (a + c) - (b + d)$ e $\overline{(a,b)} \otimes \overline{(c,d)} = (ac + bd) - (ad + bc)$.

    (a) Mostre que as operações $\oplus$ e $\otimes$ estão bem definidas.

    (b) Mostre que $(E, \oplus, \otimes)$ é um domínio.

    (c) Mostre que a função $f : \mathbb{Z} \to E$, definida por

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

    é um isomorfismo de anéis. Lembre-se que se $a > b$, então $a = b + h$, para algum $h > 0$ e se $a < b$, então $b = a + h$ para algum $h > 0$.

13. Sejam A um anel comutativo com unidade e I, J ideais de A.

    (a) Mostre que $K = \{x \in A \mid xy \in I, \ \forall y \in J\}$ é um ideal de A.

    (b) Mostre que $a + I$ é inversível se, e somente se, existe $x \in A$ tal que $ax - 1 \in I$.

    (c) Mostre que $I \cup J$ é um ideal se, e somente se, $I \subseteq J$ ou $J \subseteq I$.

    (d) Mostre que $I \cap J$ é o maior ideal que está contido em I e em J.

    (e) Mostre que $I + J$ é o menor ideal que contém I e J.

14. Mostre que I é um ideal primo se, e somente se, A/I é um domínio.

15. Seja $f : A \to B$ um homomorfismo de anéis.

    (a) Se L é um subanel de A, mostre que $f(L)$ é um subanel de B.

    (b) Se f é sobrejetora, mostre que $f(1) = 1$.

    (c) Se f é sobrejetora e $a \in A$ é inversível, mostre que $f(a)$ é inversível.

    (d) Se $J \subseteq B$ é um ideal, mostre que $f^{-1}(J)$ é um ideal de A.

16. Mostre que a imagem por homomorfismo de um anel de ideais principais é um anel de ideais principais.

17. Seja A um anel não nulo. Mostre que A é um corpo se, e somente se, todo homomorfismo não nulo de A em um anel não nulo B é injetor.

18. Sejam $m, n \in \mathbb{N}$. Mostre que $\mathbb{Z}_{mn}$ e $\mathbb{Z}_m \times \mathbb{Z}_n$ são isomorfos se, e somente se, $mdc(m, n) = 1$.

11.7 Característica de um anel

Sejam A um anel comutativo com unidade e $S = \{n \in \mathbb{N} - \{0\} : na = 0, \text{ para todo } a \in A\}$ um subconjunto de $\mathbb{N} - \{0\}$. Assim, $S = \emptyset$ ou $S \neq \emptyset$.

Definição 11.7.1. *Se $S = \emptyset$, o anel A é dito que tem característica zero. Se $S \neq \emptyset$, pelo princípio do menor natural existe $h \in S$ que é mínimo de S. Se o mínimo de S é $h > 0$, o anel A é dito que tem característica $h > 0$. A característica de A é denotada por $c(A)$.*

Exemplo 11.7.1. *O Anel $\mathbb{Z}_m$ tem $c(\mathbb{Z}_m) = m$. Os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ tem característica zero.*

Teorema 11.7.1. *Se A é um domínio, então $c(A) = 0$ ou $c(A) = p$, onde p é um número primo.*

Demonstração. Seja A um domínio cuja a característica é diferente de zero, ou seja, $c(A) = h > 0$. Se h não fosse primo, então existiriam dois números naturais r, s não nulos de maneira que $h = rs$, onde $1 < r, s < h$. Assim, $r1_A \neq 0$ e $s1_A \neq 0$, mas $(r1_A)(s1_A) = (rs)1_A = h1_A = 0$, ou seja, $r1_A$ e $s1_A$ são divisores de zero em A, o que é um absurdo pois A é um domínio. □

Exemplo 11.7.2. *O anel $\mathbb{Z}$ tem característica zero, e o anel $\mathbb{Z}_n$ tem característica n, para $n \geq 2$.*

Observação 11.7.1. *Seja A um anel comutativo com unidade.*

1. *$\circ(1) = c(A)$ uma vez que $c(A)1 = 0$ e se $r.1 = 0$, onde $0 \leq r < c(A)$, então $ra = 0$ para todo $a \in A$, o que não ocorre. Portanto, $\circ(1) = c(A)$.*
2. *Se $c(A) = 0$, então A possui uma cópia de $\mathbb{Z}$. De fato, a aplicação $f : \mathbb{Z} \to A$ definida por $f(n) = n1$, onde $n \in \mathbb{Z}$, é um homomorfismo injetor, e portanto, $\mathbb{Z} \backsimeq f(\mathbb{Z}) \subseteq A$.*
3. *Se $c(A) = m \neq 0$, então a aplicação $f : \mathbb{Z}_m \to A$ definida por $f(a) = a1$, onde $a \in \mathbb{Z}_m$, é um hommomorfismo injetor, e portanto, $\mathbb{Z}_m \backsimeq f(\mathbb{Z}_m) \subseteq A$.*

11.7.1 Exercícios

1. Sejam A um anel com unidade e $m, n \in \mathbb{Z}$. Mostre que $(m + n) \times 1 = m \times 1 + n \times 1$ e $(mn) \times 1 = (m \times 1)(n \times 1)$.
2. Mostre que dois anéis isomorfos têm a mesma característica.
3. Dê exemplo de um anel A de característica zero e um elemento $a \in A$ tal que $na = 0$, para algum $n \in \mathbb{N}$.
4. Sejam A e B anéis comutativos com unidade. Mostre que $c(A \times B) = mmc(c(A), c(B))$.
5. Dê exemplo de um anel infinito cuja característica é diferente de zero.
6. Se a característica de um anel é não nula e não prima, mostre que A possui divisores próprios de zero.
7. Se A é um anel e $L \subseteq A$ um subanel, mostre que $c(L) \leq c(A)$.

8. Se $f : A \to B$ é um homomorfismo sobrejetor de anéis, mostre que $c(A) \leq c(B)$.

9. Se A é um anel tal que $a^2 = a$, para todo $a \in A$, mostre que A é comutativo e que $c(A) = 2$.

10. Determine um anel de característica um primo que não é um corpo.

11. Se A é um domínio, mostre que $ca(A) = 0$ ou $ca(A) = p$, onde p é um número primo.

12. Se $f : A \to B$ é um homomorfismo sobrejetor de anéis, mostre que $c(aA) \leq ca(B)$.

13. Se A é um anel tal que $a^2 = a$, para todo $a \in A$, mostre que A é comutativo e que $ca(A) = 2$.

Capítulo

12

Corpos e subcorpos

A teoria de Galois estabelece a relação entre polinômios, corpos e grupos. A relação entre polinômios e corpos está diretamente relacionado aos números algébricos e transcendentes. Os números transcendentes mais conhecidos são π e e. A prova da transcendência de e foi dada por C. Hermite em 1874 e da transcendência de π foi dada por F. Linderman em 1882. A transcendência de $2^{\sqrt{2}}$ foi demonstrada, independentemente, por A. Gelfond e T. Schnesider em 1884.

A conexão entre corpos e grupos é dada pelo Teorema Fundamental de Galois que estabelece uma correspondência entre os subcorpos intermediários de uma extensão finita e os subgrupos do grupo de Galois da extensão.

12.1 Corpos e subcorpos

Nesta seção, apresentemos os conceitos de corpos e subcorpos juntamente com suas principais propriedades.

Definição 12.1.1. *Um anel comutativo com identidade $\mathbb{K}$ é chamado um corpo se todo elemento não nulo de $\mathbb{K}$ é inversível.*

Em um anel A com unidade indicamos por $A^\star$ o subconjunto de A formado pelos elementos que possuem simétrico multiplicativo, ou seja, $A^\star$ é formado pelos elementos inversíveis de A. Assim, um corpo $\mathbb{K}$ é um anel comutativo com unidade tal que $\mathbb{K}^\star = \mathbb{K} - \{0\}$.

Exemplo 12.1.1. *O anel $\mathbb{Z}$ não é um corpo, pois $\mathbb{Z}^\star = \{1, -1\}$. No entanto, os anéis $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos.*

Exemplo 12.1.2. *Um exemplo de um anel (não comutativo) com divisão que não é um corpo é o anel dos quatérnios de Hamilton que é dado por*

$$\mathbb{H} = \{a + bi + cj + dk; a, b, c, d \in \mathbb{R}\},$$

onde $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$ *e* $ik = -j$. *Neste caso, se* $x = a + bi + cj + dk \in \mathbb{H}$, *com* $x \neq 0$, *então* $a^2 + b^2 + c^2 + d^2 \neq 0$ *e* $x^{-1} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2} \in \mathbb{H}$ *é tal que* $xx^{-1} = 1 = x^{-1}x$. *Logo,* $\mathbb{H}$ *é um anel com divisão que não é um corpo, pois não é comutativo.*

Proposição 12.1.1. *Todo corpo* $\mathbb{K}$ *é um domínio de integridade.*

Demonstração. Sejam a e b elementos de $\mathbb{K}$ tal que $ab = 0$. Se a é não nulo, então existe $a^{-1} \in \mathbb{K}$. Assim, $a^{-1}(ab) = a^{-1}0$, ou seja, $b = 0$. Logo, vale a lei do anulamento do produto em $\mathbb{K}$, e portanto, $\mathbb{K}$ é um domínio. □

Observação 12.1.1. *A recíproca da Proposição 12.1.1 não é válida, uma vez que* $\mathbb{Z}$ *é um domínio mas não é um corpo.*

Definição 12.1.2. *Sejam* $\mathbb{K}$ *e* $\mathbb{L}$ *corpos. Uma aplicação* $\sigma : \mathbb{K} \to \mathbb{L}$ *é chamada de homomorfismo de corpos se* $\sigma(x + y) = \sigma(x) + \sigma(y)$ *e* $\sigma(xy) = \sigma(x)\sigma(y)$, *para todo* $x, y \in \mathbb{K}$.

Definição 12.1.3. *Sejam* $\mathbb{K}$ *e* $\mathbb{L}$ *corpos e* $\sigma : \mathbb{K} \to \mathbb{L}$ *um homomorfismo.*

1. *Se* σ *é injetora,* σ *é chamado de um monomorfismo.*
2. *Se* σ *é sobrejetora,* σ *é chamado de um epimorfismo.*
3. *Se* σ *é bijetora,* σ *é chamado de um isomorfismo e que os corpos* $\mathbb{K}$ *e* $\mathbb{L}$ *são isomorfos. Neste caso, usamos a notação* $\mathbb{K} \simeq \mathbb{L}$.
4. *Se* $\mathbb{K} = \mathbb{L}$ *e* σ *é bijetora,* σ *é chamado de um automorfismo.*

Teorema 12.1.1. *Todo domínio finito é um corpo.*

Demonstração. Seja $\mathbb{K} = \{a_1, a_2, \cdots, a_n\}$ um domínio com n elementos. Para todo $a \in \mathbb{K}$, com $a \neq 0$, segue que a aplicação $f : \mathbb{K} \to \mathbb{K}$ definida por $f(a_i) = aa_i$ é injetora, uma vez que se $f(a_i) = f(a_j)$, com $i \neq j$, então $aa_i = aa_j$. Assim, $a_i = a_j$. Como $\mathbb{K}$ é finito, segue que f é sobrejetora. Logo, a unidade de $\mathbb{K}$ é expressa como $1 = aa_r$, para algum $a_r \in \mathbb{K}$. Portanto, $\mathbb{K}$ é um corpo. □

Exemplo 12.1.3. *Como* $\mathbb{Z}_p = \{0, 1, \cdots, p-1\}$, *onde* p *é um número primo, é um domínio finito, pelo Teorema 12.1.1, segue que* $\mathbb{Z}_p$ *é um corpo.*

Teorema 12.1.2. *Se* $\mathbb{K}$ *é um anel comutativo com unidade, então as seguintes condições são equivalentes:*

1. $\mathbb{K}$ *é um corpo.*

2. $\{0\}$ *é um ideal maximal em* $\mathbb{K}$.

3. *Os únicos ideais de* $\mathbb{K}$ *são os triviais.*

Demonstração. (1) $\Rightarrow$ (2) Sejam $\mathbb{K}$ um corpo e M um ideal de $\mathbb{K}$ tal que $\{0\} \subset M \subset \mathbb{K}$. Se $M \neq 0$, então existe $a \in M$, onde $a \neq 0$. Como $\mathbb{K}$ é um corpo, segue que a é inversível, e assim, $1 \in M$. Portanto, $M = \mathbb{K}$. (2) $\Rightarrow$ (3). Seja M um ideal de $\mathbb{K}$ tal que $M \neq \{0\}$. Por hipótese, segue que $M = \mathbb{K}$, e portanto, os únicos ideais de $\mathbb{K}$ são os triviais. Finalmente, (3) $\Rightarrow$ (1). Para $\mathbb{K}$ ser um corpo falta apenas mostrar que todo $a \in \mathbb{K}$ é inversível. Para isso, sejam $a \in \mathbb{K}$, com $a \neq 0$, e $I = \langle a \rangle$ o ideal principal de $\mathbb{K}$ gerado por a. Como $a = 1a \in I$, segue que $I \neq \{0\}$. Assim, por hipótese, segue que $I = \mathbb{K}$. Logo, $1 \in \mathbb{K} = \langle a \rangle$, e portanto, existe $b \in \mathbb{K}$ tal que $ba = 1$. □

Teorema 12.1.3. *Sejam A um anel comutativo com unidade e M um ideal de A. Assim, M é um ideal maximal de A se, e somente se, A/M é corpo.*

Demonstração. Suponhamos que M é um ideal maximal de A e seja $\overline{a} \in \overline{A} = A/M$, onde $\overline{a} \neq \overline{0}$. Temos que provar que existe $\overline{b} \in \overline{A}$ tal que $\overline{a}\overline{b} = \overline{1}$. De fato, se $L = \langle a \rangle$ é um ideal principal de A gerado por a, então $M + L = \{x + y : x \in M,\ y \in L\}$ é um ideal contendo L. Como $\overline{a} \neq \overline{0}$, segue que $a \notin M$. Como $a = 1a \in L \subset M + L$, segue que $M + L$ é um ideal que contém M e tal que $M + L \neq M$. Pela maximalidade de M, segue que $A = M + L$ e assim, $1 \in M + L$, ou seja, existem $u \in M$ e $v \in L$ tal que $1 = u + v$. Mas, como $v \in L = \langle a \rangle$, segue que $v = ba$, para algum $b \in A$, ou seja, existe $b \in A$ e existe $u \in M$ tal que $1 = u + ba$. Fazendo uso da congruência, segue que $\overline{1} = \overline{u + ba} = \overline{u} + \overline{ba} = \overline{0} + \overline{ba}$, isto é, $\overline{b}\overline{a} = \overline{a}\overline{b} = \overline{1}$. Reciprocamente, se $\overline{A} = A/M$ é um corpo, então $\overline{0}, \overline{1} \in \overline{A}$ e $M \neq A$. Se $J \neq M$ é um ideal de A tal que $M \subset J \subset A$, então existe $a \in J$ com $a \notin M$, ou seja, $\overline{a} \neq \overline{0}$, e $\overline{a} \in \overline{A}$. Como $\overline{A}$ é um corpo, segue que existe $\overline{b} \in \overline{A}$ tal que $\overline{a}\overline{b} = \overline{1}$. Assim, $ab - 1 \in M$, e deste modo, existe $u \in M$ tal que $ab - 1 = u$. Logo, $1 = ab - u$. Como $a \in J$, segue que $ab \in J$, e como $u \in M \subset J$, segue que $u \in J$. Assim, $1 = ab - u \in J$, e portanto, $J = A$, ou seja, M é um ideal maximal de A. □

Exemplo 12.1.4. *O ideal $\langle p \rangle$, com p um primo, é um ideal maximal em $\mathbb{Z}$. De fato, como $\mathbb{Z}/\langle p \rangle \simeq \mathbb{Z}_p$ e como $\mathbb{Z}_p$ é um corpo, segue que $\langle p \rangle$ é um ideal maximal.*

Exemplo 12.1.5. *Como $\mathbb{Z}$ é um domínio, segue que $\langle x \rangle$ é um ideal primo de $\mathbb{Z}[x]$, pois $\mathbb{Z}[x]/\langle x \rangle \simeq \mathbb{Z}$, e assim $\langle x \rangle$ é um ideal primo e não maximal, pois $\mathbb{Z}$ é um domínio mas não é um corpo. Logo, $\mathbb{Z}[x]$ não é um domínio principal.*

Proposição 12.1.2. *Se x e y são dois elementos de ordens finitas de um grupo abeliano G e se $mdc(\circ(x), \circ(y)) = 1$, então $\circ(xy) = \circ(x) \circ (y)$.*

Demonstração. Sejam $\circ(x) = a$ e $\circ(y) = b$. Como G é abeliano, segue que $(xy)^{ab} = (x^a)^b(y^b)^a = e$. Logo, xy tem ordem finita e $\circ(xy) \mid ab$. Por outro lado, se t é a ordem de xy, então $(xy)^t = e$. Assim,

$$e = [(xy)^t]^a = (x^a y^a)^t = y^{at},$$
$$e = [(xy)^t]^b = (x^b y^b)^t = x^{bt}.$$

Logo, $b \mid at$ e $a \mid bt$. Como $mdc(a,b) = 1$, segue que $b \mid t$ e $a \mid t$. Como $mdc(a,b) = 1$, segue que $ab \mid t$, e portanto, $\circ(xy) = ab = \circ(x) \circ (y)$. □

Corolário 12.1.1. *Sejam $x_1, x_2, \ldots, x_n$ elementos (distintos) de ordens finitas de um grupo G. Se $mdc(x_1, x_2, \ldots, x_n) = 1$, então $\circ(x_1 x_2 \ldots x_n) = \circ(x_1) \circ (x_2) \ldots \circ (x_n)$.*

Demonstração. A prova será feita por indução sobre n. Se $n = 2$, o resultado segue pela Proposição 12.1.2. Agora, suponhamos por indução que o resultado é verdadeiro para k, ou seja, se $mdc(x_1, x_2, \ldots, x_k) = 1$, então $\circ(x_1 x_2 \ldots x_k) = \circ(x_1) \circ (x_2) \ldots \circ (x_k)$. Agora, como $mdc(x_1, x_2, \ldots, x_k, x_{k+1}) = mdc((x_1, x_2, \ldots, x_k), x_{k+1}) = 1$, segue que $\circ(x_1 x_2 \ldots x_k, x_{k+1}) = \circ(x_1 x_2 \ldots x_k) \circ (x_{k+1})$. Por hipótese de indução, segue que

$$\circ(x_1 x_2 \ldots x_k, x_{k+1}) = \circ(x_1) \circ (x_2) \ldots \circ (x_k) \circ (x_{k+1}),$$

o que prova o resultado. □

Proposição 12.1.3. *Se x é um elemento de ordem finita n de um grupo abeliano G e se d é um divisor positivo de n, então existe em G um elemento de ordem d.*

Demonstração. Se d é um divisor positivo de n, então existe $m \in \mathbb{N}$ tal que $n = md$. Se $y = x^m$, então $y^d = (x^m)^d = x^{md} = x^n = e$. Se $\circ(y) = t$, então $t \leq d$. Se $t < d$, então $mt < md = n$, onde $m \in \mathbb{N}$. Logo, $x^{mt} = (x^m)^t = y^t = e$, com $mt < n$, o que é um absurdo, pois $\circ(x) = n$. Portanto, $t = d$, ou seja, $\circ(y) = d$. □

Proposição 12.1.4. *Se x e y são dois elementos de ordens finitas a e b, respectivamente, de um grupo abeliano G, então existe em G um elemento de ordem igual a $mmc(a,b)$.*

Demonstração. Sejam $a = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_r}^{\alpha_r}$ e $b = {p_1}^{\beta_1} {p_2}^{\beta_2} \cdots {p_r}^{\beta_r}$ as decomposições de a e b em fatores primos positivos $p_1, \cdots p_r$, onde $\alpha_i, \beta_i \in \mathbb{N}$ para $i = 1, 2, \cdots, r$, e

$$\gamma_i = max\{\alpha_i, \beta_i\}, \quad i = 1, 2 \cdots r.$$

Logo, $p_i^{\gamma_i} \mid a$ ou $p_i^{\gamma_i} \mid b$, para $i = 1, 2, \cdots, n$. Pela Proposição 12.1.3, existe $x_i \in G$ tal que $\circ(x_i) = p_i^{\gamma_i}$, para $i = 1, 2, \cdots, n$. Portanto, pelo Corolário 12.1.1, segue que

$$\circ(x_i x_2 \cdots x_r) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r} = mmc(a,b),$$

o que prova a proposição. □

Proposição 12.1.5. *Seja G um grupo abeliano, onde todo elemento de G tem ordem finita. Se n é a ordem máxima dos elementos de G, então a ordem de qualquer elemento de G é um divisor de n.*

Demonstração. Por hipótese, existe $a \in G$ tal que $\circ(a) = max\{\circ(x);\ x \in G\} = n$. Seja $x \in G$ um elemento qualquer e suponhamos, por absurdo, que $\circ(x)$ não divide n. Assim, pela Proposição 12.1.4, segue que existe $y \in G$ tal que $\circ(y) = mmc(n, \circ(x)) > n$, o que é um absurdo, pois $n = max\{\circ(x);\ x \in G\}$, e portanto, $\circ(x) \mid n$. □

Proposição 12.1.6. *Se G é um subgrupo finito de um grupo abeliano multiplicativo $\mathbb{K}^*$ de um corpo $\mathbb{K}$, então G é um grupo cíclico.*

Demonstração. Sejam $\circ(G) = n$ e $a \in G$ um elemento de ordem máxima r, ou seja, $< a >$ é um subgrupo de ordem r. Como $\langle a \rangle$ é um subgrupo de G, pelo Teorema de Lagrange, segue que $r \mid n$, e assim, $r \leq n$. Pela Proposição 12.1.5, dado $x \in G$, segue que $\circ(x) \mid r$, ou seja, existe $q \in \mathbb{N}$ tal que $r = \circ(x)q$. Logo, $x^r = x^{\circ(x)q} = (x^{\circ(x)})^q = 1$ para todo $x \in G$. Consideremos o polinômio $f(x) = x^r - 1 \in \mathbb{K}[x]$. Assim, $f(x) = 0$ para todo $x \in G$ e como $\circ(G) = n$, segue que o polinômio f possui no mínimo n raízes distintas. Logo, $r = grf \geq n$, e como tínhamos $r \leq n$, segue que $r = n$. Portanto, $G = \langle a \rangle$, ou seja, G é cíclico. □

Proposição 12.1.7. *Se $\mathbb{K}$ é um corpo finito, então o grupo abeliano multiplicativo $\mathbb{K}^*$ do corpo $\mathbb{K}$ é cíclico.*

Demonstração. Pela Proposição 12.1.6, tomando $G = \mathbb{K}^*$, o resultado segue. □

Definição 12.1.4. *Seja $\mathbb{L}$ um corpo. Um subconjunto não vazio $\mathbb{K} \subseteq \mathbb{L}$ é chamado um subcorpo de $\mathbb{L}$ se:*

1. *$\mathbb{K}$ é fechado em relação à adição e à multiplicação, e*
2. *$\mathbb{K}$ é um corpo.*

Exemplo 12.1.6. *O conjunto dos números racionais é um subcorpo do conjunto dos números reais. De modo análogo, o conjunto dos números reais é um subcorpo do conjunto dos números complexos.*

12.1.1 Exercícios

1. Se A for um anel de integridade, mostre que A é um corpo se, e somente se, os únicos ideais de A são os triviais.
2. Mostre que $\mathbb{Z}_p$ é um corpo se, e somente se, p é um número primo.
3. Determine o corpo de frações de um anel de integridade.
4. Sejam $\mathbb{L}$ um corpo e $\mathbb{K} \subseteq \mathbb{L}$ um subconjunto não vazio. Mostre que $\mathbb{K}$ é um subcorpo de $\mathbb{L}$ se, e somente se,
   (a) $0, 1 \in \mathbb{K}$,
   (b) se $x, y \in \mathbb{K}$, então $x - y \in \mathbb{K}$, e
   (c) se $x, y \in \mathbb{K}$, com $y \neq 0$, então $xy^{-1} \in \mathbb{K}$.
5. Sejam $\mathbb{K}$ um corpo e $(\mathbb{K}_i)_{i \in I}$ a família de todos os subcorpos de $\mathbb{K}$. Mostre que $\cap_{i \in I} \mathbb{K}_i$ é o menor subcorpo de $\mathbb{K}$.

6. Sejam $\mathbb{K}$, $\mathbb{L}$ corpos e $\varphi : \mathbb{K} \to \mathbb{L}$ um homomorfismo não nulo. Se $\mathbb{F}$ é um subcorpo de $\mathbb{K}$, mostre que $\varphi(\mathbb{F})$ é um subcorpo de $\mathbb{L}$.

7. Mostre que $\mathbb{K} = \{a + b\sqrt{2} : a, b \in \mathbb{R}\}$ é um subcorpo de $\mathbb{R}$.

8. Determine os subcorpos dos números racionais.

9. Seja A um anel comutativo com unidade.

   (a) Se A é finito, mostre que todo ideal primo de A é maximal.

   (b) Se A é um corpo, mostre que A é um anel de integridade.

   (c) Se A é um anel de integridade e finito, mostre que A é um corpo.

10. Mostre que $\mathbb{K} = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ é um subcorpo de $\mathbb{R}$.

11. Mostre que $\mathbb{K} = \{a + bi : a, b \in \mathbb{R}\}$ é um subcorpo de $\mathbb{C}$.

12. Seja A um anel comutativo com unidade. Mostre que I é um ideal maximal se, e somente se, A/I é um corpo.

13. Se $\mathbb{K}$ é um anel comutativo com unidade, então as seguintes condições são equivalentes:

   (a) $\mathbb{K}$ é um corpo.

   (b) $\{0\}$ é um ideal maximal em $\mathbb{K}$.

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

12.2 Corpo de frações de um anel de integridade

Seja A um anel domínio de integridade. No conjunto $A \times A - \{0\}$ seja a relação definida por

$$(a, b) \sim (c, d) \text{ se, e somente se, } ad = bc. \tag{12.1}$$

A relção $\sim$ é uma relação de equivalência sobre $A \times A - \{0\}$. A classe de equivalência determinada pelo par (a, b) será denotada por $\frac{a}{b}$. Seja $\mathbb{K} = (A \times A - \{0\})/\sim = \{\frac{a}{b} : a, b \in A, b \neq 0\}$. Assim, $\frac{a}{b} = \frac{c}{d}$ se, e somente se, $(a, b) \sim (c, d)$ se, e somente se, $ad = bc$. Sejam as operações de soma e produto de duas frações $\frac{a}{b}, \frac{c}{d} \in \mathbb{K}$ definidas como

$$\frac{a}{b} + \frac{c}{d} = \frac{ac + bc}{bd} \quad \text{e} \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}. \tag{12.2}$$

Segue que essas operações estão bem definidas, são associativas e comutativas. O elemento zero é dado por $\frac{0}{1}$ e o elemento neutro da multiplicação é dado por $\frac{1}{1}$. Assim, $\mathbb{K}$ é um corpo chamado *corpo de frações do domínio de integridade* A. Agora, seja $\mathbb{L} = \frac{a}{1} : a \in A\}$. Assim, L é um anel contido em $\mathbb{K}$. Além disso, a aplicação $f : A \to L$ definida por $f(a) = \frac{a}{1}$, onde $a \in A$, é um isomorfismo de anéis. Com essa identificação, segue que A é um anel contido em $\mathbb{K}$.

A classe de equivalência determinada pelo par (a, b) será denotada por $\overline{(a, b)}$. Seja $\mathbb{K}$ o conjunto das classes de equivalência dos elementos de S, ou seja,

$$\mathbb{K} = (A \times A^*)/\sim = \{\overline{(a, b)} : (a, b) \in S\}.$$

Denotando $\frac{a}{b} = \overline{(a, b)}$, segue que $\frac{a}{b} = \frac{c}{d}$ se, e somente se, $(a, b) \sim (c, d)$ se, e somente se, $ad = bc$ se, e somente se, $\overline{(a, b)} = \overline{(c, d)}$. Sejam as operações de soma e produto de duas frações $\frac{a}{b}, \frac{c}{d} \in \mathbb{K}$ definidas como

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{e} \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}. \tag{12.3}$$

1. As operações estão bem definidas: se $\frac{a}{b} = \frac{e}{f}$ e $\frac{c}{d} = \frac{s}{t}$, então $af = be$ e $ct = ds$. Assim, $(ft)(ad+bc) = (af)td+(cd)bf = (be)td+(ds)bf = bd(et+fs)$. Portanto, $\frac{a}{b} + \frac{c}{d} = \frac{e}{f} + \frac{s}{t}$, ou seja, está bem definida. De modo análogo, se prova que a operação produto está bem definida.

2. As operações são associativas: exercício.

3. As operações são comutativas: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{db} = \frac{c}{d} + \frac{a}{b}$.

4. O elemento zero é dado por $\frac{0}{1}$: $\frac{a}{b} + \frac{0}{1} = \frac{a\cdot 1+b\cdot 0}{b\cdot 1} = \frac{a}{b}$, para todo $\frac{a}{b} \in \mathbb{K}$.

5. O oposto de $\frac{a}{b}$ é $\frac{-a}{b}$: $\frac{a}{b} + \frac{-a}{b} = \frac{ab+b(-a)}{b^2} = \frac{0}{b^2} = \frac{0}{1}$, uma vez que $0 \cdot 1 = b^2 \cdot 0 = 0$.

6. O elemento neutro da multiplicação é dado por $\frac{1}{1}$: $\frac{a}{b}\frac{1}{1} = \frac{a\cdot 1}{b\cdot 1} = \frac{a}{b}$, para todo $\frac{a}{b} \in \mathbb{K}$.

7. O inverso de $\frac{a}{b}$, com $a \neq 0$, é $\frac{b}{a}$: $\frac{a}{b}\frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}$, ou seja, $(\frac{a}{b})^{-1} = \frac{b}{a}$.

8. As operações são distributivas: exercício.

Assim, $\mathbb{K}$ é um corpo chamado *corpo de frações do anel de integridade* A. Agora, seja

$$B = \left\{\frac{a}{1} : a \in A\right\}. \tag{12.4}$$

Assim, B é um anel contido em $\mathbb{K}$.

Proposição 12.2.1. *A aplicação $f : A \to B$ definida por $f(a) = \frac{a}{1}$, onde $a \in A$, é um isomorfismo de anéis.*

Demonstração. A aplicação f é um homomorfismo, uma vez que $f(a + b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b)$ e $f(ab) = \frac{ab}{1} = \frac{a}{1}\frac{b}{1} = f(a)f(b)$, para todo $a, b \in A$. Para a injetora, se $f(a) = f(b)$, então $\frac{a}{1} = \frac{b}{1}$. Assim, $(a, 1) \sim (b, 1)$, ou seja, $a = b$. Finalmente, se $y \in B$, então $y = \frac{a}{1}$, onde $a \in A$. Assim, $f(a) = \frac{a}{a}$. Portanto, f é um isomorfismo. □

Com a identificação pela Proposição 12.2.1, segue que A é um anel contido em $\mathbb{K}$, ou seja, identificamos A como um subanel de $\mathbb{K}$.

Corolário 12.2.1. *$\mathbb{K}$ é o menor corpo que contém A.*

Demonstração. Seja $\mathbb{L}$ um corpo tal que $A \subseteq \mathbb{L} \subseteq \mathbb{K}$. Como A é isomorfo a B, segue que $A = \{\frac{a}{1} : a \in A\}$. Seja $\frac{a}{b} \in \mathbb{K}$. Assim, $a, b \in A$ com $b \neq 0$, e desse modo, $\frac{a}{1}, \frac{1}{b} \in \mathbb{L}$. Logo, $\frac{a}{b} = \frac{a}{1}\frac{1}{b} \in \mathbb{L}$. Portanto, $\mathbb{K} = \mathbb{L}$. □

12.2.1 Exercícios

1. Mostre que as operações definidas na Equação (12.3) são associativas e distributivas.
2. Mostre que o conjunto B da Equação (12.4) é um anel.
3. Se A e B são domínios, mostre que seus corpos de frações são isomorfos.
4. Se A é um anel com divisores de zero, mostre que não existe um homomorfismo injetor de A em um corpo $\mathbb{K}$.
5. Determine o corpo de frações de um corpo $\mathbb{K}$.
6. Sejam $A = \mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in \mathbb{Z}\}$ e $B = \mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$ com as operações de soma e produto usuais.
   (a) Mostre que A e B são domínios.
   (b) Determine o corpo de frações de A e B.
7. Determine o corpo de frações do anel dos inteiros $\mathbb{Z}$.
8. Mostre que $\mathbb{Q}$ é o menor corpo que contém $\mathbb{Z}$.
9. Determine todos os homomorfismos $f : \mathbb{Q} \to \mathbb{Q}$.
10. Sejam A um domínio.
    (a) Mostre que a relação da Equação (12.1) é uma relação de equivalência sobre $A \times A - \{0\}$.
    (b) Mostre que as operações da Equação (12.2) definem a estrutura de um corpo em $\mathbb{K} = \{\frac{a}{b} : a, b \in A, b \neq 0\}$.
    (c) Determine o corpo de frações de $\mathbb{Z}[\sqrt{2}]$ e de $\mathbb{Z}[i]$.

12.3 Corpo primo

Nesta seção, apresentamos os corpos primos que são, em certo sentido, os menores corpos que existem.

Definição 12.3.1. *Um corpo $\mathbb{K}$ é chamado primo se não existe um corpo $\mathbb{L}$ tal que $\mathbb{L} \subsetneq \mathbb{K}$.*

Definição 12.3.2. *Seja $\mathbb{L}$ um corpo. Um corpo $\mathbb{K}$ é chamado um corpo primo de $\mathbb{L}$ se $\mathbb{K}$ é o menor corpo tal que $\mathbb{K} \subsetneq \mathbb{L}$.*

Teorema 12.3.1. *Se $\mathbb{K}$ é um corpo primo, então $\mathbb{K}$ é isomorfo a $\mathbb{Q}$ ou a $\mathbb{Z}_p$, onde p é um número primo.*

Demonstração. Se $\mathbb{K}$ é um corpo primo, então $0, 1 \in \mathbb{K}$, e portanto, $n = n.1 \in \mathbb{K}$ para todo $n \in \mathbb{Z}$. Assim, a aplicação $\varphi : \mathbb{Z} \to \mathbb{K}$ definida por

$$\varphi(n) = \begin{cases} n \text{ se } n > 0, \\ 0 \text{ se } n = 0 \\ -\varphi(-n) \text{ se } n < 0, \end{cases}$$

é um homomorfismo de anéis. Agora, vamos analisar o $\ker(\varphi)$, ou seja, $\ker(\varphi) \neq \{0\}$ ou $\ker(\varphi) = \{0\}$.

1. Se $\ker(\varphi) \neq \{0\}$, ou seja, se $\varphi(n) = 0$ para algum $n \in \mathbb{Z}$, com $n \neq 0$, então $\varphi(-n) = 0$. Logo, existe um menor $p \in \mathbb{N}$, $p \neq 0$, tal que $\varphi(p) = 0$. Se p for composto, então $p = mn$, onde $1 < m, n < p$. Assim, $\varphi(p) = \varphi(mn) = \varphi(m)\varphi(n) = 0$, e portanto, $\varphi(m) = 0$ ou $\varphi(n) = 0$, o que é uma contradição. Deste modo, p é primo e $\ker(\varphi) = \langle p \rangle$, uma vez que $\langle p \rangle \subseteq \ker(\varphi)$, e se $x \in \ker(\varphi)$, então $\varphi(x) = 0$ e $x = py + r$, onde $y, r \in \mathbb{Z}$ e $0 \leq r < p$. Assim, $\varphi(x) = \varphi(r) = 0$ o que implica que $x \in \langle p \rangle$. Consequentemente, o corpo $\mathbb{Z}_p = \frac{\mathbb{Z}}{\langle p \rangle}$ é isomorfo a $Im(\varphi) \subseteq \mathbb{K}$. Como $\mathbb{K}$ é um corpo primo, segue que $\mathbb{Z}_p$ é isomorfo a $\mathbb{K}$.

2. Se $\ker(\varphi) = \{0\}$, ou seja, se $\varphi(n) \neq 0$, para todo $n \in \mathbb{Z}$, $n \neq 0$, então $\mathbb{Z}$ é isomorfo a $Im(\varphi)$. Assim, a aplicação $\psi : \mathbb{Q} \to \mathbb{L}$, onde $\mathbb{L}$ é o corpo de frações de $Im(\varphi)$, definida por $\phi(m/n) = \varphi(m)/\varphi(n)$ é um isomorfismo. Como $\mathbb{K}$ é um corpo primo, segue que $\mathbb{L} = \mathbb{K}$, e portanto, $\mathbb{K}$ é isomorfo a $\mathbb{Q}$.

Portanto, $\mathbb{K}$ é isomorfo a $\mathbb{Q}$ ou $\mathbb{K}$ é isomorfo a $\mathbb{Z}_p$, para algum primo p. □

Definição 12.3.3. *Seja $\mathbb{K}$ um corpo.*

1. *Se o corpo primo de $\mathbb{K}$ é isomorfo a $\mathbb{Q}$, o corpo $\mathbb{K}$ é dito que tem característica zero.*
2. *Se o corpo primo de $\mathbb{K}$ for isomorfo a $\mathbb{Z}_p$, com p um número primo, o corpo $\mathbb{K}$ é dito que tem característica p.*

Proposição 12.3.1. *Se $\mathbb{K} \subseteq \mathbb{L}$ são corpos então $\mathbb{K}$ e $\mathbb{L}$ têm a mesma característica.*

Demonstração. Como $\mathbb{K} \subseteq \mathbb{L}$, segue que os corpos $\mathbb{K}$ e $\mathbb{L}$ tem o mesmo corpo primo. Pelo Teorema 12.3.1, segue que $\mathbb{K}$ e $\mathbb{L}$ têm a mesma característica. □

Corolário 12.3.1. *Sejam $\mathbb{K}$ um corpo, $k \in \mathbb{K}$, $k \neq 0$, e $n \in \mathbb{Z}$. Se $nk = 0$, então n é múltiplo da característica de $\mathbb{K}$.*

Demonstração. Se $car(\mathbb{K}) = 0$ então $n = 0$. Se $car(\mathbb{K}) = p$, onde p é um número primo, então $n = pq + r$, onde $p, q \in \mathbb{Z}$ e $0 \leq r < p$. Assim, $nk = (pq + r)k = pqk + rk = rk$. Como $car(\mathbb{K}) = p$ e $0 \leq r < p$, segue que $r = 0$. Portanto, $p \mid n$. □

12.3.1 Exercícios

1. Seja A um anel comutativo com identidade. Seja $\sigma : \mathbb{Z} \to A$ uma aplicação definida por $\sigma(n) = n.1$, onde 1 é a identidade de A. Mostre que:

   (a) σ é homomorfismo de anéis.

   (b) $\ker(\sigma) = \langle m \rangle$, onde m é um inteiro positivo.

   (c) m é único e que m é a característica de A.

2. Mostre que o corpo primo de um corpo $\mathbb{K}$ é único.

3. Mostre que $\mathbb{Q}$ e $\mathbb{Z}_p$, onde p é um número primo, não possuem subcorpos não triviais.

4. Seja $\mathbb{L}$ um corpo.

   (a) Mostre que $\mathbb{K} = \bigcap_{i \in I} \mathbb{K}_i$, onde $\mathbb{K}_i \subseteq \mathbb{L}$ é um subcorpo para todo $i \in I$, é um subcorpo de $\mathbb{L}$.

   (b) Mostre que $\mathbb{K}$ é um corpo primo de $\mathbb{L}$.

5. Se $\mathbb{K}$ é corpo tal que $\mathbb{K} \subseteq \mathbb{Q}$, mostre que $\mathbb{K} = \mathbb{Q}$, ou seja, $\mathbb{Q}$ é um corpo primo.

Capítulo

13

Anel de polinômios

Neste capítulo, apresentamos o conceito de anéis de polinômios com coeficientes em um anel, com ênfase para os anéis de polinômios com coeficientes em domínios e corpos. O objetivo principal é apresentar a fatoração de polinômios em produto de potências de polinômios irredutíveis e apresentar o Teorema Fundamental da Álgebra para polinômios. Também, apresentamos o algorítimo euclidiano com suas consequências.

13.1 Polinômios sobre um anel

Nesta seção, veremos o anel dos polinômios com coeficientes em um anel. Veremos que as propriedades das operações dos polinômios estão relacionadas diretamente com as propriedades da adição e multiplicação do anel.

Definição 13.1.1. *Seja A um anel. Um polinômio na variável x sobre A é uma expressão da forma*

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

onde $n \in \mathbb{N}$, os coeficientes a_i, para $i = 0, 1, \ldots, n$, são elementos de A e x é uma variável.

Definição 13.1.2. *Seja $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in A[x]$ um polinômio não nulo.*

1. *O grau de $f(x)$, e denotado por $gr(f)$, é definido como o maior número natural n tal que $a_n \neq 0$.*

2. *O termo a_n nessas condições é chamado coeficiente líder de $f(x)$.*

3. *Se o coeficiente líder de $f(x)$ é 1, o polinômio $f(x)$ é chamado um polinômio unitário ou mônico.*

Definição 13.1.3. *Dois polinômios $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$ em $A[x]$ são chamados iguais se, e somente se, $a_i = b_i$, para $i = 0, 1, \ldots, \max\{m, n\}$.*

Definição 13.1.4. *Se $f(x) = 0 + 0x + \cdots + 0x^n$, então indicamos $f(x)$ por 0, ou seja, $f(x) \equiv 0$, e $f(x)$ é chamado de polinômio identicamente nulo sobre A.*

Assim, um polinômio $f(x) = a_0+a_1x+\cdots+a_nx^n$ sobre A é identicamente nulo se, e somente se, $a_i = 0$, para todo $i = 0, 1, \ldots, n$. Se $a \in A$, enão indicamos por $a_0 = a$, e $a_i = 0$, para todo $i \geq 1$. O polinômio $f(x) = a$ é chamado de polinômio constante a.

Vamos denotar por $A[x]$ o conjunto de todos os polinômios na variável x sobre A. Definimos, a seguir, a soma e o produto de polinômios. Sejam $f(x) = \sum_{i=0}^{m} a_ix^i$ e $g(x) = \sum_{i=0}^{n} b_ix^i$ tal que $f(x), g(x) \in A[x]$.

1. A soma de $f(x)$ e $g(x)$ é definida por

$$f(x) + g(x) = \sum_{i=0}^{max\{m,n\}} (a_i + b_i)x^i.$$

   Assim, a soma de polinômios também é um polinômio.

2. O produto de $f(x)$ e $g(x)$ é definido por

$$f(x)g(x) = \sum_{k=0}^{m+n} c_kx^k,$$

   onde $c_k = \sum_{i+j=k} a_ib_j$, com $0 \leq i \leq m$ e $0 \leq j \leq n$, ou seja,

$$\begin{cases} c_0 = a_0b_0 \\ c_1 = a_0b_1 + a_1b_0 \\ c_2 = a_0b_2 + a_1b_1 + a_2b_0 \\ \vdots \\ c_k = a_0b_k + a_1b_{k-1} + \cdots + a_{k-1}b_1 + a_kb_0, \end{cases}$$

   para todo $k = 0, 1, 2, \ldots, m+n$. Assim, o produto de polinômios também é um polinômio.

Proposição 13.1.1. *Se A é um anel, então $A[x]$ é um anel.*

Demonstração. Se $f(x) = \sum_{i=0}^{m} a_ix^i$, $g(x) = \sum_{i=0}^{n} b_ix^i$ e $h(x) = \sum_{i=0}^{r} c_ix^i$ são polinômios de $A[x]$, então

1. $f(x)+(g(x)+h(x))=(f(x)+g(x))+h(x)$, uma vez que

$$\begin{aligned} f(x)+(g(x)+h(x)) &= \sum_{i=0}^{m} a_i x^i + (\sum_{i=0}^{n} b_i x^i + \sum_{i=0}^{r} c_i x^i) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{max\{n,r\}} (b_i+c_i)x^i \\ &= \sum_{i=0}^{\max\{m,n,r\}} (a_i+(b_i+c_i))x^i = \sum_{i=0}^{max\{m,n\}} (a_i+b_i)x^i + \sum_{i=0}^{r} c_i x^i \\ &= (\sum_{i=0}^{m} a_i x^i + \sum_{i=0}^{n} b_i x^i) + \sum_{i=0}^{r} c_i x^i = (f(x)+g(x))+h(x), \end{aligned}$$

   ou seja, vale a propriedade associativa para a adição.

2. $f(x)+g(x)=g(x)+f(x)$, uma vez que

$$\begin{aligned} f(x)+g(x) &= \sum_{i=0}^{m} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{max\{m,n\}} (a_i+b_i)x^i = \sum_{i=0}^{\max\{n,m\}} (b_i+a_i)x^i \\ &= \sum_{i=0}^{n} b_i x^i + \sum_{i=0}^{m} a_i x^i = g(x)+f(x), \end{aligned}$$

   ou seja, vale a comutativa para a adição.

3. Existe $0(x)=0$, polinômio nulo, tal que para todo $f(x)\in A[x]$ tem-se que $f(x)+0(x)=0(x)+f(x)=f(x)$, ou seja, existe elemento neutro.

4. Para todo $f(x)\in A[x]$, existe $-f(x)\in A[x]$ tal que $f(x)+(-f(x))=f(x)-f(x)=0$, ou seja, existe elemento inverso.

5. $f(x)(g(x)h(x))=(f(x)g(x))h(x)$. Sejam $f(x)=\sum_{i=0}^{m} a_i x^i$, $g(x)=\sum_{j=0}^{n} b_j x^j$ e $h(x)=\sum_{k=0}^{r} c_k x^k$ polinômios de $A[x]$. Sejam $g(x)h(x)=\sum_{j+k=l}^{n+r} d_l x^l$, $f(x)(g(x)h(x))=\sum_{i+l=s}^{m+(n+r)} e_s x^s$, $f(x)g(x)=\sum_{i+j=t}^{m+n} q_t x^t$, $(f(x)g(x))h(x)=\sum_{t+k=u}^{(m+n)+r} p_u x^u$. Como

$$\begin{aligned} e_s &= \sum_{i+l=s} a_i d_l = \sum_{i+l=s} a_i (\sum_{j+k=l} b_j c_k) = \sum_{i+j+k=s} a_i(b_j c_k) \\ &= \sum_{i+j+k=s} (a_i b_j)c_k = \sum_{n+k=s} (\sum_{i+j=t} a_i b_j)c_k = \sum_{t+k=s} q_t c_k = p_u, \end{aligned}$$

   segue que $f(x)(g(x)h(x))=(f(x)g(x))h(x)$, ou seja, vale a associativa para a multiplicação.

6. $f(x)(g(x)+h(x))=f(x)g(x)+f(x)h(x)$, uma vez que se $g(x)+h(x)=\sum_{j=0}^{max\{m,n\}} d_j x^j$,

$f(x)(g(x)+h(x)) = \sum_{k=0}^{m+max\{n,r\}} e_k x^k$, $f(x)g(x) = \sum_{k=0}^{m+n} d_k' x^k$, $f(x)h(x) = \sum_{k=0}^{m+r} d_k'' x^k$ e $f(x)g(x)+f(x)h(x) = \sum_{k=0}^{max\{m+n,m+r\}} e_k' x^k$. Assim, $d_j = b_j + c_j$ e $e_k = \sum_{i+j=k} a_i d_j = \sum_{i+j=k} a_i(b_j+c_j) = \sum_{i+j=k}(a_ib_j + a_ic_j) = \sum_{i+j=k} a_ib_j + \sum_{i+j=k} a_ic_j = d_k' + d_k'' = e_k'$. Portanto, $f(x)(g(x)+h(x)) = f(x)g(x)+f(x)h(x)$. De maneira análoga, segue que $(f(x)+g(x))h(x) = f(x)h(x)+g(x)h(x)$, ou seja, vale a distributiva.

Portanto, $A[x]$ é um anel. □

Proposição 13.1.2. *Se A é um anel comutativo, então $A[x]$ é um anel comutativo.*

Demonstração. Provamos que $f(x)g(x) = g(x)f(x)$, para todo $f(x), g(x) \in A[x]$. Se $f(x)g(x) = \sum_{k=0}^{m+n} c_k$ e $g(x)f(x) = \sum_{k=0}^{n+m} d_k$, então $c_k = \sum_{i+j=k} a_jb_j = \sum_{i+j=k} b_ja_j = d_k$, para todo $k \in \mathbb{N}$, e portanto, $f(x)g(x) = g(x)f(x)$. □

Proposição 13.1.3. *Se A é um anel com unidade, então $A[x]$ é um anel com unidade.*

Demonstração. Se $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $e(x) = 1$ em $A[x]$, então $e(x)$ é a unidade de $A[x]$, pois $e(x)f(x) = 1(a_0 + a_1x + \cdots + a_nx^n) = (a_0 + a_1x + \cdots + a_nx^n)1 = f(x)1 = f(x)e(x)$. Portanto, a unidade do anel $A[x]$ é o polinômio constante igual a $e(x) = 1$. □

Proposição 13.1.4. *Se A é domínio, então $A[x]$ é um domínio.*

Demonstração. Se $f(x) = a_0 + a_1x + \cdots + a_mx^m$ e $g(x) = b_0 + b_1x + \cdots + b_nx^n$ são dois polinômios não nulos em $A[x]$, com a_m, b_n não nulos, então $f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_mb_nx^{m+n} \neq 0$, pois $a_mb_n \neq 0$, uma vez que A é domínio. Portanto, $A[x]$ é domínio. □

Observação 13.1.1. *A seguir, apresentamos algumas observações importantes sobre anel de polinômios.*

1. *O anel $A[x]$ não é um corpo, uma vez que $f(x) = x \neq 0$ e se for inversível, então existe $g(x) \in A[x]$ tal que $f(x)g(x) = 1$. Para $x = 0$, segue que $0 = 1$ o que é um absurdo.*

2. *Se A é um anel principal, então $A[x]$ pode não ser principal. Por exemplo, o anel $\mathbb{Z}[x]$ não é principal, uma vez que $< 2, x >$ não é um ideal principal. De fato: se $< 2, x >$ for um ideal principal, então $< 2, x >=< f(x) >$, onde $f(x) \in \mathbb{Z}[x]$. Assim, $2, x \in < f(x) >$. Logo, $2 = f(x)g(x)$ e $x = f(x)h(x)$, onde $g(x), h(x) \in \mathbb{Z}[x]$. Aplicando o grau, segue que $0 = gr(f) + gr(g)$ e $1 = gra(f) + gr(h)$, ou seja, $f(x)$ é uma constante. Como $2 = f(x)g(x)$, segue que $f(x)|2$, ou seja, $f(x) = \pm 1, \pm 2$. Como $x = f(x)h(x)$, segue que $f(x)|x$, ou seja, $f(x) = \pm 1$. Assim, $< 2, x >=< \pm 1 >= \mathbb{Z}[x]$. Agora, se $f(x) \in \mathbb{Z}[x] =< 2, x >$, então $f(x) = 2g(x) + xh(x)$. Se $g(x) = a_0 + a_1x + \cdots + a_nx^n$*

e $h(x) = b_0 + b_1x + \cdots + a_mx^m$. *Assim,* $f(x) = 2a_0 + (2a_1 + b_0)x + \cdots$, *e portanto, o termo constante de* $f(x)$ *é par, o que é uma contradição. Portanto, o ideal* $< 2, x >$ *não é principal, ou seja, o anel* $\mathbb{Z}[x]$ *não é principal.*

3. *Sabemos que todo ideal maximal é um ideal primo. A recíproca, em geral, não é verdadeira. Por exemplo, o ideal* $< x >$ *de* $\mathbb{Z}[x]$ *é primo, uma vez que* $\mathbb{Z}[x]/ < x > \simeq \mathbb{Z}$, *mas não é um ideal maximal. De fato: as aplicações*

$$\mathbb{Z} \xrightarrow{i} \mathbb{Z}[x] \xrightarrow{\pi} \frac{\mathbb{Z}[x]}{< x >}$$

definidas por $i(a) = a$, *para todo* $a \in \mathbb{Z}$ *e* $\pi(f(x)) = f(x) + < x >$, *para todo* $f(x) \in \mathbb{Z}[x]$, *são homomorfismos de anéis. Além disso, a aplicação* $\pi \circ i : \mathbb{Z} \to \frac{\mathbb{Z}[x]}{<x>}$ *é um homomorfismo, uma vez que* i *e* π *são homomorfismos. Também,* $\pi \circ i$ *é injetora, uma vez que se* $a \in \ker(\pi \circ i)$, *então* $(\pi \circ i)(a) = a + < x >= \overline{0} = 0 + < x >$. *Assim,* $a \in < x >$, *e portanto,* $a = 0$. *Portanto,* $\ker(\pi \circ i) = \{0\}$, *Agora, se* $\overline{f}(x) \in \frac{\mathbb{Z}[x]}{<x>}$, *então* $\overline{f}(x) = f(x) + < x >$. *Pelo algoritmo euclidiano divisão, segue que* $f(x) = xq(x) + r(x)$, *onde* $q(x), r(x) \in \mathbb{Z}[x]$ *com* $r(x) \equiv 0$ *ou* $gr(r) < 1$. *Assim,* $r(x)$ *é uma constante. Logo,* $\overline{f}(x) = \overline{xq(x)} + \overline{r(x)}$. *Como* $xq(x) \in x$, *segue que* $\overline{xq(x)} = \overline{0}$. *Desse modo,* $\overline{f}(x) = \overline{r(x)} = a + < x >$, *onde* $a \in \mathbb{Z}$. *Portanto,* $\pi \circ i$ *é sobrejetora, e assim,* $\pi \circ i$ *é um isomorfismo. Como* $\mathbb{Z}$ *é um domínio de integridade, segue que* $< x >$ *é um ideal primo. Como* $\mathbb{Z}$ *não é um corpo, segue que* $< x >$ *não é um ideal maximal.*

13.1.1 Exercícios

1. Seja A é um anel.
   (a) Se A é um domínio, mostre que $A[x_1, \cdots, x_n]$ é um domínio.
   (b) Se $A[x]$ é um domínio, mostre que A é um domínio.
2. Seja A um anel.
   (a) Se I é um ideal de A, mostre que $I[x]$ é um ideal do anel $A[x]$.
   (b) Se $B \subseteq A$ é um subanel, mostre que $B[x]$ é um subanel de $A[x]$.
3. Determine os elementos inversíveis de $A[x]$, onde A é um anel comutativo.
4. Mostre que $< x > \subsetneq < 2, x >$ em $\mathbb{Z}[x]$.
5. Seja P um ideal primo em um anel de integridade infinito A.
   (a) Mostre $P[x]$ é um ideal primo de $A[x]$.
   (b) Dê um exemplo de um ideal maximal M de A tal que $M[x]$ não é um ideal maximal de $A[x]$.
   (c) Mostre que $A[x]/P[x]$ é isomorfo a $(A/P)[x]$.

6. Seja A um anel comutativo que não possui elementos nilpotentes. Se $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ é um divisor de zero, mostre que existe $b \in A$, não nulo, tal que $ba_0 = \cdots = ba_n = 0$.

7. Seja A um domínio.

   (a) Se $\alpha \in A$, mostre que $P_\alpha = \{f(x) \in A[x] : f(\alpha) = 0\}$ é um ideal primo de $A[x]$. É maximal?

   (b) Se $P \subseteq A$ é um ideal primo de A e $\varphi : A[x] \to (A/P)[x]$ uma aplicação definida por $\varphi(a_0 + a_1x + \cdots + a_nx^n) = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n$, onde $\overline{a_i}$ é a classe de resto de a_i em A/P. Mostre que φ é um homomorfismo sobrejetor de anéis e $\ker(\varphi) =< P, x >$.

8. Se $I = \{f(x) \in \mathbb{Z}[x] : f(0) = 0\}$, mostre que I não é um ideal maximal de $\mathbb{Z}[x]$.

9. Seja a aplicação $\varphi : \mathbb{Z}[x] \to \mathbb{R}$ definida por $\varphi(f(x)) = f(\sqrt{2})$, onde $f(x) \in \mathbb{Z}[x]$.

   (a) Mostre que φ é um homomorfismo de anéis.

   (b) Mostre $\ker(\varphi)$ é um ideal primo de $\mathbb{Z}[x]$. É maximal?

10. Seja A um anel de integridade. Mostre que $A[x]$ é principal se, e somente se, A é um corpo.

11. Sejam $\mathbb{K}$ um corpo e $\mathbb{K}[x_1][x_2] = \mathbb{K}[x_1, x_2]$.

    (a) Mostre $\mathbb{K}[x_1, x_2]$ é um anel.

    (b) Mostre que $\mathbb{K}[x_1, x_2] = \mathbb{K}[x_2, x_1]$.

    (c) Mostre que $\mathbb{K}[x_1, x_2]$ não é principal.

12. Seja A um anel comutativo. Mostre $< x >$ é um ideal primo de $A[x]$ se, e somente se, A é um domínio.

13. Sejam A um anel comutativo com unidade e $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$. Mostre que $f(x)$ é uma unidade em $A[x]$ se, e somente se, a_0 é uma unidade em A e $a_1, a_2, \cdots, a_n$, são nilpotentes. (Sugestão: Se $b_0 + b_1x + \cdots + b_mx^m$ é o inverso de $f(x)$, mostre por indução que $c_k = \sum_{i+j=k} a_ib_j = 0$, para $k \geq 1$. Portanto, a_n é nilpotente).

14. Seja a aplicação $\varphi : \mathbb{Q}[x] \to \mathbb{R}$ definida por $\varphi(f(x)) = f(\sqrt{2})$, onde $f(x) \in \mathbb{Q}[x]$.

    (a) Mostre que φ é um homomorfismo de anéis.

    (b) Determine o $\ker(\varphi)$ e verifique se é um ideal maximal.

15. Mostre que o polinômio $f(x) = 2$ é um elemento primo em $\mathbb{Z}[x]$. É um elemento irredutível?

13.2 Grau de um polinômio

Sejam A um anel comutativo com unidade e $A[x]$ o anel de polinômios na variável x. Relembramos que o grau de um polinômio $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ é definido como o maior número natural n tal que $a_n \neq 0$.

Proposição 13.2.1. *Se $f(x) = a_0 + a_1x + \cdots + a_mx^m$ e $g(x) = b_0 + b_1x + \cdots + b_nx^n$ são dois polinômios não nulos de $A[x]$, então*

1. *$f(x) + g(x) = 0$ ou $gr(f + g) \leq max\{gr(f), gr(g)\}$;*
2. *$gr(f + g) = max\{gr(f), gr(g)\}$, quando $gr(f) \neq gr(g)$*

Demonstração. Para (1), se $f(x) + g(x) = r(x)$ e $m = max\{gr(f), gr(g)\}$, então $r_i = 0$, para todo $i > m$, onde r_i são os coeficientes de $r(x)$. Portanto, $f(x) + g(x) = 0$ ou $gr(f + g) \leq m$. Para (2), se $m = gr(f) > gr(g)$, então $c_m = a_m + b_n = a_m + 0 \neq 0$ e $c_i = 0$, para todo $i > m$, onde a_i e b_i são os coeficientes de $f(x)$ e $g(x)$, respectivamente. Portanto, $gr(f + g) = m$. □

Proposição 13.2.2. *Se $f(x) = a_0 + a_1x + \cdots + a_mx^m$ e $g(x) = b_0 + b_1x + \cdots + b_nx^n$ são dois polinômios não nulos de $A[x]$, então*

1. *$f(x)g(x) = 0$ ou $gr(fg) \leq gr(f) + gr(g)$.*
2. *$gr(fg) = gr(f) + gr(g)$, quando o coeficiente dominante de $f(x)$ ou $g(x)$ é regular em A.*

Demonstração. (1) Sendo $gr(f) = m$, $gr(g) = n$ e $f(x)g(x) = c(x)$, segue que $c_{m+n+p} = a_0b_{m+n+p} + a_1b_{m+n+p-1} + \cdots + a_mb_{n+p} + \cdots + a_{m+n+p}b_0$, para todo $p \in \mathbb{N} - \{0\}$. Como $b_j = 0$ para $j > m$ e $a_i = 0$, para $i > m$, segue que $c_{m+n+p} = 0$, para todo $p \in \mathbb{N} - \{0\}$. Assim, ou $f(x)g(x) = 0$ ou $gr(fg) \leq m + n$. Para (2), se $gr(f) = m$ e $gr(g) = n$, então $c_{m+n} = a_0b_{m+n} + a_1b_{m+n-1} + a_mb_m + \cdots + a_{m+n}b_0 = a_mb_n$. Como a_m ou b_n é elemento regular de A, segue que $a_mb_n \neq 0$ e, portanto, $gr(fg) = m + n$. □

Observação 13.2.1. *Se A é um anel, então $A \subseteq A[x]$, uma vez que $\sigma : A \to A[x]$ definida por $\sigma(a) = a$, para todo $a \in A$, é um homomorfismo injetor de anéis. Também, segue que $U(A) \subseteq U(A[x])$. Além disso, se A é um anel de integridade, então $U(A) = U(A[x])$. De fato, se $f(x) \in A[x]$ é inversível, então $f(x)g(x) = 1$ para algum $g(x) \in A[x]$. Como $gr(fg) = gr(f) + gr(g) = 0$, segue que $f(x)$ e $g(x)$ são polinômios constantes não nulos. Portanto, $U(A[x]) \subseteq U(A)$.*

13.2.1 Exercícios

1. Dê exemplos de polinômios $f(x)$ e $g(x)$ tal que $gr(f+g) < max\{gr(f), gr(g)\}$ e $gr(fg) < gr(f) + gr(g)$.
2. Mostre que não existe um polinômio $f(x) \in \mathbb{R}[x]$ tal que $f^2(x) = f(x)f(x) = x^2 + x + 1$.

3. Determine os polinômios $f(x)$ de grau 3 tal que $f(x) - f(x-1) = x^2$.

4. Calcule $a - b$, onde $\frac{a}{x+1} + \frac{b}{x-1} = \frac{x+3}{x^2-1}$, com $x \neq \pm 1$.

5. A soma dos coeficientes do polinômio $p(x) = (ax^2 + 2bx + 3c + 1)^7$ é 128. Determine o valor de a, sabendo que -1 e 0 são raízes de $p(x)$.

6. Seja $p(x) = x^{2n}+x^{2n-1}+x^{2n-2}+x^{2n-3}+x^2+x+1$. Determine o valor de $p(1)+p(-1)+p(0)$.

7. Seja $a(x+2) + b(x-1) = 3$. Quais os valores de a e b?

13.3 Divisão de polinômios

Sejam A um anel comutativo com unidade e $A[x]$ o anel de polinômios. O conceito de divisibilidade em um anel se extende naturalmente do conceito de divisibilidade sobre o anel dos números inteiros, com certa especibilidade para a existência de máximo divisor comum e mínimo múltiplo comum de elementos em $A[x]$.

Definição 13.3.1. *Sejam $f(x), g(x) \in A[x]$. Diz-se que $f(x)$ divide $g(x)$ ou que $g(x)$ é divisível por $f(x)$ se existe $h(x) \in A[x]$ tal que $g(x) = f(x)h(x)$. Nesse caso, usa-se a notação $f(x) \mid g(x)$. Se $f(x)$ não divide $g(x)$ escreve-se $f(x) \nmid g(x)$.*

Exemplo 13.3.1. *Sejam $f(x) = 1 + x$ e $g(x) = 1 - x^2$ em $\mathbb{Z}[x]$. Como $1 - x^2 = (1 + x)(1 - x)$ e $1 - x \in \mathbb{Z}[x]$, segue que $f(x) \mid g(x)$.*

Observação 13.3.1. *A relação dada por $f(x)$ divide $g(x)$, sobre o anel $A[x]$, satisfaz as seguintes propriedades:*

1. *$f(x) \mid 0(x)$, uma vez que $0(x) = f(x)0(x)$.*

2. *$f(x) \mid f(x)$, para todo $f(x) \in A[x]$, pois $f(x) = f(x)1$.*

3. *Se $f(x) \mid g(x)$ e $g(x) \mid h(x)$, então $f(x) \mid h(x)$, pois se $g(x) = f(x)f_1(x)$ e $h(x) = g(x)g_1(x)$, então $h(x) = f(x)(f_1(x)g_1(x))$, ou seja, $f(x) \mid h(x)$.*

4. *Se $f(x) \mid g(x)$ então $f(x) \mid h(x)g(x)$, para todo $h(x) \in A[x]$, pois se $g(x) = f(x)f_1(x)$ então $h(x)g(x) = f(x)(h(x)g(x))$, para todo $h(x) \in A[x]$, ou seja, $f(x) \mid h(x)g(x)$.*

5. *Se $f(x) \mid g_1(x)$ e $f(x) \mid g_2(x)$ então $f(x) \mid (g_1(x)h_1(x) + g_2(x)h_2(x))$, para todo $h_1(x), h_2(x) \in A[x]$, pois se $g_1(x) = f(x)f_1(x)$ e $g_2(x) = f(x)f_2(x)$, então $h_1(x)g_1(x) + h_2(x)g_2(x) = f(x)(h_1(x)f_1(x) + h_2(x)f_2(x))$, para todo $h_1(x), h_2(x) \in A[x]$, ou seja, $f(x) \mid (g_1(x)h_1(x) + g_2(x)h_2(x))$.*

Teorema 13.3.1. *(Algoritmo de Euclides) Sejam $f(x) = a_0 + a_1x + \cdots + a_mx^m$ e $g(x) = b_0 + b_1x + \cdots + b_nx^n$ em $A[x]$. Se $g \neq 0$ e o coeficiente líder de $g(x)$ é inversível, então existem $q(x), r(x) \in A[x]$ de modo que $f(x) = g(x)q(x) + r(x)$, onde $r(x) = 0$ ou $gr(r) < gr(g)$.*

Demonstração. Se $f(x) = 0$, então existem $q(x) = r(x) = 0$, tal que $0 = g(x)0 + 0$. Se $f(x) \neq 0$ e $gr(f) < gr(g)$, então existem $q(x) = 0$ e $r(x) = f(x)$ tal que $g(x)0 + f(x) = f(x)$ e $gr(f) < gr(g)$. Finalmente, se $gr(f) \geq gr(g)$, procede-se pelo segundo príncipio de indução sobre $gr(f)$. Se $gr(f) = 0$, então $gr(g) = 0$. Daí $f(x) = a_0$ e $g(x) = b_0$ (coeficiente líder de g neste caso). Neste caso, é suficiente tomarmos $q(x) = b_0^{-1}a_0$ e $r(x) = 0$ uma vez que $a_0 = b_0(b_0^{-1}a_0) + 0$. Suponhamos, agora, que $gr(f) = m$ e que o teorema se verifica para todo polinômio de grau menor que m. Consideramos o polinômio $f_1(x) = f(x) - a_m b_n^{-1} x^{m-n} g(x)$. Se $f_1(x) = 0$ ou $gr(f_1) < gr(g)$, então $r(x) = f_1(x)$ e $q(x) = a_m b_n^{-1} x^{m-n}$. Caso contrário, segue que $gr(f_1) \leq m - 1$ e $gr(f_1) \geq gr(g)$. Pela hipótese de indução, segue que existem $q_1(x), r_1(x) \in A[x]$ de maneira que $f_1(x) = g(x)q_1(x) + r_1(x)$ onde $r_1(x) = 0$ ou $gr(r_1) < gr(g)$. Assim, $f(x) - a_m b_n^{-1} x^{m-n} g(x) = g(x)q_1(x) + r_1(x)$, o que acarreta que $f(x) = g(x)(q_1(x) + a_m b_n^{-1} x^{m-n}) + r_1(x)$, onde $r_1(x) = 0$ ou $gr(r_1) < gr(g)$ e isto prova o teorema. □

Corolário 13.3.1. *Se A é domínio, então é único o par $q(x), r(x)$ de polinômios.*

Demonstração. Vamos supor $f(x) = g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x)$, onde $gr(r) < gr(g)$ se $r(x) \neq 0$ e $gr(r_1) < gr(g)$, se $r_1(x) \neq 0$. Assim, $g(x)(q(x) - q_1(x)) = r_1(x) - r(x)$. Como $A[x]$ é um domínio, segue que $r_1(x) - r(x) = 0$ se, e somente se, $q(x) - q_1(x) = 0$. Se $r_1(x) - r(x) \neq 0$, então $gr(g(q - q_1)) = gr(g) + gr(q - q_1) = gr(r_1 - r)$. Logo, $gr(r_1 - r) \geq gr(g)$ o que é impossível pois $gr(r_1 - r) = gr(r_1)$ ou $gr(r_1 - r) = gr(r)$ ou $gr(r_1 - r) < max\{gr(r_1), gr(r)\}$. Portanto, o par $q(x), r(x)$ é único. □

Proposição 13.3.1. *Sejam A um domínio, $f(x), g(x) \in A[x]$ polinômios não nulos com $gr(f) = m$ e $gr(g) = n$ e $k = max\{m - n + 1, 0\}$. Se $b = b_n \neq 0$ é o coeficiente dominante de $g(x)$, então existem polinômios únicos $q(x), r(x) \in A[x]$ tal que*

$$b^k f(x) = q(x)g(x) + r(x),$$

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

Demonstração. Se m, n, é suficiente tomar $q(x) = 0$ e $r(x) = f(x)$. Se $m \geq n$, por indução sobre m, assumimos que o resultado é válido para todo polinômio de grau menor que m e mostramos que vale para $f(x)$. Se $a = a_m \neq 0$, então $ax^{m-n}g(x) = f_1(x)$ é um polinômio de grau menor que m. Por hipótese de indução, segue que existem $q_1(x), r_1(x) \in A[x]$ tal que $b^l f_1(x) = q_1(x)g(x) + r_1(x)$, com $r_1(x) = 0$ ou $gr(r_1) < gr(g) = n$, onde $l = max\{(m-1) - n + 1, 0\} = max\{m - n, 0\}$. Assim, $b^l(bf(x)) = (b^{m-n}ax^{m-n} + q_1(x))g(x) + r_1(x)$, ou seja, $b^k f(x) = q(x)g(x) + r(x)$, onde $b^k = b^l b$. Para a unicidade, se $b^k f(x) = q(x)g(x) + r(x) = q_1(x)g(x) + r_1(x)$, com $r = 0$ ou $gr(r) < n$ e $r_1(x) = 0$ ou $gr(r_1) < n$, então $(q(x) - q_1(x))g(x) = r_1(x) - r(x)$. Se $q_1(x) \neq q(x)$, então $gr((q_1 - q)g) = gr(q_1 - q) + gr(g) \geq n$ e $gr(r_1 - r) \leq max\{gr(r), gr(r_1)\} < n$, o que é uma contradição. Portanto, $q_1(x) = q(x)$ e $r_1(x) = r(x)$. □

Observação 13.3.2. *Os polinômios $q(x)$ e $r(x)$ cuja existência é assegurada pelo Teorema 13.3.1 são chamados, respectivamente, quociente e resto na divisão euclidiana de $f(x)$ por $g(x)$.*

13.3.1 Máximo divisior comum e mínimo múltiplo comum

O máximo divisor comum e mínimo múltiplo comum de dois polinômios são definidos de modo similar ao máximo divisor comum e mínimo múltiplo comum de dois números inteiros.

Definição 13.3.2. *Sejam A um anel comutativo com unidade e $f(x), g(x) \in A[x]$. Um elemento $d(x) \in A[x]$ se diz um máximo divisor comum de $f(x)$ e $g(x)$, denotado por $mdc(f(x), g(x))$, se*

1. *$d(x) \mid f(x)$ e $d(x) \mid g(x)$.*
2. *Para todo $d'(x) \in A[x]$ tal que $d'(x) \mid f(x)$ e $d'(x) \mid g(x)$ implica que $d'(x) \mid d(x)$.*

Neste caso, denotamos $d(x) = mdc(f(x), g(x))$. Dois elementos $f(x), g(x) \in A[x]$ são chamados primos entre si se $mdc(f(x), g(x))$ é uma unidade.

Observamos que a definição dada não garante a existência de máximo divisor comum de dois ou mais elementos de $A[x]$.

Proposição 13.3.2. *Sejam A um anel de integridade e $f(x), g(x) \in A[x]$.*

1. *Se $d(x), d_1(x) \in A[x]$ são máximos divisores comuns de $f(x)$ e $g(x)$, então $d(x)$ e $d_1(x)$ são associados.*
2. *Se $d(x) = mdc(f(x), g(x))$, então todo associado de $d(x)$ também é $mdc(f(x), g(x))$.*

Demonstração. Para (1), por hipótese, existem $h_1(x), h_2(x) \in A[x]$ tal que $d_1(x) = d(x)h_1(x)$ e $d(x) = d_1(x)h_2(x)$. Assim, $d(x) = d_1(x)h_2(x) = d(x)h_1(x)h_2(x)$, e deste modo, $h_1(x)h_2(x) = 1$. Portanto, $h_1(x)$ e $h_2(x)$ são unidades, ou seja, $d(x)$ e $d_1(x)$ são associados. Para (2), se $d_1(x) \in A[x]$ é tal que $d_1(x)$ é associado a $d(x)$, então $d_1(x) \mid d(x)$. Como $d(x) \mid f(x)$ e $d(x) \mid g(x)$, segue que $d_1(x) \mid f(x)$ e $d_1(x) \mid g(x)$. Agora, se existe $d'(x) \in A[x]$ tal que $d'(x) \mid f(x)$ e $d'(x) \mid g(x)$, então $d'(x) \mid d(x)$. Como $d(x) \mid d_1(x)$, segue que $d'(x) \mid d_1(x)$. Portanto, $d_1(x)$ é um $mdc(f(x), g(x))$. □

Definição 13.3.3. *Sejam A um anel comutativo com unidade e $f(x), g(x) \in A[x]$. Um elemento $m(x) \in A[x]$ se diz um mínimo mútiplo comum de $f(x)$ e $g(x)$, denotado por $mmc(f(x), g(x))$, se*

1. *$f(x) \mid m(x)$ e $g(x) \mid m(x)$.*
2. *Para todo $m'(x) \in A[x]$ tal que $f(x) \mid d'(x)$ e $g(x) \mid d'(x)$ implica que $m(x) \mid d'(x)$.*

Neste caso, denotamos $m(x) = mmc(f(x), g(x))$.

Observamos que a definição dada não garante a existência de um mínimo múltiplo comum de dois ou mais elementos de $A[x]$.

13.3.2 Exercícios

1. Determine o polinômio $f(x)$, onde $q(x) = x^2 + 1$ é o quociente e $r(x) = 3x - 5$ é o resto da divisão por $g(x) = x^2 - 3x + 5$.

2. Para que valores de a e b a divisão de$f(x) = x^3 + ax + b$ por $g(x) = 2x^2 + 2x - 6$ é exata.

3. Se $f(x)$ e $g(x)$ são divisíveis por $h(x)$, mostre que o resto da divisão de $f(x)$ por $g(x)$ é divisível por $h(x)$.

4. Sejam A um domínio que não é um corpo e $\alpha \in A$ não nulo e não inversível.

   (a) Mostre que $mdc(\alpha, x) = 1$.

   (b) Mostre que não existem $f(x), g(x) \in A[x]$ tal que $a(x)\alpha + b(x)x = 1$.

13.4 Raiz de um polinômio

Nesta seção, consideramos A um anel e $A[x]$ o anel de polinômios na variável x com coeficientes no anel A.

Definição 13.4.1. *Um elemento $\alpha \in A$ é uma raiz ou um zero de um polinômio $f(x) \in A[x]$ se $f(\alpha) = 0$.*

Definição 13.4.2. *A derivada de um polinômio $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m \in A[x]$, onde A é um anel comutativo com unidade, é definida como o polinômio $f'(x) = a_1 + 2a_2x + \cdots + ma_mx^{m-1}$ de $A[x]$.*

Proposição 13.4.1. *Se A é um domínio e $f(x) \in A[x]$ é um polinômio não nulo, então o número de raízes de $f(x)$ em A é no máximo $gr(f)$.*

Demonstração. Se o grau de $f(x)$ é zero, então é imediato a afirmação da proposição, pois neste caso, $f(x)$ não admite raiz em A. Suponhamos, agora, que $gr(f) = n > 0$ e que o resultado seja verdadeira para todo polinômio de grau $n - 1$. Se $f(x)$ não possui raiz em A, o resultado está provado. Se $f(x)$ possui uma raiz α em A, então pelo Teorema 13.3.1, segue que existe $q(x) \in A[x]$ de modo que $f(x) = (x - \alpha)q(x)$. Assim, qualquer outra raiz de $f(x)$ (caso exista) é raiz uma de $q(x)$. De fato, se $\beta \neq \alpha$ e $f(\beta) = 0$, então $(\beta - \alpha)q(\beta) = 0$. Assim, $q(\beta) = 0$ pois A é domínio. Como o número de raízes de $q(x)$ é no máximo $n - 1$, segue que o número de raízes de $f(x)$ em A é no máximo n. □

Corolário 13.4.1. *Sejam A um domínio e $f(x), g(x) \in A[x]$ tal que $gr(f) = gr(g) = n$. Se existem $n + 1$ elementos distintos $\alpha_1, \alpha_2, \cdots, \alpha_{n+1}$ tal que $f(\alpha_i) = g(\alpha_i)$ para todo $i = 1, 2, \cdots, n + 1$, então $f = g$.*

Demonstração. O polinômio $h(x) = f(x) - g(x)$ tem mais que n raízes em A e tem grau menor ou igual a n. Logo, $h(x) = 0$. □

Observação 13.4.1. *Na Proposição 13.4.1, o fato de A ser um anel de integridade é importante, uma vez que o polinômio $f(x) = x^2 + x$ tem grau 2 e tem $0, 2, 3, 5$ como raízes em $\mathbb{Z}_6$. Além disso, o fato de A ser comutativo é importante, uma vez que o polinômio $f(x) = x^2 + 1$ sobre o anel dos quatérnios $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j\}$ tem grau 2 e possui i, j, k como raízes em $\mathbb{H}$.*

Exemplo 13.4.1. *O ideal $< x >$ em $\mathbb{Z}[x]$ é um ideal primo. De fato, $< x > \neq \mathbb{Z}[x]$, uma vez que $1 \notin < x >$, pois x não divide 1. Sejam $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_nx^m$ em $\mathbb{Z}[x]$. Assim $f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + (a_nb_m)x^{n+m}$. Se $f(x)g(x) \in < x >$, então $f(x)g(x) = xh(x)$, para algum $h(x) \in A[x]$. Assim, $a_0b_0 = 0$, e deste modo, $a_0 = 0$ ou $b_0 = 0$. Logo, x divide $f(x)$ ou x divide $g(x)$. Assim, $f(x) \in < x >$ ou $g(x) \in < x >$, e portanto, $< x >$ é um ideal primo de $\mathbb{Z}[x]$.*

Proposição 13.4.2. *Se $\alpha \in A$ e $f(x) = a_0 + b_1x + \cdots + a_nx^n$ em $A[x]$, com $a_n \neq 0$, é um polinômio não constante, então $f(x) = (x - \alpha)q(x) + f(\alpha)$, para algum $q(x) \in A[x]$.*

Demonstração. Se $\alpha \in A$, então $x^n - \alpha^n = (x - \alpha)(x^{n-1} + \alpha x^{n-2} + \cdots + \alpha^{n-2}x + \alpha^{n-1})$, para todo $n > 0$ e todo $x \in A$. Se $f(x) = a_o + a_1x + \cdots + a_nx^n \in A[x]$, com $a_n \neq 0$ para algum $n > 0$. Assim, $f(x) - f(\alpha) = a_1(x - \alpha) + a_2(x^2 - \alpha^2) + \cdots + a_n(x^n - \alpha^n)$, ou seja, $f(x) - f(\alpha) = (x-\alpha)(a_1 + a_2(x+\alpha) + a_3(x^2+\alpha x+\alpha^2) + \cdots + a_n(x^{n-1}+\alpha x^{n-2}+\cdots+\alpha^{n-2}x+\alpha^{n-1}) = (x-\alpha)q(x)$, onde $q(x) = a_1 + a_2(x + \alpha) + a_3(x^2 + \alpha x + \alpha^2) + \cdots + a_n(x^{n-1} + \alpha x^{n-2} + \cdots + \alpha^{n-2}x + \alpha^{n-1})$. Portanto, $f(x) = q(x)(x - \alpha) + f(\alpha)$. □

Corolário 13.4.2. *Seja $f(x) = a_0 + b_1x + \cdots + a_nx^n$ em $A[x]$, com $a_n \neq 0$ e A um anel de integridade. Se α é uma raíz de $f(x)$, então $f(x) = (x - \alpha)q(x)$, para algum $q(x) \in A[x]$.*

Demonstração. Segue diretamente da Proposição 13.4.2. □

Corolário 13.4.3. *Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n$ em $A[x]$, com $a_n \neq 0$ e A um anel de integridade. Se $\alpha_1, \alpha_2 \cdots, \alpha_m$ são raízes distintas de $f(x)$, então*

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m)q_m(x),$$

para algum $q_m(x) \in A[x]$.

Demonstração. Como α_1 é uma raiz de $f(x)$, segue que existe $q_1(x) \in A[x]$ tal que $f(x) = (x - \alpha_1)q_1(x)$. Assim, $f(\alpha_2) = (\alpha_2 - \alpha_1)q_1(\alpha_2) = 0$, e portanto, $q_1(\alpha_2) = 0$. Analogamente, $q_1(x) = (x - \alpha_2)q_2(x)$, para algum $q_2(x) \in A[x]$. Por recorrência, segue que

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m)q_m(x),$$

para algum $q_m(x) \in A[x]$. Finalmente, se $\alpha \in A$ é uma raiz de $f(x)$ distinta das α_i, para $i = 1, 2, \cdots, m$, então $f(\alpha) = (\alpha - \alpha_1)(\alpha - \alpha_2) \cdots (\alpha - \alpha_m)q_m(\alpha) = 0$. Assim, $q_m(\alpha) = 0$, ou seja, α é raiz de $q_m(x)$. □

Corolário 13.4.4. *Seja $f(x) \in A[x]$ tal que $gr(f) \geq 1$. Se $\alpha \in A$, então o resto da divisão de $f(x)$ por $x - \alpha$ é $f(\alpha)$.*

Demonstração. Pelo Algoritmo da Divisão, segue que existem $q(x), r(x) \in A[x]$ tal que $f(x) = (x-\alpha)q(x) + r(x)$, com $r(x) = 0$ ou $0 \leq gr(r) < 1$. Se $r(x) \neq 0$, então $gr(r) = 0$. Assim, $r(x)$ é o polinômio constante e $f(\alpha) = r(\alpha) = r$. □

Corolário 13.4.5. *Sejam A um anel comutativo com unidade, $\alpha \in A$ e $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$, com $a_i \in A$ para $i = 0, 1, \cdots, n$. Se $q(x) = b_o + b_1x + \cdots + b_{n-1}x^{n-1}$ e $f(\alpha) = b_n$ são o quociente e o resto da divisão de $f(x)$ por $x - \alpha$, respectivamente, então $a_n = b_{n-1}$ e $b_i = \alpha b_{i+1} + a_i$ para todo $i = 0, 1, \cdots, n-1$.*

Demonstração. Pela Proposição 13.4.2, segue que $f(x) = (x-\alpha)q(x) + b_n$, ou seja, $f(x) = (b_n - \alpha b_0) + (b_0 - \alpha b_1)x + (b_1 - \alpha b_2)x^2 + \cdots + (b_{n-2} - \alpha b_{n-1})x^{n-1} + b_{n-1}x^n$. Portanto, $a_n = b_{n-1}$ e $b_i = \alpha b_{i+1} + a_i$ para todo $i = 0, 1, \cdots, n-1$. □

Definição 13.4.3. *Sejam A um anel e $f(x) \in A[x]$. Um elemento $\alpha \in A$ é uma raíz múltipla de $f(x)$ se existe $m \in \mathbb{N}$, com $m > 1$, tal que $f(x) = (x-\alpha)^m q(x)$, para algum $q(x) \in A[x]$. Neste caso, o elemento α é chamado de raiz de multiplicidade m. Se $m = 1$, o elemento α é chamado uma raiz simples de $f(x)$.*

Teorema 13.4.1. *Um elemento $\alpha \in A$ é uma raiz múltipla de $f(x) \in A[x]$ se, e somente se, α é uma raiz de $f'(x)$, onde $f'(x)$ é a derivada de $f(x)$.*

Demonstração. Se α é uma raiz múltipla de $f(x)$, então existe $g(x) \in A[x]$ tal que $f(x) = (x-\alpha)^2 g(x)$. Assim, a derivada de $f(x)$ é dada por $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$. Portanto, $f'(\alpha) = 0$. Reciprocamente, suponhamos que $f(\alpha) = f'(\alpha) = 0$. Se α é uma raiz simples de $f(x)$, então $f(x) = (x-\alpha)g(x)$, onde $g(x) \in A[x]$ com $g(\alpha) \neq 0$. Assim, $f'(x) = g(x) + (x-\alpha)g'(x)$, e portanto, $g(\alpha) = 0$, o que é um absurdo. □

Corolário 13.4.6. *Se o máximo divisor comum de $f(x)$ e $f'(x)$ é 1, então as raízes de $f(x)$ são simples.*

Demonstração. Como o $mdc(f(x), f'(x)) = 1$, segue que existem $g(x), h(x) \in A[x]$ tal que $1 = g(x)f(x) + h(x)f'(x)$. Se existir uma raiz múltipla $\alpha \in A$ de $f(x)$, então $f(\alpha) = f'(\alpha) = 0$. Assim, $1 = g(\alpha)f(\alpha) + h(\alpha)f'(\alpha) = 0$, o que é um absurdo. Portanto, todas as raízes de $f(x)$ são simples. □

Exemplo 13.4.2. *Se A é um anel de carcterística zero, então o polinômio $f(x) = x^n - 1$, com $n \geq 1$, somente admite raízes simples uma vez que $f'(x) = nx^{n-1} \neq 0$ e todas as raízes de $f'(x)$ são nulas ao passo que zero não é uma raiz de $f(x)$.*

Definição 13.4.4. *Seja A um anel. Um polinômio $f(x) \in A[x]$ é dito que decompõe (fatora) sobre A se existem $\alpha_1, \cdots, \alpha_n \in A$ e $a \in A$ tal que $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$, ou seja, $f(x)$ tem todas as raízes em A.*

Exemplo 13.4.3. *O polinômio $f(x) = x^3 - 1 = (x-1)(x - (\frac{-1+3i}{2}))(x - (\frac{-1-3i}{2}))$ se decompõe sobre $\mathbb{C}$ e o polinômio $f(x) = x^2 - 2 = (x-\sqrt{2})(x+\sqrt{2})$ se decompõe sobre $\mathbb{R}$.*

Observação 13.4.2. *Seja $f(x) \in \mathbb{R}[x]$ um polinômio. Se $\alpha \in \mathbb{C}$ é uma raiz de $f(x)$, então $\overline{\alpha}$ também é uma raiz de $f(x)$.*

13.4.1 Algoritmo de Briot-Ruffini

O algoritmo de Briot-Ruffini é um método prático para determinar a divisão de um polinômio $f(x)$ de grau $n \geq 1$ por um polinômio $g(x) = x - \alpha$. Seja $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ com $a_n \neq 0$. Seja $q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1}$ o quociente da divisão de $f(x)$ por $x - \alpha$. Assim, $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = (x - \alpha)(b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1}) + r$, onde r é o resto. Portanto, $r = a_0 + \alpha b_0$, $b_0 = a_1 + \alpha b_1$, $b_1 = a_2 + \alpha b_2$, $\cdots$, $b_{n-2} = a_{n-1} + \alpha b_{n-1}$ e $a_n = b_{n-1}$. Desse modo, o quociente e o resto pode ser obtido do seguinte modo

	a_n	a_{n-1}	a_{n-2}	.	a_1	a_0
α		αb_{n-1}	αb_{n-2}	.	αb_1	αb_0
	$b_{n-1} = a_n$	$b_{n-2} = a_{n-1} + \alpha b_{n-1}$	$b_{n-3} = a_{n-2} + \alpha b_{n-2}$	.	$b_0 = a_1 + \alpha b_1$	$r = a_0 + rb_0$

13.4.2 Relações de Girard

Albert Girard aprofundou, aproximadamente no ano de 1629, os estudos sobre as raízes de equações criando relações entre os coeficientes e as raízes da equações.

Sejam A um anel e $A[x]$ o anel de polinômios. Sejam $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$, com $a_n \neq 0$, e $\alpha_1, \alpha_2, \cdots, \alpha_n$ suas raízes. Assim,

$$\begin{aligned} f(x) &= a_n(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) \\ &= a_nx^n - a_n(\alpha_1 + \cdots + \alpha)x^{n-1} + a_n(\alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n)x^{n-2} \\ &\quad + \cdots + a_n(-1)^n(\alpha_1 \cdots \alpha_n). \end{aligned}$$

Portanto, igualando os coeficientes deste último polinômio, dois a dois, respectivamente, como os coeficientes iniciais $a_0, a_1, a_2, \cdots, a_nn$, obtemos n relações entre as raízes e os coeficientes de $f(x)$, denominadas Relações de Girard, e são as seguintes:

$$\begin{cases} \alpha_1 + \alpha_2 + \cdots + \alpha_n = -a_{n-1}/a_n \\ \alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n = a_{n-2}/a_n \\ \vdots \\ \alpha_1\alpha_2 \cdots \alpha_n = (-1)^n a_0/a_n. \end{cases}$$

13.4.3 Exercícios

1. Sejam $\alpha_1, \alpha_2, \alpha_3$ as raízes do polinômio $f(x) = x^3 - 2x^2 + 3x - 4 \in \mathbb{Z}[x]$. Calcule:

   (a) $\alpha_1 + \alpha_2 + \alpha_3$ e $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3$.

   (b) $\alpha_1\alpha_2\alpha_3$ e $\frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \frac{1}{\alpha_3}$.

2. Calcule as raízes do polinômio $f(x) = x^4 - 4x^3 - x^2 + 16x - 12 \in \mathbb{Z}[x]$, sabendo que duas de suas raízes são simétricas em relação à adição.

3. Determine m para que o polinômio $f(x) = x^3 + mx - 2 \in \mathbb{Z}[x]$ tenha uma raiz dupla.

4. Calcule as raízes do polinômio $f(x) = x^3 + 5x^2 - 12x - 36 \in \mathbb{Z}[x]$ sabendo que uma raiz é igual ao produto das outras duas.

5. Determine a e b tal que o polinômio $f(x) = x^4 + ax^3 + 2x^2 - x + b \in \mathbb{Z}[x]$ tenha duas raizes inversas entre si e a soma das outras duas raízes seja 1.

6. Se $a + b\sqrt{b}$, onde $a, b \in \mathbb{Z}$, é uma raiz do polinômio $f(x) \in \mathbb{Z}[x]$, mostre que $a - b\sqrt{b}$ também é uma raiz.

7. Determine:

   (a) Um polinômio $f(x) \in \mathbb{Z}[x]$ de grau mínimo que tenha $1, 2$ e $1 - \sqrt{2}$ como raízes.

   (b) As raízes da equação $2x^4 - 5x^3 - 2x^2 - 4x + 3 = 0$.

   (c) Um polinômio de grau mínimo que tenha como raízes $i, 2i$ e $3i$.

8. Sejam $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{C}[x]$ e $\overline{f}(x) = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n$. Mostre que $\alpha \in \mathbb{C}$ é uma raiz de $f(x)$ se, e somente se, $\overline{\alpha}$ é uma raiz de $\overline{f}(x)$.

9. Determine a soma dos coeficientes do polinômio $f(x) = (1-2x+x^4)^2(1+x+x^3)^{240} \in \mathbb{Z}[x]$.

10. Sejam $f(x) \in \mathbb{Z}[x]$ um polinômio mônico e $\alpha \in \mathbb{Q}$. Se $f(\alpha) = 0$, mostre que $\alpha \in \mathbb{Z}$.

11. Seja A um anel. Mostre que $A[x_1, x_2, \cdots, x_n] = A[x_{i_1}, x_{i_2}, \cdots, x_{i_n}]$, onde $(i_1, i_2, \cdots, i_n)$ é uma permutação de $(1, 2, \cdots, n)$.

12. Seja A um anel fatorial.

    (a) Mostre que $A[x]$ é um anel fatorial.

    (b) Mostre que $A[x_1, \cdots, x_n]$ é um anel fatorial.

13. Determine o polinômio $f(x)$, onde $q(x) = x^2 + 1$ é o quociente e $r(x) = 3x - 5$ é o resto da divisão por $g(x) = x^2 - 3x + 5$.

14. Para que valores de a e b a divisão de $f(x) = x^3 + ax + b$ por $g(x) = 2x^2 + 2x - 6$ é exata.

Capítulo

14

Polinômios sobre um corpo

Neste capítulo, veremos polinômios sobre um corpo $\mathbb{K}$, que é um anel comutativo com identidade, onde todo elemento não nulo de $\mathbb{K}$ é inversível. Se $\mathbb{K}$ é um corpo, então um ideal principal de $\mathbb{K}[x]$ é o conjunto dos múltiplos de um elemento $f(x) \in \mathbb{K}[x]$, isto é, o conjunto $I =< f(x) >= \{f(x)g(x) : g(x) \in \mathbb{K}[x]\}$. Além disso, apresentamos polinômios irredutíveis sobre um corpo. Um ponto importante é saber dizer, através do exame de seus coeficientes, se um polinômio é redutível ou irredutível. Não existe um critério geral de irredutibilidade, mas existem várias regras que são bastante úteis. Os anéis considerados serão sempre comutivo com unidade.

14.1 Anel de polinômios sobre um corpo

Seja $\mathbb{K}$ um corpo de característica 0 ou de característica p, onde p é um número primo. Como $\mathbb{K}$ é um anel comutativo com unidade, segue que $(\mathbb{K}[x], +, \cdot)$ é um anel comutativo com unidade. Além disso, Finalmente, pelo algoritmo da divisão, Corolário 13.3.1, dados $f(x) = a_0 + a_1x + \cdots + a_mx^m$ e $g(x) = b_0 + b_1x + \cdots + b_nx^n$ em $\mathbb{K}[x]$, com $g(x) \neq 0$, segue que existem únicos $q(x), r(x) \in \mathbb{K}[x]$ de modo que $f(x) = g(x)q(x) + r(x)$, onde $r(x) = 0$ ou $gr(r) < gr(g)$.

Teorema 14.1.1. *Todo ideal em $\mathbb{K}[x]$ é principal.*

Demonstração. Seja I um ideal de $\mathbb{K}[x]$. Se $I = \{0\}$, então $I =< 0 >$, e assim, I é principal. Agora, se $I \neq< 0 >$ e I possui polinômios constantes não nulos, então $I = \mathbb{K}[x]$, uma vez as constantes são inversíveis. Neste caso, $I =< 1 >$. Agora, vamos supor que I não possui polinômios constantes. Dentre os elementos não nulos de I seja $g(x)$ um polinômio não nulo

de grau mínimo. Assim, $< g(x) > \subset I$, pois $g(x) \in I$. Agora, se $f(x) \in I$, pelo algoritmo da divisão, segue que existe um único par de polinômios $q(x), r(x) \in \mathbb{K}[x]$ de maneira que $f(x) = g(x)q(x) + r(x)$, onde $r(x) = 0$ ou $gr(r) < gr(g)$. Assim, $r(x) = f(x) - g(x)q(x)$. Como $f(x)$ e $g(x)$ estão em I, segue que o mesmo acontece com $r(x)$. Mas não podemos ter que $r(x) \in I$ e $gr(r) < gr(g)$, do que resulta que somente existe a alternativa $r(x) = 0$. Assim, $f(x) = g(x)q(x)$ o que mostrar que $f(x) \in < g(x) >$. Logo, $I \subset < g(x) >$. Portanto, $I = < g(x) >$. □

Corolário 14.1.1. *O anel $\mathbb{K}[x]$ é um anel principal.*

Demonstração. Segue diretamente do Teorema 14.1.1. □

Proposição 14.1.1. *Se $f(x), g(x) \in \mathbb{K}[x]$, então existem $h_1(x), h_2(x) \in \mathbb{K}[x]$ de maneira que o polinômio $d(x) = f(x)h_1(x) + f(x)h_2(x)$ é um máximo divisor de $f(x)$ e $g(x)$.*

Demonstração. Seja o ideal $I = < f(x), g(x) > = \{f(x)m_1(x) + g(x)m_2(x) \mid m_1(x), m_2(x) \in \mathbb{K}[x]\}$. Como todo ideal em $\mathbb{K}[x]$ é principal, segue que existe $d(x) \in I$ de maneira que $I = < d(x) >$. Mostremos que $d(x)$ é um máximo divisor comum de $f(x)$ e $g(x)$. Como $f(x) \in I$, segue que existe $q_1(x) \in \mathbb{K}[x]$ tal que $f(x) = d(x)q_1(x)$, ou seja, $d(x) \mid f(x)$. Como $g(x) \in I$, segue que existe $q_2(x) \in \mathbb{K}[x]$ tal que $g(x) = d(x)q_2(x)$, ou seja, $d(x) \mid g(x)$. Agora, como $d(x) \in I$, segue que existem $h_1(x), h_2(x) \in \mathbb{K}[x]$ de modo que $d(x) = f(x)h_{1(x)} + g(x)h_2(x)$. Finalmente, se $d'(x) \in \mathbb{K}[x]$ divide $f(x)$ e divide $g(x)$, então $d'(x) \mid d(x)$. □

Proposição 14.1.2. *Sejam $f(x), g(x) \in \mathbb{K}[x]$ e $d(x) \in \mathbb{K}[x]$ um máximo divisor comum de $f(x)$ e $g(x)$. Um elemento $d'(x) \in \mathbb{K}[x]$ é um máximo divisor comum de $f(x)$ e $g(x)$ se, e somente se, existe $k \in \mathbb{K}^\star$ tal que $d'(x) = kd(x)$.*

Demonstração. Se $d'(x)$ é um máximo divisor comum de $f(x)$ e $g(x)$, então $d'(x) \mid f(x)$ e $d'(x) \mid g(x)$. Logo, $d'(x) \mid d(x)$. De maneira análoga, segue que $d(x) \mid d'(x)$. Agora, se $d'(x) \mid d(x)$, então existe $q_1(x) \in \mathbb{K}[x]$ tal que $d(x) = d'(x)q_1(x)$ e se $d(x) \mid d'(x)$, então existe $q_2(x) \in \mathbb{K}[x]$ tal que $d'(x) = d(x)q_2(x)$. Donde $d(x) = d(x)(q_1(x)q_2(x))$. O caso $d(x) = 0$ somente ocorre quando $f(x) = g(x) = 0$. Portanto, $d'(x) = 0$ e qualquer $k \in \mathbb{K}^\star$ satisfaz a igualdade $d'(x) = kd(x)$. Se $d(x) \neq 0$, então $q_1(x)q_2(x) = 1$, e portanto, $q_1(x), q_2(x) \in \mathbb{K}^\star$. Fazendo $q_2(x) = k$, segue que $d'(x) = kd(x)$. Reciprocamente, se $d'(x) \in \mathbb{K}[x]$ é um máximo divisor comum de $f(x)$ e $g(x)$, então $d'v = kd(x)$. Como $d(x) \mid f(x)$, segue que existe $q(x) \in \mathbb{K}[x]$ tal que $f(x) = d(x)q(x)$. Assim, $f(x) = (kd(x))(\frac{1}{k}q(x)) = d'(x)(\frac{1}{k}q(x))$, e deste modo, $d'(x) \mid f(x)$. De maneira análoga, segue que $d'(x) \mid g(x)$. Agora, se $d_1(x) \mid f(x)$ e $d_1(x) \mid g(x)$ então $d_1(x) \mid d(x)$, e assim, $d_1(x) \mid kd(x)$. □

As Proposições 14.1.1 e 14.1.2 afirmam que dois elementos $f(x), g(x) \in \mathbb{K}[x]$ possui tantos máximos divisores comuns quanto são os elementos de $\mathbb{K}^\star$. Se o máximo divisor comum for unitário, então a unicidade do máximo divisor comum. Dois polinômios $f(x)$, $g(x) \in \mathbb{K}[x]$ são chamados *primos entre si* se a unidade de $\mathbb{K}$ é um máximo divisor comum de $f(x)$ e $g(x)$. Assim, o subconjunto dos elementos de $\mathbb{K}[x]$ que satisfazem as condições (1) e (2) da definição de máximo divisor comum é $\mathbb{K}^\star$, o conjunto dos polinômios constantes.

Exemplo 14.1.1. *Os polinômios $f(x) = x + x^2$ e $g(x) = 2 + x + x^2 \in \mathbb{R}[x]$ são primos entre si, uma vez que se $p(x) \mid f(x)$ e $p(x) \mid g(x)$, então $p(x) \mid (g(x) - f(x))$, isto é, $p(x) \mid 2$. Logo, $f(x)$ e $g(x)$ somente admitem divisores comuns constantes.*

Vamos abordar um método prático para obter um fator comum entre dois polinômios e posteriormente mostrar que com este método obtemos um maior fator comum entre eles. Assim, considere $f(x)$ e $g(x)$ e $m(x)$ um maior fator comum entre eles. Aplicando o algoritmo de Euclides sucessivamente, segue que

$$\begin{cases} f(x) &= q_1(x)g(x) + r_1(x), & gr(r_1) < gr(g) \\ g(x) &= q_2(x)r_1(x) + r_2(x), & g(r_2) < gr(r_1) \\ r_1(x) &= q_3(x)r_2 + r_3(x), & gr(r_3) < gr(r_2) \\ & \vdots & \\ r_i(x) &= q_{i+2}(x) + r_{i+2}(x), & gr(r_{i+2}) < gr(r_{i+1}). \end{cases}$$

Utilizando por conveniência $f(x) = r_{-1}(x)$ e $g(x) = r_0(x)$, segue que os graus de $r_i(x)$ formam uma sequência decrescente de inteiros não negativos, após um número finito de divisões obtemos um resto igual a zero, digamos r_{s+2}, e nesse momento o processo para. Sendo assim, a última equação desta lista cujo resto não é zero é dado por

$$r_{s-1} = q_{s+1}(x)r_s(x) + r_{s+1} \tag{14.1}$$

Assim, podemos tomar $m(x) = r_{s+1}(x)$.

Teorema 14.1.2. *$m(x) = r_{s+1}(x)$ é um maior fator comum para $f(x)$ e $g(x)$.*

Demonstração. Primeiramente, mostramos que $r_{s+1}(x)$ divide $f(x)$ e $g(x)$. Para isso, vamos usar indução decrescente para mostrar que $r_{s+1}(x) \mid r_i(x)$ para todo i. Claramente, $r_{s+1}(x) \mid r_{s+1}(x)$, e ainda, pela equação 14.1, segue que $r_{s+1}(x) \mid r_s(x)$. Pelo algoritmo, se $r_{s+1}(x) \mid r_{i+2}(x)$ e $r_{s+1}(x) \mid r_{i+1}(x)$, então $r_{s+1}(x) \mid r_i(x)$, e assim, $r_{s+1}(x)$ divide $r_i(x)$ para todo i. Em particular, $r_{s+1}(x)$ divide $f(x)$ e $g(x)$. Agora, suponhamos que $e(x) \mid f(x)$ e $e(x) \mid g(x)$. Pelo algoritmo e pela indução, segue que $e(x) \mid r_i(x)$, para todo i. Portanto, $e(x) \mid r_{s+1}(x)$, provando o teorema. □

Exemplo 14.1.2. *Considere $f(x) = 4x^4 + 3x^3 + 2x^2 + 2x + 1$ e $g(x) = x^2 - 1$ em $\mathbb{Q}[x]$. Vamos calcular o maior fator comum utilizando o método. Utilizando o método descrito anteriormente, e dividindo o polinômio $f(x)$ por $g(x)$, segue que $(x^2 + 2x + 3)(x^2 - 1) + 4x + 4$. Agora, dividido $x^2 - 1$ por $4x + 4$, segue que*

$$x^2 + 1 = (4x + 4)(\frac{1}{4}x - \frac{1}{4}).$$

Assim, podemos tomar $4x + 4$ como o maior fator comum entre esses polinômios. Note que $x + 1$ também é um máximo fator em comum.

14.1.1 Exercícios

1. Sejam $f(x), g(x), h(x) \in \mathbb{K}[x]$, onde $\mathbb{K}$ é um corpo.

(a) Mostre que $f(x)|f(x)$.

(b) Se $f(x)|g(x)$, mostre que $f(x)|g(x)h(x)$.

(c) Se $f(x)|g(x)$ e $g(x)|h(x)$, mostre que $f(x)|h(x)$.

2. Sejam $f(x), g(x), h(x) \in \mathbb{K}[x]$, onde $\mathbb{K}$ é um corpo.

(a) Se $mdc(f, g)$ é uma unidade, mostre que existem $a(x), b(x) \in \mathbb{K}[x]$ tal que $a(x)f(x) + b(x)g(x) = 1$.

(b) Se $mdc(f, g)$ é uma unidade e $f(x)|g(x)h(x)$, mostre que $f(x)|h(x)$.

(c) Se $mdc(f, g) = 1$ e $mdc(f, h) = 1$, mostre que $mdc(f, gjh) = 1$.

(d) Se $mdc(f, g) = 1$, $f(x)|h(x)$ e $g(x)|h(x)$, mostre que $f(x)g(x)|h(x)$.

3. Mostre que $\mathbb{Z}[x]$ é um subanel de $\mathbb{Q}[x]$, mas não é um ideal.

4. Mostre que $< 2, x >$ é um ideal maximal de $\mathbb{Z}[x]$. O ideal $< 4, x >$ é maximal em $\mathbb{Z}[x]$?

5. Se $\mathbb{K}$ é um corpo, mostre que $< x >$ é um ideal maximal de $\mathbb{K}[x]$.

6. Determine a soma dos coeficientes de $f(x) = (2 + 2x - x^3)^4(1 + 3x + x^3)^{240} \in \mathbb{Q}[x]$.

7. Se $f(x) \in \mathbb{R}[x]$ é divisível por $x - a$ e por $x - b$, com $a \neq b$, mostre que $f(x)$ é divisível por $(x - a)(x - b)$.

8. Seja $f(x) \in \mathbb{R}[x]$. Se $u \in \mathbb{C}$ é uma raiz de $f(x)$, mostre que $\overline{u}$ também é uma raiz de $f(x)$.

9. Seja $\sigma : \mathbb{Q} \to \mathbb{Q}$ um homomorfismo tal que $\sigma(n) = n$, para todo $n \in \mathbb{Z}$. Se $u \in \mathbb{Q}$ é uma raiz de $f(x) \in \mathbb{Q}[x]$, mostre que $\sigma(u)$ também é uma raiz de $f(x)$.

10. Seja $f(x) \in \mathbb{K}[x]$, onde $\mathbb{K}$ é um corpo.

(a) Mostre que u é uma raiz de $f(x)$ se, e somente se, $x - u$ divide $f(x)$.

(b) Mostre que u é uma raiz múltipla se, e somente se, $f'(u) = 0$, onfe f' é a derivada de f.

14.2 Polinômios irredutíveis

Sejam $\mathbb{K}$ um corpo e $\mathbb{K}[x]$ o anel de polinômios sobre $\mathbb{K}$ na variável x.

Definição 14.2.1. *Um polinômio não nulo $p(x) \in \mathbb{K}[x]$ é chamado irredutível em $\mathbb{K}[x]$ ou irredutível sobre $\mathbb{K}$ se:*

1. *$p(x) \notin \mathbb{K}$, ou seja, $p(x)$ não é um polinômio constante, e*

2. *Dado $f(x) \in \mathbb{K}[x]$, se $f(x) \mid p(x)$, então $f(x) \in \mathbb{K}^\star$ ou existe $c \in \mathbb{K}^\star$ tal que $f(x) = cp(x)$, ou seja, se $p(x) = g(x)h(x)$, onde $g(x), h(x) \in \mathbb{K}[x]$, então $g(x) \in \mathbb{K}^\star$ ou $h(x) \in \mathbb{K}^\star$.*

Diremos que $f(x)$ é redutível em $\mathbb{K}[x]$ se

1. *$f(x) \in \mathbb{K}^\star$, ou*
2. *se existe $g(x) \in \mathbb{K}[x]$ tal que $g(x) \mid f(x)$ e $g(x) \notin \mathbb{K}^\star$.*

Exemplo 14.2.1. *Todo polinômio de grau 1 sobre um corpo $\mathbb{K}$ é irredutível, uma vez que se $f(x) = ax + b \in \mathbb{K}[x]$ é um polinômio de grau 1, então $a \neq 0$. Por outro lado, se $g(x) \mid f(x)$, então existe $h(x) \in \mathbb{K}[x]$ de modo que $f(x) = g(x)h(x)$. Assim, $1 = gr(g) + gr(h)$. Portanto, $gr(g) = 0$ ou $gr(h) = 0$. No primeiro caso, segue que $g(x) = c \in \mathbb{K}^\star$, e no segundo, segue que $h(x) = k \in \mathbb{K}^\star$, e assim, $g(x) = \frac{1}{k}f(x)$. Portanto, $f(x)$ é irredutível.*

Exemplo 14.2.2. *O polinômio $f(x) = x^4 + x^3 + x^2 + x + 1$ é irredutível sobre $\mathbb{Z}$. Se $f(x)$ não for irredutível, então $f(x)$ pode se fatorar em produto de dois polinômios. Como $gr(f) = 4$, os polinômios podem ter graus 3 e 1, ou 2 e 2. A primeira possibilidade não ocorre, uma vez que $f(x)$ não tem raiz em $\mathbb{Z}_2$, portanto resta somente a segunda possibilidade. Assim, se $f(x) = (a_0 + a_1x + a_2x^2)(b_0 + b_1x + b_2x^2) = (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_1b_1 + a_2b_0 + a_0b_2)x^2 + (a_1b_2 + a_2b_1)x^3 + (a_2b_2)x^4$, então*

$$\begin{cases} a_0b_0 = 1 \Rightarrow a_0 = 1 \text{ e } b_0 = 1 \\ a_0b_1 + a_1b_0 = 1 \Rightarrow b_1 + a_1 = 0 \Rightarrow b_1 = 1 + a_1 \\ a_1b_1 + a_2b_0 + a_0b_2 = 1 \Rightarrow a_1^2 + a_1 + 1 = 0, \text{ não tem solução em } \mathbb{Z}_2. \\ a_1b_2 + a_2b_1 = 1 \\ a_2b_2 = 1 \Rightarrow a_2 = 1 \text{ e } b_2 = 1 \end{cases}$$

Como o sistema não tem solução em $\mathbb{Z}_2$, segue que $f(x)$ não pode ser decomposto em um produto de polinômios de grau 2. Portanto, $f(x)$ é irredutível sobre $\mathbb{Z}_2$.

Exemplo 14.2.3. *O polinômio $f(x) = x^4 + x + 1$ é irredutível sobre $\mathbb{Z}_2$, uma vez que se $f(x)$ não for irredutível, então $f(x)$ pode se fatorar em produto de dois polinômios. Como $gr(f) = 4$, segue que os polinômios podem ter graus 3 e 1, ou 2 e 2. A primeira possibilidade não ocorre, uma vez que $f(x)$ não tem raiz em $\mathbb{Z}_2$, e portanto, resta somente a segunda possibilidade. Assim, se $f(x) = (a_0 + a_1x + a_2x^2)(b_0 + b_1x + b_2x^2) = (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_1b_1 + a_2b_0 + a_0b_2)x^2 + (a_1b_2 + a_2b_1)x^3 + (a_2b_2)x^4$, então*

$$\begin{cases} a_0b_0 = 1 \Rightarrow a_0 = 1 \text{ e } b_0 = 1 \\ a_0b_1 + a_1b_0 = 1 \Rightarrow b_1 + a_1 = 0 \Rightarrow b_1 = 1 + a_1 \\ a_1b_1 + a_2b_0 + a_0b_2 = 0 \\ a_1b_2 + a_2b_1 = 0 \Rightarrow a_1 + b_1 = 0 \Rightarrow 1 + a_1 + a_1 = 0. \text{ (Absurdo)} \\ a_2b_2 = 1 \Rightarrow a_2 = 1 \text{ e } b_2 = 1 \end{cases}$$

Como o sistema não tem solução em $\mathbb{Z}_2$, segue que $f(x)$ não pode ser decomposto em um produto de polinômios de grau 2. Portanto, $f(x)$ é irredutível sobre $\mathbb{Z}_2$.

Exemplo 14.2.4. *Os polinômios $f(x) = x^3 + x^2 + 1$ e $g(x) = x^3 + x + 1$ são irredutíveis sobre $\mathbb{Z}$, uma vez que a única maneira de $f(x)$ e $g(x)$ se fatorarem é em um produto de polinômios de graus 2 e 1, o que não ocorre uma vez que $f(x)$ e $g(x)$ não possuem raízes em $\mathbb{Z}_2$.*

Observação 14.2.1. *O polinômio $p(x) = 2x+4 = 2(x+2)$ é redutível sobre $\mathbb{Z}$ e irredutível sobre $\mathbb{Q}$.*

Definição 14.2.2. *Um corpo $\mathbb{K}$ é chamado algébricamente fechado se todo polinômio sobre $\mathbb{K}$ tem uma raíz em $\mathbb{K}$.*

O corpo $\mathbb{C}$ é algébricamente fechado cuja demonstração foi dada por Gauss em 1848, chamado Teorema Fundamental da Álgebra.

Proposição 14.2.1. *Um polinômio sobre um corpo algébricamente fechado $\mathbb{K}$ é irredutível se, e somente se, tem grau 1.*

Demonstração. Se $f(x) \in \mathbb{K}[x]$ e $\mathbb{K}$ é algébricamente fechado, então existem $u \in \mathbb{K}$ e $g(x) \in \mathbb{K}[x]$ tal que $f(x) = (x-u)g(x)$. Se $f(x)$ é irredutível, então $g(x)$ é constante. Portanto, $gr(f) = 1$. Pelo Exemplo 14.2.1, segue a recíproca. □

Corolário 14.2.1. *Seja $f(x) \in \mathbb{K}[x]$, onde $\mathbb{K}$ é um corpo algébricamente fechado. Se $gr(f) = n \geq 1$, então existem $a, u_1, u_2 \cdots, u_n \in \mathbb{K}$, com $a \neq 0$, tal que $f(x) = a(x-u_1)\cdots(x-u_n)$.*

Demonstração. A demonstração é por indução sobre $n = gr(f)$. Se $gr(f) = 1$, então $f(x) = ax+b$, com $a, b \in \mathbb{K}$ e $a \neq 0$. Logo, $f(x) = a(x+\frac{b}{a})$ e $u_1 = -\frac{b}{a}$. Agora suponhamos o resultado válido para $n-1$, onde $n-1 \geq 1$. Seja $f(x) \in \mathbb{K}[x]$ com $gr(f) = n$. Por hipótese, segue que $f(x)$ tem uma raiz $u_1 \in \mathbb{K}$. Assim, pelo algoritmo da divisão, segue que $f(x) = q(x)(x-u_1)$, para algum $q(x) \in \mathbb{K}[x]$ e $gr(q) = n-1$. Por hipótese de indução, segue que existem $a, u_2, \ldots, u_n \in \mathbb{K}$, com $a \neq 0$ tal que $q(x) = a(x-u_2)\ldots(x-u_n)$. Assim, $f(x) = a(x-u_1)(x-u_2)\ldots(x-u_n)$, o que prova o resultado. □

Proposição 14.2.2. *Todo corpo algebricamente fechado é infinito.*

Demonstração. Seja $\mathbb{K}$ um corpo algebricamente fechado e suponhamos, por absurdo, que $\mathbb{K}$ seja finito. Assim, $\mathbb{K} = \{a_1 = 0, a_2 = 1, a_3, \ldots, a_n\}$, onde $n \geq 2$. Se $f(x) = (x-a_1)\ldots(x-a_n)+1$, então $f(a_j) = 1 \neq 0$, para todo $j = 1, 2, \ldots, n$. Assim, $f(x)$ é um polinômio não constante e não tem raízes em $\mathbb{K}$, contradizendo a hipótese de $\mathbb{K}$ ser algebricamente fechado. □

Exemplo 14.2.5. *O corpo finito $\mathbb{Z}_p$, com p um primo, não é algebricamente fechado.*

Em um contexto mais geral, para todo corpo $\mathbb{K}$, segue que existe um corpo algebricamente fechado $\mathbb{L}$ tal que $\mathbb{K} \subset \mathbb{L}$.

Proposição 14.2.3. *Sejam $p(x), f(x), g(x) \in \mathbb{K}[x]$, onde $p(x)$ é irredutível. Se $p(x) \mid f(x)g(x)$, então $p(x) \mid f(x)$ ou $p(x) \mid g(x)$.*

Demonstração. Se $p(x)$ não divide $f(x)$, então $p(x)$ e $f(x)$ são primos entre si. Como $p(x)$ é irredutível, segue que se $g(x) \mid p(x)$ então $g(x) = c \in K^\star$ ou $g(x) = cp(x)$, com $c \in \mathbb{K}^\star$. Como nenhum dos polinômios $cp(x)$, onde $c \in \mathbb{K}^\star$, divide $f(x)$, segue que os divisores comuns a $f(x)$ e $p(x)$ são apenas os polinômios constantes não nulos. Tomando 1 como o máximo divisor comum

de $f(x)$ e $p(x)$, segue que existem $h_1(x), h_2(x) \in \mathbb{K}[x]$ de maneira que $1 = f(x)h_1(x)+p(x)h_2(x)$. Multiplicando por $g(x)$ esta igualdade, segue que $g(x) = (f(x)g(x))h_1(x) + p(x)g(x)(h_2(x))$. Como $p(x) \mid f(x)g(x)$ e $p(x) \mid p(x)$, segue que $p(x) \mid g(x)$, o que prova a proposição. □

Corolário 14.2.2. *Se $p(x) \in \mathbb{K}[x]$ é irredutível e $p(x) \mid f_1(x)f_2(x)\cdots f_n(x)$, onde cada $f_i(x) \in \mathbb{K}[x]$ e $n \geq 1$, então $p(x)$ divide um dos $f_i(x)$, para algum i.*

Demonstração. Se $p(x) \mid (f_1(x)f_2(x)\cdots f_{n-1}(x))f_n(x)$, pela Proposição14.2.3, segue que $p(x) \mid f_1(x)f_2\cdots f_{n-1}(x)$ ou $p(x) \mid f_n(x)$. Por indução, o resultado segue. □

Teorema 14.2.1. *(Fatoração única) Se $f(x)$ é um polinômio não constante de $\mathbb{K}[x]$, então existem polinômios irredutíveis $p_1(x), p_2(x), \cdots, p_r(x) \in \mathbb{K}[X]$, onde $r \geq 1$, de maneira que $f(x) = p_1(x)p_2(x)\cdots p_r(x)$. Além disso, se $f(x) = q_1(x)q_2(x)\cdots q_s(x)$, onde $q_1(x), q_2(x), \cdots, q_s(x) \in \mathbb{K}[x]$, onde $s \geq 1$, são também irredutíveis sobre $\mathbb{K}$, então $r = s$ e cada polinômio $p_i(x)$ é igual ao produto de um polinômio $q_j(x)$ por um elemento conveniente de $\mathbb{K}^\star$.*

Demonstração. Se $f(x)$ é irredutível, então o teorema é válido. Por outro lado, se $f(x)$ for redutível, então a prova é feita por indução sobre o grau de $f(x)$. Se $gr(f) = 1$, então $f(x)$ é irredutível. Agora, suponhamos que $gr(f) = n > 1$ e que o teorema seja verdadeiro, quanto a decomposição, para todo polinômio de grau r, com $1 < r < n$. Se $f(x)$ for redutível, então existem $g(x), h(x) \in \mathbb{K}[x]$ de maneira que $f(x) = g(x)h(x)$ e $0 < gr(g), gr(h) < gr(f)$. Devido à hipótese de indução, segue que $g(x) = p_1(x)p_2(x)\cdots p_t(x)$ e $h(x) = p_{t+1}(x)p_{t+2}(x)\cdots p_r(x)$, onde os $p_i(x)$ são irredutíveis, $t \geq 1$ e $r \geq 1$. Logo, $f(x) = p_1(x)p_2(x)\cdots p_r(x)$, é um produto de polinômios irredutíveis. Para a unicidade, seja $f(x) = p_1(x)p_2(x)\cdots p_r(x) = q_1(x)q_2(x)\cdots q_s(x)$. Como $p_1(x)$ é irredutível e $p_1(x) \mid (q_1(x)q_2(x)\cdots q_s(x))$, segue que $p_1(x)$ divide um dos $q_i(x)$. Supondo que $p_1(x) \mid q_1(x)$, e como $q_1(x)$ também é irredutível, segue que existe $c_1 \in \mathbb{K}^\star$ de maneira que $p_1(x) = c_1q_1(x)$. Voltando à igualdade do início e levando em conta a relação que acabamos de obter ficamos com $(c_1q_1(x))p_1(x)p_2(x)\cdots p_r(x) = q_1(x)q_2(x)\cdots q_s(x)$ do que resulta que $(c_1p_2(x))p_3(x)\cdots p_r(x) = q_2(x)q_3(x)\cdots q_s(x)$. Repetindo sucessivamente este raciocínio até esgotar todos os fatores $q_j(x)$ (e consequentemente todos os fatores $p_i(x)$), segue à unicidade, nos termos do enunciado, o que prova o teorema. □

Proposição 14.2.4. *Um polinômio $f(x) \in \mathbb{R}[x]$ é irredutível se, e somente se, $gr(f) = 1$ ou $gr(f) = 2$ e seu discriminante é negativo.*

Demonstração. Se $f(x) \in \mathbb{R}[x]$, então $f(x) \in \mathbb{C}[x]$. Como $\mathbb{C}$ é algébricamente fechado, segue que $f(x)$ têm uma raíz em $\alpha \in \mathbb{C}$. Se $\alpha \in \mathbb{R}$, então $f(x) = (x-\alpha)q(x)$, onde $q(x) \in \mathbb{R}[x]$ é constante. Logo, $gr(f) = 1$. Se $\alpha = a+bi \in \mathbb{C}$, então $\overline{\alpha} = a-bi$ também é raíz de $f(x)$. Assim, $f(x)$ é divisível por $(x-\alpha)(x-\overline{\alpha}) = x^2-2ax+a^2+b^2$ que é um polinômio com coeficientes reais. Assim, existe $q(x) \in \mathbb{R}[x]$ tal que $f(x) = (x^2 - 2ax + a^2 + b^2)q(x)$. Como $f(x)$ é irredutível, segue que $q(x) = c$, onde c é uma constante. Assim, $\Delta = 4a^2c^2 - 4c(a^2 + b^2) = -4a^2b^2 < 0$. Reciprocamente, se $gr(f) = 1$, então $f(x)$ é irredutível. Se $gr(f) = 2$, então $f(x)$ é irredutível ou tem uma raíz em $\mathbb{R}$. Como $\Delta < 0$, segue que $f(x)$ não têm raíz em $\mathbb{R}$, e portanto, $f(x)$ é irredutível. □

14.2.1 Exercícios

1. Mostre que:
   (a) Todo polinômio mônico e de grau 1 sobre $\mathbb{Z}$ é irredutível.
   (b) Todo polinômio de grau 2 sobre um corpo é irredutível ou decompõe sobre o corpo.
   (c) Todo polinômio de grau 3 sobre um corpo é irredutível ou possui uma raiz sobre o corpo.
   (d) Todo polinômio de grau impar sobre $\mathbb{R}$ possui uma raiz em $\mathbb{R}$.
2. Sejam $\mathbb{K}$ um corpo e $f(x) \in \mathbb{K}[x]$ um polinômio.
   (a) Mostre que $f(x)$ é irredutível se, e somente se, $\frac{\mathbb{K}[x]}{<f(x)>}$ é um corpo.
   (b) Dê um exemplo, onde o resultado não vale se $\mathbb{K}$ for apenas um anel.
3. Mostre que:
   (a) O polinômio $f(x) = x^4 + 2$ é irredutível sobr $\mathbb{Q}$.
   (b) O polinômio $f(x) = x^3 - x - 1$ é irredutível sobre $\mathbb{Q}(\sqrt{-23})$.
4. Sejam $\mathbb{K} \subseteq \mathbb{L}$ corpos. Se $f(x), g(x) \in \mathbb{K}[x]$ são relativamente primos em $\mathbb{K}[x]$, mostre que $f(x), g(x)$ são relativamente primos em $\mathbb{L}[x]$.
5. Sejam $\mathbb{K}$ um corpo e $\alpha \in \mathbb{K}$.
   (a) Mostre que $M_\alpha = \{f(x) \in \mathbb{K}[x] : f(\alpha) = 0\}$ é um ideal maximal em $\mathbb{K}[x]$.
   (b) Mostre que $\frac{\mathbb{K}[x]}{M_\alpha}$ é isomorfo a $\mathbb{K}$.
   (c) Se $\mathbb{K}$ for apenas uma anel, o ideal M_α é maximal?
6. Mostre que $f(x) \in \mathbb{C}[x]$ é irredutível se, e somente se, $f(x) = ax + b$, com $a, b \in \mathbb{C}$ e $a \neq 0$.
7. Mostre que:
   (a) Todo polinômio irredutível sobre $\mathbb{Z}$ é irredutível sobre $\mathbb{Q}$.
   (b) A recíproca é falsa.
8. Seja $f(x) \in \mathbb{Z}[x]$ mônico. Se $f(x)$ é irredudível sobre $\mathbb{Q}$, mostre que $f(x)$ é irredutível sobre $\mathbb{Z}$.
9. Determine:
   (a) Todos os polinômios irredutíveis de grau 2 sobre $\mathbb{Z}_2$.
   (b) Todos os polinômios irredutíveis de grau 3 sobre $\mathbb{Z}_2$.
   (c) Todos os polinômios irredutíveis de grau 2 sobre $\mathbb{Z}_3$.

(d) Todos os polinômios irredutíveis de grau 3 sobre $\mathbb{Z}_3$.

(e) Dois polinômios de grau 4 e irredutívels sobre $\mathbb{Z}_2$.

10. Mostre que:

(a) $p(x) \in \mathbb{Z}_2[x]$ é irredutível se, e somente se, $\frac{\mathbb{Z}_2[x]}{<p(x)>}$ é um corpo.

(b) $p(x) = x^2 + x + 1$ é irredutível sobre $\mathbb{Z}_2$ e determine os elementos do corpo $\frac{\mathbb{Z}_2[x]}{<p(x)>}$.

11. Mostre que:

(a) $p(x) = x^3 + x + 1$ é irredutível sobre $\mathbb{Z}_2$ e determine os elementos do corpo $\frac{\mathbb{Z}_2[x]}{<p(x)>}$.

(b) $p(x) = x^3 + x^2 + 1$ é irredutível sobre $\mathbb{Z}_2$ e determine os elementos do corpo $\frac{\mathbb{Z}_2[x]}{<p(x)>}$.

12. Mostre que:

(a) $p(x) \in \mathbb{Z}_3[x]$ é irredutível se, e somente se, $\frac{\mathbb{Z}_3[x]}{<p(x)>}$ é um corpo.

(b) $p(x) = x^2 + 1$ é irredutível sobre $\mathbb{Z}_3$ e determine os elementos do corpo $\frac{\mathbb{Z}_3[x]}{<p(x)>}$.

13. Sejam $\mathbb{K}$ e $\mathbb{K}'$ corpos. Sejam $\phi : \mathbb{K} \to \mathbb{K}'$ um monomorfismo e a aplicação $\phi' : \mathbb{K}[x] \to \mathbb{K}'[x]$ definida por $\phi'(f(x)) = \phi(a_0)+\phi(a_1)x+\cdots+\phi(a_n)x^n$, onde $f(x) = a_0+a_1x+\cdots+a_nx^n \in \mathbb{K}[x]$. Mostre que:

(a) ϕ é um isomorfismo se, e somente se, ϕ' é um isomorfismo.

(b) $f(x) \mid g(x)$, onde $f(x), g(x) \in \mathbb{K}[x]$ se, e somente se, $\phi'(f(x)) \mid \phi'(g(x))$.

(c) $p(x) \in \mathbb{K}[x]$ é irredutível se, e somente se, $\phi'(p(x)) \in \mathbb{K}'[x]$ é irredutível.

Capítulo

15

Polinômios irredutíveis

Neste capítulo, o objetivo é trabalhar com polinômios irredutíveis sobre o anel $\mathbb{Z}$ e sobre seu corpo de frações $\mathbb{Q}$. Um ponto importante é saber dizer, através do exame de seus coeficientes, se um polinômio é redutível ou irredutível. Não existe um critério geral de irredutibilidade, mas existem várias regras que são bastante úteis. Os anéis considerados serão sempre comutivo com unidade.

15.1 Critérios de irredutibilidade

Nesta seção, apresentamos alguns critérios para decidir quando um polinômio é irredutível sobre $\mathbb{Z}$ ou sobre $\mathbb{Q}$. Na maioria dos casos é muito difícil determinar se um polinômio é irredutível ou não. Assim, nesta seção, vamos estabelecer alguns critérios de irredutibilidade, onde requer apenas a analise dos coeficientes do polinômio garantindo a irredutibilidade. Vale ressaltar que não existe um critério geral para a irredutibilidade. Neste sentido, apresentamos dois critérios de irredutibilidade: critério de Eisenstein e a redução módulo p, com p um número primo. Porém, ambas as técnicas se aplicam no anel $\mathbb{Z}$, contudo pelo Lema de Gauss é suficiente garantir a irredutibilidade sobre o anel $\mathbb{Z}$ assegura a irredutibilidade sobre o seu corpo de frações $\mathbb{Q}$.

Definição 15.1.1. *Sejam A um domínio de integridade e $p \in A$, com $p \neq 0$.*

1. *O elemento p é chamado um elemento primo se p não é inversível, e se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

2. *O elemento p é chamado um elemento irredutível se p não é inversível, e se $p = ab$, então a ou b são inversíveis.*

3. *O elemento p é chamado redutível (ou composto) se p não é inversível e p não é irredutível.*

Definição 15.1.2. *Um polinômio não nulo e não inversível $p(x) \in \mathbb{Z}[x]$ se diz irredutível sobre $\mathbb{Z}$ se a decomposição $p(x) = f(x)g(x)$, onde $f(x), g(x) \in \mathbb{Z}[x]$, somente for possível quando $f(x)$ ou $g(x)$ for inversível. Caso contrário, $p(x)$ é chamado redutível.*

Exemplo 15.1.1. *Em $\mathbb{Z}[x]$ o polinômio $f(x) = 4 + 8x^2$ é redutível e o polinômio $f(x) = x^2 + 1$ é irredutível.*

Definição 15.1.3. *Seja $f(x) = a_o + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$.*

1. *O conteúdo de $f(x)$ é o máximo divisor comum de seus coeficientes e denotado por $c(f)$.*
2. *O polinômio $f(x)$ é chamado primitivo se $c(f) = mdc(a_0, a_1, \cdots, a_n)$ é uma unidade, ou seja, ± 1.*

Exemplo 15.1.2. *Se $f(x) = 3x^2+6x+3 \in \mathbb{Z}[x]$, então $c(f) = 3$ e não é um polinômio primitivo.*

Proposição 15.1.1. *Se $f(x) \in \mathbb{Z}[x]$ é não nulo, então existem $d \in \mathbb{Z}$ e $f_1(x) \in \mathbb{Z}[x]$ primitivo e de mesmo grau tal que $f(x) = df_1(x)$.*

Demonstração. Se $d = mdc(a_0, a_1, \cdots, a_n)$, então $d \mid a_i$, para todo $i = 0, 1, \cdots, n$. Assim, $a_i = db_i$, onde $b_i \in A$ para todo $i = 0, 1, \cdots, n$. Portanto, $f(x) = d(b_0 + b_1x + \cdots + b_nx^n) = df_1(x)$, onde $f_1(x) = b_0 + b_1x + \cdots + b_nx^n$. Como $mdc(b_0, b_1, \ldots, b_n) = 1$, segue que $f_1(x)$ é primitivo. □

Proposição 15.1.2. *Se $f(x) \in \mathbb{Z}[x]$ é irredutível, então $f(x)$ é primitivo.*

Demonstração. Suponhamos que $f(x)$ não é primitivo e $d = mdc(a_0, a_1, \cdots, a_n)$. Pela Proposição 15.1.1, segue que $f(x) = df_1(x)$, onde $f_1(x)$ é primitivo. Além disso, d é não nulo e não inversível. Portanto, $f(x) = df_1(x)$ é uma fatoração não trivial, contradizendo o fato de $f(x)$ ser irredutível. □

Exemplo 15.1.3. *A recíproca da Proposição 15.1.2 é falsa, uma vez que $f(x) = 2x^2 + 5x + 2 = (2x + 1)(x + 2) \in \mathbb{Z}[x]$ e $f(x) = x^2 + 2x + 1 = (x + 1)^2 \in \mathbb{Z}[x]$. Agora, se $gr(f) = 1$ e primitivo, então $f(x)$ é irredutível.*

Proposição 15.1.3. *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio primitivo tal que $gr(f) = 2$ ou $gr(f) = 3$. Assim, $f(x)$ é redutível sobre $\mathbb{Z}$ se, e soemnte se, $f(x)$ tem uma raiz em $\mathbb{Q}$.*

Demonstração. Suponha que $f(x)$ é primitivo. Assim, $f(x)$ é redutível se, e somente se, $f(x) = g(x)h(x)$, onde $(g(x), h(x) \in \mathbb{Z}[x]$ com $gr(g) > 1$ e $gr(h) > 1$. Como $gr(gh) = gr(g) + gr(h)$, segue que $gr(g) = 1$ ou $gr(h) = 1$. □

Proposição 15.1.4. *Se $f(x), g(x) \in \mathbb{Z}[x]$ são polinômios primitivos e $af(x) = bg(x)$, com $a, b \in \mathbb{Z}$, então a é associado a b e $f(x)$ é associado a $g(x)$.*

Demonstração. Sejam $af(x) = h(x) = h_0 + h_1x + \cdots + h_nx^n$ e $d = mdc(h_0, h_1, \cdots, h_n)$. Pela Proposição 15.1.1, segue que $h(x) = dh_1(x)$ com $h_1(x) \in \mathbb{Z}[x]$ e de mesmo grau que $h(x)$. Como $af(x) = h(x)$, segue que a divide todos os coeficientes de $h(x)$, e portanto, $a \mid d$. Logo, $d = ac$ para algum $c \in \mathbb{Z}$. Assim, $h(x) = dh_1(x) = ach_1(x) = af(x)$, e pela lei do cancelamento, segue que $f(x) = ch_1(x)$. Logo, $c \mid f(x)$, e portanto, divide seus coeficientes. Como $f(x)$ é primitivo, segue que $c = \pm 1$. Portanto, a é associado a d. De modo análogo, b é associado a d. Portanto, a é associado a b. Agora, como $af(x) = bg(x)$, segue que $af(x) = aug(x)$, onde $u = \pm 1A$. Pela lei do cancelamento, segue que $f(x) = ug(x)$, ou seja, $f(x)$ é associado a $g(x)$. □

Proposição 15.1.5. *(Lema de Gauss) Se $f(x) \in \mathbb{Z}[x]$ é irredutível sobre $\mathbb{Z}$, então $f(x)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração. Se $f(x)$ é redutível sobre $\mathbb{Q}$, então $f(x) = g(x)h(x)$, com $g(x), h(x) \in \mathbb{Q}[x]$ e $1 \leq gr(g), gr(h) < gr(f)$. Como os coeficientes de $g(x)$ e $h(x)$ são frações de elementos de $\mathbb{Z}$, segue que $af(x) = g_1(x)h_1(x)$, onde a é um denominador comum de $g(x)h(x)$, $g_1(x)$ e $h_1(x)$ tem o mesmo grau que $g(x)$ e $h(x)$, respectivamente. Sejam $b = mdc(coef\ de\ f)$, $c = mdc(coef\ de\ g_1)$ e $d = mdc(coef\ de\ h_1)$. Assim, $f(x) = bf_1(x)$, $g_1(x) = cg_2(x)$ e $h_1(x) = dh_2(x)$, onde $f_1(x), g_2(x), h_2(x) \in \mathbb{Z}[x]$ são primitivos e tem o mesmo grau de $f(x)$, $g_1(x)$ e $h_1(x)$, respectivamente. Assim, $af(x) = abf_1(x) = g_1(x)h_1(x) = cdg_2(x)h_2(x)$. Como $f_1(x)$, $g_2(x)$ e $h_2(x)$ são primitivos, pela Proposição 15.1.4, segue que ab é associado a cd e $f_1(x)$ é associado a $g_2(x)h_2(x)$, ou seja, $f_1(x) = ug_2(x)h_2(x)$, onde $u = \pm 1$. Assim, $f(x) = bf_1(x) = bug_2(x)h_2(x)$, o que é um absurdo. □

A recíproca da Proposição 15.1.5 é falsa, uma vez que $f(x) = 2x + 2$ é redutível sobre $\mathbb{Z}$ e irredutível sobre $\mathbb{Q}$.

Teorema 15.1.1. *(Lema de Gauss) Se um polinômio primitivo $f(x) \in \mathbb{Z}[x]$ fatora como o produto de dois polinômios sobre $\mathbb{Q}$, então $f(x)$ fatora como o produto de dois polinômios sobre $\mathbb{Z}$.*

Demonstração. Se $f(x) = g(x)h(x)$, com $g(x), h(x) \in \mathbb{Q}[x]$, então $f(x) = \frac{a}{b}g_1(x)h_1(x)$, onde $g_1(x), h_1(x) \in \mathbb{Z}[x]$ são primitivos e b é o produto dos denominadores. Assim, $bf(x) = ag_1(x)h_1(x)$. Pela Proposição 15.1.4, segue que $f(x) = ug_1(x)h_1(x)$, onde $u = \pm 1$. □

Corolário 15.1.1. *Se $f(x) \in A[x]$ é mônico e fatora como o produto de dois polinômios sobre $\mathbb{Q}$, então $f(x)$ fatora como o produto de dois polinômios sobre $\mathbb{Z}$.*

Demonstração. Segue diretamente do Lema de Gauss 15.1.1. □

Lema 15.1.1. *Se $f(x) \in \mathbb{Z}[x]$ é irredutível, então $f(x)$ é primo.*

Demonstração. Suponhamos que $f(x) \mid g(x)h(x)$, onde $g(x), h(x) \in \mathbb{Z}[x]$. Se $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$, então $f(x) \mid g(x)h(x)$ em $\mathbb{Q}[x]$. Também, $f(x)$ é irredutível em $\mathbb{Q}[x]$. Como $\mathbb{Q}[x]$ é um anel principal, segue que $f(x)$ é primo em $\mathbb{Q}[x]$. Logo, $f(x) \mid g(x)$ ou $f(x) \mid h(x)$ em $\mathbb{Q}[x]$. Se $f(x) \mid g(x)$, então $g(x) = f(x)m_1(x)$, onde $m_1(x) \in \mathbb{Q}[x]$. Se c é o produto dos denominadores de $m_1(x)$, então $cm_1(x) = m_2(x)$ ou $m_1(x) = \frac{1}{c}m_2(x)$, onde $m_2(x) \in \mathbb{Z}[x]$ e

tem o mesmo grau de $m_1(x)$. Além disso, $g(x) = ag_1(x)$ e $m_2(x) = dm_3(x)$, onde $a, d \in \mathbb{Z}$ e $g_1(x), m_3(x) \in \mathbb{Z}[x]$ são primitivos e tem o mesmo grau que $g(x)$ e $m_2(x)$, respectivamente. Logo, $g(x) = ag_1(x) = f(x)m_1(x) = \frac{1}{c}m_2(x)f(x) = \frac{1}{c}dm_3(x)f(x)$. Assim, $acg_1(x) = dm_3(x)f(x)$. Pela Proposição 15.1.4, segue que ac é associado a d e $g_1(x)$ é associado a $m_3(x)f(x)$. Deste modo, $g_1(x) = um_3(x)f(x)$, onde $u = \pm 1$. Assim, $g(x) = ag_1(x) = aum_3(x)f(x)$. Portanto, $f(x)$ divide $g(x)$ em $\mathbb{Z}[x]$. □

Teorema 15.1.2. *Se $f(x) \in \mathbb{Z}[x]$, então $f(x)$ se fatora de modo único como o produto de polinômios irredutíveis sobre $\mathbb{Z}$.*

Demonstração. Seja $f(x) \in \mathbb{Z}[x]$ tal que $f(x) \neq 0$ e $f(x) \neq \pm 1$. A prova será por indução sobre o grau de $f(x)$. Se $gr(f) = 0$, então $f(x) \in \mathbb{Z}$, e o resultado segue. Agora, suponhamos que $gr(f) = n$ e que o resultado seja válido para todo polinômio em $\mathbb{Z}[x]$ de grau menor que o grau de $f(x)$. Pela Proposição 15.1.1, segue que $f(x) = df_1(x)$, onde $d = mdc(coef\ f)$ e $f_1(x) \in \mathbb{Z}[x]$ é primitivo e mesmo grau que $f(x)$. Se $f_1(x)$ for irredutível, então é suficiente decompor d. Neste caso, se $d = \pm 1$, então o resultado segue. Agora, se $f_1(x)$ for redutível, então $f_1(x) = g(x)h(x)$, onde $g(x), h(x) \in \mathbb{Z}[x]$, com $1 \leq gr(g), gr(h) < gr(f)$. Por hipótese de indução o resultado segue. Para a unicidade, segue que $f(x) = df_1(x)$ é escrito de modo único com $f_1(x)$ primitivo e $d = mdc(coef\ f)$. Agora, se $f_1(x) = p_1(x)p_2(x)\cdots p_r(x) = q_1(x)q_2(x)\cdots q_s(x)$, onde $p_i(x)q_j(x) \in \mathbb{Z}[x]$, para $i = 1, 2, \cdots, r$ e $j = 1, 2, \cdots, s$, são irredutíveis. Suponhamos, ainda, que $r < s$. Pelo Lema 15.1.1, segue que os $p_i(x)$ e $q_j(x)$ são primos. Assim, $p_1(x) \mid q_1(x)$ (digamos), e deste modo, $q_1(x) = p_1(x)h_1(x)$, onde $h_1(x) \in \mathbb{Z}[x]$. Assim, $p_2(x)\cdots p_r(x) = h_1(x)q_2(x)\cdots q_s(x)$. Continuando desse modo, segue que $1 = h_1(x)\cdots h_r(x)q_{r+1}(x)\cdots q_s(x)$, o que não ocorre. Portanto, $r = s$ e os $p_i(x)$ e $q_j(x)$ são associados. □

Exemplo 15.1.4. *O anel $\mathbb{Z}[x]$ não é principal, pois se fosse $I = \langle 2, x\rangle = \langle f(x)\rangle$, onde $f(x) \in \mathbb{Z}[x]$. Assim, $2 = f(x)f_1(x)$ e $x = f(x)f_2(x)$, onde $f_1(x), f_2(x) \in \mathbb{Z}[x]$. Logo, $f(x) \mid 2$ e $f(x) \mid x$. Desse modo, $0 = gr(f) + gr(f_1)$, ou seja, $gr(f) = gr(f_1)$. Assim, $f(x) = \pm 1, \pm 2$. Como $2 \nmid x$, segue que $f(x) = \pm 1$. Logo, $\langle f(x)\rangle = \mathbb{Z}[x]$. Portanto, se $g(x) \in \mathbb{Z}[x]$, então $g(x) = 2(a_0 + a_1x + \cdots + a_mx^m) + x(b_0 + b_1x + \cdots + b_nx^n) = 2a_0 + (2a_1 + b_1)x + \cdots$, onde o o coeficiente constante é par, o que não ocorre.*

15.1.1 Critério de Eisenstein

Nesta seção, apresentamos alguns resultados que auxiliam na determinação de polinômios irredutíveis sobre o anel dos inteiros $\mathbb{Z}$ e sobre seu corpo de frações $\mathbb{Q}$.

Proposição 15.1.6. *(Critério de Eisenstein) Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. Se existe um primo $p \in A$ tal que $p \mid a_i$, para todo $i = 0, 1, \cdots, n-1$, $p \nmid a_n$ e $p^2 \nmid a_0$, então $f(x)$ é irredutível sobre A.*

Demonstração. Se $f(x)$ não é irredutível, então $f(x) = (b_0+b_1x+\cdots+b_rx^r)(c_0+c_1x+\cdots+c_sx^s)$, com $r, s \geq 1$. Como $p \mid a_0 = b_0c_0$ e $p^2 \nmid a_0$, segue que $p \mid b_0$ ou $p \mid c_0$ (exclusivo). Suponhamos que $p \mid b_0$. Como $p \nmid a_n = b_rc_s$, segue que $p \nmid b_r$. Seja t, com $0 < t \leq r < n$, o menor índice tal

que $p \nmid b_t$. Assim, p divide $b_0, b_1, \cdots, b_{t-1}$. Mas $a_t = b_0c_t + b_1c_{t-1} + \cdots + b_{t-1}c_1 + b_tc_0$. Logo, $p \mid b_tc_0$. Como $p \nmid b_t$, segue que $p \mid c_0$, o que é um absurdo. □

Lema 15.1.2. *A aplicação*

$$\begin{array}{rccc} \varphi: & \mathbb{Z}[x] & \longrightarrow & \mathbb{Z}[x] \\ & f(x) & \longmapsto & f(x+c), \end{array}$$

onde $c \in \mathbb{Z}$, é um isomorfismo.

Demonstração. Se $f(x) \in \mathbb{Z}[x]$, então $gr(f) = gr(\varphi(f))$. Se $f(x), g(x) \in \mathbb{Z}[x]$, então

1. $\varphi(f(x) + g(x)) = \varphi((f+g)(x)) = (f+g)(x+c) = f(x+c) + g(x+c) =$
   $= \varphi(f(x)) + \varphi(g(x))$.
2. $\varphi(f(x)g(x)) = \varphi((fg)(x)) = (fg)(x+c) = f(x+c)g(x+c) = \varphi(f(x))\varphi(g(x))$.

Portanto, φ é homomorfismo de anéis. Para a injetividade, se $\varphi(f_1(x)) = \varphi(f_2(x))$, então

$$a_0 + a_1(x-c) + a_2(x-c)^2 + \cdots + a_n(x-c)^n = b_0 + b_1(x-c) + b_2(x-c)^2 + \cdots + b_n(x-c)^n,$$

que possui o mesmo grau, pois supomos imagens iguais. Agora, fazendo a mudança de variável $y = x - c$, segue que a igualdade

$$a_0 + a_1(y) + a_2(y)^2 + \cdots + a_n(y)^n = b_0 + b_1(y) + b_2(y)^2 + \cdots + b_n(y)^n$$

na varável y. Pela igualdade de polinômios, segue que $a_i = b_i$, para todo $i = 0, 1, \ldots, n$, o que implica que $f_1(x) = f_2(x)$, e portanto, φ é injetora. Agora, como o domínio de φ é igual ao contradomínio, segue que φ é sobrejetora, e portanto, φ é um isomorfismo. □

Teorema 15.1.3. *Seja $f(x) \in \mathbb{Z}[x]$ e $c \in \mathbb{Z}$, com $c \neq 0$. Assim, $f(x)$ é irredutível sobre $\mathbb{Z}[x]$ se, e somente se, $f(x+c)$ é irredutível sobre $\mathbb{Z}[x]$.*

Demonstração. Sejam $f(x)$ irredutível sobre $\mathbb{Z}$ e φ o isomorfismo do Lema 15.1.2. Se $\varphi(f(x)) = f(x+c)$ for redutível, então existem $h(x+c),\ m(x+c) \in \mathbb{Z}[x]$ tal que $f(x+c) = g(x+c)m(x+c)$, e assim, $\varphi(f(x)) = \varphi(g(x))\varphi(m(x)) = \varphi(g(x)m(x))$. Como φ é um injetora, segue que

$$f(x) = f(x) = g(x)m(x),$$

contradizendo o fato de $f(x)$ ser irredutível. Finalmente, se $f(x+c)$ for irredutível e supondo que $f(x)$ redutível sobre $\mathbb{Z}[x]$, então

$$f(x) = p(x)q(x), \quad \text{com } p(x), q(x) \in \mathbb{Z}[x],$$

$p(x)$ $q(x)$ não são unidades. Assim, $\varphi(f(x)) = \varphi(p(x)q(x)) = \varphi(p(x))\varphi(q(x))$, ou seja, $f(x+c) = p(x+c)q(x+c)$, o que é uma contradição, uma vez que $f(x+c)$ é irredutível. □

Exemplo 15.1.5. *Seja o polinômio $f(x) = x^4 + 4x + 1 \in \mathbb{Q}[x]$. Note que não podemos utilizar o critério de Eisenstein, porém se utilizarmos o Teorema 15.1.3 com $c = 1$, segue que*

$$f(x+1) = (x+1)^4 + 4(x+1) + 1 = f(x+1) = x^4 + 4x^3 + 6x^2 + 8x + 6.$$

Agora, tomando o número primo $p = 2$, segue que $f(x+1)$ é irredutível sobre $\mathbb{Q}$ pelo critério de Eisenstein. Assim, $f(x)$ é irredutível sobre $\mathbb{Q}$.

Exemplo 15.1.6. *O polinômio $f(x) = x^{p-1} + x^{p-2} + x^{p-3} + \cdots + x + 1$ é irredutível sobre $\mathbb{Z}[x]$, uma vez que se $f(x) = g(x)h(x)$, onde $g(x), h(x) \in \mathbb{Z}[x]$ e $1 \leq gr(g), gr(h) < gr(f)$, então $f(x+1) = g(x+1)h(x+1)$, onde $g(x+1)$ e $h(x+1)$ são polinômios em $\mathbb{Z}[x]$. Mas,*

$$\begin{aligned} f(x+1) &= (x+1)^{p-1} + (x+1)^{p-2} + (x+1)^{p-3} + \cdots + (x+1) + 1 \\ &= \tfrac{(x+1)^p - 1}{(x+1) - 1} = \tfrac{(x+1)^p - 1}{x} \\ &= \frac{\binom{p}{0} x^p + \binom{p}{1} x^{p-1} + \cdots + \binom{p}{p-1} x + \binom{p}{p} - 1}{x} \\ &= \binom{p}{0} x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{p-2} x + p. \end{aligned}$$

Como $p \mid \binom{p}{i}$, para todo $i = 0, 1, \cdots, p-1$, pelo Critério de Eiseinstein, segue que $f(x+1)$ é irredutível. Portanto, $f(x)$ é irredutível em $\mathbb{Z}[x]$.

Observação 15.1.1. *Segue pelo critério de Eisenstein que $\sqrt[n]{p}$, onde p é primo e $n > 1$, é irracional.*

Exemplo 15.1.7. *Os polinômios $p(x) = x^{60} + 14x + 7$, $p(x) = x^4 + 2x + 2$ e $p(x) = x^4 + x^3 + x^2 + x + 1$ sobre $\mathbb{Z}[x]$ são irredutíveis.*

Teorema 15.1.4. *Seja $f(x) \in \mathbb{Z}[x]$. Se $\alpha = \frac{p}{q}$ é uma raiz de $f(x)$ com $mdc(p, q) = 1$ e $f(\alpha) = 0$, então $p \mid a_0$ e $q \mid a_n$.*

Demonstração. Por hipótese, segue que

$$a_0 + a_1 \frac{p}{q} + \cdots + a_n \frac{p^n}{q^n} = 0. \tag{15.1}$$

Multiplicando por q^n a Equação (15.1), segue que

$$a_0 q^n + a_1 p q^{n-1} + \cdots + a_n p^n = 0. \tag{15.2}$$

Organizando de maneira conveniente a Equação (15.2), segue que

$$a_0 q^n = p(-a_1 q^{n-1} - a_2 p q^{n-2} - \cdots - a_n p^{n-1}).$$

Desta forma, $p \mid a_0 q^n$, mas como $mdc(p,q) = 1$, segue pelo teorema de Euclides que $p \mid a_0$. Ainda, como $q \mid a_0 q^n$, segue que $q \mid p(-a_1 q^{n-1} - a_2 pq^{n-2} - \ldots - a_n p^{n-1})$. Pelo mesmo argumento, segue que $q \mid -a_1 q^{n-1} - a_2 pq^{n-2} - \cdots - a_{n-1} p^{n-2} q - a_n p^{n-1}$. Note que $q \mid a_i q^{i-1}$, onde $i = 1, 2, \cdots, n$. Logo, $q \mid a_n p^{n-1}$, e pelo mesmo argumento, segue que $q \mid a_n$. □

Observação 15.1.2. *O Teorema 15.1.4 é bem útil para saber se um polinômio com coeficientes em $\mathbb{Q}$ possui raízes em $\mathbb{Q}$, e em particular, se o grau desse polinômio for 2 ou 3, e for redutível, então necessariamente possui uma raiz racional, ou seja, nestas condições se o polinômio não possuir raízes racionais, então é irredutível sobre $\mathbb{Q}$.*

Exemplo 15.1.8. *O polinômio $f(x) = x^3 + 3x^2 + 6x + 2$ é irredutível, uma vez que as possíveis raízes racionais são ± 1 ou ± 2. Substituindo esses valores em $f(x)$, segue que*

$$\begin{array}{cc} f(-1) = -2 & f(-2) = -6 \\ f(1) = 12 & f(2) = 34 \end{array} .$$

Como o grau de $f(x)$ é 3 e $f(x)$ não possui raízes racionais, segue que $f(x)$ é irredutível sobre $\mathbb{Q}$.

15.1.2 Redução módulo um primo

Nesta subseção, apresentamos um critério de irredutibilidade que é a redução módulo p, onde p é um primo. Para isso, vamos utilizar a aplicação

$$\varphi_n : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_n[x],$$

definido por $\varphi_n(f(x)) = \overline{f}(x) = \overline{a_0} + \overline{a_1} x + \overline{a_2} x^2 + \cdots + \overline{a_n} x^n$, onde $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in \mathbb{Z}[x]$, ou seja, é a redução dos coeficientes de um polinômio $f(x) \in \mathbb{Z}[x]$ módulo n. A aplicação φ_n é um homomorfismo, uma vez que se $f(x), g(x) \in \mathbb{Z}[x]$, então

1. $\varphi_n((f+g)(x)) = \overline{(f+g)}(x) = \overline{f(x) + g(x)} = \overline{f}(x) + \overline{g}(x) = \varphi_n(f(x)) + \varphi_n(g(x))$.
2. $\varphi_n((fg)(x)) = \overline{(fg)}(x) = \overline{f(x)g(x)} = \overline{f}(x)\overline{g}(x) = \varphi_n(f(x))\varphi_n(g(x))$.

Portanto, φ_n é um homomorfismo de anéis. Por exemplo, se $f(x) = 3x^4 + 6x^2 + 8x + 9 \in \mathbb{Z}[x]$, então fazendo a redução dos coeficientes deste polinômio módulo 4, segue que

$$\overline{f}(x) = \overline{3} x^4 + \overline{2} x^2 + \overline{1}.$$

Desse modo, faremos uso desse homomorfismo com p um número primo, pois neste caso $\mathbb{Z}_p$ é um corpo e podemos usar a teoria de corpos.

Teorema 15.1.5. *Sejam $f(x) \in \mathbb{Z}[x]$ um polinômio não constante e p um número primo tal que p não divide o coeficiente líder de $f(x)$. Seja o homomorfismo*

$$\varphi_p : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$$

definido por $\varphi_p(f(x)) = \overline{f}(x) = \overline{a_0} + \overline{a_1}x + \overline{a_2}x^2 + \cdots + \overline{a_n}x^n$, *onde* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x]$. *Se* $\varphi_p(f(x))$ *for irredutível sobre* $\mathbb{Z}_p$, *então* $f(x)$ *é irredutível sobre* $\mathbb{Q}$.

Demonstração. Se $f(x)$ redutível sobre $\mathbb{Z}$, então a $f(x) = g(x)h(x)$, onde $f(x), g(x) \in \mathbb{Z}[x]$ não são unidades e os graus de $g(x)$ e $h(x)$ são menores que o de $f(x)$. Aplicando o homomorfismo φ_p, segue que

$$\varphi_p(f(x)) = \varphi_p(g(x))\varphi_p(h(x)).$$

Por hipótese, $p \nmid a_n$, onde a_n é o coeficiente líder de $f(x)$. Como p é primo e $a_n = b_rc_s$, onde b_r é o coeficiente líder de $g(x)$ e c_s o de $h(x)$, segue que $p \nmid b_r$ e $p \nmid c_s$, e portanto, $\overline{b_r} \neq \overline{0}$ e $\overline{c_s} \neq \overline{0}$ módulo p. Assim, o grau de $g(x)$ e $\overline{g}(x)$ é o mesmo e o grau de $h(x)$ e $\overline{h}(x)$ é o mesmo. Portanto, $\varphi_p(f(x))$ é redutível sobre $\mathbb{Z}_p$, o que é uma contradição. □

Exemplo 15.1.9. *Sejam* $f(x) = x^4 + 15x^3 + 7 \in \mathbb{Z}[x]$ *e* $p = 5$. *Assim,* $\varphi_5(f(x)) = x^4 + \overline{2}$, *que pode ser fatorado em dois polinômios sobre* $\mathbb{Z}_p$ *de graus* 1 *e* 3 *ou dois polinômios de grau* 2. *Mas, se* $\overline{f}(x)$ *tem um fator de grau* 1, *então* $\overline{f}(x)$ *tem raiz em* $\mathbb{Z}_5$, *o que não ocorre, uma vez que*

$$\begin{cases} \overline{f}(\overline{0}) = \overline{2} & \overline{f}(\overline{1}) = \overline{3} & \overline{f}(\overline{2}) = \overline{2} \\ \overline{f}(\overline{3}) = \overline{3} & \overline{f}(\overline{4}) = \overline{3}. & \end{cases}$$

Agora, considerando a decomposição em dois polinômios de grau 2, *ou seja,*

$$x^4 + \overline{2} = (x^2 + ax + c)(x^2 + x + d),$$

onde $a, b, c, d \in \mathbb{Z}_5$. *Logo,*

$$x^4 + \overline{2} = x^4 + x^3(c + a) + x^2(d + ac + b) + x(ad + bc) + bd,$$

e assim,

$$\begin{cases} c + a = \overline{0} \\ d + ac + b = \overline{0} \\ ad + bc = \overline{0} \\ bd = \overline{2} \end{cases}$$

Pela primeira equação, segue que $c = -a$, *e substituindo na segunda e na terceira equações, segue que*

$$b + d = a^2 \text{ e } a(d - b) = \overline{0}.$$

Como $\mathbb{Z}_5$ *é um corpo, segue que* $a = \overline{0}$ *ou* $d = b$. *Desse modo,*

1. *se* $a = \overline{0}$, *então* $b = -d$, *e substituindo na ultima equação, segue que* $-d^2 = \overline{2}$, *onde*

testando todos os valores de $\mathbb{Z}_5$ nessa equação, segue que

$$\begin{cases} Se\ d=0 & \longrightarrow \quad \overline{0}^2=\overline{0}\neq\overline{2} \\ Se\ d=1 & \longrightarrow \quad \overline{1}^2=\overline{1}\neq\overline{2} \\ Se\ d=2 & \longrightarrow \quad \overline{2}^2=\overline{4}\neq\overline{2} \\ Se\ d=3 & \longrightarrow \quad \overline{3}^2=\overline{4}\neq\overline{2} \\ Se\ d=4 & \longrightarrow \quad \overline{4}^2=\overline{1}\neq\overline{2}. \end{cases}$$

Logo, este caso não ocorre. Para o caso em que $b=d$ a solução é análoga, ou seja, $d^2=\overline{2}$ o que também não ocorre testando os valores. Logo, $\varphi_5(f(x))$ é irredutível sobre $\mathbb{Z}_5$, e portanto, $f(x)$ é irredutível sobre $\mathbb{Z}$, e consequentemente, sobre $\mathbb{Q}$.

Exemplo 15.1.10. *Considere o polinômio*

$$f(x)=\frac{2}{9}x^5+\frac{5}{3}x^4+x^3+\frac{1}{3}$$

sobre $\mathbb{Q}$. Pelo critério de Eisenstein, segue que $f(x)$ é irredutível, pois considerando o polinômio

$$9f(x)=2x^5+15x^4+9x^3+3$$

e tomando o primo $p=3$ podemos aplicar o critério e concluir que $9f(x)\in\mathbb{Z}[x]$ é irredutível e pelo lema de Gauss, segue que $f(x)$ é irredutível sobre $\mathbb{Q}$.

Exemplo 15.1.11. *Em $\mathbb{Z}[x]$ o polinômio $f(x)=4+8x^2$ é redutível e o polinômio $f(x)=x^2+1$ é irredutível.*

Proposição 15.1.7. *Seja $f(x)\in\mathbb{Z}[x]$ um polinômio primitivo tal que $gr(f)=2$ ou $gr(f)=3$. Assim, $f(x)$ é redutível sobre $\mathbb{Z}$ se, e somente se, $f(x)$ tem uma raiz em $\mathbb{Q}$.*

Demonstração. Suponha que $f(x)$ é primitivo. Assim, $f(x)$ é redutível se, e somente se, $f(x)=g(x)h(x)$, onde $g(x),h(x)\in\mathbb{Z}[x]$ com $gr(g)>1$ e $gr(h)>1$. Como $gr(gh)=gr(g)+gr(h)$, segue que $gr(g)=1$ ou $gr(h)=1$. □

15.1.3 Exercícios

1. Mostre que:

   (a) $p(x)=10x^{11}+6x^3+6$ é irredutível em $\mathbb{Q}[x]$ mas não em $\mathbb{Z}[x]$.

   (b) $p(x)=x^5+2x^3+(1+i)$ é irredutível em $\mathbb{Z}[i][x]$.

   (c) $p(x)=2x+2x^2$ é redutível sobre $\mathbb{Z}$ e irredutível sobre $\mathbb{Q}$.

2. Se $f(x)\in\mathbb{Z}[x]$ é irredutível sobre $\mathbb{Z}$, mostre que $f(x)$ é irredutível sobre $\mathbb{Q}$.

3. Mostre que os seguintes polinômios são irredutíveis sobre $\mathbb{Q}$.

(a) $p(x) = x^{201} - 6x^{107} + 21$ e $p(x) = 3(x^2 + x + 1)^2 - 2(x - 1)(x^3 - x - 1)$.

(b) $p(x) = x^3 - 6x^2 + 9x + 3$, $r(x) = x^4 - 3$ e $p(x) = x^4 - 2x^3 + 9$.

4. Sejam $f(x), g(x) \in \mathbb{Q}[x]$.

   (a) Mostre que $c(fg) = c(f)c(g)$.

   (b) Se $f(x), g(x)$ são primitivos, mostre que $f(x)$ e $g(x)$ são associados em $\mathbb{Z}[x]$ se, e somente se, são associados em $\mathbb{Q}[x]$.

   (c) Se $f(x) \in \mathbb{Q}[x]$ tem algum coeficiente igual a 1, mostre que existe $d \in \mathbb{Z}$ tal que $df(x) \in \mathbb{Z}[x]$ é primitivo.

5. Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Mostre que $f(x)$ é irredutível em $A[x]$ se, e somente se, $f(x)$ é irredutível em $\mathbb{K}[x]$ e primitivo em $A[x]$.

6. Sejam $f(x), g(x) \in \mathbb{Q}[x]$ ambos com algum coeficiente igual a 1. Se $f(x)g(x) \in \mathbb{Z}[x]$, mostre que $f(x), g(x) \in \mathbb{Z}[x]$.

7. Se $gr(f) \geq 1$, mostre que $f(x)$ não é o produto de dois fatores de grau ≥ 1 em $\mathbb{Z}[x]$ se, e somente se, $f(x)$ não é o produto de dois fatores de grau ≥ 1 em $\mathbb{Q}[x]$.

8. Sejam A um domínio fatorial, $\mathbb{K}$ seu corpo de frações e $f(x), g(x) \in A[x]$.

   (a) Mostre que $c(fg) = c(f)c(g)$.

   (b) Se $f(x), g(x) \in A[x]$ são primitivos, mostre que $f(x)$ e $g(x)$ são associados em $A[x]$ se, e somente se, são associados em $\mathbb{K}[x]$.

   (c) Se $f(x) \in \mathbb{K}[x]$ tem algum coeficiente igual a 1, mostre que existe $d \in A$ tal que $df(x) \in A[x]$ é primitivo.

   (d) Sejam $f(x), g(x) \in \mathbb{K}[x]$ ambos com algum coeficiente igual a 1. Se $f(x)g(x) \in A[x]$, mostre que $f(x), g(x) \in A[x]$.

9. Se $gr(f) \geq 1$, mostre que $f(x)$ não é o produto de dois fatores de grau ≥ 1 em $A[x]$ se, e somente se, $f(x)$ não é o produto de dois fatores de grau ≥ 1 em $\mathbb{K}[x]$.

10. Mostre que um polinômio sobre um corpo algebricamente fechado é irredutível se, e somente se, tem grau 1.

11. Mostre que:

    (a) $p(x) \in \mathbb{Q}[x]$ é irredutível sobre $\mathbb{Q}$ se, e somente se, $< p(x) >$ é um ideal maximal.

    (b) $p(x) \in \mathbb{Q}[x]$ é irredutível se, e somente se, o anel quociente $\frac{\mathbb{Q}[x]}{<p(x)>}$ é um corpo.

    (c) Se $f(x) \in \mathbb{Q}[x]$ tem grau 2 ou 3, então $p(x)$ é irredutível ou tem pelo menos uma raiz em $\mathbb{Q}$.

12. Mostre que um polinômio $p(x) \in \mathbb{R}[x]$ é irredutível sobre $\mathbb{R}$ se, e somente e, $gr(p(x)) = 1$ ou $gr(p(x)) = 2$ e seu discriminante é negativo.

13. Se $\mathbb{K}$ é um corpo algébricamente fechado e $f(x) \in \mathbb{K}[x]$ é um polinômio de grau $n \geq 1$ com coeficiente dominante a, mostre que existem $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{K}$ tal que $f(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$.

14. Se $\mathbb{K} \subseteq \mathbb{L}$ são corpos e $f(x), g(x) \in \mathbb{K}[x]$, mostre que $mdc_{\mathbb{K}[x]}(f(x), g(x)) = mdc_{\mathbb{L}[x]}(f(x), g(x))$.

15. Seja a aplicação $\varphi : \mathbb{Q}[x] \to \mathbb{R}$ definida por $\varphi(f(x)) = f(\sqrt{5})$, onde $f(x) \in \mathbb{Q}[x]$. Mostre que φ é um homomorfismo de anéis e determine o $\ker(\varphi)$.

16. Determine os elementos inversíveis de $A[x]$, onde A é um anel comutativo com unidade.

17. Mostre que:

    (a) Todo polinômio de grau 2 sobre um corpo é irredutível ou decompõe sobre o corpo.

    (b) Todo polinômio de grau 3 sobre um corpo $\mathbb{K}$ é irredutível ou possui uma raiz sobre o corpo $\mathbb{K}$.

    (c) Todo polinômio de grau impar sobre $\mathbb{R}$ possui uma raiz em $\mathbb{R}$.

18. Mostre que:

    (a) O polinômio $f(x) = x^4 + 2$ é irredutível sobre $\mathbb{Q}$.

    (b) O polinômio $f(x) = x^3 - x - 1$ é irredutível sobre $\mathbb{Q}$.

19. Mostre que $\mathbb{Z}[x]$ não é um anel principal.

20. Se $\mathbb{K}$ é um corpo e p é um número primo, mostre que $x^p - a \in \mathbb{K}[x]$ é irredutível ou tem uma raiz em $\mathbb{K}$.

21. Sejam $\mathbb{K}$ um corpo e $f(x) \in \mathbb{K}[x]$ um polinômio de grau maior ou igual a 1. Se $g(x) \in \mathbb{K}[x]$ é um polinômio de grau maior ou igual a 1, mostre que $g^2(x) \mid f(x)$ se, e somente se, $g(x) \mid f(x)$ e $g(x) \mid f'(x)$.

22. Mostre que:

    (a) A é um domínio se, e somente se, $\langle x \rangle$ é um ideal primo de $A[x]$.

    (b) $f(x) = x^4 + x^3 + x + 1$ não é irredutível sobre $\mathbb{Z}[x]$.

23. Sejam A um domínio e $f(x) \in A[x]$ um polinômio. Mostre que:

    (a) $f(x)$ é irredutível se, e somente se, $\frac{A[x]}{\langle f(x) \rangle}$ é um corpo.

    (b) $f(x)$ é irredutível se, e somente se, $\langle f(x) \rangle$ é um ideal maximal.

24. Mostre que:

    (a) $\frac{\mathbb{Z}_{11}[x]}{\langle x^2+1 \rangle}$ é um corpo.

    (b) $\frac{\mathbb{R}[x]}{\langle x^2+1 \rangle}$ é um corpo isomorfo a $\mathbb{C}$.

(c) Existe um polinômio irredutível sobre $\mathbb{Q}[x]$ e redutível sobre $\mathbb{Z}[x]$.

25. Sejam A um domínio, $\mathbb{K}$ seu corpo de frações e $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$, com $a_n \neq 0$. Se $r/s \in \mathbb{K}$, com $mdc(r, s) = 1$, é uma raiz de $f(x)$, mostre que $r|a_0$ e $s|a_n$.

26. Sejam A um domínio fatorial e $\mathbb{K}$ seu corpo de frações. Seja $f(x) \in A[x]$ um polinômio primitivo tal que $gr(f) = 2$ ou $gr(f) = 3$. Mostre que $f(x)$ é redutível sobre A se, e soemnte se, $f(x)$ tem uma raiz em $\mathbb{K}$.

27. Sejam A um domínio fatorial e $\mathbb{K}$ seu corpo de frações. Seja $f(x) = a_0+a_1x+\cdots+a_nx^n \in A[x]$. Se existe um primo $p \in A$ tal que $p \mid a_i$, para todo $i = 0, 1, \cdots, n-1$, $p \nmid a_n$ e $p^2 \nmid a_0$, mostre que $f(x)$ é irredutível sobre A.

Referências Bibliográficas

[1] A. Azevedo e R. Piccinini. *Introdução à Teoria dos Grupos*. IMPA - CNPq, Rio de Janeiro, 1969.

[2] A. Garcia e Y. Lequain. *Álgebra: Uma Introdução*. IMPA - CNPq, Rio de Janeiro, 1983.

[3] A. Garcia e Y. Lequain *Álgebra: um curso de introdução*. Projeto Euclides, IMPA - CNPq, Rio de Janeiro, 1988.

[4] A. Gonçalves. *Introdução à Álgebra*. IMPA - CNPq, Rio de Janeiro, 1979.

[5] A. Hefez. *Curso de Álgebra*. Coleção Matemática Universitária, Impa, Rio de Janeiro, 2010.

[6] A. Simis. *Introdução à Algebra*. IMPA - CNPq, Rio de Janerio, 1977.

[7] H. H. Domingues e G. Iezzi. *Álgebra Moderna*. Atual Editora, São Paulo, 2003.

[8] I. N. Herstein. *Topics in Algebra*. John Wiley and Sons, New York, 1975.

[9] J. B. Fraleigh. *A First Course in Abstract Algebra*. Addison-Wesley Publishing Company, New York, 1989.

[10] L. H. J. Monteiro. *Elementos de Álgebra*. IMPA - CNPq, Rio de Janeiro, 1969.

Índice Remissivo