UEMS – UNIVERSIDADE ESTADUAL DO MATO GROSSO DO SUL
Campus: Nova Andradina

Apostila- Estruturas Algébricas

Professor: Oyran Silva Rayzaro

Nova Andradina-2018

Conteúdo

1 Números Inteiros **5**

1.1 Indução 8
1.2 Múltiplos e Divisores 8
1.3 Algoritmo da Divisão 8
1.4 Máximo Divisor Comum 9
1.5 Números Primos 10
1.6 Congruências 10
1.7 Critério de Divisibilidade 11
1.8 Exercícios 12

2 Relações,Aplicações e Operações **14**

2.1 Relações Binárias 14
2.1.1 Domínio e Imagem 14
2.1.2 Representações 15
2.1.3 Inversa de um Relação 16
2.1.4 Representação de R^{-1} 16
2.1.5 Relação sobre um Conjunto 17
2.1.6 Relações de Equivalência 18
2.1.7 Partição de um conjunto 19
2.1.8 Relações de Ordem 20
2.1.9 Limites Superiores e Inferiores, Máximo e Mínimo 21
2.1.10 Exercícios 22
2.2 Aplicações 24
2.2.1 Exercícios 28

3 Operações-Leis de Composição Internas **31**

3.0.2 Propriedades das Operações 32
3.0.3 Parte Fechada Para Uma Operação 40
3.1 Tábua de Uma Operação 40

3.2 Operações em $\mathbb{Z}_m$ . . . 43
3.3 Exercícios . . . 45

4 Grupos **48**
4.1 Subgrupos . . . 50
4.2 Homomorfismo e Isomorfismo . . . 51
4.2.1 Proposições sobre Homomorfismos de Grupos . . . 51
4.2.2 Isomorfismo de Grupos . . . 52
4.3 Grupos Cíclicos . . . 53
4.3.1 Potências e Múltiplos . . . 53
4.4 Classes Laterais . . . 56
4.5 Teorema de Lagrange . . . 57
4.6 Subgrupos Normais . . . 58
4.7 Teorema Do Homomorfismo . . . 59
4.8 Exercícios . . . 60

5 Anéis **66**
5.1 Anéis e Propriedades . . . 66
5.2 Subanéis . . . 69
5.3 Tipos de Anéis . . . 70
5.4 Anéis de Integridade e Corpos . . . 71
5.5 Homomorfismo-Isomorfismo de Anéis . . . 73
5.5.1 Homomorfismos . . . 73
5.5.2 Proposições sobre Homomorfismo de Anéis . . . 74
5.5.3 Núcleo de um Homomorfismo de Anéis . . . 74
5.5.4 Isomorfismo de Anéis . . . 75
5.6 Exercícios . . . 76

6 Anéis de Polinômios **79**
6.1 Sequências Quase-Nulas ou Polinômios . . . 81
6.2 Grau de um Polinômio . . . 82
6.3 Imersão de A em $A[X]$ . . . 84
6.4 Polinômios Inversíveis . . . 84
6.5 Divisão em $A[X]$ . . . 85
6.6 Algoritmo da Divisão (ou de Euclides) . . . 86
6.7 Raízes de Polinômios . . . 87
6.8 Algoritmo de Briot-Ruffini . . . 88
6.9 Máximo Divisor Comum . . . 88

6.10 Polinômios Irredutíveis 89
6.11 Raízes Múltiplas 90
6.12 Relações entre coeficientes e raízes 92
6.13 Exercícios 93

Referências Bibliográficas **96**

Capítulo 1

Números Inteiros

Denotamos por $\mathbb{Z}$ o conjunto dos números inteiros, ou seja, $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$. O conjunto $\mathbb{Z}$ é munido de duas operações:

- **Adição**

  $\forall a, b, \in \mathbb{Z},\ a + b \in \mathbb{Z}$;

- **Multiplicação**

  $\forall a, b, \in \mathbb{Z},\ a \cdot b \in \mathbb{Z}$

  ou

  $ab \in \mathbb{Z}$.

Propriedades:
1-Adição

(a) *Associativa*:

$$a + (b + c) = (a + b) + c, \quad \forall a, b, c \in \mathbb{Z}.$$

(b) *Comutativa*:

$$a + b = b + a, \quad \forall a, b \in \mathbb{Z}.$$

(c) *Elemento Neutro da Adição*:

$$a + 0 = 0 + a = a \quad \forall a \in \mathbb{Z}.$$

(d) *Elemento Simétrico*:

$$a + (-a) = (-a) + a = 0, \forall a \in \mathbb{Z}.$$

2-Multiplicação

(a) *Associativa*:

$$a(bc) = (ab)c, \ \ \forall a, b, c \in \mathbb{Z};$$

(b) *Comutativa*:

$$ab = ba, \ \ \forall a, b \in \mathbb{Z};$$

(c) *Elemento Neutro da Multiplicação*:

$$a \cdot 1 = 1 \cdot a = a \ \ \forall a \in \mathbb{Z};$$

(d) *Lei do Anulamento do Produto*:

$$ab = 0 \Rightarrow a = 0 \ ou \ b = 0;$$

(e):

$$ab = 1 \Rightarrow a = \pm 1 \ e \ b = \pm 1;$$

(f): *A Multiplicação é Distributiva em Relação à Adição*:

$$a(b + c) = ab + ac, \ \ \forall a, b, c \in \mathbb{Z}.$$

A relação "menor ou igual" em $\mathbb{Z}$ é denotada pelo símbolo $\leq$, e valem as seguintes propriedades:

(a) *Reflexiva*:

$$a \leq a, \ \ \forall a \in \mathbb{Z};$$

(b) *Transitiva*:

$$a \leq b \ \ e \ \ b \leq c \Rightarrow a \leq c;$$

(c) *Anti-Simétrica*:

$$a \leq b \ \ e \ \ b \leq a \Rightarrow a = c.$$

(d) *Totalidade*:

Dados $a, b \in \mathbb{Z}$ então ou $a \leq b$ ou $b \leq a$.

(e) *Compatibilidade com Adição*:

$$a \leq b \Rightarrow a + c \leq b + c, \ \ \forall c \in \mathbb{Z}.$$

(f) *Compatibilidade com a Multiplicação*:

$$0 \leq a \, e \, 0 \leq b \Rightarrow 0 \leq ab.$$

Observação 1.0.1. *O conjunto formado pelos inteiros positivos será denotado por* $\mathbb{Z}_+ = \{0, 1, 2, 3, ...\}$. *Agora, os elementos de* $\mathbb{Z}_+^* = \{1, 2, 3, ...\}$ *são os inteiros estritamente positivos.*

(g) *Regra de Sinais*:

Com o símbolo " $<$ " valem as seguintes implicações:

- $0 < a$ e $0 < b \Rightarrow 0 < ab$
- $0 < a$ e $b < 0 \Rightarrow ab < 0$
- $a < 0$ e $b < 0 \Rightarrow 0 < ab$

(h) *Princípio do menor número inteiro*:

Seja L um subconjunto não vazio de $\mathbb{Z}$. Dizemos que L é limitado inferiormente, se existe um elemento $a \in \mathbb{Z}$, tal que $a \leq x, \ \forall x \in L$.

Exemplo 1.0.1. *O conjunto* $L = \{-2, 0, 2, 4, ...\}$ *é limitado inferiormente, e os limites inferiores de* L *são* $-2, -3, -4, ...$

Dizemos que um conjunto L limitado inferiormente possui um mínimo, se existe $l \in L$ tal que $l \leq x, \ \forall x \in L$. O mínimo do Exemplo 1.0.1 é -2.

1.1 Indução

"*Princípio da Indução*"

"Dado $k \in \mathbb{Z}$, suponhamos que a cada inteiro $n \geq k$ esteja associado uma afirmação $P(n)$. Então $P(n)$ será verdadeira para todo $n \geq k$ desde que seja possível provar o seguinte:

(i) $P(k)$ é verdadeira;

(ii) Se $P(r)$ é verdadeira para $r \geq k$, então $P(r+1)$ também é verdadeira".

Exemplo 1.1.1. *Provar que* $1 + n \leq 2^n$, $\forall n \geq 0$.

Exemplo 1.1.2. *Provar que* $1 + 2 + 3 + ... + n = \dfrac{n(n+1)}{2}$ $\forall n \geq 1$.

1.2 Múltiplos e Divisores

Seja a um número inteiro. Os múltiplos de a são os números:

$$0, \pm a, \pm 2a, \pm 3a, ...,$$

ou seja, os números ka, onde k é um elemento qualquer de $\mathbb{Z}$.

Note que, se ka e ha são múltiplos de a com $k, h \in \mathbb{Z}$, então sua soma e seu produto também são múltiplos de a. De fato:

Quando se tem $c = ab$, com $a, b, c \in \mathbb{Z}$, dizemos que a é um divisor de c ou que a divide c ou que c é divisível por a. Notação $a|c$.

Propriedades:

(a) $a|a$, $\forall a \in \mathbb{Z}$;

(b) Se $a|b$ e $b|a$, com $a, b \in \mathbb{Z}_+$, então $a = b$;

(c) Se $a|b$ e $b|c$, então $a|c$;

(d) Se $a|b$ e $a|c$, então $a|bx + cy$, $\forall x, y \in \mathbb{Z}$;

(e) Se $a|b$ e $c|d$, então $ac|bd$.

1.3 Algoritmo da Divisão

Seja $b \in \mathbb{Z}_+$. Dado $a \in \mathbb{Z}$, então ou a é múltiplo de b ou está situado entre dois múltiplos consecutivos qb e $(q+1)b$ de b, ou seja $qb < a < q + 1)b$.

Logo somando $-(qb)$ na desigualdade anterior, obtemos $0 < a - qb < b$. Tomando $r = a - qb$, logo $a = bq + r$, onde $0 < r < b$. Portanto, temos o seguinte algoritmo :

"Dados $a, b \in \mathbb{Z}$, com $b \in \mathbb{Z}_+$. Existem $q, r \in \mathbb{Z}$ de maneira única, tal que $a = bq + r$, com $0 \leq r < b$."

Os elementos q e r acima, chamam-se respectivamente, quociente e resto da divisão de a por b.

Exemplo 1.3.1. *Determine o resto e o quociente da divisão de a por b, onde:*

(a) $a = 60$, $b = 7$;

(b) $a = -60$, $b = 7$.

1.4 Máximo Divisor Comum

Definição 1.4.1. *Dados $a, b \in \mathbb{Z}$, dizemos que $d \in \mathbb{Z}$ é o máximo divisor comum entre a e b, se:*

(i) $d \geq 0$;

(ii) $d|a$ *e* $d|b$;

(iii) *Se* d_1 *é um inteiro tal que* $d_1|a$ *e* $d_1|b$ *então* $d_1|d$.

Observação 1.4.1. .

1. *Se* $a = b = 0$, *então* $d = 0$;
2. *Se* $a = 0$ *e* $b \neq 0$, *então* $d = |b|$;
3. *Se* d *e* d_1 *são máximos divisores comuns ente* a *e* b, *então* $d = d_1$. *Pois como* $d|d_1$ *e* $d_1|d$, *e ambos são positivos, concluímos que* $d = d_1$.

Proposição 1.4.1. *Quaisquer que sejam $a, b \in \mathbb{Z}$, existe $d \in \mathbb{Z}$ que é o máximo divisor comum de a e b.*

(Notação:) Indicaremos por $mdc(a, b)$ o máximo divisor comum entre a e b.

Observação 1.4.2. *Se $d = mdc(a, b)$, então existem inteiros x_0 e y_0 tais que $d = ax_0 + by_0$. Os elementos x_0 e y_0 que satisfazem tal identidade não são únicos. E essa identidade recebe o nome de* Identidade de Bezout *em $\mathbb{Z}$ para os elementos a e b.*

Exemplo 1.4.1. *Determinar o máximo divisor comum entre* 41 *e* 12 *e encontrar os elementos x_0 e y_0 que satisfazem a Identidade de Bezout para os números* 41 *e* 12.

1.5 Números Primos

Definição 1.5.1. *Um número $p \in \mathbb{Z}$ é chamado número primo, se:*

1. $p \neq 0$;
2. $p \neq \pm 1$;
3. *e os únicos divisores de p são: ± 1 e $\pm p$.*

Observação 1.5.1. .

1. *Os divisores $\pm a, \pm 1$ de $a \in \mathbb{Z}$ são chamados divisores triviais de a;*
2. *Dizer que a não é primo, quando $a \neq 0$ e $a \neq \pm 1$, significa que existem outros divisores de a além dos triviais;*
3. *Um número $a \in \mathbb{Z}$ tal que $a \neq 0$ e $a \neq \pm 1$ e não é primo, será chamado de número inteiro composto.*

Proposição 1.5.1. *Se p é primo e $p|ab$, então $p|a$ ou $p|b$.*

Prova 1.

Como consequência da Proposição 1.5.1 por indução, se $p|a_1a_2...a_n$, então p divide um dos a_i.

Teorema 1.5.1. *(**Teorema Fundamental da Aritmética**)*
Dado um número inteiro $a > 1$, existem r inteiros primos estritamente positivos $p_1, ..., p_r$ de maneira que $a = p_1p_2...p_r (r \geq 1)$.

Proposição 1.5.2. *Sejam a, b inteiros e primos entre si. Se $a|c$ e $b|c$, então $ab|c$.*

1.6 Congruências

Exemplo 1.6.1. *Se hoje é "...", que dia da semana será daqui* 1520 *dias ?*

Definição 1.6.1. *Seja $m > 1$ um número inteiro. Dados $a, b \in \mathbb{Z}$, dizemos que a* é côngruo a b módulo m *se, e somente se, $m|(a - b)$.*

Notação: $a \equiv b(mod m)$.

Exemplo 1.6.2. *Verifique se a é côngruo a b módulo m nos seguintes casos:*

(a) $a = 21$,$b = 1$,$m = 5$;

(b)$a = 100$,$b = 1$,$m = 9$.

Propriedades de Congruências

(a)$a \equiv a(\text{mod m})$, $\forall a \in \mathbb{Z}$;

(b) Se $a \equiv b(\text{mod m})$, então $b \equiv a(\text{mod m})$;

(c) Se $a \equiv b(\text{mod m})$ e $b \equiv c(\text{mod m})$, então $a \equiv c(\text{mod m})$;

(d) Se $a \equiv b(\text{mod m})$ e $c \equiv d(\text{mod m})$, então $a + c \equiv b + d(\text{mod m})$;

(e) Se $a \equiv b(\text{mod m})$, então $ac \equiv bc(\text{mod m})$, $\forall c \in \mathbb{Z}$;

(f) Se $a \equiv b(\text{mod m})$, então $a^r \equiv b^r(\text{mod m})$, $\forall r \geq 1$;

Exemplo 1.6.3. *Mostrar que* $10^{200} - 1$ *é divisível por* 11.

(g) Se $a \equiv b(\text{mod m})$ e $0 \leq b < m$ então b é o resto da divisão euclidiana de a por m;

Exemplo 1.6.4. *Seja a um inteiro ímpar qualquer. Mostre que o resto da divisão de* a^2 *por* 8 *é* 1.

(h) $a \equiv b(\text{mod m}) \Leftrightarrow a$ e b dão o mesmo resto da divisão por m

1.7 Critério de Divisibilidade

Seja N um número natural, então usando a base 10, podemos representar N da seguinte forma:

$$N = a_0 + a_1 10 + a_2 10^2 + ... + a_n 10^n, \ \ com \ \ 0 \leq a_0, a_1, a_2, ..., a_n \leq 9.$$

Isso da origem a seguinte notação sequencial para indicar o número $N = a_n a_{n-1} ... a_2 a_1 a_0$.

Agora, veremos alguns critérios de divisibilidade, provado através de congruências.

Critério de Divisibilidade por 2:

Critério de Divisibilidade por 3:

Critério de Divisibilidade por 4:

Critério de Divisibilidade por 5:

Critério de Divisibilidade por 6:

1.8 Exercícios

1- Demonstre usando o princípio da indução finita:

(a) $1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$, $n \geq 1$

(b) $1 + 3 + 5 + 7 + ... + (2n - 1) = n^2$, $n \geq 1$

(c) $1^2 + 2^2 + 3^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$, $n \geq 1$

(d) $1^3 + 2^3 + 3^3 + ... + n^3 = (1 + 2 + ... + n)^2$, $n \geq 1$

(e) $1.2 + 2.3 + 3.4 + ... + n.(n+1) = \frac{n(n+1)(n+2)}{3}$, $n \geq 1$

2- Sejam m e n ímpares. Prove que:

(a) $4 \mid (2m - 2n)$

(b) $8 \mid (m^2 - n^2)$

3- Encontre o máximo divisor comum dos pares de números que seguem e, para cada caso, de uma identidade Bezout.

(a) 20 e 74

(b) 68 e 120

(c) 42 e -96

4- O máximo divisor comum de dois números é 48 e o maior deles é 384. Encontre o outro número.

5- Decomponha em fatores primos 234,456 e 780.

6- Ache o máximo divisor comum dos seguintes pares de números através da decomposição desses números em fatores primos.

(a) 234 e 456

(b) 456 e 780

(c) 200 e 480

7- Ache o resto das seguintes divisões:

(a) 2^{45} por 7

(b) 11^{100} por 100

8- Mostre que o número $2^{20} - 1$ é divisível por 41.

9- Sejam $a, b \in \mathbb{Z}$ de modo que o $mdc(a, b) = 1$. Se $a \mid c$ e $b \mid c$, mostre que $ab \mid c$.

10- Use o resultado do exercício anterior para provar que $6 \mid n(2n + 7)(7n + 1)$, $\forall n \in \mathbb{Z}$.

11- Justifique os critérios de divisibilidade por $2, 3, 4, 5, 6$

12- Qual é o menor inteiro positivo que têm 15 divisores ?

Sugestão: Se $a = p_1^{x_1} p_2^{x_2} ... p_m^{x_m}$ é a decomposição do número procurado em fatores primos, então $15 = (x_1+1)(x_2+1)...(x_m+1)$. Observe que só há duas possibilidades(salvo quanto á ordem) de decompor 15 em fatores inteiros positivos.

Capítulo 2

Relações,Aplicações e Operações

2.1 Relações Binárias

Definição 2.1.1. *Dados dois conjuntos E e F, não vazios, chama-se produto cartesiano de E por F o conjunto formado por todos pares ordenados (x, y) com $x \in E$ e $y \in F$, ou seja:*

$$E \times F = \{(x, y) | x \in E \text{ e } y \in F\}.$$

Definição 2.1.2. *Chama-se relação binária de E em F todo subconjunto R de $E \times F$. (R é relação binária de E em $F \Leftrightarrow R \subset E \times F$).*

Observação 2.1.1. .

1. *Para indicar que $(a, b) \in R$ usaremos algumas vezes a notação aRb, que lê-se "a relaciona com b segundo R". Se $(a, b) \notin R$, escreveremos $a \not R b$;*
2. *Os conjuntos E e F são chamados respectivamente de conjunto de partida e conjunto de chegada da relação R.*

Exemplo 2.1.1. *Em cada caso, determine o produto cartesiano de $E \times F$, e encontre uma relação binária de E em F :*

(a) $E = \{0, 1, 2\}$ *e* $F = \{-2, -1, 0, 1, 2\}$*;*

(b) $E = \mathbb{Z}$ *e* $F = \mathbb{Z}$*;*

2.1.1 Domínio e Imagem

Considere R uma relação de E em F.

Definição 2.1.3. *Chama-se* **domínio** *de R o subconjunto de E constituído pelos elementos x para cada um dos quais existe algum y em F tal que xRy.*

Notação: $D(R) = \{x \in E | \exists y \in F; xRy\}$.

Definição 2.1.4. *Chama-se* **imagem** *de R o subconjunto de F constituído pelos elementos y para cada um dos quais existe algum $x \in E$, tal que xRy.*

Notação: $Im(R) = \{y \in E | \exists x \in E; xRy\}$.

Observação 2.1.2. *Assim, em uma relação R, $D(R)$ é o conjunto formado pelos primeiros termos, e $Im(R)$ é formado pelos segundos termos.*

Exemplo 2.1.2. *Determine o domínio e a imagem das relações do Exemplo 2.1.1.*

2.1.2 Representações

Podemos representar uma relação de duas formas:
1-Gráfico Cartesiano: O gráfico de uma relação é o conjunto dos pontos de um plano dotado de um sistema de coordenadas cartesianas ortogonais, cujas abscissas são os primeiros termos e as ordenadas os segundos termos.

Exemplo 2.1.3. *Represente as relações pelo gráfico cartesiano.*

(a) $R_1 = \{(0,0), (1,-1), (1,1)\}$*;*

(b) $R_2 = \{(0,1), (1,2), (2,-2), (0,-1), (1,0)\}$*;*

(c) $E = F = \mathbb{Z}$ $R_3 = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} | x = y\}$*;*

(d) $E = F = \mathbb{R}$ $R_4 = \{(x,y) \in \mathbb{R} \times \mathbb{R} | y \geq 0\}$.

2-Esquema de Flexas: Quando E e F são conjuntos finitos, podemos representar-los por meio de diagramas, e indicamos cada $(x,y) \in R$ por uma flexa com "origem x" e "extremidade y".

Exemplo 2.1.4. *Represente por meio de diagrama a relação $R = \{(0,0), (1,-1), (1,1)\}$ dos conjuntos $E = \{0,1,2\}$ e $F = \{-2,-1,0,1,2\}$*

2.1.3 Inversa de um Relação

Definição 2.1.5. *Seja R uma relação de E em F. Chama-se* relação inversa *de R, e indica-se por R^{-1}, a seguinte relação de F em E:*

$$R^{-1} = \{(y, x) \in F \times E | (x, y) \in R\}.$$

Exemplo 2.1.5. *Determine as relações inversa em cada caso:*

(a) *Se $E = \{a_1, a_2, a_3\}$, $F = \{b_1, b_2, b_3, b_4\}$ e $R = \{(a_1, b_1), (a_1, b_2), (a_2, b_3), (a_3, b_4)\}$, então $R^{-1} =?$;*

(b) *Se $E = F = \mathbb{R}$ e $R = \{(x, y) \in \mathbb{R}^2 | y = 2x\}$, então $R^{-1} =?$*

(c) *Se $E = F = \mathbb{R}$ e $R = \{(x, y) \in \mathbb{R}^2 | x^2 + (y-2)^2 \leq 1\}$, então $R^{-1} =?$*

2.1.4 Representação de R^{-1}

(a)-Cartesiano:

$$(x, y) \in R \Leftrightarrow (y, x) \in R^{-1}$$

Logo, se R admite o gráfico cartesiano, então R^{-1} também admite. E o gráfico de R^{-1} é simétrico do gráfico de R, em relação à reta da equação $y = x$.

Exemplo 2.1.6. *Faça o gráfico cartesiano da relação $R = \{(x, y) \in \mathbb{R}^2 | y = 2x\}$ e sua inversa $R^{-1} = \{(x, y) \in \mathbb{R}^2 | x = 2y\}$*

(b)-Diagrama: Dado o diagrama de R obtemos o diagrama de R^{-1} invertendo o sentido das flexas:

Exemplo 2.1.7. *Faça o diagrama da relação $R = \{(a_1, b_1), (a_1, b_2), (a_2, b_3), (a_3, b_4)\}$ e da relação inversa $R^{-1} = \{(b_1, a_1), (b_2, a_1), (b_2, a_2), (b_4, a_3)\}$, dos conjuntos $E = \{a_1, a_2, a_3\}$ e $F = \{b_1, b_2, b_3, b_4\}$*

Exercício 2.1.1. *Mostre que:*

1. $D(R^{-1}) = Im(R)$;
2. $Im(R^{-1}) = D(R)$;
3. $(R^{-1})^{-1} = R$

2.1.5 Relação sobre um Conjunto

Definição 2.1.6. *Quando $E = F$ e R é uma relação de E em F, diz-se que R é* uma relação sobre E, *ou ainda, R é* uma relação em E.

Propriedades:
(a)-Reflexiva

Definição 2.1.7. *Dizemos que R é* reflexiva, *quando $\forall x \in E$, xRx.*

Seja $\Delta_E = \{(x, x) | x \in E\}$, então R é reflexiva se $\Delta_E \subset R$.
Exemplos:

1. A relação $R = \{(a, a), (b, b), (c, c), (a, c), (b, a)\}$ sobre $E = \{a, b, c\}$ é reflexiva, pois aRa,bRb e cRc.

2. A relação R de igualdade sobre $\mathbb{Z}$, $xRy \Leftrightarrow x = y$ é reflexiva, pois $\forall x \in \mathbb{Z}$, $x = x$.

Contra-Exemplo:
A relação R sobre E não é reflexiva, se $\exists x \in E$; $x \not R x$. Por exemplo, $R = \{(a, a), (b, b), (a, b), (b, a), (a, c), (c, a), (b, c), (c, b)\}$ sobre $E = \{a, b, c\}$ não é reflexiva, pois $c \not R c$.

(b)-Simétrica

Definição 2.1.8. *Dizemos que R é* simétrica, *quando $\forall x, y \in E$, se xRy então yRx.*

Exemplos:

1. A relação $R = \{(a, a), (a, b), (b, a), (b, b)\}$ sobre $E = \{a, b, c\}$ é simétrica.

2. A relação R de perpendicularismo definida sobre o conjunto E das retas do espaço, ou seja, $\forall x, y \in E$, temos $xRy \Leftrightarrow x \perp y$. É simétrica, pois para duas retas x e y quaisquer de E, se $x \perp y$ então $y \perp x$.

Contra-Exemplo:
A relação R sobre E não é simétrica, se existirem $x, y \in E$; tais que xRy e $y \not R x$. Por exemplo, a relação $R = \{(a, a), (b, b), (a, b)\}$ sobre $E = \{a, b, c\}$ não é simétrica, pois aRb e $b \not R a$.

(c)-Transitiva

Definição 2.1.9. *Dizemos que R é* transitiva, *quando $\forall x, y, z \in E$, se xRy e yRz então xRz.*

Exemplos:

1. A relação $R = \{(a,a),(a,b),(b,c),(a,c)\}$ sobre $E = \{a,b,c\}$ é transitiva.

2. A relação R da semelhança definida sobre o conjunto E dos triângulos do espaço:$\forall x, y \in E$, $xRy \Leftrightarrow x \sim y$. É transitiva, pois dado $x, y, z \in E$, se $x \sim y$ e $y \sim z$ então $x \sim z$.

Contra-Exemplo:

A relação R sobre E não é transitiva, se existirem $x, y, z \in E$; tais que xRy, yRz e $x\not Rz$. Por exemplo, $R = \{(a,a),(a,b),(a,b),(b,c),(c,c)\}$ sobre $E = \{a,b,c\}$ não é transitiva, pois aRb,bRc mas $a\not Rc$.

2.1.6 Relações de Equivalência

Definição 2.1.10. *Uma relação R sobre um conjunto E não vazio é chamada* **relação de equivalência** *sobre E se R é* **reflexiva, simétrica e transitiva**.

Exemplos 2.1.1.

1. A relação $R = \{(a,a),(b,b),(c,c),(a,c),(c,a)\}$ é uma relação de equivalência.

2. A relação de congruência módulo m sobre $\mathbb{Z}$ é uma relação de equivalência.

3. A relação de paralelismo $xRy \Leftrightarrow x \parallel y$ é uma relação de equivalência, onde as retas pertencem ao mesmo espaço.

Definição 2.1.11. *Seja R uma relação de equivalência sobre E. Dado $a \in E$, chama-se* **classe de equivalência de** *a* **módulo** *R, o subconjunto $\overline{a}$ de E constituído pelos elementos $x \in E$, tais que x se relaciona com a (xRa). Em símbolos:*

$$\overline{a} = \{x \in E | xRa\}.$$

O conjuntos das classes de equivalência módulo R será indicado por E/R e será chamado **conjunto quociente de E por R.**

Exemplos 2.1.2.

1. Na relação de equivalência $R = \{(a,a),(b,b),(c,c),(a,c),(c,a)\}$ temos:
   $\overline{a} =$,
   $\overline{b} =$,
   $\overline{c} =$,
   $E/R =$.

2. A relação R de congruência módulo m com $m \in \mathbb{Z}$ e $m > 1$ sobre $\mathbb{Z}$ ou seja, $xRy \Leftrightarrow x \equiv y(mod\ m)$ é uma relação de equivalência. Determine seu conjunto quociente $\mathbb{Z}/R$.

Proposição 2.1.1. *Seja R uma relação de equivalência sobre E e considere $a, \in E$. Os itens seguintes são equivalentes:*

1. aRb;
2. $a \in \overline{b}$;
3. $b \in \overline{a}$;
4. $\overline{a} = \overline{b}$.

Demonstração. □

2.1.7 Partição de um conjunto

Definição 2.1.12. *Seja E um conjunto não vazio. Diz-se que uma classe $\mathfrak{F}$ de subconjuntos não-vazios de E é uma* **partição de** *E se:*

- *2 membros quaisquer de $\mathfrak{F}$ ou são iguais ou são disjuntos;*
- *a união dos membros de $\mathfrak{F}$ é igual a E.*

Exemplos 2.1.3.

1. A classe $\mathfrak{F} = \{\{1\}.\{2,3\},\{4\}\}$ é uma partição do conjunto $E = \{1,2,3,4\}$.
2. Sejam $P = \{x \in \mathbb{Z} | x\text{é par}\}$ e $I = \{x \in \mathbb{Z} | x\text{é ímpar}\}$. Então $\mathfrak{F} = \{P, I\}$ é uma partição de $\mathbb{Z}$.
3. Sejam $F_1 =]-\infty, -2[$, $F_2 = [-2, 2]$, $F_3 =]2, \infty[$, então $\mathfrak{F} = \{F_1, F_2, F_3\}$ é uma partição de $\mathbb{R}$.

Proposição 2.1.2. *Se R é uma relação de equivalência sobre um conjunto E, então E/R é uma partição de E.*

Demonstração. □

Proposição 2.1.3. *Se $\mathfrak{F}$ é uma partição do conjunto E, então existe uma relação R de equivalência sobre E tal que $E/R = \mathfrak{F}$.*

Exemplo 2.1.8. *Dada a partição* $\mathfrak{F} = \{\{a, b, c\}, \{d, e\}\}$ *de* $E = \{a, b, c, d, e\}$ *a ela podemos associar a relação de equivalência* $R = \{(a, a), (a, b), (b, a), (b, b), (b, c), (c, b), (c, c), (a, c), (c, a), (d, d), (d, e), (e, d), (e, e)\}$. *Note que* $E/R = \mathfrak{F} = \{\{a, b, c\}, \{d, e\}\}$.

2.1.8 Relações de Ordem

Definição 2.1.13. *Uma relação* R *sobre um conjunto* E *não vazio é chamada* **relação de ordem parcial** *sobre* E *se* R *é reflexiva, anti-simétrica e transitiva, isto é:*

- $\forall x \in E \Rightarrow xRx$;
- *Dado* $x, y \in E$, *se* xRy *e* $yRx \Rightarrow x = y$;
- *Dado* $x, y, z \in E$, *se* xRy *e* $yRz \Rightarrow xRz$.

Observação 2.1.3. *Quando* R *é uma relação de ordem parcial sobre* E, *para exprimirmos que* $(a, b) \in R$, *usaremos a notação* $a \preceq b(R)$, *que se lê: "a precede b na relação* R*". Para exprimirmos que* $(a, b) \in R$ *e* $a \neq b$, *usaremos a notação* $a \prec b(R)$, *que se lê: "a precede estritamente b na relação* R*".*

Definição 2.1.14. *Um conjunto* **parcialmente ordenado** *é um conjunto sobre o qual se definiu uma certa relação de ordem parcial.*

Definição 2.1.15. *Seja* R *uma relação de ordem parcial sobre* E. *Os elementos* $a, b \in E$ *se dizem* **comparáveis mediante** R *se* $a \preceq b$ *ou* $b \preceq a$.

Definição 2.1.16. *Se dois elementos quaisquer de* E *forem comparáveis mediante* R, *então* R *será chamada* **relação de ordem total sobre** E. *O conjunto* E, *neste caso é chamado de conjunto* **totalmente ordenado.**

Exemplos 2.1.4.

1. A relação R sobre $\mathbb{R}$ definida por $xRy \Leftrightarrow x \leq y (\leq$: menor ou igual que) é uma relação de ordem total, denominada ordem habitual.
2. A relação R sobre $\mathbb{N}$ definida por $xRy \Leftrightarrow x|y (x$ divide $y)$, é uma relação de ordem parcial.
3. A relação de inclusão sobre uma família $\mathfrak{F}$ de subconjuntos de um dado conjunto E é uma relação de ordem parcial.

2.1.9 Limites Superiores e Inferiores, Máximo e Mínimo

Seja E um conjunto parcialmente ordenado mediante a relação $\preceq$. Seja A um subconjunto de E, com $A \neq \emptyset$.

Definição 2.1.17. *Um elemento $L \in E$ é um* **limite superior de** *A se: $\forall x \in A \Rightarrow x \preceq L$, isto é, se qualquer elemento de A precede L.*

Definição 2.1.18. *Um elemento $l \in E$ é um* **limite inferior de** *A se: $\forall x \in A \Rightarrow l \preceq x$, isto é, l precede qualquer elemento de A.*

Definição 2.1.19. *Um elemento $M \in A$ é um* **máximo de** *A se: $\forall x \in A \Rightarrow x \preceq M$, isto é,$M$ é um limite superior de A e pertence a A.*

Definição 2.1.20. *Um elemento $m \in A$ é um* **mínimo de** *A se: $\forall x \in A \Rightarrow m \preceq x$, isto é, m é um limite inferior de A e pertence a A.*

Proposição 2.1.4. *Se A é um subconjunto do conjunto parcialmente ordenado E. Se existe um máximo(ou mínimo) de A, então ele é único.*

Demonstração. □

Definição 2.1.21. *Chama-se* **supremo de** *A o mínimo, caso exista, do conjunto dos limites superiores de A. Chama-se* **ínfimo de** *A o máximo, caso exista, do conjunto dos limites inferiores de A.*

Definição 2.1.22. *Um elemento $m_1 \in A$ é um* **elemento maximal de** *A quando o único elemento de A precedido por m_1 é ele próprio, isto é:*

$$\forall x \in A, \text{ se } m_1 \preceq x \Rightarrow m_1 = x.$$

Definição 2.1.23. *Um elemento $m_0 \in A$ é um* **elemento minimal de** *A quando o único elemento de A que precede m_0 é ele próprio, isto é:*

$$\forall x \in A, \text{ se } x \preceq m_0 \Rightarrow m_0 = x.$$

Exemplos 2.1.5.

1. Se $E = \mathbb{R}$, $A = \{x \in \mathbb{R} | 0 < x \leq 1\} =]0, 1]$ e a ordem é a habitual, temos:

   - São limites superiores de A os números:
   - São limites inferiores de A os números:
   - o máximo de A é:

- o mínimo de A é:
- o supremo de A é:
- o ínfimo de A é:
- os elementos maximais de A são:
- os elementos minimais de A são:

2. Se $E = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$, $A = \{2, 4, 6\}$ e a ordem é a divisibilidade, temos:

   - São limites superiores de A os números:
   - São limites inferiores de A os números:
   - o máximo de A é:
   - o mínimo de A é:
   - o supremo de A é:
   - o ínfimo de A é:
   - os elementos maximais de A são:
   - os elementos minimais de A são:

2.1.10 Exercícios

1. Sejam $E = \{1, 3, 5, 7, 9\}$ e $F = \{0, 2, 4, 6\}$:

   (a) Enumere os elementos das seguintes relações de E em F:
   $R_1 = \{(x, y)|y = x - 1\}$
   $R_2 = \{(x, y)|x < y\}$
   $R_3 = \{(x, y)|y = 3x\}$

   (b) Estabeleça o domínio e a imagem de cada uma das relações anteriores.

2. Sabe-se que E é um conjunto com 5 elementos e $R = \{(a, b), (b, c), (c, d), (d, e)\}$ é uma relação sobre E. Pode-se obter:

   (a) os elementos de E

   (b) domínio e imagem de R

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

(d) esquemas de flexas de R.

3. Seja R a relação em $E = \{1, 2, 3, 4, 5\}$ tal que : $xRy \Leftrightarrow (x - y)$ é múltiplo de 2. Quais são os elementos de R. Faça o diagrama de flexas para R. Que propriedades R apresenta?

4. Seja $E = \{1, 2, 3\}$. Considerando as seguintes relações em A:

   $R_1 = \{(1, 2), (1, 1), (2, 2), (2, 1), (3, 3)\}$

   $R_2 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 3)\}$

   $R_3 = \{(1, 1), (2, 2), (1, 2), (2, 3), (3, 1)\}$

   $R_4 = E \times E$

   $R_5 = \emptyset$

   Quais são reflexivas ? simétricas ? transitivas ? anti-simétricas ?

5. Seja $E = \{a, b, c\}$. Quais das relações abaixo são relações de equivalência sobre E:

   $R_1 = \{(a, a), (a, b), (b, a), (b, b), (c, c)\}$

   $R_2 = \{(a, a), (a, b), (b, a), (b, b), (b, c)\}$

   $R_3 = \{(a, a), (b, b), (b, c), (c, b), (c, a), (a, c)\}$

   $R_4 = E \times E$

   $R_5 = \emptyset$

6. Seja E o conjunto dos triângulos do espaço euclidiano. Seja R a relação em E definida por :

   $$xRy \Leftrightarrow x \text{ é semelhante a } y.$$

   Mostrar que R é uma relação de equivalência.

7. Seja E o conjunto das retas de um plano α. Quais das relações abaixo definidas são relações de equivalência em E.

(a) $xRy \Leftrightarrow x//y$

(b) $xRy \Leftrightarrow x \perp y$.

2.2 Aplicações

Definição 2.2.1. *Seja f uma relação de E em F. Dizemos que f é uma* aplicação *de E em F se:*

1. $D(f) = E$;
2. *Dado $a \in D(f)$, é único o elemento $b \in F$ de modo que $(a, b) \in f$.*

Se f é uma aplicação de E em F, escrevemos $b = f(a)$(lê-se "b é imagem de a pela f"), para indicar que $(a, b) \in f$.

Usaremos a notação $f : E \to F$ para indicar que f é uma aplicação de E em F. O conjunto F é chamado contradomínio de f.

Observação 2.2.1. .

1. *Sejam $f : E \to F$ e $g : E \to F$, então $f = g$ se $f(x) = g(x), \forall x \in E$.*
2. *Se o contradomínio de uma aplicação f é um conjunto numérico, é usual chamar-se f de função.*

X

Exemplo 2.2.1. *Sejam $E = \{a, b, c, d\}$ e $F = \{m, n, p, q\}$. Consideremos as relações de E em F seguintes:*

1. $R_1 = \{(a, n), (b, p), (c, q)\}$;
2. $R_2 = \{(a, m), (b, n), (c, q), (d, r)\}$;
3. $R_3 = \{(a, n), (b, n), (c, q), (d, r)\}$;
4. $R_4 = \{(a, m), (b, n), (b, p), (c, r), (d, q)\}$.

Verifique quais das seguintes relações são aplicações.

A partir de agora, vamos sempre considerar $f : E \to F$ uma aplicação.

Definição 2.2.2. *Dado $A \subset E$, chama-se* imagem direta *de A segundo f, e indica-se por $f(A)$, o seguinte subconjunto de F:*

$$f(A) = \{f(x) | x \in A\}.$$

Definição 2.2.3. *Dado $B \subset F$, chama-se* imagem inversa *de B, segundo f e indica-se por $f^{-1}(B)$, o seguinte subconjunto de E:*

$$f^{-1}(B) = \{x \in E | f(x) \in B\}.$$

Exemplo 2.2.2. *Se $E = \{1, 3, 5, 7, 9\}$, $F = \{0, 2, 4, 6, 8, 10, 12\}$ e $f : E \to F$ dada por $f(x) = x + 1$. então:*

- $f(\{3, 5, 7\}) =$
- $f(E) =$
- $f(\emptyset) =$
- $f^{-1}(\{2, 4, 10\}) =$
- $f^{-1}(\{0, 12\}) =$

Exemplo 2.2.3. *Se $E = F = \mathbb{R}$ e $f : \mathbb{R} \to R$ é dada pela lei $f(x) = x^2$, temos:*

- $f(\{1, 2, 3\}) =$
- $f([0, 2]) =$
- $f(]-1, 3[) =$
- $f^{-1}(\{0, 4, 16\}) =$
- $f^{-1}([1, 9]) =$
- $f^{-1}(\mathbb{R}_-^*) =$

Definição 2.2.4. *Dizemos que f é uma* aplicação injetora *quando:*

$$\forall x_1, x_2 \in E, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2);$$

isto é, quando elementos distintos de E tem imagens distintas em F.

Observação 2.2.2. .

1. *Equivalente a definição anterior, f é injetora se:*

$$\forall x_1, x_2 \in E, f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

2. *Uma aplicação não é injetora quando $\exists x_1, x_2 \in E$, com $x_1 \neq x_2$ e $f(x_1) = f(x_2)$.*

Definição 2.2.5. *Dizemos que f é uma* aplicação sobrejetora *quando $Im(f) = B$, isto é, quando:*

$$\forall y \in F, \exists x \in E | f(x) = y.$$

Observação 2.2.3. *Uma aplicação $f : E \to F$ não é sobrejetora se:*

$$\exists y \in F | \forall x \in E, f(x) \neq y.$$

Definição 2.2.6. *Dizemos que f é uma* aplicação bijetora *quando f é injetora e sobrejetora.*

Exemplo 2.2.4. *Verifique se as aplicações são bijetora:*

1. *Sejam $E = \{a, b, c, d\}$ e $F = \{0, 1, 2, 3, 4\}$, e considere a aplicação $f = \{(a, 1), (b, 2), (c, 3), (d, 4)\}$ de E em F.*

2. *Considere a aplicação $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = 3x - 1$.*

Considere $f : E \to F$ uma aplicação. Seja f^{-1} a relação inversa de F em E. Pode ocorrer que f^{-1} não seja uma aplicação de F em E.

Exemplo 2.2.5. *Sejam $E = \{a, b, c, d\}$,$F = \{0, 1, 2, 3, 4\}$ e $f = \{(a, 1), (b, 2), (c, 3), (d,)\}$. Logo a relação inversa de f, é $f^{-1} = \{(1, a), (2, b), (3, c), (4, d)\}$. Então f^{-1} não é relação de F em E, pois $D(f^{-1}) = \{1, 2, 3, 4\} \neq F$.*

Proposição 2.2.1. *Seja $f : E \to F$ uma aplicação. Então f^{-1} é uma aplicação de F em E se, e somente se, f^{-1} é bijetora.*

Exemplo 2.2.6. *Sabemos pelo exercício 2.2.4 que a aplicação $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = 3x - 1$ é bijetora. Determine a aplicaçãof^{-1}, inversa de f.*

Definição 2.2.7. *Sejam $f : E \to F$ e $f : F \to G$ duas aplicações. Chama-se* aplicação composta de f e g *a aplicação(indicada por $g \circ f$) de E em G, definida da seguinte maneira:*

$$(g \circ f)(x) = g(f(x)), \forall x \in E.$$

Exemplo 2.2.7.

1. Sejam $E = \{a_1, a_2, a_3, a_4\}$, $F = \{b_{1,2}, b_3, b_4, b_5\}$ e $G = \{c_1, c_2, c_3\}$. Consideremos as aplicações $f = \{(a_1, b_1), (a_2, b_2), (a_3, b_4), (a_4, b_3), \}$ de E em F e $g = \{(b_1, c_1), (b_2, c_1), (b_3, c_2), (b_4, c_2), (b_5, c_3)\}$ de F em G. Determine a aplicação composta $g \circ f$.

2. Sejam $f : \mathbb{R} \to \mathbb{R}_+$, tal que $f(x) = 2^x$ e $g : \mathbb{R}_+ \to \mathbb{R}$ tal que $g(x) = \sqrt{x}$.Determine a aplicação composta $g \circ f$.

3. Sejam $f : \mathbb{R} \to \mathbb{R}$, tal que $f(x) = 3x$ e $g : \mathbb{R} \to \mathbb{R}$ tal que $g(x) = x^2$.Determine a aplicação composta $g \circ f$.

Observação 2.2.4.

1. A composta de f e g só é definida quando o contra-domínio de f coincide com o domínio de g(conjunto F).

2. A composta de f e g tem o mesmo domínio de f(conjunto$E$) e o mesmo contra-domínio de g(conjunto G).

3. Quando $E = G$, iso é, $f : E \to F$ e $g : F \to E$, então é possível definir, além de $g \circ f$, a composta de g e f(indicada por $f \circ g$), como sendo a aplicação de F em F, que obedece a lei $(f \circ g)(x) - f(g(x)), \forall x \in F$. Em geral, temos $g \circ f \neq f \circ g$.

Proposição 2.2.2. *Se $f : E \to F$ e $g : F \to G$ são injetoras, então a composta $g \circ f$ é injetora.*

Demonstração. □

Proposição 2.2.3. *Se $f : E \to F$ e $g : F \to G$ são sobrejetora, então a composta $g \circ f$ é sobrejetora.*

Demonstração. □

Definição 2.2.8. *Dado $E = \emptyset$, a aplicação $i_E : E \to R$ definida pela lei $i_E(x) = x$, é chamada* **aplicação idêntica de E**.

Proposição 2.2.4. *Se $f : E \to F$ é bijetora, então: $f \circ f^{-1} = i_F$ e $f^{-1} \circ f = i_E$.*

Proposição 2.2.5. *Se $f : E \to F$ e $g : F \to G$, então:*

1. $f \circ i_E = f$, $i_F \circ f = f$, $g \circ i_F = g$, $i_E \circ g = g$.

2. Se $g \circ f = i_E$ e $f \circ g = i_F$, então f e g são bijetora e $g = f^{-1}$.

Definição 2.2.9. *Seja $f : E \to F$ uma aplicação.*

1. Dizemos que f é uma **aplicação crescente** em E se:

$$\forall x, x', x \leq x' \Rightarrow f(x) \leq f(x').$$

2. Dizemos que f é uma **aplicação decrescente** em E se:

$$\forall x, x', x \leq x' \Rightarrow f(x') \leq f(x).$$

Uma aplicação crescente ou decrescente sera chamada de **aplicação monótona**

Definição 2.2.10. *Uma* **aplicação estritamente monótona em E** *é uma aplicação* $f : E \to F$ *que satisfaça a uma das seguintes propriedades:*

1. Estritamente crescente, isto é:

$$\forall x, x', x < x' \Rightarrow f(x) < f(x').$$

2. Dizemos que f é uma **aplicação decrescente** em E se:

$$\forall x, x', x < x' \Rightarrow f(x') < f(x).$$

Exemplo 2.2.8.

1. Mostre que a aplicação $f : \mathbb{R} \to R$ dada por $f(x) = 2^x$ é estritamente crescente.
2. Mostre que a aplicação $g : \mathbb{R} \to R$ dada por $g(x) = 1 - x$ é estritamente decrescente.

2.2.1 Exercícios

1. Seja $E = \{1, 2, 3, 4\}$ e $F = \{a, b, c\}$, quais das relações abaixo são aplicações de E em F.

   $R_1 = \{(1, a), (2, b), (3, c)\}$

   $R_2 = \{(1, a), (2, b), (3, c), (4, c)\}$

   $R_3 = \{(1, b), (1, c), (2, b), (3, c), (4, a)\}$

   $R_4 = \{(1, c), (2, c), (3, c), (4, c)\}$

2. Determinar todas as aplicações de $E = \{0, 1, 2\}$ em $F = \{3, 4\}$

3. Seja a função $f : \mathbb{R} \to \mathbb{R}$, dada pela seguinte lei: $f(x) = |x|$. Determinar:

   (a) $f(1)$

   (b) $f(-3)$

   (c) $f([-1, 1])$

   (d) $f(]-1, 2[)$

4. Quais das seguintes aplicações abaixo de $E = \{a, b, c, d\}$ em $F = \{0, 1, 2, 3, 4\}$ são injetoras?

   $f_1 = \{(a, 0), (b, 1), (c, 2), (d, 4)\}$

   $f_2 = \{(a, 1), (b, 2), (c, 3), (d, 1)\}$

   $f_3 = \{(a, 2), (b, 4), (c, 3), (d, 0), \}$

   $f_4 = \{(a, 3), (b, 0), (c, 0), (d, 4)\}$

5. Quais das seguintes aplicações abaixo de $E = \{a, b, c\}$ em $F = \{0, 1\}$ são sobrejetora?

   $f_1 = \{(a, 0), (b, 0), (c, 0)\}$

   $f_2 = \{(a, 0), (b, 0), (c, 1)\}$

   $f_3 = \{(a, 1), (b, 0), (c, 1)\}$

   $f_4 = \{(a, 1), (b, 1), (c, 1)\}$

6. Sejam $A = \{1, 2, 3\}$, $B = \{4, 5, 6, 7\}$ e $C = \{8, 9, 0\}$. Seja $f : A \to B$ dada por $f(1) = 4$, $f(2) = 5$, $f(3) = 6$. Seja $g : B \to C$ dada por $g(4) = 8$, $g(5) = 8$, $g(6) = 9$, $g(7) = 0$. Quais são os pares ordenados de $g \circ f$. A função $g \circ f$ é injetora ? É sobrejetora?

7. Sejam f, g, h funções reais definidas por $f(x) = x + 1$, $g(x) = x^2 + 2$ e $h(x) = x + 1$.

   (a) Determinar $f \circ g$, $g \circ h$, $f \circ h$, $g \circ f$, $h \circ f$, $h \circ g$.

(b) Verificar que $(f \circ g) \circ h = f \circ (g \circ h)$.

Capítulo 3

Operações-Leis de Composição Internas

Exemplos Preliminares:

1. Considere a aplicação $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $f(x, y) = x + y$. A aplicação f é conhecida como operação de adição sobre $\mathbb{N}$.

2. A aplicação $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ tal que $f(x, y) = x.y$, é conhecida como operação de multiplicação sobre $\mathbb{R}$.

Definição 3.0.11. *Sendo E um conjunto não vazio, toda aplicação $f : E \times E \to E$ recebe o nome de* **operação sobre** E *ou* **lei de composição interna em** E.

Uma operação f sobre E, associa a cada par $(x, y) \in E \times E$ um elemento $x * y \in E$, ou seja, $f(x, y) = x * y$. Dizemos que E é um conjunto munido da operação $*$. Os elementos $x * y$ chama-se composto de x e y pela operação f.

Outras notações para indicar operação sobre o conjunto E:

- Notação aditiva: $+$;
- Notação multiplicativa $\cdot$;
- Notação de composição: $\circ$;
- Outros símbolos: $\triangle, \times, \otimes, \perp, ...$

Outros exemplos:

1. $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
   $(x, y) \to f(x, y) = x^y$

2. $f : \mathbb{Q} \times \mathbb{Q}^* \to \mathbb{Q}^*$
   $(x, y) \to f(x, y) = \frac{x}{y}$

3. $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
   $(x, y) \to f(x, y) = x - y$

4. $f : M_{n\times n}(\mathbb{R}) \times M_{n\times n}(\mathbb{R}) \to M_{n\times n}(\mathbb{R})$
   $(A, B) \to f(A, B) = A + B$

5. $f : M_{n\times n}(\mathbb{R}) \times M_{n\times n}(\mathbb{R}) \to M_{n\times n}(\mathbb{R})$
   $(A, B) \to f(A, B) = A.B$

6. $\varphi : E \times E \to E$, onde $E = \mathbb{R}^{\mathbb{R}}$= {conjunto das funções de $\mathbb{R}$ em $\mathbb{R}$}, tal que
   $(f, g) \to \varphi(f, g) = f \circ g$.

3.0.2 Propriedades das Operações

Considere $*$ uma lei de composição interna em E.
(a)Propriedade Associativa:

Definição 3.0.12. *Dizemos que $*$ tem a propriedade associativa, quando:*

$$x * (y * z) = (x * y) * z,$$

quaisquer que sejam $x, y, z \in E$.

Exemplos 3.0.1.

1. As adições e multiplicações em $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ são operações associativas.

2. A adição e multiplicação em $M_{m\times n}(\mathbb{R})$ é associativa.

3. A composição de funções de $\mathbb{R}$ em $\mathbb{R}$ é associativa.

Contra-Exemplos 3.0.1.

1. A potenciação em $\mathbb{N}$ não é associativa, pois: $2^{(3^4)} = 2^{81}$ e $(2^3)^4 = 2^{12}$.

2. A divisão em $\mathbb{R}^*$ não é associativa, pois: $(24 \div 4) \div 2 = 6 \div 2 = 3$ e $24 \div (4 \div 2) = 24 \div 2 = 12$.

Observação 3.0.5. *Se uma operação é associativa, não precisamos colocar parênteses para indicar a ordem em uma determinada operação. Por exemplo:* $2+3+5+8 = (2+3)+(5+8) = 2+(3+5)+8 = 2+(3+5+8) = 18$.
Se uma operação não é associativa, temos a obrigação de usar parênteses. Por exemplo: $48 \div 4 \div 2 \div 6$ *não tem significado,* $(48 \div 4) \div (2 \div 6) = 12 \div \frac{1}{3} = 36$, $48 \div (4 \div 2) \div 6 = 48 \div 2 \div 6$ *não tem significado,* $48 \div ((4 \div 2) \div 6) = 48 \div (2 \div 6) = 48 \div \frac{1}{3} = 144$

(b)Propriedade Comutativa:

Definição 3.0.13. *Dizemos que* $*$ *tem a propriedade comutativa, quando:*

$$x * y = y * x,$$

quaisquer que sejam $x, y \in E$.

Exemplos 3.0.2.

1. As adições e multiplicações em $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ são operações comutativa.
2. A adição em $M_{m\times n}(\mathbb{R})$ é comutativa.

Contra-Exemplos 3.0.2.

1. A potenciação em $\mathbb{N}$ não é comutativa, pois: $2^3 = 8$ e $3^2 = 9$.
2. A divisão em $\mathbb{R}^*$ não é comutativa, pois: $24 \div 4 = 6$ e $4 \div 24 = \frac{1}{6}$.
3. A subtração em $\mathbb{Z}$ não é comutativa, pois:$2 - 4 = -2$ e $4 - 2 = 2$.
4. A multiplicação em $M_{2\times 2}(\mathbb{R})$ não é comutativa, pois:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} . \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} . \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} . \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} . \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

5. A composição em $\mathbb{R}^{\mathbb{R}}$(conjunto das funções de $\mathbb{R}$ em $\mathbb{R}$ não é comutativa, pois se $f(x) = 2x$ e $g(x) = x^2$, então:

$$(f \circ g)(x) = f(g(x)) = 2x^2$$
$$(g \circ f)(x) = g(f(x)) = (2x)^2 = 4x^2$$

(c)Elemento Neutro:

Definição 3.0.14. *Dizemos que $e \in E$ é um elemento neutro à esquerda quando:*

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

Dizemos que $e \in E$ é um elemento neutro à direita quando:

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

Dizemos que $e \in E$ é um elemento neutro quando:

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

Exemplos 3.0.3.

1. O elemento neutro da adição em $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ é o número 0, pois

$$0 + x = x = x + 0, \ \forall x.$$

2. O elemento neutro da multiplicação em $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ é o número 1, pois

$$1.x = x = x.1, \ \forall x.$$

3. O elemento neutro da adição em $M_{m\times n}(\mathbb{R})$ é a matriz nula:

$$0_{m\times n} = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

4. O elemento neutro da multiplicação em $M_n(\mathbb{R})$ é a matriz identidade:

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

5. O elemento neutro da composição de funções de $\mathbb{R}$ em $\mathbb{R}$ é a função identidade $i_{\mathbb{R}}$,pois:

$$i_{\mathbb{R}} \circ f = f \circ i_{\mathbb{R}} = f,\ \forall f \in \mathbb{R}^{\mathbb{R}}$$

Contra-Exemplos 3.0.3.

1. A subtração em $\mathbb{Z}$ admite 0 como elemento neutro à direita, pois $x - 0 = x, \forall x \in \mathbb{Z}$, mas não têm elemento neutro à esquerda, pois não existe e(fixo), tal que $e - x = x, \forall x \in \mathbb{Z}$.

2. A divisão em $\mathbb{R}^*$ admite 1 como elemento neutro à direita, pois $x \div 1 = x, \forall x \in \mathbb{R}^*$, mas não tem elemento neutro à esquerda, pois não existe e(fixo), tal que $e \div x = x, \forall x \in \mathbb{R}^*$.

Proposição 3.0.6. *Se a operação $*$ tem um elemento neutro e, então é único.*

Demonstração. □

(d)Elemento Simetrizáveis:

Definição 3.0.15. *Dizemos que $x \in E$ é um elemento simetrizável para operação $*$ que tem como elemento neutro e, se existe $x' \in E$, tal que :*

$$x * x' = x * x' = e,\ x \in E.$$

Observação 3.0.6.

1. O elemento x' é chamado simétrico de x.

2. Quando a operação é a adição $(+)$, o simétrico de x é chamado de oposto e indicado por $-x$.

3. Quando a operação é a multiplicação $(.)$, o simétrico de x é chamado de inverso e indicado por x^{-1}.

Exemplos e Contra Exemplos

1. 2 é um elemento simetrizável para a adição em $\mathbb{Z}$, e seu simétrico é -2, pois: $(-2) + (2) = 2 + (-2) = 0$;

2. 2 é um elemento simetrizável para a multiplicação em $\mathbb{Q}$ e seu simétrico é $\frac{1}{2}$, pois: $\frac{1}{2}.2 = 2.\frac{1}{2} = 1$. Mas $0 \in \mathbb{Q}$ não é simetrizável, pois $\nexists x \in \mathbb{Q}$ tal que $0.x = 1 = x.0$;

3. $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ é simetrizável para a adição em $M_2(\mathbb{R})$ e seu simétrico é $\begin{pmatrix} -1 & -2 \\ -3 & -4 \end{pmatrix}$;

4. $\begin{pmatrix} 1 & 3 \\ -2 & -5 \end{pmatrix}$ é simetrizável para a multiplicação em $M_2(\mathbb{R})$ e seu simétrico é $\begin{pmatrix} -5 & -3 \\ 2 & 1 \end{pmatrix}$
   Mas por exemplo, $A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ não é simetrizável, pois não possui inversa($\det A = 0$);

5. A função $f(x) = 2x + 1$ é bijetora de $\mathbb{R}$ em $\mathbb{R}$, logo existe a inversa de f, $f^{-1}(x) = \frac{x-1}{2}$. Portanto f é simetrizável.
   Por outro lado $g(x) = x^2$ não é bijetora de $\mathbb{R}$ em $\mathbb{R}$, logo não existe a inversa, portanto g não é simetrizável.

Proposição 3.0.7. *Se a operação $*$ em E é associativa, tem elemento neutro e, e $x \in E$ é simetrizável, então o simétrico de x é único.*

Demonstração. □

Proposição 3.0.8. *Seja $*$ uma operação sobre E com elemento neutro e. Então:*

1. *Se x é simetrizável, então o seu simétrico x' também é simetrizável, e $(x')' = x$;*
2. *Se $*$ é associativa, e $x, y \in E$ são simetrizáveis, então $x*y$ é simetrizável e $(x*y)' = y' * x'$.*

Demonstração. □

Definição 3.0.16. *Seja $*$ uma operação sobre E com elemento neutro e. Definimos por $U_*(E)$ o conjunto dos elementos simetrizáveis de E, ou seja:*

$$U_*(E) = \{x \in E | \exists x' \in E, \text{ com } x' * x = x * x' = e\}.$$

Exemplos 3.0.4. .

1. $U_+(\mathbb{N}) =$
2. $U_+(\mathbb{Z}) =$
3. $U_\cdot(\mathbb{Z}) =$
4. $U_\cdot(\mathbb{R}) =$

5. $U_+(M_{m\times n}(\mathbb{R})) =$

6. $U_\cdot(M_n(\mathbb{R})) =$

7. $U_\circ(\mathbb{R}^\mathbb{R}) =$

Observação 3.0.7. *Note que $U_*(E) \neq \emptyset$, pois $e \in U_*(E)$.*

(d)Elemento Simetrizáveis:

Definição 3.0.17. *Dizemos que $x \in E$ é um elemento simetrizável para operação $*$ que tem como elemento neutro e, se existe $x' \in E$, tal que :*

$$x * x' = x * x' = e,\ x \in E.$$

Observação 3.0.8.

1. O elemento x' é chamado simétrico de x.

2. Quando a operação é a adição $(+)$, o simétrico de x é chamado de oposto e indicado por $-x$.

3. Quando a operação é a multiplicação $(.)$, o simétrico de x é chamado de inverso e indicado por x^{-1}.

Exemplos e Contra Exemplos

1. 2 é um elemento simetrizável para a adição em $\mathbb{Z}$, e seu simétrico é -2, pois: $(-2) + (2) = 2 + (-2) = 0$;

2. 2 é um elemento simetrizável para a multiplicação em $\mathbb{Q}$ e seu simétrico é $\frac{1}{2}$, pois: $\frac{1}{2}.2 = 2.\frac{1}{2} = 1$. Mas $0 \in \mathbb{Q}$ não é simetrizável, pois $\nexists x \in \mathbb{Q}$ tal que $0.x = 1 = x.0 =$;

3. $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ é simetrizável para a adição em $M_2(\mathbb{R})$ e seu simétrico é $\begin{pmatrix} -11 & -2 \\ -3 & -4 \end{pmatrix}$;

4. $\begin{pmatrix} 1 & 3 \\ -2 & -5 \end{pmatrix}$ é simetrizável para a multiplicação em $M_2(\mathbb{R})$ e seu simétrico é $\begin{pmatrix} -5 & -3 \\ 2 & 1 \end{pmatrix}$ Mas por exemplo, $A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ não é simetrizável, pois não possui inversa(det $A = 0$);

5. A função $f(x) = 2x + 1$ é bijetora de $\mathbb{R}$ em $\mathbb{R}$, logo existe a inversa de f, $f^{-1}(x) = \dfrac{x-1}{2}$. Portanto f é simetrizável.
   Por outro lado $g(x) = x^2$ não é bijetora de $\mathbb{R}$ em $\mathbb{R}$, logo não existe a inversa, portanto g não é simetrizável.

(e)Elemento Regular:

Definição 3.0.18. *Dizemos que $a \in E$ é regular em relação à $*$ se:*

$$(1): \ a * x = a * y \Rightarrow x = y$$

e

$$(2): \ x * a = y * a \Rightarrow x = y,$$

$\forall x, y \in E$.

Observação 3.0.9.

1. Valendo (1) dizemos que a é regular à esquerda. Valendo (2) dizemos que a é regular à direita.

2. Se $*$ é comutativa, regular à esquerda significa regular à direita.

Exemplos e Contra Exemplos

1. 5 é regular para a adição em $\mathbb{N}$, pois:

$$5 + x = 5 + y \Rightarrow x = y, \forall x, y\mathbb{N}.$$

2. 5 é regular para a multiplicação em $\mathbb{Z}$, pois:

$$5.x = 5.y \Rightarrow x = y, \forall x, y\mathbb{Z}.$$

3. 0 não é regular para a multiplicação em $\mathbb{Z}$, pois:

$$0.2 = 0.3 \ e \ 2 \neq 3.$$

4. $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, é regular para à adição em $M_2(\mathbb{R})$, pois:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix} \Rightarrow \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix}.$$

5. $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ não é regular para a multiplicação em $M_2(\mathbb{R})$, pois:

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix},$$

$$e \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix}.$$

Proposição 3.0.9. *Se a operação $*$ em E é associativa, tem elemento neutro e, e $a \in E$ é simetrizável, então a é regular.*

Demonstração. □

Notação: Indica-se por $R_*(E)$ o conjunto dos elementos regulares de E pela operação $*$.

Exemplos 3.0.5.

1. $R_+(\mathbb{N}) = \mathbb{N}$;
2. $R_\cdot(\mathbb{Z}) = \mathbb{Z}^*$;
3. $R_+(M_{m\times n}(\mathbb{R})) = M_{m\times n}(\mathbb{R})$.

Observação 3.0.10.

1. Se E tem elemento neutro e, então $e \in R_*(E)$, logo $R_*(E) \neq \emptyset$.
2. Se $*$ é associativa, pela Proposição 3.0.9 $U_*(E) \subset R_*(E)$.

(f)Distributiva:

Definição 3.0.19. *Sejam $*$ e $\triangle$ duas operações sobre E. Dizemos que $\triangle$ é distributiva em relação à $*$ se:*

$$(1) : x\triangle(y * z) = (x\triangle y) * (x\triangle z)$$

$$(2) : (y * z)\triangle x = (y\triangle x) * (z\triangle x)$$

$\forall x, y, z \in E$.

Observação 3.0.11.

1. Valendo (1) dizemos que $\triangle$ é distributiva à esquerda de $*$. Valendo (2), dizemos que $\triangle$ é distributiva à direita de $*$.

2. Se $\triangle$ é comutativa, então distributiva à esquerda ou à direita de $*$ são equivalentes.

Exemplos 3.0.6.

1. A multiplicação é distributiva em relação à adição em $\mathbb{Z}$, pois $\forall x, y, z \in \mathbb{Z}$:

$$x.(y+z) = (x.y) + (x.z)$$
$$(y+z).x = (y.x) + (z.x)$$

2. A multiplicação é distributiva em relação à adição em $M_2(\mathbb{R})$, pois $\forall A, B, C \in M_n(\mathbb{R})$:

$$A.(B+C) = (A.B) + (A.C)$$
$$(B+C).A = (B.A) + (C.A)$$

3. A potenciação é distributiva à direita em relação a multiplicação em $\mathbb{N}$, pois $\forall x, y, z \in \mathbb{N}$: $(x.y)^n = x^n.y^n$, mas não é distributiva à esquerda, pois $2^{3.4} \neq 2^3.2^4$.

3.0.3 Parte Fechada Para Uma Operação

Definição 3.0.20. *Seja $*$ uma operação sobre $E \neq \emptyset$. Seja $A \subset E$ e $A \neq \emptyset$. Dizemos que A é uma parte fechada de E para a operação $*$ se:*

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

Exemplo 3.0.9. *O conjuntos dos números racionais $\mathbb{Q}$ é uma parte fechada dos $\mathbb{R}$ para a adição, pois $\mathbb{Q} \neq \emptyset$,$\mathbb{Q} \subset \mathbb{R}$ e $\forall x, y \in \mathbb{Q} \Rightarrow x * y \in \mathbb{Q}$. Já os irracionais não são uma parte fechada para a adição sobre $\mathbb{R}$, pois $\sqrt{2} \in \mathbb{R} - \mathbb{Q}$ e $1 - \sqrt{2} \in \mathbb{R} - \mathbb{Q}$, mas $\sqrt{2} + (1 - \sqrt{2}) = 1 \notin \mathbb{R} - \mathbb{Q}$.*

3.1 Tábua de Uma Operação

Seja $E = \{a_1, a_2, a_3, ..., a_n\}$, $n \geq 1$. Cada operação sobre E é uma aplicação $f : E \times E \to E$ que associa a cada par (a_i, a_j) o elemento $a_i * a_j = a_{ij}$. Dessa forma, podemos indicar o elemento a_{ij} para cada par (a_i, a_j) por meio de uma tabela de dupla entrada.

$*$	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}
$\vdots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
a_i	a_{i1}	a_{i2}	$\ldots$	a_{ii}	$\ldots$	$\mathbf{a_{ij}}$	$\ldots$	a_{in}
$\vdots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
a_j	a_{j1}	a_{j2}	$\ldots$	a_{ji}	$\ldots$	a_{jj}	$\ldots$	a_{jn}
$\vdots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
a_n	a_{n1}	a_{n2}	$\ldots$	a_{ni}	$\ldots$	a_{nj}	$\ldots$	a_{jn}

Exemplos 3.1.1.

1. Tábua da multiplicação em $E = \{-1, 0, 1\}$.

.	-1	0	1
-1			
0			
1			

2. Tábua das operações da união e da intersecção sobre $E = \{A, B, C, D\}$ em que A, B, C, D são conjuntos tais que $A \subset B \subset C \subset D$.

$\cup$	A	B	C	D
A				
B				
C				
D				

e

$\cap$	A	B	C	D
A				
B				
C				
D				

3. Tábua da operação $*$ sobre $\{1, 3, 5, 15\}$ tal que $x * y = mdc(x, y)$

$*$	1	3	5	15
1				
3				
5				
15				

4. Tábua da operação de composição sobre $E = \{f_1, f_2, f_3\}$ em que f_1, f_2, f_3 são funções assim descritas: $f_1 = \{(a, a), (b, b), (c, c)\}$,$f_2 = \{(a, b), (b, c), (c, a)\}$, $f_3 = \{(a, c), (b, a), (c, b)\}$

$\circ$	f_1	f_2	f_3
f_1			
f_2			
f_3			

Como Verificar Propriedades:

Vejamos agora como se pode verificar uma a uma as propriedades de uma operação $*$ sobre $E = \{a_1, a_2, ..., a_n\}$ quando $*$ é dada por meio de uma tábua.

(a)Propriedade Associativa:

Calculam-se todos os compostos do tipo $a_i * (a_j * a_k)$ e $(a_i * a_j) * a_k$ com $i, j, k \in \{1, 2, ..., n\}$. Compara-se os compostos que têm os mesmos i, j, k. Esse método requer o cálculo de $2n^3$ compostos.

(b)Propriedade Comutativa:

Sabemos que uma operação é comutativa se : $a_i * a_j = a_j * a_i$, ou seja, se $a_{ij} = a_{ji}$, $\forall i, j \in \{1, 2, ..., n\}$.

Chamamos de diagonal principal da tábua o conjunto formado pelos elementos a_{11}, a_{22},

$..., a_{nn}$. Note que a_{ij} e a_{ji} ocupam posições simétricas relativamente à diagonal principal. Portanto uma operação $*$ é comutativa se os compostos colocados simetricamente em relação à diagonal são iguais.

(c)Elemento Neutro:

Sabemos que um elemento e é neutro para a operação $*$ quando:

$(i) : \ e * x = x, \ \forall x \in E,$

$(ii) : \ x * e = x, \ \forall x \in E.$

Da condição (i) decorre que a linha de e é igual a linha fundamental. Da condição (ii) decorre que a coluna de e é igual à coluna fundamental.

Assim, uma operação $*$ tem elemento neutro, desde que exista um elemento cuja linha e coluna são respectivamente iguais à linha e coluna fundamentais.

(d)Elementos Simetrizáveis:

Sabemos que um elemento $a_i \in E$ é simetrizável para a operação $*$ que tem elemento neutro e, quando $\exists a_j \in E$, tal que

$(i) : \ a_i * a_j = e,$

$(ii) : \ a_j * a_i = e.$

Da condição (i) decorre que a linha de a_i na tábua deve apresentar ao menos um composto igual á e. Da condição (ii) decorre que a coluna de a_i deve apresentar um composto igual a e.

Como $a_{ij} = a_{ji} = e$, decorre que o elemento neutro deve figurar em posições simétricas relativamente à diagonal principal. Portanto, um elemento a_i é simetrizável quando o elemento neutro figura ao menos uma vez na linha i e na coluna j da tábua, ocupando posições simétricas em relação à diagonal principal.

(e)Elementos Regulares:

Sabemos que um elemento $a \in E$ é regular em relação a operação $*$ quando:

$(i) : a * a_i \neq a * a_j$ sempre que $a_i \neq a_j$ e

$(ii) : a_i * a \neq a_j * a$ sempre que $a_i \neq a_j$.

Isso significa que a é regular quando composto com elementos distintos de E, tanto à esquerda como à direita, produz resultados distintos. Assim, um elemento a é regular quando na linha e na coluna de a não há elementos iguais.

Exemplo 3.1.1. *Considere um conjunto $E = \{e, a, b, c, d\}$ onde os elementos regulares são e, a, d. Note que nas linhas e colunas de b, c ocorrem repetições:*

$*$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	b	c	a
c	c	d	c	a	b
d	d	e	a	b	c

3.2 Operações em $\mathbb{Z}_m$

Lembre-se que $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$, ou seja, $\overline{x} \in \mathbb{Z}_m$, significa que $\overline{x} = \{y \in \mathbb{Z} | x \equiv y (mod\ m)\}$.

Vamos definir as operações de adição e multiplicação no conjunto $\mathbb{Z}_m (m > 1)$ de classes de restos.

Definição 3.2.1. *Dadas duas classes $\overline{a}, \overline{b} \in \mathbb{Z}_m$, definimos a soma e o produto por:*

$$\overline{a} + \overline{b} = \overline{ab};$$

$$\overline{a}.\overline{b} = \overline{a.b}.$$

Propriedades da Adição:

1. Associativa: Dados $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$ então:

$$\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}.$$

2. Comutativa: Dados $\overline{a}, \overline{b} \in \mathbb{Z}_m$ então:

$$\overline{a} + \overline{b} = \overline{a} + \overline{b}.$$

3. Elemento Neutro: O elemento $\overline{0} \in \mathbb{Z}_m$ é o elemento neutro da adição em $\mathbb{Z}_m$, pois $\forall \overline{a} \in \mathbb{Z}_m$, temos:

$$\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}.$$

4. Elementos Simetrizáveis; Dado $\overline{a} \in \mathbb{Z}_m$, seu simétrico aditivo é $\overline{(m-a)}$, pois:

$$\overline{a} + \overline{(m-a)} = \overline{(m-a)} + \overline{a} = \overline{0}.$$

Propriedades da Multiplicação:

1. Associativa: Dados $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$ então:

$$\overline{a}.(\overline{b}.\overline{c}) = (\overline{a}.\overline{b}).\overline{c}.$$

2. Comutativa: Dados $\overline{a}, \overline{b} \in \mathbb{Z}_m$ então:

$$\overline{a}.\overline{b} = \overline{a}.\overline{b}.$$

3. Elemento Neutro: O elemento $\overline{1} \in \mathbb{Z}_m$ é o elemento neutro da multiplicação em $\mathbb{Z}_m$, pois $\forall \overline{a} \in \mathbb{Z}_m$, temos:

$$\overline{a}.\overline{1} = \overline{1}.\overline{a} = \overline{a}.$$

4. Elementos Simetrizáveis; Dado $\overline{a} \in \mathbb{Z}_m$, então a é simetrizável se $mdc(a.m) = 1$(justificar).

3.3 Exercícios

1. Em cada caso abaixo, considere a operação $*$ sobre E e verifique se é associativa, se é comutativa, se existe elemento neutro e determine os elementos simetrizáveis.

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

   (b) $E = \mathbb{R}$ e $x * y = x$

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

   (d) $E = \mathbb{R}$ e $x * y = \dfrac{x}{y}$

2. Em cada caso abaixo, está definida uma operação sobre $\mathbb{Z} \times \mathbb{Z}$. Verifique se é associativa, se e´comutativa, se existe neutro e determine os elementos simetrizáveis.

   (a) $(a, b) * (c, d) = (ac, 0)$

   (b) $(a, b) \triangle (c, d) = (a + c, c + d)$

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

3. Em que condições, sobre $m, n \in \mathbb{Z}$ a operação dada por $x * y = mx + ny$ sobre $\mathbb{Z}$:

   (a) é associativa ?

   (b) é comutativa ?

   (c) admite elemento neutro ?

4. Consideremos a operação $*$ em $\mathbb{R}$ definida por $x * y = ax + by + cxy$, onde a, b, c são números reais dados. Determinar as condições para a, b, c de modo que $*$ seja associativa e tenha elemento neutro.

5. Determinar todos os elementos neutros à esquerda no conjunto $E = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$, para a operação de multiplicação.

6. Determinar os elementos regulares dos exercícios $1, 2$, $R_*(E)$ e $R_*(\mathbb{Z} \times \mathbb{Z})$.

7. Mostrar que nenhum elemento de $\mathbb{R}$ é regular para a operação $\triangle$ assim definida:

$$x \triangle y = x^2 + y^2 + xy$$

.

8. Verificar se a lei dada por $(a, b) \triangle (c, d) = (ac, ad + bc)$ é distributiva em relação à lei $(a, b) + (c, d) = (a + c, b + d)$ tudo em $\mathbb{Z} \times \mathbb{Z}$.

9. Em cada caso abaixo, está definida uma operação $*$ sobre E. Pede-se: fazer a tábua da operação, verificar se é comutativa, e se existe elemento neutro, determinar $U_*(E)$ e $R_*(E)$.

   (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) $E = \{1, i, -1, -i\}$ e $x * y = x \times y$

   (d) $E = \{0, 1, 2, 3\}$ e $x * y =$ resto da divisão em $\mathbb{Z}$ de $x + y$ por 4

10. Construir a tábua da operação de composição de funções em $E = \{f_1, f_2, f_3\}$, onde:

    $f_1 = \{(a, a), (b, b), (c, c)\}$

    $f_2 = \{(a, b), (b, bc), (c, a)\}$

    $f_3 = \{(a, c), (b, a), (c, cb)\}$

11. Construi a tábua de uma operação $*$ sobre o conjunto $E = \{a, b, c, d\}$ de modo que:

    (I) seja comutativa;

    (II) a seja o elemento neutro;

    (III) $U_*(E) = E$

(IV) $R_*(E) = E$

(V) $b * c = a$

12. Construi a tábua de uma operação $*$ sobre o conjunto $E = \{e, a, b, c\}$ de modo que:

(I) seja comutativa;

(II) e seja o elemento neutro;

(III) $x * a = a$ para qualquer x

(IV) $R_*(E) = E - \{a\}$

Capítulo 4

Grupos

Definição 4.0.1. *Sejam G um conjunto não vazio e $(x, y) \mapsto x * y$ uma operação em G. Dizemos que G é um grupo se esta operação vale:*

(a) Associativa:
$\forall a, b, c \in G \quad a * (b * c) = (a * b) * c$;
(b) Elemento Neutro:
$\exists e \in G$ tal que $a * e = e * a = a \ \forall a \in G$;
(c) Simétrico:
$\forall a \in G$, $\exists a' \in G$ tal que $a * a' = a' * a = e$.
Notação: $(G, *)$.

Observação 4.0.1. .

1. *Se a operação for adição, diremos grupo aditivo. Se for a multiplicação, diremos grupo multiplicativo;*

2. *Na maior parte da teoria, usaremos a notação multiplicativa.*

Propriedades de um Grupo:
Considere $(G, *)$ um grupo, então:

1. Unicidade do elemento neutro de $(G, *)$;

2. Unicidade do elemento simétrico de cada elemento de G;

3. Para todo elemento $a \in G$, $(a')' = a$;

4. $\forall a, b \in G$, $(a * b)' = b' * a$;

5. Todo elemento de G é regular, pois e $a * x = a * y \Rightarrow x = y$.

Definição 4.0.2. *Dizemos que um grupo* $(G, *)$ *é* **abeliano ou comutativo**, *se* $\forall a, b \in G$,

$$a * b = b * a.$$

Definição 4.0.3. *Dizemos que um grupo* $(G, *)$ *é um* **grupo finito** *quando o conjunto* G *for finito.*

Observação 4.0.2. .

(a) O número de elementos de G*, é chamado ordem do grupo* G*, e denotado por* $o(G)$*.*

(b) A tábua de um grupo finito $(G, *)$ *será a tábua da operação em* G*.*

Exemplo 4.0.1. *Note que* $G = \{-1, 1\}$ *é um grupo em relação a multiplicação usual. Trata-se de u grupo finito de ordem* 2 *cuja tábua é:*

$\cdot$	*1*	*-1*
1		
-1		

(4.1)

Exemplos de Grupos

1. **Grupo Aditivo dos Inteiros**
2. **Grupo Aditivo os Racionais**
3. **Grupo Aditivo dos Reais**
4. **Grupo Aditivo dos Complexos**
5. **Grupo Multiplicativo dos Racionais**
6. **Grupo Multiplicativo dos Reais**
7. **Grupo Multiplicativo dos Complexos**
8. **Grupo aditivo das Matrizes** $m \times n$
9. **Grupo Lineares de Grau** n
10. **Grupos Aditivos de Classes de Restos**
11. **Grupos Multiplicativos de Classes de Restos**

4.1 Subgrupos

Definição 4.1.1. *Seja $(G, *)$ um grupo. Dizemos que um subconjunto não vazio $H \subset G$ é um* **subgrupo** *de G se:*

(a) $\forall a, b \in H \Rightarrow a * b \in H$*.(Isto é, H é fechado para a lei de composição interna de G).*

(B) $(H, *)$ *também é um grupo. (Aqui a lei de composição interna é a mesma de G, só que restrita a H).*

Observação 4.1.1. *Seja $e \in G$ o elemento neutro de G, então os conjuntos $\{e\}, G$ são subgrupos de G, chamados de* **subgrupos triviais** *de G.*

Proposição 4.1.1. *Seja $(G, *)$ um grupo. Então $H \subset G$ é um subgrupo de G se, e somente se, $\forall a, b \in H \Rightarrow a * b' \in H$, onde b' é o simétrico de b.*

Demonstração. □

Observação 4.1.2. .

1. *Se o grupo G é aditivo, a condição para H ser subgrupo é: $a, b \in H \Rightarrow a + (-b) \in H$.*
2. *Se o grupo G é multiplicativo, a condição para H ser subgrupo é:$a, b \in H \Rightarrow a.b^{-1} \in H$.*

Exemplos 4.1.1. .

(a) Verifique que $(\mathbb{Z}, +)$ é um subgrupo do grupo $(\mathbb{R}, +)$.

(b) Seja $H = \{x \in \mathbb{R} | x > 0\}$. Mostre que $(H, \cdot)$ é um subgrupo de $(\mathbb{R}^*, \cdot)$.

(c) Considere o grupo $(M_2(\mathbb{R}), +)$. Seja $H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}) | a + d = 0 \right\}$. Então $(H, +)$ é um subgrupo de $(M_2(\mathbb{R}), +)$.

(d) Sejam $(G, \cdot)$ e $(L, \cdot)$ grupos multiplicativos e 1 o elemento neutro de G e L. Então os conjuntos :

$$\{1\} \times L = \{(x, y) \in G \times L | x = 1\}$$
$$G \times \{1\} = \{(x, y) \in G \times L | y = 1\}$$

são subgrupos do produto direto $G \times L$.

4.2 Homomorfismo e Isomorfismo

Definição 4.2.1. *Dados dois grupos $(G, *)$ e $(J, \triangle)$, dizemos que uma aplicação $f : G \to H$ é um* **homomorfismo** *de G em J, se:*

$$\forall a, b \in G \Rightarrow f(a * b) = f(a) \triangle f(b) \tag{4.2}$$

Observação 4.2.1. .

1. *Quando $G = J$, diremos apenas homomorfismo de G.*
2. *Se f for injetora, diremos homomorfismo injetor ou monomorfismo.*
3. *Se f for sobrejetora, diremos homomorfismo sobrejetor ou epimorfismo.*
4. *Se f for bijetora, diremos isomorfismo.*

Exemplos 4.2.1. .

(a) *A aplicação $f : \mathbb{Z} \to \mathbb{C}^*$, dada por $f(m) = i^m, \forall m \in \mathbb{Z}$, é um homomorfismo de $(\mathbb{Z}, +)$ em $(\mathbb{C}^*, \cdot)$.*

(b) *A aplicação $f : \mathbb{R}_+^* \to \mathbb{R}$ dada por $f(x) = \log x, \forall x \mathbb{R}_+^*$ é um homomorfismo de $(\mathbb{R}_+^*, \cdot)$ em $(\mathbb{R}, +)$.*

(c) *A aplicação $f : \mathbb{C}^* \to \mathbb{R}_+^*$ dada por $f(z) = |z|, \forall z \mathbb{C}^*$ é um homomorfismo sobrejetor de $(\mathbb{C}^*, \cdot)$ em $(\mathbb{R}_+^*, \cdot)$.*

(d) *Seja $a \in \mathbb{Z}$. A aplicação $f : \mathbb{Z} \to \mathbb{Z}$ dada por $f(m) = a.m$ é u homomorfismo.*

4.2.1 Proposições sobre Homomorfismos de Grupos

Vamos considerar notação multiplicativa na maioria dos casos para simplificar as notações.

Sejam $(G, .)$ e $(J, .)$ grupos multiplicativos, cujos elementos neutros são e,u de G e J respectivamente, e seja $f : G \to J$ um homomorfismo de grupos.

Proposição 4.2.1. $f(e) = u$.

Demonstração. □

Proposição 4.2.2. $\forall a \in G$, $f(a^{-1}) = (f(a))^{-1}$.

Demonstração. □

Proposição 4.2.3. *Se H é um subgrupo de G, então $f(H)$ é um subgrupo de J.*

Demonstração. □

Observação 4.2.2. *Em particular Imf é um subgrupo de J.*

Proposição 4.2.4. *Sejam $(G,.),(J,.),(L,.)$ grupos quaisquer, e $f : G \to J$, $g : J \to L$ homomorfismo do grupos. Então $g \circ f : G \to L$ também é um homomorfismo de grupos.*

Demonstração. □

Corolário 4.2.1. *Pelas hipóteses da proposição anterior, se f, g são monomorfismo(ou epimorfismo), então $g \circ f$ também é um monomorfismo(também é um epimorfismo).*

Definição 4.2.2. *Sejam $(G,*)$ e $(J,\triangle)$ grupos e $f : G \to J$ um homomorfismo. Chama-se* **núcleo** *de f o seguinte subconjunto de G:*

$$N(f) = KerF = \{x \in G | f(x) = u\},$$

onde u é o elemento neutro de J.

Exemplo 4.2.1. *Determine o núcleo de $f(N(f))$ para os seguintes homomorfismos:*

(a) Seja $f : (\mathbb{Z},+) \to (\mathbb{C},.)$ dada por $f(m) = i^m$.

(b) Seja $f : (\mathbb{R}_+^*,.) \to (\mathbb{R},+)$ dada por $f(x) = \log x$.

(c) Seja $f : (\mathbb{C}^*,.) \to (\mathbb{R}_+^*,.)$ dada por $f(z) = |z|$.

Proposição 4.2.5. *Seja $f : G \to J$ um homomorfismo de grupos. Então:*

(a) $N(f)$ é um subgrupo de G.

(b) f é injetora se, e somente se, $N(f) = \{e\}$, onde e é o elemento neutro de G.

Demonstração. □

4.2.2 Isomorfismo de Grupos

Definição 4.2.3. *Sejam $(G,*)$ e $(J,\triangle)$ grupos. Dizemos que uma aplicação $f : G \to J$ é um* **isomorfismo** *do grupo G no grupo J, se:*

(a) f é bijetora;

(b) f é um homomorfismo de grupos.

Observação 4.2.3. *Se $G = J$, um isomorfismo $f : G \to G$ é chamado de automorfismo de G.*

Exemplo 4.2.2. *A função $f : \mathbb{R}_+^* \to \mathbb{R}$ dada por $f(x) = \log x$ é bijetora e um homomorfismo, então f é um isomorfismo de $(\mathbb{R}_+^*, .)$ em $(\mathbb{R}, +)$*

Observação 4.2.4. *Todas as proposições já provadas para homomorfismos também valem para isomorfismos.*

Proposição 4.2.6. *Se f é um isomorfismo de $(G, *)$ em $(J, \triangle)$ então f^{-1} é um isomorfismo de $(J, \triangle)$ em $(G, *)$.*

Observação 4.2.5. *Quando existe um isomorfismo $f : G \to J$, também existe um isomorfismo de J em G, que é a aplicação f^{-1}. Assim dizemos que G e J são isomorfos e denotamos por $G \simeq J$. O isomorfismo f^{-1} é chamado isomorfismo inverso de f.*

4.3 Grupos Cíclicos

4.3.1 Potências e Múltiplos

Definição 4.3.1. *Seja G um grupo multiplicativo. Dado $a \in G$, define-se potência $m-$ésima de a, para todo $m \in \mathbb{Z}$ da seguinte maneira:*

(i) Se $m \geq 0$, por recorrência temos:

$$a^0 = e(\text{elemento neutro de } G)$$

$$a^m = a^{m-1}.a, \text{se } m \geq 1$$

(ii) Se $m < 0$, fazemos $a^m = (a^{-m})^{-1}$.

Exemplos 4.3.1. *1. No grupo multiplicativo $GL_2(\mathbb{R})$ das matrizes reais 2×2 inversíveis, seja $A = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$. Calcule $A^0, A^1, A^2, A^{-1}, A^{-2}$.*

2. No grupo multiplicativo $\mathbb{Z}_5^* = \overline{1}, \overline{2}, \overline{3}, \overline{4}$, tomando o elemento $\overline{2}$, calcule: $\overline{2}^0, \overline{2}^1, \overline{2}^2, \overline{2}^3, \overline{2}^4, \overline{2}^{-1}, \overline{2}^{-2}$.

Proposição 4.3.1. *Seja G um grupo multiplicativo. Se $m, n \in \mathbb{Z}$ e $a \in G$ então:*

(a) $a^m.a^n = a^{m+n}$.

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

(c) $(a^m)^n = a^{m.n}$.

Definição 4.3.2. *Seja G um grupo aditivo. Se $a \in G$ e $m \in \mathbb{Z}$, o múltiplo $m-$ésimo de a é o elemento de G denotado por $m.a$, definido da seguinte maneira:*

(i) Se $m \geq 0$, por recorrência temos:

$$0.a = e(\textit{elemento neutro de } G)$$
$$m.a = (m-1).a + a, \textit{se } m \geq 1$$

(ii) Se $m < 0$, fazemos $m.a = -[(-m).a]$

Exemplo 4.3.1. *No grupo aditivo $M_2(\mathbb{R})$ das matrizes reais 2×2, seja $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$. Calcule $0.A, 1.A, 2.A, 3.A, (-1).A, (-2).A$.*

Proposição 4.3.2. *Seja G um grupo aditivo. Se $m, n \in \mathbb{Z}$ e $a \in G$ então:*

(a) $m.a + n.a = (m+n).a$.

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

(c) $n.(m.a) = (n.m).a$.

Seja $a \in G$(grupo multiplicativo), denotaremos por $[a]$ o subconjunto de G formado pelas potências inteiras de a, ou seja,

$$[a] = \{a^m | m \in \mathbb{Z}\}. \tag{4.3}$$

Note que $[a] \neq \emptyset$, pois o elemento neutro de G pertence a ele, uma vez que $a^0 = e$.

Proposição 4.3.3. *$[a]$ é um subgrupo de G.*

Demonstração. □

Definição 4.3.3. *Um grupo multiplicativo G será chamado* **grupo cíclico** *se, para algum elemento $a \in G$, temos $G = [a]$. O elemento a é dito* **gerador** *de G.*

Observação 4.3.1.

1. *Dizer que um grupo multiplicativo é cíclico significa dizer que $G = \{a^m | m \in \mathbb{Z}\}$.*
2. *No caso aditivo, se G é cíclico, então existe $a \in G$, tal que $G = \{m.a | m \in \mathbb{Z}\} = \{..., -2.a, -a, e = 0, a, 2.a, ...\}$.*

3. Um grupo cíclico pode ter mais do que um gerador.

Exemplo 4.3.2. *(a) O grupo multiplicativo* $G = \{-1, 1\}$ *é cíclico pois* $\{(-1)^m | m \in \mathbb{Z}\} = \{-1, 1\} = G$.

(b) O grupo multiplicativo $G = \{1, -1, i, -i\}$ *é cíclico, pois* $\{i^m | m \in \mathbb{Z}\} = \{1, -1, i, -i\} = G$.

(c) O grupo aditivo $\mathbb{Z}$ *é cíclico, pois todos os seus elementos são múltiplos de* 1 *ou de* -1. *De fato,* $\mathbb{Z} = \{m.1 | m \in \mathbb{Z}\}$ *ou* $\mathbb{Z} = \{m.(-1) | m \in \mathbb{Z}\}$. *Portanto* $\mathbb{Z} = [1] = [-1]$. *Os números* 1 *e* -1 *são os únicos geradores de* $\mathbb{Z}$.

Proposição 4.3.4. *Todo grupo cíclico é abeliano.*

Demonstração. □

Seja G um grupo multiplicativo, e $e \in G$ elemento neutro de G. Suponhamos que a seja um elemento de G, com a seguinte propriedade $a^m = e \Leftrightarrow m = 0$. Por exemplo, o elemento 2 no grupo multiplicativo dos reais tem essa propriedades, pois $2^m = 1 \Leftrightarrow m = 0$. Neste caso, vale a seguinte proposição:

Proposição 4.3.5. *A aplicação* $f : \mathbb{Z} \to [a]$ *dada por* $f(m) = a^m$, $\forall m \in \mathbb{Z}$ *é um isomorfismo do grupo aditivo* $\mathbb{Z}$ *no grupo* $[a]$.

Definição 4.3.4. *Dado um elemento a de um grupo multiplicativo G, se:*

$$a^m = e \Rightarrow m = 0$$

dizemos que o elemento a tem **período** *zero (ou ordem zero). E o grupo* $[a]$ *é um grupo cíclico infinito.*

Exemplo 4.3.3. *Como* 2 *tem período zero no grupo multiplicativo dos reais, então pela Proposição 4.3.5, os grupos* $\mathbb{Z}$ *e* $[2]$ *são isomorfos.*

Agora, suponha que $a \in G$ e $\exists m \in G$, $m \neq 0$ de modo que $a^m = e$. Neste caso, $a^{-m} = (a^m)^{-1} = e^{-1} = e$. Assim, considerando essa hipótese, existe um número inteiro $r > 0$, de maneira que $a^r = e$.

Definição 4.3.5. *O menor número inteiro* $h > 0$ *tal que* $a^h = e$ *chama-se período ou ordem do elemento a.*

Notação: $o(a) = h$.

Exemplo 4.3.4. *Considere o grupo multiplicativo* $\mathbb{C}^*$, *logo* $o(1) = 1$, $o(-1) = 2$,$o(i) = 4$ *e* $o(-i) = 4$

Proposição 4.3.6. *Seja a um elemento de um grupo multiplicativo G. Se a ordem de a é $h > 0$, então $[a]$ é um grupo finito de ordem h, dado por $[a] = \{e, a, a^2, a^3, ..., a^{h-1}\}$.*

Demonstração. □

Observação 4.3.2. *Pela Proposição 4.3.6, se $a \in G$ e $o(a) = h$, então a ordem do subgrupo gerado por a é h, ou seja, $o(a) = o([a])$.*

Definição 4.3.6. *Seja $G = [a]$ um grupo cíclico. Dizemos que G é um grupo cíclico finito se o período do elemento a for um número natural $h > 0$.*

Proposição 4.3.7. *Seja a um elemento de período $h > 0$ de um grupo G. Então $a^m = e \Rightarrow h|m$.*

Demonstração. □

Proposição 4.3.8. *Seja G um grupo cíclico finito de ordem h. Então G é isomorfo ao grupo aditivo $\mathbb{Z}_h$.*

Demonstração. □

Esta proposição significa que quando pensarmos em grupos cíclicos finitos, podemos pensar em grupos aditivos de classes de restos.

4.4 Classes Laterais

Definição 4.4.1. *Seja H um subgrupo de um grupo $(G, *)$. Dado $a \in G$, indicaremos por $a * H$ (respectivamente $H * a$) e chamaremos de classe lateral à esquerda (respectivamente à direita), módulo H, definida por a, o seguinte subconjunto de G:*

$$a * H = \{a * x | x \in H\}$$

$$H * a = \{x * a | x \in H\}.$$

Observação 4.4.1. *Se G é um grupo comutativo, é claro que $a * H = H * a, \forall a \in G$.*

Exemplo 4.4.1. *Determine as classes laterais para cada subgrupo H:*

(a) Considere o grupo multiplicativo $G = \{1, i, -1, -i\}$ e seu subgrupo $H = \{1, -1\}$.

(b) Sejam $G = \mathbb{Z}_6$ grupo aditivo e $H = \{\overline{0}, \overline{3}\}$ seu subgrupo.

(c) Sejam G o grupo multiplicativo dos reais e $H = \{x \in \mathbb{R}^* | x > 0\}$ seu subgrupo.

Vamos ver algumas proposições considerando G um grupo multiplicativo, H um subgrupo de G e classes laterais à esquerda.

Proposição 4.4.1. *A união de todas as classes laterais módulo H é igual à G.*

Demonstração. □

Proposição 4.4.2. *$\forall a, b \in G$, $aH = bH$ se, e somente se, $a^{-1}.b \in H$.*

Demonstração. □

Proposição 4.4.3. *Sejam aH e bH duas classes laterais módulo H quaisquer. Então $aH \cap bh = \emptyset$ ou $aH = bH$.*

Demonstração. □

Proposição 4.4.4. *Seja H um subgrupo de G. Então duas classes laterais quaisquer módulo H são subconjuntos de G que têm a mesma cardinalidades.*

4.5 Teorema de Lagrange

A partir de agora, consideraremos apenas os grupos finitos.

Observação 4.5.1. *Se o conjunto das classes laterais à esquerda é finito, o número de classes laterais à esquerda é igual ao de classes laterais à direita. Isto pode ser verificada provando que $aH \mapsto Ha^{-1}$ é uma bijeção.*

Definição 4.5.1. *Sejam G um grupo finito e H um subgrupo de G. O índice de H em G é o número de classes laterais distintas módulo H e G, denotada por $(G : H)$.*

Exemplo 4.5.1. *Sejam $G = \{1, i, -1, -i\}$ grupo multiplicativo e $H = \{1, -1\}$ subgrupo de H. Determine G/H e $(G : H)$.*

Exemplo 4.5.2. *Sejam $G = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ grupo aditivo e $H = \{\overline{0}, \overline{3}\}$ subgrupo de H. Determine G/H e $(G : H)$.*

Teorema 4.5.1. Teorema de Lagrange
Seja H um subgrupo de um grupo finito G. Então $o(H)|o(G)$ e $o(G) = o(H).(G : H)$

Demonstração. □

Corolário 4.5.1. *Sejam $a \in G$ e $H = [a]$. Então o período de a divide a ordem de G e o quociente nessa divisão é $(G : H)$.*

Demonstração. □

Corolário 4.5.2. *Se $a \in G$, então $a^{o(G)} = e$(elemento neutro de G).*

Demonstração. □

Corolário 4.5.3. *Seja G um grupo finito cuja ordem é um numero primo. Então G é cíclico e os únicos subgrupos de G são os triviais, ou seja, $\{e\}$ e o próprio G.*

Demonstração. □

4.6 Subgrupos Normais

Definição 4.6.1. *Um subgrupo N de um grupo G se diz* **normal** *de G, se:*

$$x.N = N.x, \ \ \forall x \in G.$$

Notação: $N < G$

Observação 4.6.1. .

1. *Pela definição de subgrupo normal, a classe lateral à direita módulo N, determinada por x, é igual a classe lateral à esquerda módulo N, determinada por x, $\forall x \in G$.*
2. *Se G é abeliano, todo subgrupo de G é normal.*
3. *No caso de N ser subgrupo normal de G, indicaremos por G/N o conjunto das classes laterais à esquerda (que é o mesmo das classes laterais à direita) módulo N em G.*

Propriedades Seja N um subgrupo normal de G. Então vale:

(a) $(a.N).(b.N) = (a.b).N$, $\forall a, b \in G$.

(b) $[(a.N).(b.N)].(c.N) = (a.N).[(b.N).(c.N)]$, $\forall a, b, c \in G$.

(c) $\forall a \in G \Rightarrow (a.N).(e.N) = (e.N).(a.N) = a.N$.

(d) $\forall a \in G \Rightarrow (a.N).(a^{-1}.N) = (a^{-1}.N).(a.N) = a.N = N$

Isto tudo nos mostra que $(G/N, \cdot)$ é um grupo.

Definição 4.6.2. *O conjunto G/N é um grupo chamado grupo quociente de G por N. É claro que a existência de G/N pressupõe que N seja normal.*

Exemplo 4.6.1. *Em cada caso, determine o grupo de quociente de G por H.*

(a) $G = \{1, i, -1, -i\}$ *e* $H = \{1, -1\}$.

(b) $G = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ *e* $H = \{\overline{0}, \overline{3}\}$.

Definição 4.6.3. *Seja G um grupo multiplicativo e consideremos A e B dois subconjuntos quaisquer de G. Indicaremos por $A.B$ e chamaremos de produto de A por B o seguinte subconjunto de G:*

$$A.B = \emptyset \text{ se } A = \emptyset \text{ ou } B = \emptyset$$

ou

$$A.B = \{x.y | x \in A \text{ e } y \in B\} \text{ se} A \neq \emptyset \text{ e } B \neq \emptyset.$$

Exemplo 4.6.2. *Seja $G = \{e, a, b, c\}$ u grupo de Klein. Sua tábua é a seguinte:*

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Se $A = \{e, a\}$ e $B = \{b, c\}$ então
$A.B = \{e.b, e.c, a.b, a.c\} = \{b, c, c, b\} = \{b, c\} = B$

Exemplo 4.6.3. *Construa a tábua dos grupos G/H do exemplo 4.6.1.*

4.7 Teorema Do Homomorfismo

Proposição 4.7.1. *Seja $f : G \to L$ um homomorfismo de grupos. Se N é um subgrupo normal de G, então a aplicação $f : G \to G/N$ definida por $f(a) = a.N$ é um homomorfismo sobrejetor.*

Demonstração. □

Definição 4.7.1. *Se N é um subgrupo normal de G, então o homomorfismo $f : G \to G/N$ definida por $f(a) = a.N$ é chamado de* **homomorfismo canônico** *de G sobre G/N.*

Proposição 4.7.2. *Com as hipóteses da Proposição 4.7.1, $N = Ker f$, logo $Ker f$ é um subgrupo normal de G.*

Demonstração. □

Lema 4.7.1. *Se $f : G \to L$ é um homomorfismo de grupos, então $Ker(f) = N$ é um subgrupo normal de G, e portanto G/N tem uma estrutura de grupos.*

Demonstração. □

Teorema 4.7.1. Teorema do Homomorfismo Para Grupos *Seja $g : G \to L$ um homomorfismo sobrejetor de grupos. Se $N = \ker f$, então o grupo quociente G/N é isomorfo ao grupo L.*

Demonstração. □

Exemplo 4.7.1. *Seja $m \in \mathbb{Z}$, $m > 1$. Mostre que $\mathbb{Z}/[m]$ e $\mathbb{Z}_m$ são isomorfos.*

4.8 Exercícios

1. Escreva sobre os seguintes grupos:

   (a) Grupos de permutações

   (b) Grupos de Rotações

   (c) Grupos diedrais.

   Observação, estes grupos se encontram no livro de Álgebra Moderna, nas páginas 83 a 88

2. Mostrar que o conjunto $E = \{a + b\sqrt{2} \in \mathbb{R}^* \mid a, b \in \mathbb{Q}\}$ é um grupo multiplicativo abeliano.

3. Consideramos o conjunto dos números reais $\mathbb{R}$ munido da operação $*$ definida por $x * y = x + y - 3$. Mostrar que $(\mathbb{R}, ast)$ é um grupo abeliano.

4. Verifique se $\mathbb{Z} \times \mathbb{Z}$ é um grupo em relação a alguma das seguintes operações:

   (a) $(a, b) + (c, d) = (a + c, b + d)$

   (b) $(a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$

5. Mostrar que cada uma das tábuas abaixo define uma operação que confere ao conjunto $E = \{e, a, b, c\}$ um estrutura de grupo

(a)

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(b)

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

6. Construir a tábua de um grupo $G = \{e, a, b, c, d, f\}$, de ordem 6, sabendo que:

(I) G é abeliano;

(II) o elemento neutro é o elemento e;

(III) $a * f = b * d = e$;

(IV) $a * d = b * c = f$;

(V) $a * c = b * b = d$;

(VI) $c * d$.

7. Mostrar que se x é o elemento de um grupo multiplicativo e $x.x = x$, então x é o elemento neutro.

8. Se G é um grupo multiplicativo e $x.x = 1$, $\forall x \in G$, então G é abeliano. Sugestão $(x.y)^2 = 1$.

9. Verificar se são subgrupos:

   (a) $\{x \in \mathbb{Q} \mid x > 0\}$, de $(\mathbb{Q}^*, \cdot)$

   (b) $\{0, \pm 2, \pm 4, ...\}$, de $(\mathbb{Z}, +)$

   (c) $\{x \in \mathbb{C} \mid |z| = 1\}$, de $(\mathbb{C}^*, \cdot)$

   (d) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, de $(\mathbb{R}, +)$

10. Mostrar que as matrizes do tipo $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, com $a, b \in \mathbb{R}$ e não nulos simultaneamente, constituem um subgrupo do grupo linear $GL_2(\mathbb{R})$.

11. Provar que se H_1 e H_2 são subgrupos de um grupo G, então $H_1 \cap H_2$ é um subgrupo de G.

12. Verificar em cada caso, se f é um homomorfismo.

    (a) $f : \mathbb{Z} \to \mathbb{Z}$ dada por $f(x) = a.x$, sendo $\mathbb{Z}$ o grupo aditivos dos inteiros e a um número inteiro dado

    (b) $f : \mathbb{R}^* \to \mathbb{R}^*$ dada por $f(x) = |x|$, sendo $\mathbb{R}^*$ o grupo multiplicativo dos reais.

    (c) $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ dada por $f(x) = (x, 0)$, sendo $\mathbb{Z}$ e $\mathbb{Z} \times \mathbb{Z}$ denotam grupos aditivos.

    (d) $f : \mathbb{Z} \to \mathbb{R}_+^*$ dada por $f(x) = 2^x$, onde $\mathbb{Z}$ é o grupo aditivo e $\mathbb{R}_+^*$ é grupo multiplicativo.

13. Determinar os homomorfismos injetor e os sobrejetor do exercício anterior.

14. Determinar o núcleo em cada homomorfismo do exercício 12.

15. A aplicação $f = \{(\overline{0}, e), (\overline{1}, a), (\overline{2}, b), (\overline{3}, c)\}$ é um isomorfismo do grupo $(\mathbb{Z}_4, +)$ no grupo $(G, .)$. Construir a tábua de G, calcular a^2 e b^{-3}.

16. Construir a tábua de um grupo $G = \{e, a, b, c\}$ que seja isomorfo ao grupo multiplicativo $H = \{1, -1, i, -i\}$.

17. Construa os seguintes subgrupos:

    (a) $[-1]_+$ em $(\mathbb{Q}, +)$;

    (b) $[3]_+$ em $(\mathbb{Z}, +)$;

    (c) $[3]_+$ em $(\mathbb{Q}^*, \cdot)$;

    (d) $[i]_+$ em $(\mathbb{C}^*, \cdot)$;

18. Mostre que todo grupo de ordem 2 ou 3 é cíclico.

19. Mostre que $(\mathbb{Z}_m, +)$ é cíclico.

20. Mostre que todo subgrupo $H \neq \{e\}$ de um grupo cíclico infinito é também infinito.

21. A tábua abaixo define uma operação $\cdot$ que confere ao conjunto $E = \{e, a, b, c, d, f\}$ uma estrutura de grupo. Pede-se determinar:

    (a) o subgrupo gerado por b

    (b) o período de d

    (c) os geradores de g

    (d) $x \in G$ tal que $bxc = d^{-1}$

$\cdot$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	d	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

22. Seja $G = \{e, a, b, c, d, f, g, h\}$ um grupo cuja tábua está abaixo. Pede-se determinar:

    (a) o subgrupo gerado por b

    (b) o período de d

(c) os geradores de G

(d) $x \in G$ tal que $axb^{-1} = d$

$\cdot$	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	d	c	g	f	e	h	b
b	b	h	d	a	g	c	e	f
c	c	b	f	d	h	g	a	e
d	d	f	g	h	e	a	b	c
f	f	e	h	b	a	d	c	g
g	g	c	e	f	b	h	d	a
h	h	g	a	e	c	b	f	d

23. Mostre que o único elemento de um grupo de período um é o elemento neutro.

24. Seja $a \neq e$ um elemento de um grupo G. Prove que $o(a) = 2$ se, e somente se, $a = a^{-1}$.

25. Sejam a e b elementos de um grupo multiplicativo G. Suponha $o(ab) = h > 0$, mostre que $o(ba) = h$.

26. Seja $G = [a]$ um grupo cíclico de ordem h. Mostre que: $a^t \in G$ é um gerador de G se, e somente se, $mdc(h, t) = 1$.

27. Determinar todas as classes laterais de $H = \{\overline{0}, \overline{2}\}$ no grupo aditivo $\mathbb{Z}_4$.

28. Determinar todas as classe laterais de $3\mathbb{Z}$ no grupo aditivo $\mathbb{Z}$.

29. Se H é um subgrupo de G tal que $(G : H) = 2$, mostre que $aH = Ha$, $\forall a \in G$.

30. Seja $G = [a]$ um grupo cíclico de ordem 6. Sendo $H = [a^2]$, construa a tábua do grupo G/H.

31. Construa a tábua dos seguintes grupos quocientes:

    (a) $\mathbb{Z}_8/H$, onde $H = \{\overline{0}, \overline{4}\}$

    (b) $\mathbb{Z}/2\mathbb{Z}$.

32. Sejam M e N subgrupos normais de G. Mostre que $M \cap N$ e MN também o são.

33. Seja G um grupo multiplicativo. Mostre que $H = \{x \in G | xa = ax, \forall a \in G\}$ é um subgrupo normal de G.

Capítulo 5

Anéis

5.1 Anéis e Propriedades

Definição 5.1.1. *Um conjunto não vazio A munido de 2 operações:*

$$(x, y) \to x + y$$

$$(x, y) \to x.y$$

é chamado **anel** *se:*

(i) $(A, +)$ *é um grupo abeliano.*

(ii) *A multiplicação é associativa, isto é: se* $a, b, c \in A$ *então* $a.(b.c) = (a.b).c$.

(iii) *A multiplicação é distributiva em relação a adição:se* $a, b, c \in A$, *então* $a.(b + c) = a.b + a.c$

Notação: (A,+,·)

Alguns Anéis Importantes:

1. **Anéis Numéricos**:

   - Anel dos inteiros:$(\mathbb{Z}, +, \cdot)$;

- Anel dos racionais:$(\mathbb{Q}, +, \cdot)$;
- Anel dos reias:$(\mathbb{R}, +, \cdot)$;
- Anel dos Complexos:$(\mathbb{C}, +, \cdot)$.

2. **Anel das classes de resto módulo** m
   Seja $\mathbb{Z}_m = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}$, $m > 1$ em relação as operações definidas por $\overline{a} + \overline{b} = \overline{a+b}$ e $\overline{a}.\overline{b} = \overline{a.b}$. Lembramos que o zero desse anel é classe $\overline{0}$ e que o oposto de $\overline{a} \in \mathbb{Z}_m$ é a classe $\overline{m-a}$.

   Observação 5.1.1. *As vezes escreveremos apenas* $\mathbb{Z}_m = \{0, 1, ..., m-1\}$ *e lembramos que* $a + b$ *é igual ao resto da divisão de* $a + b$ *por* m *e* $a.b$ *é igual ao resto da divisão de* $a.b$ *por* m. *Por exemplo,* $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ *logo* $2 + 2 = 0$ *e* $2.3 = 2$.

3. **Anéis de Matrizes**
   São anéis: $(M_n(\mathbb{Z}), +, \cdot)$,$(M_n(\mathbb{Q}), +, \cdot)$,$(M_n(\mathbb{R}), +, \cdot)$ e $(M_n(\mathbb{C}), +, \cdot)$. Em geral, se A é um anel, então o conjunto $(M_n(A), +, \cdot)$ das matrizes $n \times n$ sobre A é um anel.

   Por exemplo, $(M_n(\mathbb{Z}_3), +, \cdot)$ é um anel, e se $A = \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{2} & \overline{1} \end{pmatrix}$ e $B = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{2} \end{pmatrix}$, então $A + B = \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{2} & \overline{0} \end{pmatrix}$ e $A.B = \begin{pmatrix} \overline{2} & \overline{2} \\ \overline{2} & \overline{1} \end{pmatrix}$

4. **Anéis de Funções**

   Seja $A = \mathbb{Z}^{\mathbb{Z}} = \{f | f : \mathbb{Z} \to \mathbb{Z}\}$. Dadas duas funções quaisquer $f, g \in A$, definindo $f + g$ e $f.g$ da seguinte forma:

$$f + g : \mathbb{Z} \to \mathbb{Z} \text{ por } (f + g)(x) = f(x) + g(x), \forall x \in \mathbb{Z}.$$
$$f.g : \mathbb{Z} \to \mathbb{Z} \text{ por } (f.g)(x) = f(x).g(x), \forall x \in \mathbb{Z}.$$

   Temos definidas uma adição e uma multiplicação em A. Nessas condições A é um anel, o anel das funções de $\mathbb{Z}$ em $\mathbb{Z}$.(Verifique!)

   Da mesma forma introduzem-se os anéis $\mathbb{Q}^{\mathbb{Q}}$,$\mathbb{R}^{\mathbb{R}}$ e $\mathbb{C}^{\mathbb{C}}$. De um modo geral, se A é um anel e X é um conjunto não vazio, então pode-se transformar A^X em anel. Por exemplo, se $X = \{a, b\}$ e $A = \mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ então o anel A^X das aplicações de X em $\mathbb{Z}_2$ são constituídas de 4 elemento:

- $f(a) = 0$ e $f(b) = 0$;
- $g(a) = 1$ e $g(b) = 1$;
- $h(a) = 0$ e $h(b) = 1$;
- $j(a) = 1$ e $f(b) = 0$.

5. **Produtos Diretos**

   Sejam A, B anéis quaisquer e consideramos o produto cartesiano $A \times B$. Definimos a soma e o produto dos elementos de $A \times B$ do seguinte modo:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1) + (a_2, b_2) = (a_1.a_2, b_1.b_2).$$

   Logo $(A \times B, +, \cdot)$ é um anel chamado de produto direto de $A \times B$. (Verifique!)

Propriedades Imediatas de um anel:

Consideremos um anel $(A, +, \cdot)$.

1. Em relação a operação de adição, A é um grupo abeliano, então são verdadeiras as seguintes propriedades:
   - O zero do anel A é único.
   - $\forall a \in A$, existe um único simétrico aditivo.
   - Dados $a_1, a_2, ..., a_n \in A$ com $n \geq 2$, então $-(a_1 + a_2 + ... + a_n) = (-a_1) + (-a_2) + ... + (-a_n)$.
   - $\forall a \in A,\ (-(-a)) = a$.
   - $\forall a, x, y$ se $a + x = a + y \Rightarrow x = y$, ou seja, todo elemento de A é regular em relação a adição.
   - A equação $a + x = b$ tem apenas uma solução, o elemento $b + (-a)$.
2. Se $a \in A$ então $a.0 = 0.a = 0$.
3. Se $a, b \in A$, então $a.(-b) = (-a).b = -(a.b)$.
4. Se $a, b \in A$ então $(-a).(-b) = a.b$

Definição 5.1.2. *Sejam $a, b \in A$, Chama-se diferença entre a e b e indica-se por $a - b$ o elemento $a + (-b) \in A$. Assim,*

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

5. Se $a, b, c \in A$, então $a(b - c) = ab - ac$.

Definição 5.1.3. *Dados $a \in A$ e $n \in \mathbb{N}^*$, defini-se a^n por recorrência do seguinte modo:*

$$\begin{cases} a^1 = a \\ a^n = a^{n-1}.a \quad \forall n > 1 \end{cases}$$

6. $\forall a \in A$ e $\forall m, n \in \mathbb{N}^*$ temos:

   - $a^m.a^n = a^{m+n}$.
   - $(a^m)^n = a^{m.n}$.

Definição 5.1.4. *Um anel $(A, +, \cdot)$ em que o conjunto A é finito, chama-se* **anel finito**.

Exemplo 5.1.1. *Os anéis $\mathbb{Z}_m$ com $m > 1$ são exemplos importantes de anéis finitos. Vamos construir as tábuas do anel $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.*

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{(3)}$
$\overline{0}$				
$\overline{1}$				
$\overline{2}$				
$\overline{3}$				

e

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{(3)}$
$\overline{0}$				
$\overline{1}$				
$\overline{2}$				
$\overline{3}$				

5.2 Subanéis

Definição 5.2.1. *Seja $(A, +, \cdot)$ um anel e $L \subset A$, $L \neq \emptyset$. Dizemos que L é um subanel de A se:*

(i) L é fechado para ambas as operações de A, isto é: $\forall a, b \in L \Rightarrow a + b \in L$ e $a.b \in L$.

(ii) $(L, +, .)$ também é um anel.

Exemplos 5.2.1. *Exemplos de subanéis.*

1. *$\mathbb{Z}$ é subanel de $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\mathbb{Q}$ é subanel de $\mathbb{R}, \mathbb{C}$ e $\mathbb{R}$ é subanel de $\mathbb{C}$.*

2. *$2\mathbb{Z}$ é subanel de $\mathbb{Z}$.*

3. *$M_n(L)$ é subanel de $M_n(A)$ desde que L seja subanel de A.*

Proposição 5.2.1. *Sejam A um anel e $L \subset A$, com $L \neq \emptyset$. Então L é um subanel de A se, e somente se, $a - b \in L$ e $a.b \in L$, $\forall a, b \in L$.*

Demonstração. □

Exemplo 5.2.1. *Verifique em cada caso se L é um subanel de A usando a Proposição 5.2.1.*

(a) $L = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} | a, b \in \mathbb{Z} \right\}$ *e* $A = M_2(\mathbb{Z})$.

(b) $L = \{a + b.\sqrt{2} | a, b \in \mathbb{Z}\}$ *e* $A = \mathbb{R}$.

(c) $L = \{f \in A | f(1) = 0\}$ *e* $A = \mathbb{R}^{\mathbb{R}}$*(anel das funções reais de uma variável real).*

(d) L *é um subanel de* $\mathbb{Z}$ *se* $L = \{0, \pm 1, \pm 2, \pm 3, ...\}$ *com* $n \in \mathbb{Z}$. *Denotamos* $L = n.\mathbb{Z}$.

5.3 Tipos de Anéis

Definição 5.3.1. *Dizemos que um anel A é um* **anel comutativo** *se*

$$\forall a, b \in A \Rightarrow a.b = b.a.$$

Exemplos de anéis comutativo:

(a) Os anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ são anéis comutativo.

(b) Os anéis $\mathbb{Z}_m$, com $m > 1$ são comutativo, pois $\forall \overline{a}, \overline{b} \in \mathbb{Z}_m$, temos $\overline{a}.\overline{b} = \overline{b}.\overline{a}$.

(c) Os anéis de funções A^X são comutativo, sempre que A é comutativo.

Contra-exemplo de anéis que não comutativo, são os anéis $M_n(A)$(com $n > 1$) em que A indica $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Definição 5.3.2. *Dizemos que A é um* **anel com unidade** *se A possui elemento neutro da multiplicação, isto é, se $\exists 1_A \in A$, com $1_A \neq 0_A$, tal que:*

$$a.1_A = 1_A.a = a, \ \forall a \in A.$$

Dizemos que 1_A é a unidade do anel A.

Exemplos de anéis com unidade:

(a) Os anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ são anéis com unidade, cuja unidade é o elemento 1.

(b) O anel $\mathbb{Z}_m$, com $m > 1$ é um anel com unidade, cuja unidade é o elemento $\overline{1}$.

(c) O anel $M_n(A)$ em que A indica $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, é un anel com unidade, cuja unidade é a matriz identidade I_n.

(d) Se o anel A possui unidade, então o anel A^X também é um anel com unidade.

Um contra-exemplo de anel que não possui unidade, são os anéis $n.\mathbb{Z}$ quando $n \neq \pm 1$.

Definição 5.3.3. *Um anel cuja multiplicação é comutativa e que possui unidade é chamado de* **anel comutativo com unidade.**

Definição 5.3.4. *Se A é um anel com unidade e se B é um subanel de A tal que existe unidade de B, e $1_A = 1_B$, então diremos que B é um* **subanel unitário de** *A.*

Vejamos alguns exemplos:

(a) $2\mathbb{Z}$ é um subanel de $\mathbb{Z}$. Existe a unidade de $\mathbb{Z}$, mas não existe a unidade de $2\mathbb{Z}$.

(b) $\mathbb{Z}$ é subanel de $\mathbb{Q}$ e ambos admitem a mesma unidade.

(c) Note que $\{0\} \times \mathbb{Z}$ é um subanel de $\mathbb{Z} \times \mathbb{Z}$. Logo $(1, 1)$ é a unidade de $\mathbb{Z} \times \mathbb{Z}$ e $(0, 1)$ é a unidade de $\{0\} \times \mathbb{Z}$, pois $(0, 1).(0, a) = (0, a), \forall (0, a) \in \{0\} \times \mathbb{Z}$.

5.4 Anéis de Integridade e Corpos

Considere os anéis $\mathbb{Z}$ e $\mathbb{Z}^{\mathbb{Z}}$, ambos comutativo com unidade.

Note que, $\forall a, b \in \mathbb{Z}$, se $a.b = 0$ então $a = 0$ ou $b = 0$. Mas no anel $\mathbb{Z}^{\mathbb{Z}}$ não acontece o mesmo. Por exemplo, considere as funções $f, g : \mathbb{Z} \to \mathbb{Z}$ definidas por:

$$f(0) = 1 \; e \; f(x) = 0, \forall x \neq 0$$

e

$$g(0) = 0 \; e \; g(x) \neq 1, \forall x \neq 0.$$

Ambas as funções são não nulas. Apesar disso o produto $f.g$ é nulo, pois:

$$(f.g)(0) = f(0).g(0) = 1.0 = 0$$

e $\forall x \neq 0$

$$(f.g)(x) = f(x).g(x) = 0.1 = 0.$$

Definição 5.4.1. *Um anel A comutativo com unidade, onde é verdadeira a seguinte frase:*

$$\forall a, b \in A, \text{ se } a.b = 0_A \Rightarrow a = 0_A \text{ ou } b = 0_A,$$

recebe o nome de **anel de integridade(ou domínio)**.

Observação 5.4.1. .

1. *A frase acima recebe o nome de lei do anulamento do produto.*
2. *Se $a, b \in A$ e $a \neq 0_A$ e $b \neq 0_A$ e $a.b = 0_A$ ou $b.a = 0_A$, dizemos que a e b são* **divisores próprios do zero em** A.

Exemplos:

1. Todos os anéis numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são anéis de integridade.
2. No anel $\mathbb{Z}_6$ os elementos $\overline{2}$ e $\overline{3}$ são divisores próprios do zero, pois $\overline{2}.\overline{3} = \overline{0}$. Em geral, se $m > 1$ é um inteiro composto, isto é, $a.b = m$, então $\mathbb{Z}_m$ não é un anel de integridade, basta observar que $\overline{a}.\overline{b} = \overline{a.b} = \overline{m} = \overline{0}$.

Proposição 5.4.1. *$\mathbb{Z}_m$ é um anel de integridade se, e somente se, m é um número primo.*

Demonstração. □

Proposição 5.4.2. *U anel A comutativo com unidade é um anel de integridade se, e somente se, todo elemento não nulo de A é regular em relação à multiplicação:($\forall a, b, c \in A, a \neq 0$ e $a.b = a.ac \Rightarrow b = c$.)*

Demonstração. □

Definição 5.4.2. *Um anel K, comutativo com unidade, recebe o nome de* **corpo**, *se todo elemento não nulo de K admite o simétrico multiplicativo, ou seja:*

$$\forall a \in K, a \neq 0_K \Rightarrow \exists b \in K | a.b = 1_K.$$

Observação 5.4.2. .

1. *O elemento b é chamado de inverso de a e será indicado por a^{-1}.*

2. *Indicamos por $U(A)$ o subconjunto de A formado pelos elementos de A que admitem inverso.*

3. *Assim, K é um corpo, se $U(K) = K - 0$*

Exemplos:

1. O anel $\mathbb{Z}$ não é um corpo, pois $U(\mathbb{Z}) = \{1, -1\}$.

2. Os anéis numéricos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ são corpos.

3. O anel $\mathbb{R}^{\mathbb{R}}$ é comutativo com unidade, mas não é corpo. De fato, considere a função $f : \mathbb{R} \to \mathbb{R}$ dada por $f(0) = 0$ e $f(x) = 1$, $\forall x \neq 0$. Note que f não é inversível, pois não existe nenhuma função $g : \mathbb{R} \to \mathbb{R}$ tal que $f.g = e$(função constante 1), pois:

$$(f.g)(0) = f(0).g(0) = 0.g(0) = 0 \neq e(0) = 1.$$

Proposição 5.4.3. *Todo corpo K é um anel de integridade.*

Observação 5.4.3. *A recíproca da Proposição 5.4.3 não é verdadeira, pois $\mathbb{Z}$ é anel de integridade, mas não é um corpo.*

Proposição 5.4.4. *Todo anel de integridade finito é um corpo.*

Demonstração. □

5.5 Homomorfismo-Isomorfismo de Anéis

5.5.1 Homomorfismos

Definição 5.5.1. *Sejam $(A, +, .)$,$(B, +, .)$ anéis. Uma aplicação $f : A \to B$ é chamada de* **homomorfismo de A em B,** *se $\forall x, y \in A$:*

(i) $f(x + y) = f(x) + f(y)$

(ii) $f(x.y) = f(x).f(y)$.

Exemplos de Homomorfismos:

1. Sejam A e B anéis quaisquer e $f : A \to B$, $f(x) = 0_B$,$\forall x \in A$. Então f é um homomorfismo de anéis.(Verifique!)

2. Sejam $A = \mathbb{Z}$ e $B = \mathbb{Z} \times \mathbb{Z}$(produto direto) e a aplicação $f : A \to B$ definido por $f(n) = (n, 0)$, logo f é um homomorfismo de anéis.(Verifique!)

3. Sejam $A = \mathbb{Z}$ e $B = \mathbb{Z}_m (m > 1)$. A aplicação $p_m : \mathbb{Z} \to \mathbb{Z}_m$ definida por $p_m(r) = \overline{r}$, $\forall r \in \mathbb{Z}$ é um homomorfismo de anéis.(Verifique!)

4. Sejam $A = \mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2} | m, n \in \mathbb{Z}\}$ e $f : A \to A$ definida por $f(m + n\sqrt{2}) = m - n\sqrt{2}$ é um homomorfismo de anéis.(Verifique!)

5.5.2 Proposições sobre Homomorfismo de Anéis

Proposição 5.5.1. *Se $f : A \to B$ é um homomorfismo de anéis, então:*

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

(ii) $f(-a) = -f(a)$;

(iii) $f(a - b) = f(a) - f(b)$.

Estas propriedades decorrem do fato de que f é um homomorfismo do grupo aditivo A no grupo aditivo B.

Proposição 5.5.2. *Seja $f : A \to B$ um homomorfismo sobrejetor de anéis e suponhamos que A possui unidade. Então:*

(i) $f(1_A)$ *é a unidade de B, logo B também é um anel com unidade;*

(ii) Se $a \in A$ é inversível, então $f(a)$ também é, e $[f(a)]^{-1} = f(a^{-1})$.

Demonstração. □

Proposição 5.5.3. *Sejam $f : A \to B$ um homomorfismo de anéis e L um subanel de A, então $f(L)$ é um subanel de B.*

Demonstração. □

Proposição 5.5.4. *Sejam $f : A \to B$ e $g : B \to C$ homomorfismos de anéis, então $g \circ f : A \to C$ também é um homomorfismo de anéis.*

5.5.3 Núcleo de um Homomorfismo de Anéis

Definição 5.5.2. *Dado um homomorfismo de anéis $f : A \to B$ o* **núcleo** *de f é o subconjunto $N(f) \subset A$, definido por:*

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

Observação 5.5.1. *Note que $N(f) \neq \emptyset$, pois $f(0_A) = 0_B$. Uma outra notação usada para o núcleo de f é $Ker(f) = N(f)$.*

Exemplo 5.5.1. *Determine o núcleo para os seguintes homomorfismos:*

(a) Seja $f : A \to B$ definida por $f(x) = 0_B$, $\forall x \in A$.

(b) Seja $p_m : \mathbb{Z} \to \mathbb{Z}$ definida por $p_m(r) = \overline{r}$, $\forall r \in \mathbb{Z}$.

(c) Seja $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, definida por $f(x) = (x, 0)$, $\forall x \in \mathbb{Z}$.

(d) Seja $f : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$, definida por $f(a + b\sqrt{2}) = a - b\sqrt{2}$, $\forall a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

Proposição 5.5.5. *Seja $f : A \to B$ um homomorfismos de anéis, Então:*

(a) $N(f)$ é um subanel de A.

(b) f é injetora se, e somente se, $N(f) = \{0_A\}$.

Demonstração. □

5.5.4 Isomorfismo de Anéis

Definição 5.5.3. *Sejam A e B anéis quaisquer. Uma aplicação $f : A \to B$ é chamada* **isomorfismo** *de A em B se:*

(i) f é bijetora;

(ii) f é um homomorfismo de anéis.

Observação 5.5.2. *:*

1. *Todos os resultados válidos para homomorfismos de anéis também são válidas para isomorfismos.*

2. *Um isomorfismo do anel A no anel B é em particular um isomorfismo do grupo aditivo $(A,+)$ no grupo aditivo $(B, +)$.*

Exemplos de Isomorfismos

1. A aplicação identidade $i_A : A \to A$, definida por $i_A(x) = x$ é um isomorfismo de anéis. (Verifique!)

2. A aplicação $f : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$, definida por $f(a+b\sqrt{2}) = a-b\sqrt{2}$ é um isomorfismo de anéis.(Verifique!)

3. A aplicação $f : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ definida por $f(\overline{a}_6) = (\overline{a}_2, \overline{a}_3)$ é um isomorfismo de anéis.(Verifique!)

Proposição 5.5.6. *Seja $f : A \to B$ um isomorfismo de anéis. Então $f^{-1} : B \to A$ também é um isomorfismo de anéis.*

Assim, pela Proposição 5.5.6, se $f : A \to B$ um isomorfismo de anéis, dizemos que A e B são isomorfos.

Exercício: Mostre que nenhuma aplicação de $\mathbb{Z}_4$ em $\mathbb{Z}_2 \times \mathbb{Z}_2$ é um isomorfismo. Ou seja, $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$ não são isomorfos.

5.6 Exercícios

1. Considere em $\mathbb{Z} \times \mathbb{Z}$ as operações $+$ e $\cdot$, definidas por: $(a, b) + (c, d) = (a + c, b + d)$ e $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$. Mostre que $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ é um anel comutativo com unidade.

2. Consideremos as operações $*$ e $\triangle$ em $\mathbb{Q}$, definidas por: $x * y = x + y - 3$ e $x \triangle y = x + y - \frac{xy}{3}$. Mostre que $(\mathbb{Q}, *, \triangle)$ é um anel comutativo com unidade.

3. Sabe-se que $A = \{a, b, c, d\}$ e $(A, +, \cdot)$ é um anel em que os elementos neutros das operações $+$ e $\cdot$ são, respectivamente, a e b. Conhecendo-se os compostos $b + b = a$, $c + c = a$, $cd = a$, construir as tábuas das duas operações.

4. Verifique quais dos seguintes subconjunto de $\mathbb{Q}$ são subanéis:

   (a) $\mathbb{Z}$;

   (b) $B = \{x \in \mathbb{Q} | x \notin \mathbb{Z}\}$;

   (c) $C = \{\frac{a}{2^n} \in \mathbb{Q} | a \in \mathbb{Z} \; e \; n \in \mathbb{Z}\}$.

5. Verifique se o conjunto $L = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ é um subanel do anel $\mathbb{R}$.

6. Quais dos conjuntos abaixo são subanéis de $M_2(\mathbb{R})$?

   (a) $L_1 = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} | a, b \in \mathbb{R} \right\}$;

   (b) $L_2 = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} | a, b, c \in \mathbb{R} \right\}$.

7. Se B e C são subanéis de A, então mostre que $B \cap C$ é subanel de A.

8. Determinar o conjunto dos elementos regulares para a multiplicação e o conjunto dos elementos inversíveis de cada um dos seguintes anéis:

   (a) $\mathbb{Z}$

   (b)$\mathbb{Q}$

   (c)$\mathbb{Z} \times \mathbb{Z}$(produto direto)

   (d)$\mathbb{Z}_3$

9. .

   (a) Quais são os elementos inversíveis do anel $\mathbb{Z}_{18}$

   (b) Resolver em $\mathbb{Z}_{18}$ o sistema:

$$\begin{cases} \overline{5}x & + & \overline{2}y & = & \overline{1} \\ \overline{x} & + & \overline{11}y & = & \overline{7} \end{cases}$$

   Definição 5.6.1. *Dado um corpo K, um subconjunto $M \subset K$, $M \neq \emptyset$, se diz subcorpo de K se:*

   (a) $1 \in M$*;*

   (b)$a, b \in M \Rightarrow a - b \in M$*;*

   (c)$a, b \in M$ *e* $b \neq 0 \Rightarrow a \cdot b^{-1} \in M$

10. Verifique se são subcorpos:

    (a) $M = \{0, 1\}$ de um coro K qualquer;

    (b)$M = \{a + bi | a, b \in \mathbb{Q}\}$ do corpo $\mathbb{C}$;

    (c)$M = \{a + b\sqrt{3} | a, b \in \mathbb{Q}\}$ do corpo $\mathbb{R}$.

11. Provar que se M_1 e M_2 são subcorpos de um corpo K, então $M_1 \cap M_2$ é um subcorpo de K.

12. Verificar em cada caso, se $f : A \to B$ é um homomorfismo do anel A no anel B. E quando f for um homomorfismo, determinar o núcleo.

(a) $A = \mathbb{Z}$, $B = \mathbb{Z}$ e $f(x) = x + 1$;

(b) $A = \mathbb{Z}$, $B = \mathbb{Z}$ e $f(x) = 2x$;

(c) $A = \mathbb{Z}$, $B = \mathbb{Z} \times \mathbb{Z}$ e $f(x) = (x, 0)$;

(d) $A = \mathbb{Z} \times \mathbb{Z}$, $B = \mathbb{Z}$ e $f(x, y) = x$;

(e) $A = \mathbb{Z} \times \mathbb{Z}$, $B = \mathbb{Z} \times \mathbb{Z}$ e $f(x, y) = (0, y)$;

(f) $A = \mathbb{Z} \times \mathbb{Z}$, $B = \mathbb{Z} \times \mathbb{Z}$ e $f(x, y) = (2x, 0)$.

13. Mostre que $f : \mathbb{C} \to M_2(\mathbb{R})$, dada por $f(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, $\forall a, b \in R$ é um monomorfismo de anéis.

Capítulo 6

Anéis de Polinômios

Definição 6.0.2. *Uma função $f : \mathbb{N} \to A$, definida por $f(a_i) = a_i$ é chamada* **sequência** *de elementos de A, onde A é um anel. Tal sequência é indicado por:*

$$f = (a_1, a_2, ..., a_i, ...).$$

Os elementos $a_0, a_1, ..., ai, ...$ são chamados termos da sequência.

Notação: $f = (a_i)_{i \in \mathbb{N}}$.

Igualdade:

Dados duas sequências $f = (a_i)$ e $g = (b_i)$ de elementos de um anel. Então dizemos que duas sequências são iguais($f = g$), se $a_i = b_i \ \forall i \in \mathbb{N}$

Adição:

Dados duas sequências $f = (a_i)$ e $g = (b_i)$ de elementos de um anel, chama-se **soma** de f com g a sequência $h = (c_i)$ tal que $c_i = a_i + b_i$, $\forall i \in \mathbb{N}$.

Exemplos:

1. Se $f = (a_i)$ tal que $a_i = 2i$ e $g = (b_i)$ tal que $b_i = i + 1$ são duas sequências sobre $\mathbb{R}$, sua soma é $h = (c_i)$, onde:

   $$c_i = a_i + b_i = 2i + (i + 1) = 3i + 1, \forall i \in \mathbb{N}.$$

   Portanto $h = (1, 4, 7, 10, 13, ..., 3i + 1, ...)$.

2. Se $f = (1, 2, 4, 8, 16, 32, ..., 2^i, ...)$ e $g = (0, 0, 0, ..., 0, ...)$ então $h = f + g =$
   $= (1, 2, 4, 8, 16, 32, ..., 2^i, ...)$.

3. Se $f = (3, 2, 1, 0, 0, 0, ..., 0, ...)$ e $g = (4, 4, 4, 4, 0, 0, ..., 0, ...)$ então $h = f + g = (7, 6, 5, 4, 0, 0, 0, ..., 0, ...)$.

Multiplicação:

Dadas duas sequências $f = (a_i)$ e $g = (b_i)$ sobre um anel A, chama-se produto de f por g a sequência $h = (c_k)$, tal que:

$c_0 = a_0.b_0$
$c_1 = a_0.b_1 + a_1.b_0$
$c_2 = a_0.b_2 + a_1.b_1 + a_2.b_0$
$c_3 = a_0.b_3 + a_1.b_2 + a_2.b_1 + a_3.b_0$
.....
$c_k = a_0.b_k + a_1.b_{k-1} + a_2.b_{k-2} + ... + a_k.b_0$
.....

isto é:

$$c_k = \sum_{i=0}^{k} a_i b_{k-i},\ \forall k \in \mathbb{N}.$$

Exemplos:

1. Calcular os seis termos iniciais do produto das sequências $f = (a_i)$ tal que $a_i = i$ e $g = (b_i)$ tal que $b_j = 2.j$, sobre $\mathbb{R}$.

2. Calcular o produto das sequências $f = (2, 1, 0, 0, 0, ...)$ e $g = (3, 4, 5, 0, , 0, 0, ...)$ sobre $\mathbb{R}$.

Dispositivo Prático:

Para multiplicar o polinômio $f = (a_0, a_1, a_2, ..., a_n, 0, 0, 0, ...)$ por $g = (b_0, b_1, b_2, ..., b_m, 0, 0, 0, ...)$ usaremos a seguinte tabela:

Considere $n = 5$ e $m = 5$:

$f \setminus g$	b_0	b_1	b_2	b_3	b_4	b_5
a_0	a_0b_0	a_0b_1	a_0b_2	a_0b_3	a_0b_4	a_0b_5
a_1	a_1b_0	a_1b_1	a_1b_2	a_1b_3	a_1b_4	a_1b_5
a_2	a_2b_0	a_2b_1	a_2b_2	a_2b_3	a_2b_4	a_2b_5
a_3	a_3b_0	a_3b_1	a_3b_2	a_3b_3	a_3b_4	a_3b_5
a_4	a_4b_0	a_4b_1	a_4b_2	a_4b_3	a_4b_4	a_4b_5
a_5	a_5b_0	a_5b_1	a_5b_2	a_5b_3	a_5b_4	a_5b_5

Assim, calculamos todos os produtos $a_i b_j$ e em cada diagonal somamos todos os produtos.

Exemplo 6.0.1. *Construa a tábua do produto de* $f = (4, 3, 2, 1, 0, 0, ..., 0, ...)$ *por* $g = (5, 6, 0, 0, ..., 0, 0, 0, ...)$.

6.1 Sequências Quase-Nulas ou Polinômios

Definição 6.1.1. *Dado um anel* A*, uma sequência* $(a_0, a_1, a_2, ...)$ *sobre* A *recebe o nome de polinômio sobre* A *se existe um índice* $r \in \mathbb{N}$ *tal que* $a_m = 0$, $\forall m > r$.

Observação 6.1.1. *:*

1. *A definição nada impõe para* $a_0, a_1, a_2, ..., a_r$ *que podem ser alguns deles ou mesmo todos iguais a zero.*

2. *Uma sequência é um polinômio, quando apresenta um número finito de termos não nulos.*

Exemplos:

1. A sequência $f = (4, 3, 2, 1, 0, 0, 0, ...)$ onde $a_i = 0$ para $i > 3$ é um polinômio sobre o anel $\mathbb{Z}$.

2. A sequência $(0, 0, 0, 0, ...)$ onde 0 indica o zero do anel A é chamado de polinômio nulo. As sequências $(1, 0, 0, 0, ...)$ e $(0, 1, 0, 0, 0, ...)$ são polinômios sobre A. Já a sequência $(1, 1, 1, 1, ..., 1, ...)$ não é um polinômio sobre A.

3. Dado o anel $A = \mathbb{Z}\times\mathbb{Z}$(produto direto), a sequência $(1, 1), (1, 1), (0, 0), (0, 0), ..., (0, 0), ...$ é um polinômio sobre A. Enquanto a sequência $(1, 0), (1, 0), (1, 0), (1, 0), ..., (1, 0), ...$ não é um polinômio sobre A.

Notação: Denotamos o conjunto dos polinômios sobre o anel A, por $A[X]$.

Proposição 6.1.1. *A soma de dois polinômios sobre* A *também é um polinômio sobre* A.

Demonstração. □

Proposição 6.1.2. *O produto de dois polinômios sobre* A *também é um polinômio sobre* A.

Demonstração. □

Proposição 6.1.3. *Se A é um anel, então $A[X]$ também é um anel.*

Demonstração. □

Proposição 6.1.4. *Se A é um anel comutativo, então $A[X]$ também é um anel comutativo.*

Demonstração. □

Proposição 6.1.5. *Se A é um anel com unidade, então $A[X]$ também é um anel com unidade.*

Demonstração. □

Proposição 6.1.6. *Se A é um anel de integridade, então $A[X]$ também é um anel de integridade.*

Demonstração. □

6.2 Grau de um Polinômio

Definição 6.2.1. *Seja $f = (a_i)$ um polinômio não nulo. Chama-se* **grau de f**, *e representa-se por $gr(f)$ ou ∂f, o número natural n tal que $a_n \neq 0$ e $a_i = 0$, $\forall i > n$.*

Observação 6.2.1. *:*

1. *O termo a_n é chamado de coeficiente dominante de f.*
2. *Se o coeficiente dominante de f é 1(unidade do anel A), diz-se que f é um polinômio unitário.*

Exemplos:

1. O polinômio $f = (4, 7, 0, 2, 0, 0, 0, ..., 0, ...)$ em $\mathbb{Z}[X]$ tem grau 3.
2. O polinômio $g = (-1, \frac{1}{2}, 0, 5, -1, 0, 0, 0, ..., 0, ...)$ em $\mathbb{Q}[X]$ tem grau 4.
3. O polinômio $h = \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, ..., \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, ... \right)$ em $M_2(\mathbb{Z})[X]$ tem grau 0.

Proposição 6.2.1. *Se $f = (a_i)$ e $g = (b_i)$ são dois polinômios não nulos de $A[X]$, então:*

(a) ou $f + g = 0$ ou $\partial(f + g) \leq \max\{\partial f, \partial g\}$.

(b) $\partial(f+g) = \max\{\partial f, \partial g\}$, *quando* $\partial f \neq \partial g$.

Demonstração. □

Exemplo 6.2.1. *Determine o grau de* $f+g$ *nos seguintes casos:*

(a) Em $\mathbb{R}[X]$ *seja* $f = (4, 5, -1, 7, 2, 0, 0, 0, ..., 0, ...)$ *e* $g = (1, 7, 4, 0, 0, ..., 0, ...)$.

(b) Em $\mathbb{Z}[X]$ *seja* $f = (7, 3, -2, 0, 0, 0, 0, 0, ..., 0, ...)$ *e* $g = (-7, -3, 2, 0, 0, ..., 0, ...)$.

(c) Em $\mathbb{Z}_4[X]$ *seja* $f = (\overline{1}, \overline{2}, \overline{3}, \overline{0}, \overline{0}, \overline{0}, ..., \overline{0}, ...)$ *e* $g = (\overline{2}, \overline{1}, \overline{1}, \overline{0}, \overline{0}, ..., \overline{0}, ...)$.

Proposição 6.2.2. *Se* $f = (a_i)$ *e* $g = (b_j)$ *são dois polinômios não nulos de* $A[X]$, *então:*

(a) ou $f.g = 0$ *ou* $\partial(f.g) \leq \partial f + \partial g$.

(b) $\partial(f.g) = \partial f + \partial g$, *quando o coeficiente dominante de* f *ou* g *é regular em* A.

Demonstração. □

Exemplo 6.2.2. *Determine o grau de* $f.g$ *em cada caso:*

(a) Sejam $f = (4, 3, 0, 0, ..., 0, ...)$ *e* $g = (1, 2, 5, 0, 0, ..., 0, ...)$ *em* $\mathbb{R}[X]$.

(b) Sejam $f = (\overline{2}, \overline{2}, \overline{0}, \overline{0}, ..., \overline{0}, ...)$ *e* $g = (\overline{0}, \overline{0}, \overline{2}, \overline{0}, ..., \overline{0}, ...)$ *em* $\mathbb{Z}_4[X]$.

(c) Sejam $f = (\overline{2}, \overline{1}, \overline{3}, \overline{0}, ..., \overline{0}, ...)$ *e* $g = (\overline{1}, \overline{2}, \overline{0}, \overline{0}, ..., \overline{0}, ...)$ *em* $\mathbb{Z}_6[X]$.

Notação Usual dos Polinômios

Consideremos o polinômio $X = (0, 1, 0, 0, ..., 0, ...)$, assim $X^2 = X.X = (0, 0, 1, 0, 0, ..., 0, ...)$, $X^3 = X^2.X = (0, 0, 0, 1, 0, ..., 0, ...)$ e $X^n = X^{n-1}.X = (0, 0, 0, ..., 0, 1, 0, ...)$, ou seja, X^n é um polinômio em que os n primeiros termos são nulos e $a_n = 1$.

Dado um polinômio $f = (a_0, a_1, a_2, ..., a_n, 0, 0, ...)$ em $A[X]$ temos:
$f = (a_0, 0, 0, 0, ..., 0, ...)+(0, a_1, 0, 0, ..., 0, ...)+(0, 0, a_2, 0, ..., 0, ...)+\cdots+(0, 0, ..., 0, a_n, 0, 0, ...) = a_0 + a_1X + a_2X^2 + \cdots + a_xX^n$.

A notação $f = a_0 + a_1X + a_2X^2 + ... + a_nX^n$ é a notação usual para indicar um polinômio.

6.3 Imersão de A em $A[X]$

Observamos que A e $A[X]$ são conjuntos cujos elementos são distintos. Vamos verificar que $A \subset A[X]$.

Proposição 6.3.1. *Se A é um anel, então $L = \{(a, 0, 0, ..., 0, ...)|a \in A\}$ é um subanel de $A[X]$.*

Demonstração. □

Teorema 6.3.1. *Sendo A um anel, A é isomorfo ao subanel $L = \{(a, 0, 0, ..., 0, ...)|a \in A\}$ de $A[X]$.*

Demonstração. □

Observação 6.3.1. *Devido ao isomorfismo de A e L, podemos identificar cada $a \in A$ ao polinômio $(a, 0, 0, 0, ...) \in L$, ou seja, $a = (a, 0, 0, 0, ...)$. Por esta igualdade, temos $0 = (0, 0, 0, ..., 0, ...)$ e $1 = (1, 0, 0, 0, ...)$ e ainda $A = L$, e portanto $A \subset A[X]$.*

Os elementos de A, que são polinômio especiais, são chamados polinômios constantes. Note que se $a \in A$ e $g = (b_0, b_1, b_2, ..., b_n, 0, 0, ...) \in A[X]$ então:

$$a.g = (a, 0, 0, ...).(b_0, b_1, b_2, ..., b_n, 0, 0, ...) = (a.b_0, a.b_1, ab_2, ..., a.b_n, 0, 0, ...).$$

6.4 Polinômios Inversíveis

Observamos que nem todo polinômio é inversível. De fato, considere o polinômio $f(x) = x$. Note que f não é o polinômio identicamente nulo. Se $f(x)$ fosse inversível, existiria um polinômio $g(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ com $a_n \neq 0$ tal que $f(x).g(x) = a_0x + a_1x^2 + a_2x^3 + ... + a_nx^{n+1} = 1$(unidade de um anel), $\forall x \in A$.

Assim, para $x = 0$(zero do anel), teríamos o seguinte absurdo $1 = 0$.

Agora, seja $f(x) = a$ polinômio constante. Se $a \neq 0$ é um elemento inversível de A o polinômio constante g definida por $g(x) = a^{-1}$ é seu inverso, pois $\forall x \in A$ temos $(f.g)(x) = f(x).g(x) = a.a^{-1} = 1$.

Observação 6.4.1. *Se A é um corpo, todos os polinômios constantes de $A[X]$, exceto o polinômio nulo, são inversíveis.*

Note que, como $A \subset A[X]$, então $U(A) \subset U(A[X])$. Agora, se A é um anel de integridade, vale a inclusão contrária, isto é, $U(A[X]) \subset U(A)$.

De fato, dado $f \in U(A[X])$, então $\exists g \in A[X]$, tal que $f.g = 1$. Logo $\partial(f.g) = \partial(1)$, ou seja, $\partial f + \partial g = 0$. Assim, $\partial f = \partial g = 0$, logo $f, g \in A$. Como $f.g = 1$ decorre que $f \in U(A)$.

Portanto se A é um anel de integridade, então $U(A[X]) = U(A)$.

Exemplos:

(a) $U(\mathbb{Z}[X]) = U(\mathbb{Z}) = \{1, -1\}$.

(b) $U(\mathbb{R}[X]) = U(\mathbb{R}) = \mathbb{R}^*$.

(c) $U(\mathbb{Z}_5[X]) = U(\mathbb{Z}_5) = \mathbb{Z}_5^*$.

Observação 6.4.2. *Quando A não é anel de integridade, pode ocorrer que $U(A) \subsetneq U(A[X])$, isto é, podem existir polinômio não constantes mas inversíveis. Por exemplo, em $\mathbb{Z}_4[X]$ o polinômio $f = \overline{1} + \overline{2}X$ é inversível, pois $f.f = (\overline{1} + \overline{2}X).(\overline{1} + \overline{2}X) = \overline{1} + \overline{4}X + \overline{4}X^2 = \overline{1}$.*

6.5 Divisão em $A[X]$

Considere $A[X]$ um anel comutativo com unidade.

Definição 6.5.1. *Dado $f, g \in A[X]$, diz-se que f divide g, se $\exists q \in A[X]$ tal que $g = f.q$.*

Notação: $f \mid g$.

Observação 6.5.1. *:*

1. *Se f não divide g, escreve-se $f \nmid g$.*
2. *Se $f \mid g$ então $g = f.q$, logo $\partial g = \partial f + \partial q$.*

Exemplo 6.5.1. *Em $\mathbb{R}[X]$ o polinômio $f = x - 1$ divide o polinômio $g = x^2 - 1$, pois existe $q = x + 1$, tal que $q = f.q$, ou seja, $x_2 - 1 = (x - 1).(x + 1)$.*

Propriedades: A relação "f divide g" sobre o anel $A[X]$ tem as seguintes propriedades:

1. $f \mid f$, $\forall f \in A[X]$.
2. Se $f \mid g$ e $g \mid h$, então $f \mid h$.
3. Se $f \mid g$, então $f \mid g.h$, $\forall h \in A[X]$.
4. Se $f \mid g_1$ e $f \mid g_2$, então $f \mid (g_1h_1 + g_2h_2)$, $\forall h_1, h_2 \in A[X]$.

Demonstração. □

Definição 6.5.2. *Dois polinômios $f, g \in A[X]$, tais que $f \mid g$ e $g \mid f$, dizem-se* **associados**.

Proposição 6.5.1. *Seja $f \in A[X]$ um polinômio não-nulo. Então um polinômio $g \in A[X]$ é associado de f se, e somente se, $g = c.f$, onde c é um polinômio constante inversível.*

Demonstração. □

6.6 Algoritmo da Divisão (ou de Euclides)

Considere os polinômios $f = 1 + X^2$ e $g = 1 - X$, ambos em $\mathbb{Z}[X]$. Logo $f \nmid g$, pois $\partial f > \partial g$.

Por outro lado, g também não divide f, pois se dividisse, existira um polinômio de grau $1 (a + bX)$ tal que:

$$1 + X^2 = (1 - X).(a + bX) = a + (b - a)X - bX^2$$

Resolvendo essa igualdade de polinômios, chegaríamos que $a = 1$, $b - a = 1 \Rightarrow b = 1$ e $b = -1$, absurdo.

Veremos que sob certas condições será possível conseguir uma "divisão aproximada" de um polinômio por outro.

Teorema 6.6.1. Algoritmo de Euclides.
Dados os polinômios $f, g \in A[X]$, com $g \neq 0$ e o coeficiente dominante de g inversível, então existem polinômios q e r tais que $f = g.q + r$ em que $r = 0$ ou $\partial(r) < \partial(g)$.

Demonstração. □

Corolário 6.6.1. *Se A é um anel de integridade, então é único o par (q, r) de polinômios que figuram no enunciado do Teorema 6.6.1.*

Demonstração. □

Corolário 6.6.2. *Seja A um corpo. Dados $f, g \in A[X]$ com $g \neq 0$, existe um único par (q, r) de polinômios de $A[X]$ de forma que $f = g.q + r$ em que $\partial(r) < \partial(g)$ quando $r \neq 0$.*

Demonstração. □

Observação 6.6.1. *Os polinômios q e r cuja existência é assegurado pelo Teorema 6.6.1, são chamados de quociente e resto respectivamente na divisão euclideana de f por g.*

Exemplo 6.6.1. *Determine o quociente e o resto da divisão euclideana de $f(x) = x^3 - 1$ por $g(x) = x + 3$, ambos em $\mathbb{Z}[X]$.*

6.7 Raízes de Polinômios

Seja B um anel comutativo com unidade e A um subanel unitário de B. Dados $f = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in A[X]$ e $u \in B$. Chama-se **valor de f em u** o seguinte elemento de B :

$$f(u) = a_0 + a_1u + a_2u^2 + ... + a_nu^n.$$

Quando $f(u) = 0$(zero do anel B), dizemos que u é **raiz** de f.

Exemplos:

1. As raízes do polinômio $f(x) = x^2 - 3$ são $\pm\sqrt{3}$.
2. Sejam $A = \mathbb{R}$, $B = \mathbb{C}$, $f = 1 + x^2$, $u = i$ e $v = 1 + i$. Então u é raiz de f, mas v não é.

Propriedades:$\forall f, g \in A[X]$ e $\forall u \in B$, temos:

(a) $(f + g)(u) = f(u) + g(u)$.

(b) $(f.g)(u) = f(u).g(u)$.

Demonstração. □

Teorema 6.7.1. (Teorema do Resto:)
Considere f um polinômio sobre A de grau ≥ 1. Se A é um subanel unitário do anel de integridade L e u é um elemento de L, então o resto da divisão de $f(x)$ por $(x - u)$ em $L[X]$ é $f(u)$.

Demonstração. □

Corolário 6.7.1. *$f \in A[X]$ é divisível por $x - u$ se, e somente se, $f(u) = 0$.*

Demonstração. □

Exemplo 6.7.1. *Se n é um número inteiro positivo ímpar, então $x^n + 1$ é divisível por $x + 1$. Pois $(-1)^n + 1 = -1 + 1 = 0$.*

Exercício: Verifique que o resto da divisão de $f(x)$ por $ax - b$ com $a \neq 0$ e inversível é $f(\frac{b}{a})$.

Exemplo 6.7.2. *O resto da divisão de $f(x) = x^3 - 2x^2 - 3$ por $g(x) = 2x + 1$ é $f(-\frac{1}{2}) = (-\frac{1}{2})^3 - 2.(-\frac{1}{2})^2 - 3 = -\frac{1}{8} - \frac{1}{2} - 3 = -\frac{29}{8}$.*

Proposição 6.7.1. *Sejam A um anel de integridade e $f \in A[X]$ um polinômio não nulo. Então o número de raízes de f em A não ultrapassa $\partial(f)$.*

Demonstração. □

Proposição 6.7.2. *Seja f um polinômio sobre $A[X]$. Se L é um anel de integridade do qual A é um subanel unitário e $u_1, u_2, ..., u_r \in L$ são raízes distintas de f, então existe um polinômio $q \in L[X]$ de grau $n - r$, tal que:*

$$f(x) = (x - u_1).(x - u_2).(x - u_3)...(x - u_r).q(x).$$

Exemplo 6.7.3. *Considere $f(x) = 2x^3 + 2x^2 - 12x$, logo 2 e -3 são raízes de f, pois $f(2) = 16 + 8 - 24 = 0$ e $f(-3) = -54 + 18 + 36 = 0$. Então existe $q(x)$ tal que $f(x) = (x - 2).(x + 3).q(x)$. De fato, $(x - 2).(x + 3) = x^2 + x - 6$, logo $q(x) = 2x$, pois $2x^3 + 2x^2 - 12x = (x - 2).(x + 3).2x$.*

6.8 Algoritmo de Briot-Ruffini

Na divisão de um polinômio $f = a_0x^n + a_1x^{n-1} + ... + a_n$ de grau n por $d = x - u$, sejam $q = b_0x^{n-1} + b_1x^{n-2} + ... + b_{n-1}$ e $r = b_n$ o quociente e o resto da divisão respectivamente, então $b_0 = a_0$ e $b_i = ub_{i-1} + a_i$, com $i = 1, 2, ..., n$.

Observe a seguinte tabela, um dispositivo para a divisão de f por $x - u$:

u	a_0	a_1	a_2	$\cdots$	a_{n-1}	a_n
	a_0	$u.b_0$	$u.b_1$	$\cdots$	$u.b_{n-2}$	$u.b_{n-1}$
	$b_0 = a_0$	$b_1 = u.b_0 + a_1$	$b_2 = u.b_1 + a_2$	$\cdots$	$b_{n-1} = u.b_{n-2} + a_{n-1}$	$b_n = u.b_{n-1} + a_n = r$

Exemplos: Efetue a divisão de f por d usando o dispositivo prático:

(a) $f = x^4 - 1$ e $d = x - 2$.

(b) $f = (1, -1)x^2 + (1, 2)x + (1, 1)$ e $d = x - (-1, 1)$.

6.9 Máximo Divisor Comum

Definição 6.9.1. *Seja K um corpo. Dados $f, g \in K[X]$, um polinômio $d \in K[X]$ se diz* **máximo divisor comum** *de f e g se:*

(i) $d \mid f$ *e* $d \mid g$.

(ii) $\forall d_1 \in K[X]$, *se* $d_1 \mid f$ *e* $d_1 \mid g$ *então* $d_1 \mid d$.

Notação: $mdc(f, g)$

Exemplo 6.9.1. *Dados* $f = 2x + 2 \in \mathbb{R}[X]$ *e* $g = -x^2 + 1 \in \mathbb{R}[X]$, *verifique que o polinômio* $d = x + 1$ *é o máximo divisor comum de* f *e* g.

Proposição 6.9.1. *Seja* K *um corpo. Se* $f, g \in K[X]$ *e* $d \in K[X]$ *é um máximo divisor comum de* f *e* g, *então* $d' \in K[X]$ *também será um máximo divisor comum de* f *e* g *se, e somente se,* $\exists c \in K^*$, *tal que* $d' = c.d$.

Demonstração. □

Proposição 6.9.2. *Seja* K *um corpo. Então, dados* $f, g \in K[X]$ *existem* $h_1, h_2 \in K[X]$ *de maneira que o polinômio* $d = f.h_1 + g.h_2$ *é um máximo divisor comum de* f *e* g.

Demonstração. □

Veremos agora um algoritmo para determinar o máximo divisor comum entre dois polinômios.

Seja K um corpo e considere $f, g \in K[X]$ dois polinômios não nulos. Suponhamos que $\partial(f) \geq \partial(g)$. Para determinar o máximo divisor comum entre f, g , aplicaremos sucessivamente o algoritmo de Euclides da seguinte maneira:

$f = g.q + r(r = 0 \text{ ou } \partial(r) < \partial(g))$
$g = r.q_1 + r_1(r_1 = 0 \text{ ou } \partial(r_1) < \partial(r))$
$r = r_1.q_2 + r_2(r_2 = 0 \text{ ou } \partial(r_2) < \partial(r_1))$
$r_1 = r_2.q_3 + r_3(r_3 = 0 \text{ ou } \partial(r_3) < \partial(r_2))$
::
$r_{n-2} = r_{n-1}.q_n + r_n(r_n = 0 \text{ ou } \partial(r_n) < \partial(r_{n-1}))$
$r_{n-1} = r_n.q_{n+1}$

Assim, como $r_n \mid r_{n-1}$ então $r_n \mid r_{n-2}$ e sucessivamente $r_n \mid g$ e $r_n \mid f$. Por outro lado, todos os divisores de f e g divide r, logo se divide g e r divide também r_1. Nessa ordem chegaremos que esse polinômio também divide r_n. Portanto o máximo divisor comum de f e g é r_n, ou seja, é último resto não nulo das divisões sucessivas.

Exemplo 6.9.2. *Em* $\mathbb{R}[X]$ *determine o máximo divisor comum de* $f = 1+2x+x^2+x^3+x^4$ *e* $g = 1 + x + x^2 + x^3$.

6.10 Polinômios Irredutíveis

Definição 6.10.1. *Seja* K *um corpo. Dizemos que um polinômio* $p \in K[X]$ *é* **irredutível** *em* $K[X]$ *ou irredutível sobre* K *se:*

(i) $p \notin K$ *(ou seja,* p *não é um polinômio constante).*

(ii) Dado $f \in K[X]$*, se* $f \mid p$*, então ou* $f \in K^*$ *ou* $\exists \in K^*$ *tal que* $f = c.p$*.*

Observação 6.10.1. *Um polinômio* $g \in K[X]$ *não constante e não irredutível, chama-se de redutível ou composto.*

Exemplos:

1. O polinômio de grau $f = 1 - x^3\mathbb{R}[X]$ é redutível.
2. Todo polinômio de grau 1 é irredutível.
3. O polinômio $p = 1 + x^2 \in \mathbb{R}[X]$ é irredutível.

Proposição 6.10.1. *Sejam* K *um corpo e* $p, f, g \in K[X]$*. Se* p *é irredutível e* $p \mid f.g$*, então* $p \mid f$ *ou* $p \mid g$*.*

Demonstração. □

Corolário 6.10.1. *Se* $p \in K[X]$ *é irredutível e* $p \mid (f_1.f_2....f_n)$*, onde cada* $f_i \in K[X]$ *e* $n \geq 1$*, então* p *divide um dos* f_i*.*

Demonstração. □

Teorema 6.10.1. (Fatoração Única)
Seja K *u corpo e* f *um polinômio não constante de* $K[X]$*. Então existe polinômios irredutíveis* $p_1, p_2, ..., p_r \in K[X]$ *tal que*

$$f = p_1.p_2.\cdots p_r.$$

Demonstração. □

6.11 Raízes Múltiplas

Definição 6.11.1. *Sejam* K *um corpo,* $f \in K[X]$ *e* $u \in K$*. Se* $\exists r \in \mathbb{N}$ *tal que* $f = (x - u)^r.q$*, onde* q *é um polinômio com coeficiente em* K *e* u *não é raiz de* q*, então dizemos que* u *é* **raiz de multiplicidade** r **de** f*.*

Observação 6.11.1. *Se* $r > 1$*, diz-se que* u *é raiz múltipla. E se* $r = 1$*, diz-se que* u *é raiz simples.*

Definição 6.11.2. *Dado um polinômio* $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[X]$, *denomina-se derivada formal de* f *e indica-se por* f', *o seguinte polinômio:*

$$f' = a_1 + (2a_2)x + (3a_3)x^2 + \cdots + (n.a_n)x^{n-1}.$$

Proposição 6.11.1. *Para que* $u \in K$ *seja raiz múltipla de* $f \in K[X]$ *é necessário e suficiente que* u *seja uma raiz de* f'.

Demonstração. □

Corolário 6.11.1. *Se o máximo divisor comum unitário de* f *e* f' *é* 1, *então todas as raízes de* f *são simples.*

Demonstração. □

Exemplos:

1. Verifique que $f(x) = 1 + x + x^2$ não tem raízes múltiplas.
2. Verifique que $f(x) = x^n - 1$ não tem raízes múltiplas para $n \geq 0$.
3. Verifique que o polinômio $f = 1 + x + x^3$ só admite raízes simples.

Definição 6.11.3. *Um corpo* K *é chamado* **algebricamente fechado** *se todo polinômio não constante* $f \in K[X]$ *admite pelo menos uma raiz em* K.

Exemplos:

1. O corpo $\mathbb{C}$ dos números complexos é algebricamente fechado, pelo "Teorema Fundamental da Algebra".
2. O corpo $\mathbb{R}$ dos números reais não é algebricamente fechado. Basta tomar como exemplo o polinômio $f = 1 + x^2$, pois não possui raízes reais.

Proposição 6.11.2. *Seja* K *um corpo algebricamente fechado. Dado* $f \in K[X]$, *então* f *é irredutível se, e somente se,* $\partial(f) = 1$.

Demonstração. □

6.12 Relações entre coeficientes e raízes

Consideremos um corpo algebricamente fechado K e $f = a_0 + a_1K + ... + a_nX^n$ um polinômio de $K[X]$ de grau n. Se $u_1, u_2, ..., u_n \in K$ são as raízes de f, então este polinômio pode ser decomposto da seguinte forma:

$$f = a_n(X - u_1)(X - u_2)...(X - u_n).$$

Desenvolvendo o produto indicado no segundo membro e levando em conta a condição de igualdade de dois polinômios obtemos:
$a_{n-1} = -a_n(u_1 + u_2 + ... + u_n)$
$a_{n-2} = a_n(u_1u_2 + u_1u_3 + ... + u_{n-1}u_n)$
e, de uma maneira geral, observando que o coeficiente de $X^{n-k}(1 \leq K \leq n)$ é a soma dos produtos

$$(-1)^k u_{i_1}u_{i_2}...u_{i_k}$$

estendida a todas as combinações possíveis $i_1, i_2, ..., i_k$ dos n índices $1, 2, ..., n$ temos:

$$a_{n-k} = (-1)^k a_n \Sigma u_{i_1}u_{i_2}...u_{i_n}.$$

Em particular

$$a_0 = a_n(-1)^n u_1u_2...u_n.$$

Se adotarmos as notações:
$\sigma_1 = u_1 + u_2 + ... + u_n$
.....
$\sigma_k = \Sigma u_{i_1}u_{i_2}...u_{i_k}$
.....
$\sigma_n = u_1u_2...u_n,$

teremos

$$\frac{a_{n-k}}{a_n} = (-1)^k \sigma_k$$

e portanto:

$$f = a_n[X^n - \sigma_1 X^{n-1} + ... + (-1)^k \sigma_k X^{n-k} + ... + (-1)^n \sigma_n].$$

Exemplos:

1. **Polinômios de Grau 2.**
   Seja $f = aX^2 + bX + c \in K[X]$($k$ algebricamente fechado). um polinômio de grau 2. Se u_1 e u_2 indicam as raízes de f em K, então:

   $\sigma_1 = u_1 + u_2 = -\frac{b}{a}$
   $\sigma_2 = u_1 u_2 = \frac{c}{a}$

   e daí:

   $$f = a(X^2 - \sigma_1 X + \sigma_2)$$

   .

2. Polinômios de grau 3.

   Seja $f = aX^3 + bX^2 + cX + d$ um polinômio de grau 3. Indicando por u_1, u_2 e u_3 as raízes de f (todas em K), temos:

   $\sigma_1 = u_1 + u_2 + u_3 = -\frac{b}{a}$
   $\sigma_2 = u_1 u_2 + u_2 u_3 + u_1 u_3 = \frac{c}{a}$
   $\sigma_3 = u_1 u_2 u_3 = -\frac{d}{a}$

   e então:

   $$f = a(X^3 - \sigma_1 + \sigma_2 X - \sigma_3)$$

   .

6.13 Exercícios

1. Seja a função polinomial sobre $\mathbb{Z}$, dada por $f(x) = x^{15}+x^{14}+x^{13}+x^{12}+...+x^2+x+1$. Calcule $f(0), f(1)$ e $f(-1)$.

2. Seja $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ um polinômio e observe $p(1) = a_n + a_{n-1} + ... + a_1 + a_0$, soma dos coeficientes do polinômio $p(x)$. Qual a soma dos coeficientes do polinômio $(4x^3 - 2x^2 - 2x - 1)^{36} \in \mathbb{R}[X]$?

3. Dados os polinômios sobre $\mathbb{Z}$: $f(x) = 7 - 2x + 4x^2$, $g(x) = 5 + x + x^2 + 5x^3$, $h(x) = 2 - 3x + x^4$. Calcule $(f + g)(x)$, $(g - h)(x)$ e $(h - f)(x)$.

4. Dados os polinômios sobre $\mathbb{Z}$: $f(x) = 2+3x-4x^2$, $g(x) = 7+x^2$, $h(x) = 2x-3x^2+x^3$. Calcule $(f \cdot g)(x)$, $(g \cdot h)(x)$ e $(h \cdot f)(x)$.

5. Se $f = (1, 2) + (2, 0)X$, $g = (1, -1)X + (1, 1)X^2$ e $h = (-4, -1) + (-2, 1)X$. Calcule $f + g + h$, $f \cdot g - h^2$ e $f \cdot h + g$. Todos os polinômios estão em $\mathbb{Z} \times \mathbb{Z}[X]$.

6. Se $f = a + bX$, $g = c + bX + aX^2$ e $h = b + cX^2$ são polinômios dos anel $M_2(\mathbb{Z})[X]$, onde $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix}$ e $c = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$, calcular f^2, $f^2 - g^2$, $g^2 + 2 \cdot g \cdot h + h^2$ e h^3.

7. Determinar os graus dos seguintes polinômios de $A[X]$:

   (a) $(1 + x^2)^3 \cdot (1 - x^2)^2$, $A = \mathbb{Q}$;

   (b) $(1 + x^2)^3 \cdot (1 - x^2)^3 + x^2$, $A = \mathbb{Z}_3$;

   (c) $(1 + x + x^2 + x^3 + x^4)^7$ $A = \mathbb{Z}_7$;

   (d) $(1 + 2x^2)^4$, $A = \mathbb{Z}_8$;

8. Obter $a, b \in \mathbb{Z}_5$, para que $(x^4 + 3x^2 + 2x^2 + ax + b)$ seja um quadrado perfeito em $\mathbb{Z}_5[X]$.

9. Se f, g são polinômios do anel $A[X]$ tais que $\partial f^2 = 8$ e $\partial(f \cdot g) = 7$, determine $\partial(f + g)$, $\partial(f - g)$, $\partial(f)^3$ e $\partial(g)^2$, sabendo que A é um anel de integridade.

10. Determinar o quociente e o resto da divisão euclidiana de f por g, polinômios pertencentes a $A[X]$, nos seguintes casos:

    (a) $f = 0$, $g = 5x^2 - 1$ e $A = \mathbb{Q}$.

    (b) $f = x^2 - 1$, $g = x^3 + x^2 - 1$ e $A = \mathbb{Z}$.

    (c) $f = 4x^2 - 6x + 2$, $g = x^2 - 1$ e $A = \mathbb{R}$.

    (d) $f = 4x^4 - 6x + 2$, $g = 3x^3 - 3x + 2$ e $A = \mathbb{Z}_7$.

(e) $f = x^10 - x$, $g = x^4 + x^3 + 4x^2 + x$ e $A = \mathbb{Z}_{17}$.

(f) $f = (1,1) + (1,1)x^2$, $g = (0,1) + (1,1)x$ e $A = \mathbb{Z} \times \mathbb{Z}$.

11. Determinar a de modo que a divisão euclideana de $f = 4x^3 - 6x + a$ por $g = x + 3$ seja exata, supondo que f, g pertençam a $\mathbb{Z}_7[X]$.

12. Determinar a, b, c para que $f = 3x^4 + ax^3 + 6x^2 + bx + c$ seja divisível por $g = x^3 - 5x^2 + 6x$, supondo que f, g pertençam a $\mathbb{Q}[X]$.

13. Determinar $a, b \in \mathbb{Z}$ de modo que o polinômio $f = x^4 + 3x^3 + 2x^2 + ax + b$ divido por por $g = x^2 + x + 1$ de resto $r = 7x - 5$. Qual é o quociente da divisão?

14. Provas que se um polinômio $f \in A[X]$ é divisível separadamente por $(x-a)$ e $(x-b)$, com $a, b \in A$ e $a \neq b$, então f é divisível por $(x - a) \cdot (x - b)$.

15. Aplique o algoritmo de Briot-Ruffini nos seguintes casos:

(a) $f = x^4 - 4x^3 + 5x^2 + 6x - 2$, $g = x - 3$ e $A = \mathbb{Z}$.

(b) $f = x^3 + 2x^2$, $g = x + 1$ e $A = \mathbb{Z}_7$.

(c) $f = (1,0) + (2,0)X + (3,0)X^3$, $g = X + (1,0)$ e $A = \mathbb{Z} \times \{0\}$.

16. Determine o máximo divisor comum d dos polinômios f, g de $K[X]$, nos seguintes casos:

(a) $f = x^4 - x^2 + \overline{1}$, $g = x^3 + x^2 + x + \overline{1}$; $K = \mathbb{Z}_5$;

(b) $f = x^4 + x^3 + x + \overline{1}$, $g = \overline{2}x^3 + \overline{2}x^2 + x + \overline{1}$; $K = \mathbb{Z}_3$;

(c) $f = x^4 + x^3 + x + 1$, $g = 2x + 2$; $K = \mathbb{Q}$.

17. Prove que todo polinômio de grau 1 é irredutível.

18. Prove que $2 + 2x + x^4 \in \mathbb{Q}[X]$ é irredutível.

19. Prove detalhadamente que o polinômio $f = 1 + x + x^2 \in \mathbb{R}[X]$ é irredutível.

20. Obter as relações entre coeficientes e raízes de polinômios de grau 2 e 3.

21. Dividindo o polinômio f por $x^2 - 3x + 5$, obtemos o quociente $x^2 + 1$ e resto $3x - 5$. Determine f.

22. Efetue a divisão de $f = x^3 + ax + b$ por $g = 2x^2 + 2x - 6$. Qual é a condição para que a divisão seja exata?

23. Determine as raízes do polinômio $p(x) = x^4 - 5x^2 - 10x - 6$, sabendo que o polinômio p seja divisível por $(x + 1) \cdot (x - 3)$.

24. O polinômio $p(x) = x^5 - x^4 - 13x^2 + 36x - 36$ é tal que $p(1) = 0$. Quais as outras raízes de $p(x)$?

25. Determine o polinômio f do segundo grau que, dividido por x, $x - 1$ e $x - 2$ apresenta restos $4, 9, 18$, respectivamente.

26. Aplicando Briot-Ruffini, determine o quociente q e o resto r da divisão de $f = x^3 - x^2 + x - 1$ por $g = (x - 2) \cdot (x - 3)$.

Bibliografia