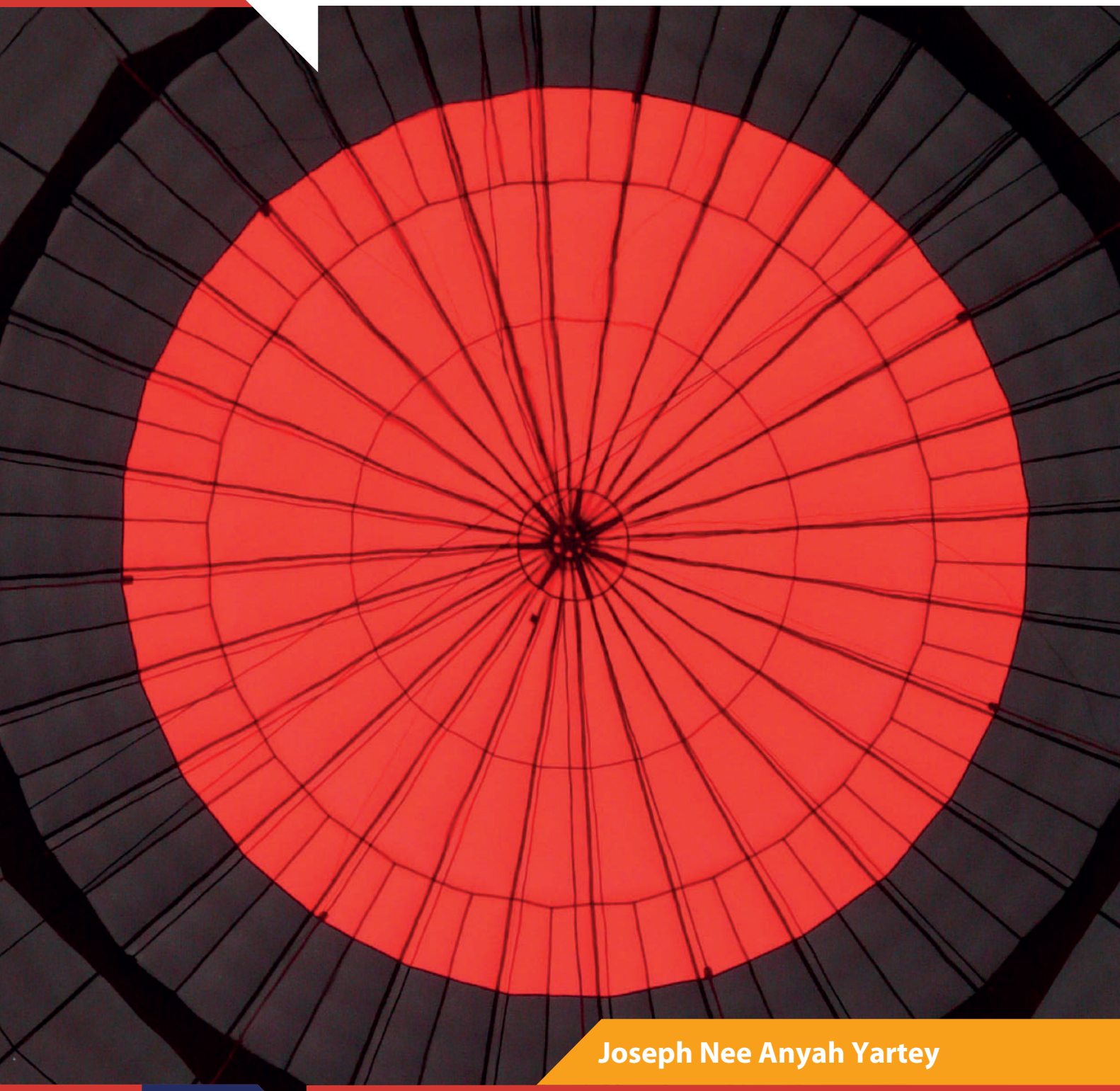
Instituto de Matemática
UNIVERSIDADE FEDERAL DA BAHIA



Joseph Nee Anyah Yartey

MATB98

Álgebra II

UNIVERSIDADE FEDERAL DA BAHIA

LICENCIATURA EM MATEMÁTICA
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

ÁLGEBRA II

Joseph Nee Anyah Yartey

UNIVERSIDADE FEDERAL DA BAHIA
Reitor: João Carlos Salles Pires da Silva
Vice-Reitor: Paulo César Miguez de Oliveira

Pró-Reitoria de Ensino de Graduação
Pró-Reitor: Penildon Silva Filho

Instituto de Matemática
Diretor: Evandro Ferreira dos Santos

Superintendência de Educação a Distância -SEAD
Superintendente: Márcia Tereza Rebouças Rangel

Coordenação de Tecnologias Educacionais CTE-SEAD
Haenz Gutierrez Quintana
Coordenação Administrativa CAD-SEAD
Sofia Souza
Coordenação de Design Educacional CDE-SEAD
Lanara Souza

UAB -UFBA

Licenciatura em Matemática
Coordenador:
Prof. Marco Antonio N. Fernandes

Produção de Material Didático
Coordenação de Tecnologias Educacionais CTE-SEAD

Núcleo de Estudos de Linguagens & Tecnologias - NELT/UFBA

Coordenação
Prof. Haenz Gutierrez Quintana

Projeto gráfico
Prof. Haenz Gutierrez Quintana
Capa: Prof. Alessandro Faria
Foto de capa: Pixabay

Equipe de Revisão:
Edivalda Araujo
Julio Neves Pereira
Márcio Matos

Equipe de Design
Supervisão: Prof. Alessandro Faria

Editoração
Joseph Nee Anyah Yartey

Design de Interfaces
Raissa Bomtempo

Equipe Audiovisual
Direção:
Prof. Haenz Gutierrez Quintana

Câmera / Iluminação
Maria Christina Souza
Edição:
Flávia Ferreira Braga

Imagens de cobertura:
Maria Christina Souza

Animação e videografismos:
Arthur Farrot

Trilha Sonora:
Pedro Queiroz Barreto

Ficha catalográfica elaborada pela Biblioteca Universitária Reitor Macedo Costa
SIBI - UFBA

Y29 Yartey, Joseph Nee Anyah.

Álgebra II / Joseph Nee Anyah Yartey. - Salvador: UFBA, Instituto de Matemática e Estatística; Superintendência de Educação a Distância, 2017.
244 p. : il.

ISBN: 978-8292-144-9
1. Álgebra. 2.Teoria dos grupos. 3. Anéis (Álgebra). I. Universidade Federal da Bahia. Instituto de Matemática e Estatística. II. Universidade Federal da Bahia. Superintendência de Educação a Distância. III. Título.

CDU 512.5

Sumário

CARTA DE APRESENTAÇÃO

Caro (a)s aluno (a)s,

Sejam bem vindos ao curso de Álgebra II.

A disciplina de Álgebra II - MATB98 é uma continuação natural da disciplina Álgebra I - MATB91 que vocês estudaram no 4º semestre. Nesta disciplina de Álgebra II, estudaremos com um certo rigor matemático os conceitos de anéis comutativos com unidade, anéis de polinômios e uma introdução à teoria dos grupos.

Bom aprendizado e sucesso!!

UNIDADE 1

TEORIA DOS GRUPOS

Aula 1.1

Grupos

Nesta aula vamos estudar os conceitos de grupos e seus propriedades. Apresentamos vários exemplos de grupos.

1.1.1 Definições e Exemplos de grupos

Definição 1.1.1 (Operação binária). *Seja G um conjunto não vazio. Uma operação binária definida em G é uma função*

$$\begin{aligned} * : G \times G &\longrightarrow G \\ (a, b) &\longmapsto a * b. \end{aligned}$$

Isto é, ao cada para ordenado (a, b) de $G \times G$ corresponde, pela operação $*$, um único elemento de G, que se designa por $a * b$.

Exemplo 1.1.1.

(a) As quatro operações $+$, $-$, $\div$, $\times$ são operações binárias em $\mathbb{R}$.

(b) A soma e multiplicação de matrizes são operações binárias no conjunto de todos $n \times n$ matrizes.

Definição 1.1.2 (Grupo). *Sejam G um conjunto não vazio e $* : G \times G \to G$ uma operação binária. Dizemos que $(G, *)$ é um grupo se as condições são satisfeitas:*

(G1) A operação $*$ definida em G é associativa, ou seja,

$$(a * b) * c = a * (b * c), \quad \forall a, b, c \in G;$$

(G2) Existe um elemento neutro em G, ou seja,

$$\exists\, e \in G \text{ tal que } a * e = e * a = a, \quad \forall a \in G;$$

(G3) Existe elemento inverso para todo elemento de G, ou seja,

$$\forall\, a \in G,\ \exists\, b \in G \text{ tal que } a * b = b * a = e.$$

Observações.

(1) Em geral, denotaremos um grupo $(G, *)$ simplesmente por G, ficando a operação subentendida, e $a * b$ por ab.

(2) Estabeleçamos dois tipos de notações para grupos que serão utilizadas no decorrer destas aulas:

(a) ***Grupo Aditivo:*** *Neste tipo de notação temos:*

- *Operação: "+";*
- *Elemento Neutro: "0";*
- *Inverso de $a \in G$: " $-a$".*

(b) ***Grupo Multiplicativo:*** *Neste tipo de notação temos:*

- *Operação: "$\cdot$" ou "$*$";*
- *Elemento Neutro: "e" ou "1";*
- *Inverso de $a \in G$: "a^{-1}".*

Definição 1.1.3 (Grupo Abeliano). *Um grupo G é chamado de grupo* **abeliano** *(ou grupo comutativo) se a operação $*$ for comutativa, ou seja,*

$$a * b = b * a \text{ para todo } a, b \in G.$$

Definição 1.1.4 (Grupo Finito). *Um grupo G é chamado de grupo* **finito**, *quando G contiver um número finito de elementos. Neste caso, definimos a* **ordem** *de G, denotada por $|G|$, sendo o número de elementos de G.*
Quando G não é um grupo finito, dizemos que G é um grupo de **ordem infinita,** *ou seja, isto ocorre quando o grupo G contém infinitos elementos.*

Agora ilustramos como grupos surgem em varias áreas de matemática fornecendo uma variedade de exemplos.

Exemplo 1.1.2 (Grupo de Números).

(a) Considere o conjunto dos números inteiros $\mathbb{Z}$ com a operação usual de soma $+$. Temos que $(\mathbb{Z}, +)$ é um grupo, pois

- *a soma de 2 inteiros é um inteiro, logo $+$ é uma operação binária em $\mathbb{Z}$;*
- *a soma é associativa, pois*

$$x + (y + z) = (x + y) + z, \ \forall\, x, y, z \in \mathbb{Z};$$

- *o elemento neutro é 0, pois*

$$x + 0 = 0 + x = x, \ \forall\, x \in \mathbb{Z};$$

- *o inverso de x é $-x$, pois*

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

Além disto $(\mathbb{Z}, +)$ *é um grupo abeliano, pois*

$$x + y = y + x, \ \forall\, x, y \in \mathbb{Z}.$$

(b) Analogamente $(\mathbb{Q}, +)$ *e* $(\mathbb{R}, +)$ *são grupos aditivos abelianos, infinitos com elemento neutro* 0 *e o inverso aditivo de* x *igual* $-x$.

(c) Considere o conjunto dos números racionais não nulo $\mathbb{Q}^*$ *com a operação usual de multiplicação* $\cdot$ *. Temos que* $(\mathbb{Q}^*, \cdot)$ *é um grupo, pois*

- *a multiplicação de 2 números racionais não nulos é um numero racional não nulo, logo* $\cdot$ *é uma operação binária em* $\mathbb{Q}^*$;
- *a multiplicação é associativa, pois*

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z, \ \forall\, x, y, z \in \mathbb{Q}^*;$$

- *o elemento neutro é* 1, *pois*

$$x \cdot 1 = 1 \cdot x = x, \ \forall\, x \in \mathbb{Q}^*;$$

- *o inverso de* x *é* $\frac{1}{x}$, *pois*

$$x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1, \ \forall\, x \in \mathbb{Q}^*.$$

Além disto $(\mathbb{Q}^*, \cdot)$ *é um grupo abeliano, pois*

$$x \cdot y = y \cdot x, \ \forall\, x, y \in \mathbb{Q}^*.$$

(d) Analogamente $(\mathbb{R}^*, \cdot)$ *é um grupo multiplicativo abeliano infinito, com elemento neutro igual* 1 *e o inverso multiplicativo de* $x \in \mathbb{R}^*$ *é* $\frac{1}{x}$.

(e) $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$ *e* $(\mathbb{R}, \cdot)$ *não são grupos pois por exemplo* 0 *não possui inverso em nenhum destes conjuntos.*

Exemplo 1.1.3 (Classes residuais módulo n).

(a) O conjunto $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ *de classes residuais módulo* n *com a operação da soma*

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

é um grupo aditivo abeliano finito, ordem n *com elemento neutro* $\overline{0}$ *e o inverso de* $\overline{a}$ *é* $\overline{(n-a)}$.

(b) O conjunto $\mathbb{U}_n = \{\overline{a} \in \mathbb{Z}_n : \ mdc(a,n) = 1\}$ *dos elementos invertíveis de* $\mathbb{Z}_n$ *com a operação*

$$\overline{a} \cdot \overline{b} = \overline{ab}$$

é um grupo multiplicativo abeliano finito, ordem $\varphi(n)$ *com elemento neutro* $\overline{1}$ *e o inverso multiplicativo de* $\overline{a} \in U(n)$ *é o elemento* $\overline{b}$ *tal que* $\overline{a} \cdot \overline{b} = \overline{1}$ *ou* $a \cdot b \equiv_n 1$.
Por exemplo $\varphi(28) = \varphi(2^2)\varphi(7) = 2 \cdot 6 = 12$. *Portanto*

$$\mathbb{U}_{28} = \{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}, \overline{15}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{27}\}.$$

Como

$3 \cdot 19 = 57 \equiv_{28} 1$ *temos que* $\overline{19}$ *é o inverso multiplicativo de* $\overline{3}$

$5 \cdot 17 = 85 \equiv_{28} 1$ *temos que* $\overline{17}$ *é o inverso multiplicativo de* $\overline{5}$

$9 \cdot 25 = 225 \equiv_{28} 1$ *temos que* $\overline{25}$ *é o inverso multiplicativo de* $\overline{5}$

$11 \cdot 23 = 253 \equiv_{28} 1$ *temos que* $\overline{23}$ *é o inverso multiplicativo de* $\overline{11}$

$13 \cdot 13 = 169 \equiv_{28} 1$ *temos que* $\overline{13}$ *é seu proprio inverso multiplicativo*

$15 \cdot 15 = 225 \equiv_{28} 1$ *temos que* $\overline{15}$ *é seu proprio inverso multiplicativo*

$27 \cdot 27 = 729 \equiv_{28} 1$ *temos que* $\overline{27}$ *é seu proprio inverso multiplicativo*

Exemplo 1.1.4 (Matrizes).

(a) $(M_n(X), +)$ *o conjunto de matrizes* $n \times n$ *com entradas em* X*, com a operação usual de soma é um grupo aditivo abeliano.*

(b) $(GL_n(X), \cdot)$ *o conjunto de matrizes* $n \times n$ *inversíveis com entradas em* X*, isto é*

$$GL_n(X) = \{A \in M_n(X),\ \det(A) \neq 0\}$$

com a operação usual de produto é um grupo multiplicativo.

(c) $(SL_n(X), \cdot)$ *o conjunto de matrizes* $n \times n$ *com determinante igual 1, isto é*

$$SL_n(X) = \{A \in GL_n(X),\ \det(A) = 1\}$$

com a operação usual de produto é um grupo multiplicativo.

Faremos alguns exercícios variados com intuito de trabalhar as operações que poderemos definir para que um determinado conjunto não vazio seja grupo.

Exemplo 1.1.5. *Verifique quais dos conjuntos abaixo* G *é um grupo sob a operação* $*$:

(i) $G = \mathbb{R}$; $\quad a * b = a + b - 1,\ \forall a, b \in G = \mathbb{R}$.

(ii) $G = \{1, 2, 3, 4, 5\}$; $\quad a * b = ab \pmod 6,\ \forall a, b \in G$.

Solução.

(i) $G = \mathbb{R}$; $\quad a * b = a + b - 1$

- *Seja* $a, b \in G$*. Então* $a * b = a + b + 1 \in G$*. Portanto,* G *é fechado com relação ao* $*$.
- *G1: Associativa*

  Seja $a, b, c \in G$*. Então*

$$\begin{aligned}(a * b) * c &= (a + b - 1) * c \\ &= (a + b - 1) + c - 1 \\ &= a + (b + c - 1) - 1 \\ &= a + (b * c) - 1 \\ &= a * (b * c).\end{aligned}$$

Portanto a operação $*$ é associativa.

- *G2: Elemento neutro*

  Seja e o elemento neutro de G. Então

$$\begin{aligned} a * e &= a, \quad \forall\, a \in G \\ \Rightarrow a + e - 1 &= a \\ \Rightarrow e &= 1. \end{aligned}$$

- *G3: Elemento inverso*

  Seja a^{-1} o elemento inverso de a. Então

$$\begin{aligned} a * a^{-1} &= e \\ \Rightarrow a + a^{-1} - 1 &= 1 \\ \Rightarrow a^{-1} &= 2 - a. \end{aligned}$$

Portanto $(G, *)$ é um grupo.

(ii) $G = \{1, 2, 3, 4, 5\}$; $a * b = ab \ (mod\ 6),\ \forall a, b \in G$

$(G, *)$ *não é um grupo, pois G é não fechada com relação ao $*$. Por exemplo*

$$3, 4 \in G \quad mas \quad 3 * 4 = 0 \notin G.$$

Portanto $(G, *)$ não é um grupo.

1.1.2 A tabela de Cayley para Grupos Finitos

Seja $(G, *)$ um grupo finito com n elementos. Vamos suponha que $G = \{e, a_1, \cdots, a_{n-1}\}$, onde e é o elemento neutro. A operação binária $*$ em G pode ser dada através de uma tabela da forma:

$*$	e	a_1	a_2	$\cdots$	a_{n-1}
e	e	e	e	e	e
a_1	e	$a_1 * a_1$	$a_1 * a_2$	$\cdots$	$a_1 * a_{n-1}$
a_2	e	$a_2 * a_1$	$a_2 * a_2$	$\cdots$	$a_2 * a_{n-1}$
$\vdots$	e	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_{n-1}	e	$a_{n-1} * a_1$	$a_{n-1} * a_2$	$\cdots$	$a_{n-1} * a_{n-1}$

Esta tabela é chamada a tabela de Cayley para o grupo $(G, *)$. *Observemos que na construção da tabela não podemos ter repetições de elementos nem nas linhas e nem nas colunas.*

Exemplo 1.1.6. *Construa a tabela de Cayley para o grupo multiplicativo* $\mathbb{U}_5$.

Solução.

$$\mathbb{U}_5 = \{\overline{x} \in \mathbb{Z}_5,\ mdc(x,5) = 1\} = \{\overline{1},\ \overline{2},\ \overline{3},\ \overline{4}\}$$

$*$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Exemplo 1.1.7. *Construa as tabelas de Cayley de grupos finitos de ordens 1, 2, 3 e 4.*

Solução.

(a) Seja G um grupo de ordem 1. Logo G contém somente o elemento neutro, isto é, $G = \{e\}$. *A tabela de Cayley do grupo G está no lado. Neste caso G é abeliano.*

$*$	e
e	e

(b) Seja G um grupo de ordem 2. Logo G contém o elemento neutro e mais outro elemento. Vamos representar G por $G = \{e, a\}$. *A tabela de Cayley do grupo G está no lado. Neste caso G é abeliano.*

$*$	e	a
e	e	a
a	a	e

(c) Seja G um grupo de ordem 3. Logo G possui o elemento neutro mais 2 outros elementos. Vamos representar G por $G = \{e, a, b\}$.

- $a * b$ *pode ser* e *ou* a *ou* b. *Se* $a * b = a$ *então* $b = e$ *impossível. Da mesma forma* $a * b \neq b$. *Portanto* $a * b = e$ *e* $a = b^{-1}$.
- $a * a \neq a$ *(a fim de que não temos* $a = e$*) e* $a * a \neq e$ *(a fim de que não temos* $a = a^{-1} = b$*). Portanto* $a * a = b$.
- *Da mesma forma* $b * a = e$ *e* $b * b = a$.

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Portanto G possui a tabela de Cayley no lado. Neste caso G é abeliano.

(d) Seja G um grupo de ordem 4. Logo G possui o elemento neutro e mais 3 outros elementos. Vamos representar G por $G = \{e, a, b, c\}$. *Temos 2 possíveis tabelas de Cayley para G:*

- *Se* $a * a = b * b = c * c = e$ *então* $a * b = b * a = c$, $a * c = c * a = b$ *e* $b * c = c * b = a$. *Portanto G possui a tabela de Cayley abaixo. Este grupo é chamado de* ***grupo-4 de Klein****, ou simplesmente* ***grupo de Klein****. Neste caso G é abeliano.*

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

- *Agora suponha que* $a * a \neq e$. *Então* $a * a$ *pode ser b ou c. Vamos suponha que* $a * a = b$. *Então* $a * b$ *ou igual a* e *ou* c. *Se* $a * b = e$ *então*

$$\begin{cases} a * c \neq e \quad (\text{a fim de que não temos } c = a^{-1} = b) \\ a * c \neq b \quad (\text{a fim de que não temos } c = a) \\ a * c \neq a \quad (\text{a fim de que não temos } c = e) \\ a * c \neq c \quad (\text{a fim de que não temos } a = e) \end{cases}$$

Portanto não podemos ter $a * b = e$, *logo* $a * b = c$. *Portanto G possui a tabela de Cayley*

abaixo. Observe $a * a = b$, $a * a * a = c$ *e* $a * a * a * a = e$. *Este grupo é chamado de grupo cíclico de 4 elementos. Neste caso G é abeliano.*

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

Exemplo 1.1.8. *Construa a tabela de Cayley para o grupo dos* ***quatérnios***

$$Q = \{1, i, j, k, -i, -j, -k, -1\}$$

com operações

$$i^2 = j^2 = k^2 = ijk = -1 \quad \text{e} \quad (-1)^2 = 1.$$

1 *é o elemento neutro e* -1 *comutam com todos os elementos.*

Solução. *Como estas operações podemos deduzir os restantes das operações:*

- $ij =?$
  Como $ijk = -1$ *e* $k^2 = -1$ *temos que* $ijk^2 = (-1)k \Rightarrow -ij = -k \Rightarrow ij = k$
  Observe que $(ij)(ji) = i(j^2)i = i(-i) = -i^2 = 1$. *Portanto* ji *é a inversa de* ij. *Logo* $ji = -k$.

- $ik =?$
  De fato $k = ij \Rightarrow ik = i(ij) = -j$.

- *Com deduções similares achamos os restantes das operações.*

Portanto a tabela do Quatérnios é

$\cdot$	1	i	j	k	$-i$	$-j$	$-k$	-1
1	1	i	j	k	$-i$	$-j$	$-k$	-1
i	i	-1	k	$-j$	1	$-k$	j	$-i$
j	j	$-k$	-1	i	k	1	$-i$	$-j$
k	k	j	$-i$	-1	$-j$	i	1	$-k$
$-i$	$-i$	1	$-k$	j	-1	k	$-j$	i
$-j$	$-j$	k	1	$-i$	$-k$	-1	i	j
$-k$	$-k$	$-j$	i	1	j	$-i$	-1	k
-1	-1	$-i$	$-j$	$-k$	i	j	k	1

Vantagens da tabela de Cayley:

- *Fácil de entender.*
- *Elemento neutro e inversos são relativamente fácil de encontrar.*
- *É fácil de determinar se o grupo é abeliano ou não (basta observar simetria do diagonal).*

Desvantagens da tabela de Cayley:

- *Só pode ser usados para grupos finitos de ordens pequenos.*

1.1.3 Propriedades básicas de grupos

Proposição 1.1.1. *Sejam* $(G, \cdot)$ *um grupo e* $a, b, c \in G$.

(1) O elemento neutro é único.

(2) O elemento inverso é único.

(3) A equação $a \cdot x = b$ *admite uma única solução em G, a saber,* $x = a^{-1} \cdot b$.

(4) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

Observe que se G é um grupo abeliano, então $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.

(5) (Lei do Cancelamento)

Se $a \cdot b = a \cdot c$, *então* $b = c$ *ou Se* $b \cdot a = c \cdot a$, *então* $b = c$.

Demonstração.

(1) Suponha que e e e' são 2 elementos neutros de G, isto é $a \cdot e = a \cdot e' = a$, $\forall a \in G$. Em particular

$$e' = e \cdot e' = e.$$

(2) Suponha que a' e a'' são inversos de $a \in G$, isto é $a \cdot a' = a' \cdot a = e$ e $a \cdot a'' = a'' \cdot a = e$ onde e é o elemento neutro de G. Então

$$\begin{aligned} a'' &= e \cdot a''; && \text{pois } e \text{ é o elemento neutro} \\ &= (a' \cdot a) \cdot a''; && \text{pois } a' \text{ é um elemento inverso de } a \\ &= a' \cdot (a \cdot a''); && \text{pois a operação é associativa} \\ &= a' \cdot e; && \text{pois } a'' \text{ é um elemento inverso de } a \\ &= a'; && \text{pois } e \text{ é o elemento neutro} \end{aligned}$$

Portanto o elemento inverso de $a \in G$ é único.

(3) $ax = b \Longrightarrow a^{-1}ax = a^{-1}b$

Portanto $x = a^{-1}b$.

(4) Devemos provar que

$$(ab) \cdot (b^{-1}a^{-1}) = e \quad \text{e} \quad (b^{-1}a^{-1}) \cdot (ab) = e.$$

Agora

$$\begin{aligned} (ab) \cdot (b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} \\ &= a \cdot e \cdot a^{-1} = aa^{-1} = e. \end{aligned}$$

e

$$\begin{aligned} (b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b \\ &= b^{-1} \cdot e \cdot b = b^{-1}b = e. \end{aligned}$$

(5) $ab = ac$. Multiplicar cada lado por a^{-1} temos

$$\begin{aligned} a^{-1} \cdot (ab) &= a^{-1} \cdot (ac) \\ \Rightarrow (a^{-1} \cdot a)b &= (a^{-1} \cdot a)c \\ \Rightarrow e \cdot b &= e \cdot c \\ \Rightarrow b &= c. \end{aligned}$$

■

1.1.4 Potências de um Elemento

Definição 1.1.5 (Potências de um Elemento). *Sejam $(G, \cdot)$ um grupo e $a \in G$. Definimos as potências de a por*

$$a^n = \begin{cases} e, & se\ n = 0 \\ \underbrace{a \cdot a \cdots a}_{n\ vezes}, & se\ \ n > 0 \\ \\ (a^{-1})^{|n|}, & se\ ,\ n < 0. \end{cases}$$

Se G é um grupo aditivo então as potências de a é definida por:

$$na = \begin{cases} e, & se\ n = 0 \\ \underbrace{a + a + \cdots + a}_{n\ vezes}, & se\ \ n > 0 \\ \\ |n|(-a), & se\ ,\ n < 0. \end{cases}$$

Exemplo 1.1.9. *Considere o grupo aditivo* $\mathbb{Z}_{12} = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}\right\}$.
As potências de 8 são:

$$\begin{aligned}
1 \cdot \overline{8} &= \overline{8};\\
2 \cdot \overline{8} &= \overline{8} + \overline{8} = \overline{4};\\
3 \cdot \overline{8} &= \overline{8} + \overline{8} + \overline{8} = \overline{0};\\
4 \cdot \overline{8} &= \overline{8} + \overline{8} + \overline{8} + \overline{8} = \overline{8};\\
5 \cdot \overline{8} &= \overline{8} + \overline{8} + \overline{8} + \overline{8} + \overline{8} = \overline{4};
\end{aligned}$$

assim por diante.

Exemplo 1.1.10. *Considere o grupo multiplicativo* $\mathbb{U}_{11} = \left\{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}\right\}$.
As potências de 4 são:

$$\begin{aligned}
\overline{4}^1 &= \overline{4};\\
\overline{4}^2 &= \overline{4} \cdot \overline{4} = \overline{5};\\
\overline{4}^3 &= \overline{4} \cdot \overline{4} \cdot \overline{4} = \overline{9};\\
\overline{4}^4 &= \overline{4} \cdot \overline{4} \cdot \overline{4} \cdot \overline{4} = \overline{3};\\
\overline{4}^5 &= \overline{4} \cdot \overline{4} \cdot \overline{4} \cdot \overline{4} \cdot \overline{4} = \overline{1};
\end{aligned}$$

assim por diante.

Proposição 1.1.2. *Seja G um grupo. Para* $a \in G$ *e* $m, n \in \mathbb{Z}$ *valem*

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

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

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

Demonstração. A demonstração é deixada a cargo do leitor como exercício. ■

Exemplo 1.1.11. *Suponha que G é um grupo com elemento neutro e. Mostre que se* $x^2 = e$ *para todo elemento* $x \in G$, *então G é abeliano.*

Solução. *Suponha que a e b são elementos arbítrios em G.*
Queremos mostrar que ab = ba.

Por hipótese,

$$(ab)^2 = abab = e. \qquad (*)$$

Multiplicando cada lado de $(*)$ *por a pela esquerda temos que*

$$aabab = a.$$

Mas, como $aa = e$*, isto ficara*

$$bab = a \qquad (**)$$

Multiplicando cada lado de $(**)$ *por b pela direta temos que*

$$babb = ab.$$

Mas, como $bb = e$*, isto ficara* $ba = ab$*.*
Portanto G é abeliano.

Exemplo 1.1.12. *Mostre que se G é um grupo tal que* $(ab)^2 = a^2b^2,\ \forall a, b \in G$*, então G é um grupo abeliano.*

Solução.

$$\begin{aligned}
(ab)^2 &= a^2b^2 \\
\Rightarrow abab &= a^2b^2 \\
\Rightarrow a^{-1}abab &= a^{-1}a^2b^2 \quad \textit{multiplicando cada lado pela esquerda por } a^{-1} \\
\Rightarrow (a^{-1}a)bab &= (a^{-1}a)ab^2 \quad \textit{por associatividade} \\
\Rightarrow bab &= ab^2 \quad \textit{elemento neutro} \\
\Rightarrow babb^{-1} &= ab^2b^{-1} \quad \textit{multiplicando cada lado pela direta por } b^{-1} \\
\Rightarrow ba &= ab.
\end{aligned}$$

Portanto G é abeliano.

1.1.5 Subgrupos

Definição 1.1.6 (Subgrupo). *Sejam $(G, \cdot)$ um grupo e H um subconjunto não vazio de G. Dizemos que H é um subgrupo de G se H, munido da operação $\cdot$ do grupo G, for um grupo, ou seja, se $(H, \cdot)$ for um grupo.*

Como a operação $\cdot$ já é associativa em G, logo, ela já satisfaz a propriedade associativa para os elementos de H. Portanto, as propriedades a serem satisfeitas para que H seja um subgrupo de G são dadas pelos seguintes axiomas.

*SG*1. *H é fechado pela operação de G, isto é,*

$$a \cdot b \in H \ \text{ para todo } \ a, b \in H;$$

*SG*2. $e \in H$;

*SG*3. *Se $a \in H$ então $a^{-1} \in H$.*

Notação: *Se H é subgrupo de G, então denotamos $H \leq G$.*

Observações.

- *$\{e\}$ e G são subgrupos de G chamados* **subgrupos triviais** *de G.*
- *Se H é um subgrupo de G, diferente de $\{e\}$ e G então dizemos que H é um subgrupo próprio de G e escrevemos $H < G$.*

Exemplo 1.1.13. *Temos a seguinte sequência de subgrupos:*

- $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$.
- $(\mathbb{Q}^*, \cdot) < (\mathbb{R}^*, \cdot) < (\mathbb{C}^*, \cdot)$.

Exemplo 1.1.14. *Verifique, em cada um dos itens abaixo, se H é subgrupo de G.*

(a) $H = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}\}$, $(G, *) = (\mathbb{Z}_{15}, +)$.

(b) $H = \{2^a 3^b | \, a, b \in \mathbb{Z}\}$, $(G, *) = (\mathbb{R}^+, \times)$.

(c) $H = \{z \in \mathbb{Z};\ z \text{ é um número ímpar}\},\ \ G = \mathbb{Z};\quad a * b = a + b + 1,\ \ a, b \in G.$

Solução.

(a) $H = \{\overline{0},\ \overline{3},\ \overline{6},\ \overline{9},\ \overline{12}\}, (G, *) = (\mathbb{Z}_{15,\ +}).$

Temos que o conjunto $H \neq \emptyset$.

Observemos a tabela da operação $+$ *em* H.

$+$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{12}$
$\overline{0}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{12}$
$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{12}$	$\overline{0}$
$\overline{6}$	$\overline{6}$	$\overline{9}$	$\overline{12}$	$\overline{0}$	$\overline{3}$
$\overline{9}$	$\overline{9}$	$\overline{12}$	$\overline{0}$	$\overline{3}$	$\overline{6}$
$\overline{12}$	$\overline{12}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$

- SG_1 : $\forall\ a, b \in H$ *temos que* $a + b \in H$.
- SG_2 : *Sabemos que o elemento neutro de* $\mathbb{Z}_{15} = G$ *é* $e_G = 0 \in H$.
- SG_1 : $\forall\ a \in H$ *temos* $a^{-1} \in H$.

Logo H *é um subgrupo de* $(G, *) = (\mathbb{Z}_{15}, +)$.

(b) $H = \{2^a 3^b | a, b \in \mathbb{R}\},\ \ (G, *) = (\mathbb{R}^+, \times)$

Temos que $H \neq \emptyset$

- SG_1 : *H é fechado, pois*
  para $w, y \in H$, *então* $w = 2^a 3^b$ *e* $y = 2^r 3^s \in H$ *com* $a, b, r, e \in \mathbb{Z}$.
  Portanto $w \cdot y = 2^a 3^b \cdot 2^r 3^s = 2^{(a+r)} 3^{(b+s)} \in H$.
- SG_2 : *O elemento neutro é 1 pertencem a H pois* $1 = 2^0 3^0 \in H$.
- SG_3 : *Se* $w \in H$, *então* $w = 2^a 3^b$ *para inteiros a e b. Então* $-a$ *e* $-b$ *também são inteiros, logo* $w^{-1} = (2^a 3^b)^{-1} = 2^{-a} 3^{-b} \in H$.

Logo H *é um subgrupo de* $(G, *) = (\mathbb{R}^+, \times)$.

(c) $H = \{z \in \mathbb{Z};\ \text{é um número ímpar}\},\ \ G = \mathbb{Z};\ \ a * b = a + b + 1,\ \ a, b \in G$

Temos que $H \neq \emptyset$

- SG_1 : *H é fechado, pois para*
  $a,\ b \in H$, *então* $a = 2n+1\ \ e\ \ b = 2k+1$ *com* $n, k \in \mathbb{Z}$. *Portanto*

$$\begin{aligned} a * b = (2n+1) * (2k+1) &= (2n+1) + (2k+1) + 1 = 2n + 2k + 2 + 1 = \\ &= 2(n+k+1) + 1 \in H. \end{aligned}$$

- SG_2 : *O elemento neutro é (-1) pertencem a H pois* $a * (-1) = a,\ \forall a \in H$.
- SG_3 : *Se* $a \in H,\ e\ \ a * a^{-1} = e$ *temos que*

$$\begin{aligned} (2n+1) * a^{-1} &= -1 \\ 2n + 1 + a^{-1} + 1 &= -1 \\ a^{-1} &= (-2n-2) - 1 \Rightarrow a^{-1} \in H. \end{aligned}$$

Logo H é um subgrupo de $G = \mathbb{Z}$.

Exemplo 1.1.15. *Seja G um grupo abeliano com elemento neutro e. Prove que*

$$H = \{x \in G \mid x^2 = e\}$$

é um subgrupo de G.

Solução.

- *Sejam* $x, y \in H$. *Assim, temos* $x^2 = e$ *e* $y^2 = e$. *Daí,*

$$(xy)^2 = (xy)(xy) = x(yxy) = x(xyy) = x(xy^2) = x(xe) = xx = x^2 = e,$$

  isto é, $xy \in H$.

- $e \in H$, *pois* $e^2 = e$.

- *Seja* $x \in H$, *temos:* $x.x = x^2 = e \Rightarrow x = x^{-1} \in H$.
  Outra maneira de provar que $x^{-1} \in H$:

$$(x^{-1})^2 = x^{-1} \cdot x^{-1} = (x \cdot x)^{-1} = (x^2)^{-1} = (e)^{-1} = e.$$

Então, H é subgrupo de G.

Proposição 1.1.3 (Critério do Subgrupo). *Seja H um subconjunto não vazio de um grupo G. Então, H é um subgrupo de G se, e somente se,*

$$a \cdot b^{-1} \in H \text{ para todo } a, b \in H.$$

Demonstração. Claro que se H é um subgrupo de G, então $ab^{-1} \in H$ sempre que $a, b \in H$. Resta provar que o recíproco também vale.

- Como a operação em H é a mesma que a considerada em G, ela é associativa.
- Vejamos agora que $e \in H$. Seja $x \in H$ (note-se que H é não vazio, por hipótese). Então $e = x \cdot x^{-1} \in H$.
- Seja agora $x \in H$ e vejamos que $x^{-1} \in H$. Para isso basta tomar $a = e$ e $b = x$ no enunciado da proposição.
- Resta provar que H é fechado para operação. Sejam então $x, y \in H$. Já sabemos que $y^{-1} \in H$. Logo $xy = x(y^{-1})^{-1} \in H$.

■

Observação. *Resulta da demonstração que a condição de H ser não vazio pode ser substituída por $e \in H$. Note-se que se mostrarmos que $e \notin H$ fica automaticamente provado que H não é um subgrupo.*

Exemplo 1.1.16. *Prove que* $H = \left\{ \begin{bmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{bmatrix},\ \theta \in \mathbb{R} \right\}$ *é um subgrupo de* $G = SL(2, \mathbb{R})$.

Solução.

- *H não é vazio, pois* $\begin{bmatrix} \cos 0 & -\operatorname{sen} 0 \\ \operatorname{sen} 0 & \cos 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$

- *Seja* $A, B \in H$, *onde* $A = \begin{bmatrix} \cos\theta_1 & -\operatorname{sen}\theta_1 \\ \operatorname{sen}\theta_1 & \cos\theta_1 \end{bmatrix}$ *e* $B = \begin{bmatrix} \cos\theta_2 & -\operatorname{sen}\theta_2 \\ \operatorname{sen}\theta_2 & \cos\theta_2 \end{bmatrix}$. *Então*

$$\begin{aligned} AB^{-1} &= \begin{bmatrix} \cos\theta_1 & -\operatorname{sen}\theta_1 \\ \operatorname{sen}\theta_1 & \cos\theta_1 \end{bmatrix}\begin{bmatrix} \cos\theta_2 & \operatorname{sen}\theta_2 \\ -\operatorname{sen}\theta_2 & \cos\theta_2 \end{bmatrix} \\ &= \begin{bmatrix} \cos\theta_1\cos\theta_2 + \operatorname{sen}\theta_1\operatorname{sen}\theta_2 & \cos\theta_1\operatorname{sen}\theta_2 - \operatorname{sen}\theta_1\cos\theta_2 \\ \operatorname{sen}\theta_1\cos\theta_2 - \cos\theta_1\operatorname{sen}\theta_2 & \operatorname{sen}\theta_1\operatorname{sen}\theta_2 + \cos\theta_1\cos\theta_2 \end{bmatrix} \\ &= \begin{bmatrix} \cos(\theta_1-\theta_2) & -\operatorname{sen}(\theta_1-\theta_2) \\ \operatorname{sen}(\theta_1-\theta_2) & \cos(\theta_1-\theta_2) \end{bmatrix} \in H. \end{aligned}$$

Portanto $H < G$.

Proposição 1.1.4. *Se H e K são dois subgrupos de G, então* $H \cap K$ *é um subgrupo de G.*

Demonstração. Sejam $a, b \in H \cap K$. Então $a, b \in H$ e $a, b \in K$. Como $H < G$ e $K < G$ temos que

$$\left.\begin{array}{c} ab^{-1} \in H \\ \text{e} \\ ab^{-1} \in K \end{array}\right\} \Rightarrow ab^{-1} \in H \cap K.$$

Portanto $H \cap K < G$. ■

Definição 1.1.7. *Sejam G um grupo e* $a \in G$.

(a) O **centro de G** *é o conjunto* $Z(G) = \{x \in G;\ xa = ax\ \forall a \in G\}$.

(b) O **centro de a** *é o conjunto* $N(a) = \{x \in G;\ xa = ax\}$.

Exemplo 1.1.17. *Seja G o conjunto de todas as matrizes da forma*

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \text{ onde } a, b, c \in \mathbb{Q}.$$

[Assume que G é um grupo]. Determine o o centro $Z(G)$ de G.

Solução. *Para determinarmos o centro $Z(G)$ de G, precisamos encontrar todas as matrizes que comutam com as matrizes de G,*

Sejam $A, X \in G$, então

$$A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \; e \; X = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

para alguns $a, b, c, x, y, z \in \mathbb{Q}$. Então temos que

$$AX = \begin{pmatrix} 1 & x+a & y+az+b \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{pmatrix} \; e \; XA = \begin{pmatrix} 1 & a+x & b+xc+y \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{pmatrix}$$

e portanto $AX = XA$ se e somente se $az = xc$, ou seja, $A \in Z(G) \Leftrightarrow az = xc$ para todo $x, z \in \mathbb{R}$; mas isto é possível somente no caso em que $a = c = 0$.

Portanto, o centro $Z(G)$ de G consiste dos matrizes A acima com $a = c = 0$.

Proposição 1.1.5. *Sejam G um grupo e $a \in G$. Então $Z(G)$ e $N(a)$ são subgrupos de G.*

Demonstração.

(a) $Z(G) = \{x \in G; xa = ax, \forall a \in G\}$.

Para mostrar que $Z(G)$ é subgrupo de G, utilizaremos a definição de subgrupo

- Como $ea = a = ae, \;\; \forall a \in G$, temos que $e \in Z(G)$.
  Portanto $Z(G) \neq \emptyset$.
- Seja $x, y \in Z(G)$. Então como $xa = ax$ e $ya = ay, \;\; \forall a \in G$, temos que

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy), \;\; \forall a \in G.$$

  Portanto $xy \in Z(G)$.
- Agora seja $x \in Z(G)$, então $ax = xa, \;\; \forall a \in G$ e portanto

$$x^{-1}a = (x^{-1}a)(xx^{-1}) = x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} = x^{-1}xax^{-1} = ax^{-1}, \;\; \forall a \in G.$$

Portanto $x^{-1} \in Z(G)$.

Portanto $Z(G)$ é um subgrupo de G.

(b) $N(a) = \{x \in G; xa = ax\}$.

Vamos utilizar o critério de subgrupo.

- Como $ea = ae = a$, temos que $e \in N(a)$. Portanto $N(a) \neq \emptyset$.
- Seja $x, y \in N(a)$. Então $xa = ax$ e $ya = ay$.

$$\begin{aligned} a(xy^{-1}) &= (xy^{-1}yx^{-1})(axy^{-1}), \quad \text{pois } xy^{-1}yx^{-1} = e \\ &= xy^{-1}y(x^{-1}ax)y^{-1} \\ &= xy^{-1}y(x^{-1}xa)y^{-1}, \quad \text{pois } ax = xa \\ &= xy^{-1}yay^{-1} \\ &= xy^{-1}(yay^{-1}) \\ &= xy^{-1}(ayy^{-1}), \quad \text{pois } ay = ya \\ &= (xy^{-1})a. \end{aligned}$$

Logo, $(xy^{-1}) \in N(a)$.

Portanto $N(a)$ é um subgrupo de G.

■

1.1.6 Ordem de um elemento

Definição 1.1.8 (Ordem de um Elemento). *Sejam G um grupo e $a \in G$. Dizemos que*

(a) a tem ordem finita se existe $n \in \mathbb{Z}^+$ tal que $a^n = e$.

Neste caso, o menor inteiro positivo n_0 tal que $a^{n_0} = e$, chama-se a ordem de a, denotamos por $o(a) = n_0$ ou $ord(a) = n_0$.

(b) a tem ordem infinita caso não existe $n \in \mathbb{N}$ tal que $a^n = e$ e escrevemos $o(a) = \infty$ ou $ord(a) = \infty$.

Exemplo 1.1.18.

(a) Seja G um grupo. Então $ord(e) = 1$ pois $e^1 = e$.

(b) Em $\mathbb{Z}_{12}$ temos que $ord(\overline{8}) = 3$ pois $3 \cdot 8 = 24 = 0$ (mod 12).

(c) Em $\mathbb{U}_{11}$ temos que $ord(\overline{4}) = 5$ pois $4^5 = 1024 = 1$ (mod 11).

(d) Em $\mathbb{Z}$ temos que $ord(5) = \infty$ pois não existe $n \in \mathbb{Z}$ tal que $n \cdot 5 = 0$.

Exemplo 1.1.19. *Mostre que $A = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ tem ordem 3 em $GL(2, \mathbb{R})$ e $B = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ tem ordem 4, mas AB tem ordem infinito.*

Solução.

$$A^2 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}.$$

$$A^3 = A^2 \cdot A = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = e.$$

Portanto $ord(A) = 3$.

$$B^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

$$B^4 = B^2 \cdot B^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = e.$$

Portanto $ord(B) = 4$.

$$AB = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}.$$

$$(AB)^2 = (AB) \cdot (AB) = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix}.$$

$$(AB)^3 = (AB)^2 \cdot (AB) = \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix}.$$

Podemos provar por indução que

$$(AB)^n = \underbrace{(AB)(AB)\cdots(AB)}_{n \text{ vezes}} = \begin{bmatrix} 1 & 0 \\ -n & 1 \end{bmatrix}.$$

Ou seja $(AB)^n \neq e$, *para* $n > 0$. *Portanto* $ord(AB) = \infty$.

Proposição 1.1.6. *Seja G um grupo finito. Então todo elemento* $a \in G$ *tem ordem finita.*

Demonstração.

Considere o conjunto

$$\{a^n, \ n \in \mathbb{N}\} = \left\{e, a, a^2, a^3, \cdots\right\}.$$

Como G é finito, este conjunto de potências de a não pode infinito. (Segue pelo Principio de Casa dos Pombos). Portanto 2 potências de a devem ser iguais, digamos $a^i = a^j$ com $i \neq j$.
Se assumimos que $i > j$ então temos que

$$a^{i-j} = a^i \cdot a^{-j} = a^i \cdot a^{-i} = e.$$

Em particular $\text{ord}(a) \leq i - j$. Portanto a ordem de a é finita. ■

Proposição 1.1.7. *Sejam G um grupo e* $a \in G$. *Então* $ord(a) = ord(a^{-1})$.

Demonstração.

Caso I: Suponha que ordem de a é finita, ou seja $\text{ord}(a) = n$. Então

$$(a^{-1})^n = (a^n)^{-1} = e^{-1} = e.$$

$$\text{Isto implica que } \ \text{ord}(a^{-1]}) \leq n = \text{ord}(a).$$

Por outro lado se $m = \text{ord}(a^{-1})$ então

$$a^m = \left((a^{-1})^{-1}\right)^m = (a^{-1})^{-m} = \left((a^{-1})^m\right)^{-1} = e^{-1} = e.$$

Isto implica que $\text{ord}(a) \leq m = \text{ord}(a^{-1})$.

Portanto $n = m$, ou $\text{ord}(a) = \text{ord}(a^{-1})$.

Caso II: Suponha que a tem ordem infinta. Então para todo $n \in \mathbb{Z}^+$ temos que $a^n \neq e$. Mas então

$$\left(a^{-1}\right)^n = (a^n)^{-1} \neq e, \ \ \forall\, n \in \mathbb{Z}^+.$$

Portanto a^{-1} tem ordem infinita. ■

Proposição 1.1.8. *Se $\text{ord}(a) = n$ e $m \in \mathbb{Z}^+$ então $a^m = e \iff n|m$.*

Demonstração.

($\Leftarrow$) Suponha que $n|m$. Então existe $k \in \mathbb{Z}^+$ tal que $m = kn$. Portanto

$$a^m = a^{kn} = (a^n)^k = e^k = e.$$

($\Rightarrow$) Suponha que $a^n = e$. Suponha que $m \geq n$. Pelo algoritmo da divisão existem $q, r \in \mathbb{Z}$ tal que $m = q \cdot n + r$, com $0 \leq r < n$. Portanto

$$e = a^m = a^{qn+r} = a^{qn} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r.$$

Como $r < n = \text{ord}(a)$ temos que $r = 0$. Portanto $m = qn \Rightarrow n|m$. ■

Proposição 1.1.9. *Sejam G um grupo e $a \in G$ com $\text{ord}(a) = n$. Então*

$$a^i = a^j \iff i \equiv j \ (mod\ n)$$

Demonstração. Segue de Proposição (1.1.8) ■

Corolário 1. *Sejam G um grupo e $a \in G$ com $ord(a) = \infty$. Então*

$$a^i = a^j \iff i = j.$$

Em particular todas as potências de a são distintas.

Proposição 1.1.10. *Sejam G um grupo e $a \in G$ tal que $ord(a) = n$ e $k \in \mathbb{Z}$. Então*

$$ord(a^k) = \frac{n}{mdc(k,n)}$$

Demonstração.
Seja $d = \text{mdc}(k,n)$. Queremos provar que $\text{ord}(a^k) = \dfrac{n}{d}$. Observemos que

$$\left(a^k\right)^{n/d} = (a^n)^{k/d} = e. \tag{1.1.1}$$

Falta provar que n/d é o menor inteiro positivo tal que (1.1.1) é valido. Suponha que existe $t \in \mathbb{N}$ tal que $(a^k)^t = e$. Ou seja $a^{nk} = e$. Então pelo Proposição (1.1.8) temos que

$$n \mid (kt) \Rightarrow \left(\frac{n}{d}\right) \Big| \left(\frac{k}{d}\right) t. \tag{1.1.2}$$

Afirmação: $\dfrac{n}{d}$ e $\dfrac{k}{d}$ são relativamente primos, isto é $\text{mdc}\,(n/d,\ k/d) = 1$.
De fato como $d = \text{mdc}(k,n)$ pelo Teorema de Bezout existem inteiros x, y tal que

$$kx + ny = d.$$

Dividindo por d temos que

$$(k/d)x + (n/d)y = 1.$$

Portanto pelo Teorema de Bezout, temos que n/d e k/d são coprimos. Logo pela equação (1.1.2) temos que n/d divide t. Em particular $n/d \leq t$, portanto $\text{ord}(a^k) = n/d$. ■

Exemplo 1.1.20. *Se $ord(a) = 12$ determine as ordens de a^k, $1 \leq k \leq 11$.*

Solução.

a^k	1	2	3	4	5	6	7	8	9	10	11
$ord(a^k)$	12	6	4	3	12	2	12	3	4	6	12

1.1.7 Grupos e Subgrupos Cíclicos

Sejam G um grupo e $a \in G$. Denotamos por $< a >$ o conjunto de todas as potências de a, ou seja,

$$\begin{aligned} < a > &:= \{a^n \mid n \in \mathbb{Z}\} \\ &= \{\cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots\}. \end{aligned}$$

Proposição 1.1.11 (O subgrupo cíclico gerado por a). *Sejam $(G, \cdot)$ um grupo e $a \in G$. Então $< a >$ é um subgrupo de G, chamado de subgrupo cíclico gerado por a.*

Demonstração.

(a) Para todo n, m inteiros temos que $a^n \cdot a^m = a^{n+m} \in < a >$.

(b) $e = a^0 \in < a >$.

(c) Para todo n, temos que $(a^n)^{-1} = a^{-n} \in < a >$.

■

Exemplo 1.1.21. *Seja $\mathbb{Z}$ o grupo aditivo. Mostre que $< n >$, o subgrupo cíclico gerado por n é $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$. Em particular, $2\mathbb{Z} =< 2 >$. Observe também que $\mathbb{Z} =< 1 >$.*

Solução. *Por definição*

$$< n >= \{\cdots, -3n, -2n, -n, 0, n, 2n, 3n, \cdots\} = n\mathbb{Z}.$$

Em particular

$$< 2 >= \{\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots\} = 2\mathbb{Z}.$$

Exemplo 1.1.22. *Considere o grupo $(\mathbb{Z}_4, +)$. Determine $< \overline{2} >$ o subgrupo cíclico gerado por $\overline{2}$.*

Solução. *Por definição*

$$< \overline{2} >= \{\overline{0}, \overline{2}\}.$$

Exemplo 1.1.23. *Seja* $\mathbb{R}^*$ *o grupo multiplicativo. Determine* $< 2 >$*, o subgrupo cíclico gerado por* 2.

Solução. *Por definição*

$$< 2 >= \{2^k \mid n \in \mathbb{Z}\} = \left\{\cdots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \cdots\right\}.$$

Teorema 1.1.12. *Seja G um grupo e seja* $a \in G$.

- *Se a for um elemento de ordem finita n, então n será o menor inteiro positivo que satisfaz* $a^n = e$.
  Mais ainda, $< a >= \{e, a, a^2, \cdots, a^{n-1}\}$.
- *Se a for um elemento de ordem infinita, então* $a^n \neq e$ *para todo inteiro* $n \neq 0$.
  Mais ainda, $< a >= \{\cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots\}$ *e todas as potências de a serão distintas.*

Demonstração. Segue da Proposição (1.1.9) e Corolário (1). ■

Definição 1.1.9 (Grupo Cíclico). *Um grupo G é chamado grupo* **cíclico** *se* $G =< a >$ *para algum* $a \in G$*, ou seja, G é gerado por um elemento.*
Neste caso, dizemos que a é um gerador de G.

Exemplo 1.1.24. *Considere o grupo aditivo* $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

- $< \overline{0} >= \{0\}$.
- $< \overline{1} >= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} = \mathbb{Z}_4$.
- $< \overline{2} >= \{\overline{0}, \overline{2}\}$.
- $< \overline{3} >= \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} = \mathbb{Z}_4$.

Portanto $\mathbb{Z}_4$ *é cíclico com geradores* $\overline{1}$ *e* $\overline{3}$.

Observação. *Se G é um grupo cíclico, então o gerador de G, isto é, o elemento* $a \in G$ *tal que* $G =< a >$, *em geral, não é único. Por exemplo,* $\mathbb{Z}_4 =< \overline{1} >$ *e* $\mathbb{Z}_4 =< \overline{3} >$.

Proposição 1.1.13. *Se* $G =< a >$ *é cíclico então* $|G| = ord(a)$.

Demonstração. Segue do Teorema 1.1.12. ■

Exemplo 1.1.25. *Determine se o grupo multiplicativo* $(\mathbb{U}_9, \cdot)$ *é cíclico. Caso seja, determine seus geradores.*

Solução.

$$\mathbb{U}_9 = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}.$$

$$\begin{array}{l|l|l|l|l}
(\overline{2})^1 =_9 \overline{2} & & (\overline{5})^1 =_9 \overline{5} & & \\
(\overline{2})^2 =_9 \overline{4} & & (\overline{5})^2 =_9 \overline{7} & & \\
(\overline{2})^3 =_9 \overline{8} & (\overline{4})^1 =_9 \overline{4} & (\overline{5})^3 =_9 \overline{8} & (\overline{7})^1 =_9 \overline{7} & (\overline{8})^1 =_9 \overline{8} \\
(\overline{2})^4 =_9 \overline{7} & (\overline{4})^2 =_9 \overline{7} & (\overline{5})^4 =_9 \overline{4} & (\overline{7})^2 =_9 \overline{4} & (\overline{8})^2 =_9 \overline{1} \\
(\overline{2})^5 =_9 \overline{5} & (\overline{4})^3 =_9 \overline{1} & (\overline{5})^5 =_9 \overline{2} & (\overline{7})^3 =_9 \overline{1} & \Downarrow \\
(\overline{2})^6 =_9 \overline{1} & \Downarrow & (\overline{5})^6 =_9 \overline{1} & \Downarrow & ord(\overline{8}) = 2. \\
\Downarrow & ord(\overline{4}) = 3 & \Downarrow & ord(\overline{7}) = 3 & \\
ord(\overline{2}) = 6 & & ord(\overline{5}) = 6 & &
\end{array}$$

Portanto $\mathbb{U}_9$ *é cíclico e* $\mathbb{U}_9 =< \overline{2} >=< \overline{5} >$.

Exemplo 1.1.26. *Determine se o grupo multiplicativos* $(\mathbb{U}_8, \cdot)$ *é cíclico. Caso seja, determine seus geradores.*

Solução.

$$\mathbb{U}_8 = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}.$$

$(\overline{3})^1 =_8 \overline{3}$	$(\overline{5})^1 =_8 \overline{5}$	$(\overline{7})^1 =_8 \overline{7}$
$(\overline{3})^2 =_8 \overline{1}$	$(\overline{5})^2 =_8 \overline{1}$	$(\overline{7})^2 =_8 \overline{1}$
$\Downarrow$	$\Downarrow$	$\Downarrow$
$ord(\overline{3}) = 2$	$ord(\overline{5}) = 2$	$ord(\overline{7}) = 2.$

Portanto $\mathbb{U}_8$ *não é cíclico.*

Proposição 1.1.14. *Seja* $G =< a >$ *um grupo finito cíclico de ordem* n*. Os geradores de* G *são da forma* a^r *se e somente se* r *e* n *são coprimos, isto é* $mdc(r, n) = 1$.

Demonstração.

$(\Rightarrow)$: Suponha que a^r é um gerador de G. Se r e n não são coprimos então eles tem um fator comum, digamos k isto é, $k = \text{mdc}(r, n)$. Logo

$$r = kx \text{ e } n = ky \text{ para algun } x, y \in \mathbb{Z}.$$

Portanto

$$a^{ry} = a^{kxy} = a^{xky} = a^{xn} = (a^n)^x = e^x = e.$$

Portanto a ordem de a^r é $y < n = ky$, contradizendo o fato que a^r gera G. Logo r e n devem ser coprimos.

$(\Leftarrow)$: Suponha que r e n não coprimos. Queremos provar que a^r gera G, isto é precisamos provar que $\text{ord}(a^r) = n$ e se $(a^r)^k = e$, então $k = xn$ para algum inteiro x.

Observe que $\text{ord}(a) = \dfrac{n}{\text{mdc}(r, n)} = n$. Agora suponha que $(a^r)^k = a^{rk} = 1$. Então pelo Proposição 1.1.8 temos que

$$n \mid (rk) \Rightarrow n \mid k \text{ pois } \text{mdc}(r, n) = 1.$$

Portanto $k = xn$, algun $x \in \mathbb{Z}$. Logo a^r gera G. ■

Exemplo 1.1.27. *Seja $G =< a >$ um grupo cíclico de ordem 28. Quais dos seus elementos gera G.*

Solução.

$$G = \{e, a, a^2, \cdots, a^{27} \mid a^{28} = e\}.$$

$$mdc(r, 28) = 1 \Rightarrow r = 1, 3, 5, 9, 11, 13, 17, 19, 23, 25, 27.$$

Portanto os geradores de G são a, a^3, a^5, a^9, a^{11}, a^{13}, a^{17}, a^{19}, a^{23}, a^{25}, a^{27}.

Teorema 1.1.15. *Todo grupo cíclico é abeliano.*

Demonstração. Como G é cíclico, existe $a \in G$ tal que $G =< a >$.
Sejam $x, y \in G$. Então $x = a^n$, $y = a^m$, $n, m \in \mathbb{Z}$. Portanto,

$$x \cdot y = a^n \cdot a^m = a^{n+m} = a^{m+n} = a^m \cdot a^n = yx.$$

Como x, y são arbitrários, temos que G é abeliano. ■

Observação. *A recíproca do Teorema 1.1.15 é falsa, ou seja, nem todo grupo abeliano é um grupo cíclico. Por exemplo,*

(1) o grupo multiplicativo $\mathbb{U}_8$, é abeliano, mas ele não é um grupo cíclico.

(2) o 4-grupo de Klein

$$V = \{e, a, b, c\}, \quad tal\ que \quad a^2 = e,\ b^2 = e,\ c^2 = e$$

é abeliano, mas não é cíclico.

Teorema 1.1.16. *Um subgrupo de um grupo cíclico é cíclico.*

Demonstração. Sejam $G =< a >$ um grupo cíclico e H um subgrupo de G. Vamos assumir que $H \neq \{e\}$, pois $\{e\}$ é cíclico. Então H contém um elemento diferente de e da forma a^m, para algum $m \in \mathbb{Z}$, pois G é cíclico. Suponha que m é o menor inteiro tal que $a^m \in H$.

Afirmação: $H =< a^m >$.

Como $a^m \in H$ temos que $< a^m > \subseteq H$.

Vamos provar que $H \subseteq < a^m >$, isto é precisamos provar que se $a^n \in H$, então a^n é uma potência de a^m. De fato, suponha que $a^n \in H$ então pelo algoritmo da divisão podemos escrever

$$n = qm + r, \quad \text{onde} \quad 0 \leq r < |m|.$$

Então

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

Como H é um subgrupo, $(a^m)^{-q} \in H$, portanto $(a^m)^{-q}a^n \in H$, e segue que

$$a^r = (a^m)^{-q}a^n \in H.$$

Mas $r < m$ e como m é o menor inteiro que $a^m \in H$ temos que $r = 0$. Em outras palavras, $a^n = (a^m)^q$, logo $a^n \in < a^m >$. Como a^n é um elemento arbitrário em H, temos que $H \subseteq < a^m >$. Portanto $H =< a^m >$ e H é cíclico. ■

Corolário 2. *Os únicos subgrupos de $\mathbb{Z}$ são os subgrupos cíclicos $< n >= n\mathbb{Z}$, para algum $n \in \mathbb{Z}$.*

Corolário 3. *Os únicos subgrupos de $\mathbb{Z}_n$ são os subgrupos cíclicos $< a >=< d >$, sendo que $mdc(a, n) = d$.*

Exemplo 1.1.28. *Determine todos os subgrupos de $\mathbb{Z}_{12}$.*

Solução. *Observe que*

$$\mathbb{Z}_{12} =< \overline{1} >=< \overline{5} >=< \overline{7} >=< \overline{11} >,$$

isto é, existem 4 geradores de $\mathbb{Z}_{12}$.

Como $\mathbb{Z}_{12}$ é cíclico, existe um único subgrupo de ordem d para cada divisor d de 12. Os divisores de 12 são 1, 2, 3, 4, 6.

- *O subgrupo de ordem 1 é $< \overline{0} >$;*

- *O subgrupo de ordem 2 é* $< \overline{6} >= \{\overline{0}, \overline{6}\}$;
- *O subgrupo de ordem 3 é* $< \overline{4} >= \{\overline{0}, \overline{4}, \overline{8}\}$;
- *O subgrupo de ordem 4 é* $< \overline{3} >= \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} =< \overline{9} >$;
- *O subgrupo de ordem 6 é* $< \overline{2} >= \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\} =< \overline{10} >$.

1.1.8 Subgrupos gerados por um conjunto

Teorema 1.1.17. *Seja G um grupo e* $\mathcal{C}$ *a coleção de todos os subgrupos de G. Então* $\bigcap_{H \in \mathcal{C}} H$ *é um subgrupo de G.*

Demonstração. A demonstração é deixada a cargo do leitor como exercício. ■

Teorema 1.1.18. *Seja G um grupo e* $S \subseteq G$. *Seja* $\mathcal{C}$ *a coleção de todos os subgrupos de G que contenha S. Então o conjunto*

$$< S >= \bigcap_{H \in \mathcal{C}} H$$

satisfazer as seguintes:

(i) $< S >$ *é um subgrupo de G que contenha S.*

(ii) Para todo $H \in \mathcal{C}$, $< S > \subseteq H$.

Portanto , $< S >$ *é o menor subgrupo de G que contenha S.*

Demonstração. A demonstração é deixada a cargo do leitor como exercício. ■

Teorema 1.1.19. $< S >$ *é o único subgrupo de G que satisfaz as condições* (*i*) *e* (*ii*) *do Teorema 1.1.18.*

Demonstração. A demonstração é deixada a cargo do leitor como exercício. ■

Definição 1.1.10. *Se G é um grupo e $S \subseteq G$ então o subgrupo $< S >$ é chamado de o* ***subgrupo de*** *G* ***gerado por*** *S. Se $G =< S >$, então dizemos que S gera G; e os elementos em S são chamados os* ***geradores****. Para $S = \{a_1, a_2, \cdots, a_n\}$ conjunto finito escrevemos $< S >=< a_1, a_2, \cdots, a_n >$*

Teorema 1.1.20. *Seja G um grupo e $S \subseteq G$. Então $< S >$ é formado por produtos finitos de elementos de S e elementos inversos de S. Isto é, se $K = \{a_1^{s_1} a_2^{s_2} \cdots a_k^{s_k},\ a_i \in S,\ s_i = \pm 1,\ k \in \mathbb{N}\}$ então $< S >= K$.*

Demonstração. A demonstração é deixada a cargo do leitor como exercício. ■

Teorema 1.1.21. *Sejam T_1 e T_2 subconjuntos de um grupo G. Então*

$$< T_1 >=< T_2 > \quad \text{se e somente se} \quad T_1 \subseteq < T_2 > \quad e \quad T_2 \subseteq < T_1 > .$$

Demonstração. A demonstração é deixada a cargo do leitor como exercício. ■

Exemplo 1.1.29. *Determine o subgrupo de $\mathbb{Z}_{12}$ gerado pelo conjunto $\{\overline{4}, \overline{6}\}$.*

Solução. *Observe que*

$$4 + 4 + 4 = 0 \ \ (mod\ 12) \Rightarrow \ ord(\overline{4}) = 3.$$

$$6 + 6 = 0 \ \ (mod\ 12) \Rightarrow \ ord(\overline{6}) = 2.$$

Portanto

$$< \overline{4}, \overline{6} >= \{\overline{4}n + \overline{6}m, \quad n = 1, 2, 3 \quad e \quad m = 1, 2\}.$$

- $n = 1,\ m = 1$ *temos* $4n + 6m = 10 \ \ (mod\ 12)$.
- $n = 1,\ m = 2$ *temos* $4n + 6m = 4 \ \ (mod\ 12)$.
- $n = 2,\ m = 1$ *temos* $4n + 6m = 2 \ \ (mod\ 12)$.
- $n = 2,\ m = 2$ *temos* $4n + 6m = 8 \ \ (mod\ 12)$.

- $n = 3,\ m = 1$ *temos* $4n + 6m = 6 \pmod{12}$.
- $n = 3,\ m = 2$ *temos* $4n + 6m = 0 \pmod{12}$.

Portanto

$$< \overline{4}, \overline{6} >= \{\overline{0},\ \overline{2},\ \overline{4},\ \overline{6},\ \overline{8},\ \overline{10}\}.$$

Exemplo 1.1.30. *Determine o subgrupo de* $\mathbb{U}_{15}$ *gerado pelo conjunto* $\{\overline{2},\ \overline{11}\}$. *Conclua que* $\mathbb{U}_{15} =< \overline{2},\ \overline{11} >$.

Solução. *Observe que*

$$2^4 = 1 \pmod{15} \Rightarrow\ ord(\overline{2}) = 4.$$

$$11^2 = 1 \pmod{15} \Rightarrow\ ord(\overline{11}) = 2.$$

Portanto

$$< \overline{2}, \overline{11} >= \{\overline{2}^n \cdot \overline{11}^m,\quad n = 1, 2, 3, 4 \quad e \quad m = 1, 2\}.$$

- $n = 1,\ m = 1$ *temos* $2^n \cdot 11^m = 7 \pmod{15}$.
- $n = 1,\ m = 2$ *temos* $2^n \cdot 11^m = 2 \pmod{15}$.
- $n = 2,\ m = 1$ *temos* $2^n \cdot 11^m = 14 \pmod{15}$.
- $n = 2,\ m = 2$ *temos* $2^n \cdot 11^m = 4 \pmod{15}$.
- $n = 3,\ m = 1$ *temos* $2^n \cdot 11^m = 13 \pmod{15}$.
- $n = 3,\ m = 2$ *temos* $2^n \cdot 11^m = 8 \pmod{15}$.
- $n = 4,\ m = 1$ *temos* $2^n \cdot 11^m = 11 \pmod{15}$.
- $n = 4,\ m = 2$ *temos* $2^n \cdot 11^m = 1 \pmod{15}$.

Portanto

$$< \overline{2}, \overline{11} >= \{\overline{1},\ \overline{2},\ \overline{4},\ \overline{7},\ \overline{8},\ \overline{11},\ \overline{13},\ \overline{14}\} = \mathbb{U}_{15}.$$

1.1.9 Produto Direto de grupos

Sejam $(H,\ \triangle)$ *e* $(K,\ *)$ *dois grupos arbitrários e seja* $H \times K$ *o produto cartesiano de H e K, isto é*

$$H \times K = \{(h,\ k) :\ h \in H\ \ e\ \ k \in K\}.$$

Em $H \times K$*, definimos:*

- *a igualdade de 2 elementos por*

$$(h_1,\ k_1) = (h_2,\ k_2) \iff h_1 = h_2\ \ e\ \ k_1 = k_2.$$

- *e a multiplicação de 2 elementos por*

$$(h_1,\ k_1)(h_2,\ k_2) = (h_1 \triangle h_2,\ k_1 * k_2).$$

Exemplo 1.1.31. *Considere* $\mathbb{Z}_2 = \{\overline{0},\ \overline{1}\}\ \ e\ \ \mathbb{U}_8 = \{\overline{1},\ \overline{3},\ \overline{5},\ \overline{7}\}$ *Então*

$$\mathbb{Z}_2 \times \mathbb{U}_8 = \left\{\left(\overline{0},\ \overline{1}\right),\ \left(\overline{0},\ \overline{3}\right),\ \left(\overline{0},\ \overline{5}\right),\ \left(\overline{0},\ \overline{7}\right),\ \left(\overline{1},\ \overline{1}\right),\ \left(\overline{1},\ \overline{3}\right),\left(\overline{1},\ \overline{5}\right),\ \left(\overline{1},\ \overline{7}\right)\right\}.$$

E o produto dos elementos $\left(\overline{1},\ \overline{5}\right)\ \ e\ \ \left(\overline{1},\ \overline{3}\right)$ *é*

$$\left(\overline{1},\ \overline{5}\right)\left(\overline{1},\ \overline{3}\right) = \left(\overline{1} + \overline{1},\ \ \overline{5} \cdot \overline{3}\right) = \left(\overline{0},\ \ \overline{7}\right).$$

Teorema 1.1.22. *Dados* $(H,\ \triangle)$ *e* $(K,\ *)$ *dois grupos. O produto cartesiano* $H \times K$ *munido da multiplicação:*

$$(h_1,\ k_1)(h_2,\ k_2) = (h_1 \triangle h_2,\ k_1 * k_2)\ \ para\ \ \ h_1, h_2 \in H\ e\ k_1, k_2 \in K$$

é um grupo (chamado **produto direto** *de H com K) com o elemento neutro* $(e_H,\ e_K)$ *onde* e_H *e* e_K *são os elementos neutros de H e K respectivamente, e o elemento inverso de* (h, k) *é* (h^{-1}, k^{-1}).

Demonstração. A demonstração é deixada a cargo do leitor como exercício. ■

Propriedades do produto direto de grupos

Lema 1.1.23 (Ordem de $H \times K$). *Sejam H e K são grupos finitos. Então a ordem $H \times K$ é o produto da ordens de H e K, isto é*

$$|H \times K| = |H|\,|K|.$$

Demonstração. Demonstração segue diretamente pelo Princípio de Contagem. ■

Lema 1.1.24 (Ordem de um elemento de $H \times K$). *Sejam H e K são grupos finitos e seja $(h,\ k) \in H \times K$. Então a ordem $(h,\ k)$ é o menor múltiplo comum das ordens de h e k, isto é*

$$ord(h,\ k) = MMC\Big(ord(h),\ ord(k)\Big).$$

Demonstração. Seja $s = \text{MMC}\Big(\text{ord}(h),\ \text{ord}(k)\Big)$ e $t = \text{ord}(h,\ k)$. Então

$$(h,\ k)^s = (h^s,\ k^s) = (e_H,\ e_K) \overset{\text{(Proposição 1.1.8)}}{\Longrightarrow} t \Big| s. \text{ Portanto } t \leq s.$$

Mas

$$(h^t,\ k^t) = (h,k)^t = (e_H,\ e_K) \Longrightarrow \text{ord}(h) \Big| t \text{ e } \text{ord}(k) \Big| t.$$

Portanto, t é um múltiplo comum de $\text{ord}(h)$ e $\text{ord}(k) \Longrightarrow s \leq t$, pois $s = \text{MMC}\Big(\text{ord}(h),\ \text{ord}(k)\Big)$. Portanto, $s = t$ e $\text{ord}(h,\ k) = \text{MMC}\Big(\text{ord}(h),\ \text{ord}(k)\Big)$.

■

Exemplo 1.1.32. *Determine a ordem de $a = (\overline{8},\ \overline{8},\ \overline{8}) \in \mathbb{Z}_{10} \times \mathbb{Z}_{24} \times \mathbb{Z}_{80}$.*

Solução.

- *Em $\mathbb{Z}_{10}$, $< \overline{8} >= \{\overline{0},\ \overline{2},\ \overline{4},\ \overline{6},\ \overline{8}\}$ e assim, $ord(\overline{8}) = 5$.*
- *Em $\mathbb{Z}_{24}$, $< \overline{8} >= \{\overline{0},\ \overline{8},\ \overline{16}\}$ e assim, $ord(\overline{8}) = 3$.*
- *Em $\mathbb{Z}_{80}$, $< \overline{8} >= \{\overline{0},\ \overline{8},\ \overline{16},\ \overline{24},\ \overline{32},\ \overline{40},\ \overline{48},\ \overline{56},\ \overline{64},\ \overline{72}\}$ e assim, $ord(\overline{8}) = 10$.*

E assim, $ord\Big((\overline{8},\ \overline{8},\ \overline{8})\Big) = MMC(3, 5, 10) = 30$ em $\mathbb{Z}_{10} \times \mathbb{Z}_{24} \times \mathbb{Z}_{80}$.

Exemplo 1.1.33. *Determine a ordem de $b = (\overline{3},\ \overline{6},\ \overline{9}) \in \mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$.*

Solução.

- *Em $\mathbb{Z}_4$, $< \overline{3} >= \{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3}\}$ e assim, $ord(\overline{3}) = 4$.*

- *Em* $\mathbb{Z}_{12}$, $< \overline{6} >= \{\overline{0}, \overline{6}\}$ *e assim,* $ord(\overline{6}) = 2$.

- *Em* $\mathbb{Z}_{15}$, $< \overline{9} >= \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}\}$ *e assim,* $ord(\overline{9}) = 3$.

E assim, $ord\Big((\overline{3}, \overline{6}, \overline{9})\Big) = MMC(2,3,4) = 12$ *em* $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$.

Lema 1.1.25 (Critério para $H \times K$ seja abeliano). *Sejam H e K são grupos. Então*

$$H \times K \text{ é abeliano} \iff H \text{ e } K \text{ são grupos abelianos.}$$

Demonstração. A demonstração é deixada a cargo do leitor como exercício. ■

Lema 1.1.26 (Critério para $H \times K$ seja cíclico). *Sejam H e K são grupos finitos e cíclicos. Então*

$$H \times K \text{ é cíclico} \iff |H| \text{ e } |K| \text{ são relativamente primos.}$$

Demonstração. Seja $|H| = m$ e $|K| = n$, portanto $|H \times K| = mn$.
($\Rightarrow$) Suponha que $H \times K$ é cíclico. Sejam $\text{MDC}(m,n) = d$ e (h,k) um gerador de $H \times K$. Então

$$(h,\ k)^{\frac{mn}{d}} = \Big((h^m)^{\frac{n}{d}},\ (k^n)^{\frac{m}{d}}\Big) = (e_H,\ e_K) \implies mn = \text{ord}(h,\ k) \leq \frac{mn}{d} \implies d = 1.$$

Portanto $|H|$ e $|K|$ são relativamente primos.
($\Leftarrow$) Suponha que $H =< h >$ e $K =< k >$ e $\text{MDC}(m,n) = 1$. Então

$$\text{ord}(h,\ k) = \text{MMC}(m,n) = mn = |H \times K|,$$

logo (h,k) é um gerador de $H \times K \implies H \times K$ é cíclico. ■

Exemplo 1.1.34.

$$\mathbb{Z}_2 \times \mathbb{Z}_5 = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{0}, \overline{3}), (\overline{0}, \overline{4}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1}), (\overline{1}, \overline{2}), (\overline{1}, \overline{3}), (\overline{1}, \overline{4})\}$$

é cíclico pois $MDC(2,5) = 1$.
De fato considere $< (\overline{1}, \overline{1}) >$. *Então*

- $2(\overline{1}, \overline{1}) = (\overline{0}, \overline{2}),\quad 3(\overline{1}, \overline{1}) = (\overline{1}, \overline{3}),\quad 4(\overline{1}, \overline{1}) = (\overline{0}, \overline{4}),\quad 5(\overline{1}, \overline{1}) = (\overline{1}, \overline{0}),$

- $6(\overline{1}, \overline{1}) = (\overline{0}, \overline{1}),\quad 7(\overline{1}, \overline{1}) = (\overline{1}, \overline{2}),\quad 8(\overline{1}, \overline{1}) = (\overline{0}, \overline{3}),\quad 9(\overline{1}, \overline{1}) = (\overline{1}, \overline{4}),\quad 10(\overline{1}, \overline{1}) = (\overline{0}, \overline{0}).$

Portanto

$$< (\overline{1},\ \overline{1}) >= \left\{(\overline{1},\ \overline{1}),\ (\overline{0},\ \overline{2}),\ (\overline{1},\ \overline{3}),\ (\overline{0},\ \overline{4}),\ (\overline{1},\ \overline{0}),\ (\overline{0},\ \overline{1}),\ (\overline{1},\ \overline{2}),\ (\overline{0},\ \overline{3}),\ (\overline{1},\ \overline{4}),\ (\overline{0},\ \overline{0})\right\}.$$

Isto é $ord(\overline{1},\ \overline{1}) = 10$.
Portanto $\mathbb{Z}_2 \times \mathbb{Z}_5 =< (\overline{1},\ \overline{1}) >$.

Exemplo 1.1.35. *Considere* $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\overline{0},\ \overline{0}),\ (\overline{0},\ \overline{1}),\ (\overline{1},\ \overline{0}),\ (\overline{1},\ \overline{2})\}$.
Excepto por $(\overline{0},\ \overline{0})$, *cada elemento tem ordem 2, portanto* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *é o grupo 4 de Klein, portanto não cíclico.*

1.1.10 Exercícios Resolvidos

Exercício 1.1.1. *Verifique quais os conjuntos abaixo G é um grupo sob a operação* $*$. *Classifique cada grupo como sendo abeliano ou não.*

(a) $G = \{\overline{2},\ \overline{4},\ \overline{6},\ \overline{8}\}$ *em* $\mathbb{Z}_{10}$; $\quad a * b = ab$.

(b) $G = \{2^x,\ x \in \mathbb{Q}\}$; $\quad a * b = ab$.

(c) $G = \{x \in \mathbb{Z};\ x \equiv 1\ mod\ 5\}$; $\quad a * b = ab$.

(d) $G = \mathbb{Z}$; $\quad a * b = a + b + 1$.

(e) $G = SL(2, \mathbb{R}) = \left\{A = \begin{bmatrix} a & b \\ c & d \end{bmatrix};\ a, b, c, d \in \mathbb{R};\ \det(A) = 1\right\}$ *sendo* $*$ *é a multiplicação de matrizes usual.*

Solução.

(a) $G = \{\overline{2},\ \overline{4},\ \overline{6},\ \overline{8}\}$ *em* $\mathbb{Z}_{10}$; $\quad a * b = ab$

$*$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$
$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$
$\overline{4}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$
$\overline{8}$	$\overline{6}$	$\overline{2}$	$\overline{8}$	$\overline{4}$

- *Da tabela, podemos ver que G é fechada com relação ao* $*$.

- $*$ *é associativa pois o grupo* $\mathbb{Z}_{10}$ *é associativa em relação ao multiplicação, logo associatividade também é valida em* G.
- *Da tabela, podemos ver que*

$$\begin{cases} \overline{6} * \overline{2} = \overline{2} * \overline{6} = \overline{2}, \\ \overline{6} * \overline{4} = \overline{4} * \overline{6} = \overline{4}, \\ \overline{6} * \overline{6} = \overline{6}, \\ \overline{6} * \overline{8} = \overline{8} * \overline{6} = \overline{8}. \end{cases}$$

Então $\overline{6}$ *é o elemento neutro de* $*$.

- *Da tabela, podemos ver que*

$$\begin{cases} \overline{2} * \overline{8} = \overline{6} \Rightarrow \overline{2} \text{ é o inverso de } \overline{8} \text{ e vice versa.} \\ \overline{4} * \overline{4} = \overline{6} \Rightarrow \overline{4} \text{ é seu proprio inverso.} \\ \overline{6} * \overline{6} = \overline{6} \Rightarrow \overline{6} \text{ é seu proprio inverso.} \end{cases}$$

- *Temos que para todo* $a,\ b \in G,\ a * b = b * a$.

Portanto, $(G, *)$ *é um grupo abeliano.*

(b) $G = \{2^x,\ x \in \mathbb{Q}\}; \quad a * b = ab$

- *Seja* $a, b \in G$. *Então* $a = 2^x$ *e* $b = 2^y$ *para algum* $x, y \in \mathbb{Q}$ *e portanto* $a * b = 2^x 2^y = 2^{x+y} \in G$ *pois* $x + y \in \mathbb{Q}$.
  Portanto, G é fechado com relação ao $*$.
- *Associatividade é herdada da propriedade associativa da multiplicação de números reais.*
- *Como* $1 = 2^0$ *e* $0 \in \mathbb{Q},\ G$ *tem elemento neutro* 1.
- *Para* $a = 2^x \in G$ *onde* $x \in \mathbb{Q}$, *temos* $a^{-1} = 2^{-x} \in G$, *pois* $-x \in \mathbb{Q}$.

Portanto $(G, *)$ *é um grupo.*
Verificando se G é um grupo abeliano :
$\forall\ 2^x, 2^y \in G$ *temos* $2^x * 2^y = 2^x 2^y = 2^y 2^x = 2^y * 2^x$.
Logo, G é um grupo abeliano.

(c) $G = \{x \in \mathbb{Z};\ x \equiv 1\ (mod\ 5)\}$ *;* $a * b = ab$.

Perceba que $G = \{1, 6, 11, 16, 21, ...\} = \{5n + 1, n \in \mathbb{Z}\}$.

1 é o elemento neutro, pois

$(5n+1) * e = (5n+1) \Rightarrow (5n+1)e = (5n+1) \Rightarrow e = 1 \in \mathbb{Z}$.

Temos que nem todos os elementos de G possui inverso, pois

$(5n+1) * a' = e \Rightarrow (5n+1)a' = 1 \Rightarrow a' = \dfrac{1}{5n+1}$ *para* $n = 1 \;\; x = \dfrac{1}{6} \notin \mathbb{Z}$.

Daí G não é um grupo.

(d) $G = \mathbb{Z}$; $a * b = a + b + 1$.

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

Temos que $G \neq \emptyset$

- G_2 : *Associativa*

$$\begin{aligned} a * (b * c) &= a * (b + c + 1) = a + (b + c + 1) + 1 = a + (1 + b + c) + 1 = \\ &= (a + 1 + b) + c + 1 = (a + b + 1) + c + 1 = (a * b) + c + 1 = (a * b) * c. \end{aligned}$$

- G_3 : *elemento neutro*

  $a * e = a \Rightarrow a + e + 1 = a \Rightarrow e = -1$.

- G_4 : *Elemento inverso*

  $a * a' = e \Rightarrow a + a' + 1 = -1 \Rightarrow e = -2 - a$.

Daí, G é um grupo.

Verificando se G é um grupo abeliano: $\forall\, a, b \in G$ *temos* $a * b = b * a$.

$a * b \;=\; a + b + 1 \;=\; b + a + 1 \;=\; b * a$.

Logo, G é um grupo abeliano.

(e) $G = SL(2, \mathbb{R}) = \left\{ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix};\ a, b, c, d \in \mathbb{R};\ \det(A) = 1 \right\}$ *sendo* $*$ *é a multiplicação de matrizes usual.*

- *Seja* $A,\ B \in SL(2, \mathbb{R})$ *temos que*

$$\det(AB) = (\det A)(\det B) = 1 \cdot 1 = 1$$

  ou seja, $AB \in SL(2, \mathbb{R})$. *Portanto* $SL(2, \mathbb{R})$ *é fechado.*

- *Associatividade seguir da associatividade de multiplicação de matrizes.*

- *Observe que* $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in SL(2, \mathbb{R})$, *portanto* $SL(2, \mathbb{R})$ *tem elemento neutro.*

- *Para* $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2, \mathbb{R})$, *uma conta simples mostra que*

$$A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in SL(2, \mathbb{R}).$$

Portanto $(G, *)$ *é um grupo não abeliano.*

Lembre que produto de matrizes não é em geral comutativa.

Exercício 1.1.2. *Seja G o grupo dada pela seguinte tabela:*

$\cdot$	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

(a) Determine $< a >$, $< r >$, $ord(a)$ *e* $ord(r)$.

(b) Quem é o elemento neutro de G?

(c) Qual o inverso de cada elemento de G?

(d) G é cíclico?

(e) G é abeliano?

Solução. $G = \{e, a, b, c, r, s, t, u\}$

(a)

$$< a > = \{e, a, b, c\} \Rightarrow ord(a) = 4.$$
$$< r > = \{e, r\} \Rightarrow ord(r) = 2.$$

(b) Elemento neutro

O elemento neutro de G é e.

(c) elemento inverso

$e \to e$, $a \to c$, $b \to b$, $c \to a$, $r \to r$, $s \to s$, $t \to t$, $u \to u$.

(d) G é NÃO cíclico, pois nenhum elemento de G tem ordem 8.

(e) G não é abeliano, pois $a \cdot r = s \neq r \cdot a = u$.

Exercício 1.1.3. *Seja G um grupo com operação* $*$. *Seja* u *um elemento de G. Define uma nova operação* $\circ$ *em G como:*

$$a \circ b = a * u * b, \quad \forall a, b \in G.$$

(a) Prove que $\circ$ é associativa.

(b) Mostre que G possui um elemento neutro sob a operação $\circ$; identifique este elemento explicitamente.

(c) Mostre que cada elemento de G possui um inverso sob a operação $\circ$.

Solução. *Sejam $a, b, c, u \in G$, temos que $a \circ b = a * u * b$*

(a) Propriedade Associativa

$$\begin{aligned}(a \circ b) \circ c &= (a * u * b) \circ c = a * u * b * u * c = a * u * (b * u * c) = \\ &= a * u * (b \circ c) = a \circ (b \circ c).\end{aligned}$$

(b) Elemento neutro

$$\begin{aligned}a \circ e &= a \\ \Rightarrow a * u * e &= a \\ \Rightarrow e &= u^{-1} * a^{-1} * a \\ \Rightarrow e &= u^{-1}.\end{aligned}$$

Verificando,

$$\begin{aligned}a \circ u^{-1} &= a * u * u^{-1} \\ &= a.\end{aligned}$$

(c) elemento inverso

$$\begin{aligned}a \circ a' &= e \\ \Rightarrow a * u * a' &= u^{-1} \\ \Rightarrow a' &= u^{-1} * a^{-1} * u^{-1}.\end{aligned}$$

Verificando,

$$\begin{aligned} a \circ (u^{-1} * a^{-1} * u^{-1}) &= a * u * (u^{-1} * a^{-1} * u^{-1}) \\ &= u^{-1} \\ \Rightarrow a \circ (u^{-1} * a^{-1} * u^{-1}) &= e. \end{aligned}$$

Exercício 1.1.4. *Seja G um grupo com elemento neutro e e $x \in G$, $x \neq e$ tal que $x^6 = x$. Considere o conjunto $H = \{x, x^2, x^3, \cdots\}$.*

(a) Quantos elementos tem H? Justifique a resposta.

(b) Determine $ord(x)$. Justifique a resposta.

(c) $H < G$? Justifique a resposta.

(d) H é cíclico? Justifique a resposta.

Solução.

(a) $H = \{x, x^2, x^3, x^4, x^5\}$, ou seja H tem 5 elementos, pois

$x^6 = x$;

$x^7 = x^6 \cdot x = x \cdot x = x^2$;

$x^8 = x^6 \cdot x^2 = x \cdot x^2 = x^3$;

$x^9 = x^8 \cdot x = x^3 \cdot x = x^4$;

$x^{10} = x^9 \cdot x = x^4 \cdot x = x^5$

$x^{11} = x^{10} \cdot x = x^5 \cdot x = x^6 = x$;

$x^{12} = x^{11} \cdot x = x \cdot x = x^2$;

$\vdots$

(b) Dada que $x^6 = x$, $\qquad (*)$

multiplicando cada lado de $(*)$ por x^{-1}, temos que

$$x^5 = x^{-1} \cdot x^6 = x^{-1} \cdot x = e.$$

Portanto, $ord(x) = 5$.

(c) SIM, pois H satisfaça todas as condições de um subgrupo.

(d) H é cíclico, pois existe $x \in G$ tal que $< x >= \{e,\ x,\ x^2,\ x^3,\ x^4\} = H$.

Exercício 1.1.5. *Mostre que* $H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix};\ n \in \mathbb{Z} \right\}$ *é um subgrupo cíclico de* $GL(2, \mathbb{R})$.

Solução. *Observamos que* $H \subseteq GL(2, \mathbb{R})$.

Vamos provar que

$$H =< a >, \ \text{sendo}\ \ a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Afirmação: $a^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ *para todo* $n \in \mathbb{Z}$.

Primeiramente usamos indução para provar que afirmação para $n \geq 0$.

- *Para* $n = 0$, *temos que* $a^0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, *ou seja a afirmação é valido para* $n = 0$.
- *Agora suponha que a afirmação é valido para* $n = k$ *para algum* $k \geq 0$. *Então*

$$a^{k+1} = a^k \cdot a = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & k+1 \\ 0 & 1 \end{bmatrix}.$$

  Logo a afirmação é valido para $n = k + 1$ *e portanto pelo indução a afirmação é provado para todo* $n \geq 0$.

- *Uma conta simples mostrar que para* $n \in \mathbb{Z}$,

$$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

  Portanto estas 2 matrizes são inversas um a outro. Portanto para $n > 0$, *temos que*

$$a^{-n} = (a^n)^{-1} = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}.$$

Portanto a afirmação é valida para todo $n \in \mathbb{Z}$ *e portanto* H *é subgrupo cíclico de* $GL(2, \mathbb{R})$.

Exercício 1.1.6. *Determine todos os subgrupos de ordem 4 de* $\mathbb{U}_{28}$, *indicando quais são cíclicos e quais não são.*

Solução. *Observe que* $\varphi(28) = \varphi(2^2)\phi(7) = 2 \cdot 6 = 12$, *que é divisível por 4. Portanto* $\mathbb{U}_{28}$ *pode ter subgrupos de ordem 4. Para determinar estes subgrupos precisamos achar as ordens dos elementos de*

$$\mathbb{U}_{28} = \{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}, \overline{15}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{27}\}.$$

- $3^3 = 27 \equiv -1 \pmod{28} \Longrightarrow 3^6 \equiv 1 \pmod{28}$. *Portanto ord*$(\overline{3}) = 6$.
- $5^2 = 25 \equiv -3 \pmod{28} \Longrightarrow 5^6 \equiv (-3)^3 = -27 \equiv 1 \pmod{28}$. *Portanto ord*$(\overline{5}) = 6$.
- $9^3 = (3^2)^3 = 3^6 \equiv 1 \pmod{28}$. *Portanto ord*$(\overline{9}) = 3$.
- $11^2 = 121 \equiv 9 \pmod{28} \Longrightarrow 11^6 \equiv 9^3 \equiv 1 \pmod{28}$. *Portanto ord*$(\overline{11}) = 6$.
- $13^2 = 169 \equiv 1 \pmod{28}$. *Portanto ord*$(\overline{13}) = 2$.
- $15 \equiv -13 \pmod{28} \Longrightarrow 15^2 \equiv (-13)^2 \equiv 1 \pmod{28}$. *Portanto ord*$(\overline{15}) = 2$.
- $17 \equiv -11 \pmod{28} \Longrightarrow 17^6 \equiv (-11)^6 \equiv 1 \pmod{28}$. *Portanto ord*$(\overline{17}) = 6$.
- $19 \equiv -9 \pmod{28} \Longrightarrow 19^6 \equiv (-9)^6 \equiv 1 \pmod{28}$. *Portanto ord*$(\overline{19}) = 6$.
- $23 \equiv -5 \pmod{28} \Longrightarrow 23^6 \equiv (-5)^6 \equiv 1 \pmod{28}$. *Portanto ord*$(\overline{23}) = 6$
- $25 \equiv -3 \pmod{28} \Longrightarrow 25^3 \equiv (-3)^3 = -27 \equiv 1 \pmod{28}$. *Portanto ord*$(\overline{25}) = 3$
- $27 \equiv -1 \pmod{28} \Longrightarrow 27^2 \equiv (-1)^2 \equiv 1 \pmod{28}$. *Portanto ord*$(\overline{27}) = 2$

Como $\mathbb{U}_{28}$ *não tem elementos de ordem 4, então não admite subgrupos cíclicos de ordem 4. Mas* $\mathbb{U}_{28}$ *tem 3 elementos de ordem 2, portanto, tem um subgrupo não cíclico de ordem 4 dado por* $\{\overline{1}, \overline{13}, \overline{15}, \overline{27}\}$.

1.1.11 Atividade

1. *Prove Teorema 1.1.22.*
2. *Mostre que se G é um grupo abeliano então* $(ab)^n = a^n b^n, \ \forall n \in \mathbb{Z}, \ \forall a, b \in G$.
3. *Seja G um grupo tal que* $(ab)^2 = (ba)^2, \ \forall a, b \in G$ *e suponha que* $x = e$ *é o único elemento de G tal que* $x^2 = e$. *Mostre que G é abeliano.*
4. *Seja G um grupo e* $a, b \in G$ *tal que* $ab \in Z(G)$, *o centro de G. Mostre que* $ab = ba$.
5. *Verifique, em cada um dos ítens abaixo, se H é subgrupo de G.*

(a) $H = \{-1, 1\}$, $(G, *) = (\mathbb{R}^*, \cdot)$

(b) $H = \mathbb{N}$, $(G, *) = (\mathbb{Z}, +)$

(c) $H = \left\{ A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix};\ a, b, c, d \in \mathbb{R};\ ab \neq 0 \right\}$, $(G, *) = (GL_2(\mathbb{R}), \cdot)$

(d) $H = \left\{ A = \begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix};\ a, b, c, d \in \mathbb{R};\ ab \neq 0 \right\}$, $(G, *) = (GL_2(\mathbb{R}), \cdot)$

(e) $H = \{z \in \mathbb{C};\ 0 < |z| < 2\}$, $(G, *) = (\mathbb{C}^*, \cdot)$

6. *Apresente dois subgrupos H e K, de um grupo G tais que $H \cup K$ não é subgrupo de G.*

7. *Seja G um grupo e sejam H e K subgrupos de G. Mostre que $H \cup K$ é um subgrupo de G se e somente se $H \subset K$ ou $K \subset H$.*

8. *Seja G um grupo de ordem par. Mostre que G possui um elemento de ordem 2.*

9. *Mostre que se G é um grupo de ordem par então existe um número ímpar de elementos de ordem 2.*

10. *Seja G um grupo e sejam $a, b \in G$. mostre que ab e ba têm a mesma ordem.*

11. *Seja G um grupo e seja $a \in G$ um elemento de ordem n. Se $n = km$, mostre que a^k tem ordem m.*

12. *Seja G um grupo e seja $a \in G$ um elemento de ordem r. Seja m um inteiro positivo tal que $mdc(m, r) = 1$. Mostre que $ord(a^m) = r$.*

13. *Seja G um grupo e sejam $a, b \in G$ tais que $a^5 = e$ e $aba^{-1} = b^2$. Mostre que $ord(b) = 31$.*

14. *Seja G um grupo e sejam $a, b \in G$ tais que $a^n = e$ e $aba^{-1} = b^s$. Mostre que $ord(b) \mid (s^n - 1)$.*

15. *Seja G um grupo e sejam $a, b \in G$. Mostre que $ord(a) = ord(b^{-1}ab)$.*

16. *Prove que se um grupo contém somente um elemento de ordem 2, então este elemento pertence o centro do grupo.*

17. *Determine o centro de j em $Q = \{1, i, j, k, -i, -j, -k, -1\}$*

18. *Determine os centros de $Q = \{1, i, j, k, -i, -j, -k, -1\}$ e do grupo 4 de Klein.*

19. *Determine a ordem de cada um dos seguintes elementos:*

(a) $(\overline{3}, \overline{4})$ *em* $\mathbb{Z}_4 \times \mathbb{Z}_6$

(b) $(\overline{6},\ \overline{15},\ \overline{4})$ *em* $\mathbb{Z}_{30} \times \mathbb{Z}_{45} \times \mathbb{Z}_{24}$

(c) $(\overline{5},\ \overline{10},\ \overline{15})$ *em* $\mathbb{Z}_{25} \times \mathbb{Z}_{25} \times \mathbb{Z}_{25}$

(d) $(\overline{8},\ \overline{8},\ \overline{8})$ *em* $\mathbb{Z}_{10} \times \mathbb{Z}_{24} \times \mathbb{Z}_{80}$

20. *Seja G um grupo. Dados H um subgrupo de G e* $a \in G$*, mostre que*

$$aHa^{-1} = \{aha^{-1}\ h \in H\}$$

é um subgrupo de G. Se H é finito, qual é a ordem de aHa^{-1}?

21. *Considere o produto direto* $G_1 \times G_2$ *dos grupos* G_1 *e* G_2*. Sejam* $a \in G_1$ *e* $b \in G_2$ *elementos de ordens m e n respectivamente. Determine a ordem de* $(a, b) \in G_1 \times G_2$.

22. *Seja G um grupo e sejam* $a, b \in G$ *tais que* $ab = ba$*. Se a e b tem ordens m e n respectivamente com* $mdc(m, n) = 1$*, mostre que a ordem de ab é mn.*

23. *Seja G um grupo abeliano que contém um elemento de ordem n e um de ordem m. Mostre que G contém um elemento de ordem* $mmc(n, m)$.

24. *Prove que se G é um grupo finito com elemento neutro e, e* $m = |G|$*, então* $x^m = e$ *para todo elemento* $x \in G$.

25. *Determine todos os subgrupos de* $\mathbb{Z}_{20}$.

26. *Determine todos os subgrupos não cíclicos de ordem 4 de* $\mathbb{U}_{33}$.

27. *Determine 2 subgrupos não cíclicos de ordem 4 de* $\mathbb{U}_{40}$.

Aula 1.2

Grupos de Permutações e Grupos Diedrais

Nesta aula vamos estudar exemplos de grupos não-abelianos (finitos), os grupos de permutações e diedrais. O grupo de permutações é formado por funções bijetoras de um conjunto em si mesmo. O grupo diedral é formado por simetrias de um polígono regular.

1.2.1 O grupo simétrico

Definição 1.2.1. *Seja X um conjunto qualquer. Uma bijeção $f : X \to X$ chama-se uma* **permutação**. *Denote-se por S_X o conjunto de todas as permutações de X, isto é*

$$S_X := \{f : X \to X \mid f \text{ é uma bijeção}\}.$$

Proposição 1.2.1. *O conjunto S_X é um grupo com respeito a operação, $\circ$, a composição de funções. Chamamos este grupo $\left(S_X, \circ\right)$ de* **grupo simétrico de** *X ou* **o grupo de permutações de** *X.*

Demonstração. A demonstração é deixada a cargo do leitor como exercício. ■

Em geral o grupo S_X não é abeliano. O grupo S_X só será abeliano se o conjunto X tiver um ou dois elementos.

Estamos particularmente interessados no caso em que o conjunto X é um conjunto finito de n elementos, por exemplo, vamos considerar $X = \{1,\ 2,\ 3, \cdots, n\}$. *Neste caso* S_X *será denotado por* S_n *e será chamado* **grupo simétrico** *ou* **grupo das permutações** *de grau n.*

Notação: *Dado* $f \in S_n$ *é usual representar* f *através de uma matriz* $2 \times n$, *da seguinte maneira:*

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$$

Tem-se na primeira linha os elementos de $\{1, 2, \cdots, n\}$ *e abaixo de cada* i, $1 \leq i \leq n$ *temos a sua imagem* $f(i)$.

Exemplo 1.2.1. *Sejam* f, g *permutações do conjunto* $\{1, 2, 3, 4, 5\}$ *dados por*

$$f(1) = 2,\ f(2) = 4,\ f(3) = 3,\ f(4) = 5,\ f(5) = 1.$$

$$g(1) = 5,\ g(2) = 4,\ g(3) = 1,\ g(4) = 2,\ f(5) = 3.$$

Expresse f, g *na notação matricial e determine* $(f \circ g)$, $(g \circ f)$ *e* f^{-1}.

Solução. *Na notação de uma matriz temos que*

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$

Composição de permutações na notação matricial é realizada da direita para a esquerda indo de cima para baixo, depois novamente a partir de cima para baixo. Primeiro precisa encontrar o número abaixo de 1 na permutação a direta e depois encontrar este número na linha superior da permutação esquerda e anote o número diretamente abaixo dele. Repita este processo para o resto do números inteiros de 2 a n.

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & & & & \downarrow \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & & & & \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ f(g(1)) & f(g(2)) & f(g(3)) & f(g(4)) & f(g(5)) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ f(5) & f(4) & f(1) & f(2) & f(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}.$$

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & \downarrow & & & \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & & & & \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ g(f(1)) & g(f(2)) & g(f(3)) & g(f(4)) & g(f(5)) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ g(2) & g(4) & g(3) & g(5) & g(1) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}.$$

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} \Rightarrow f^{-1} = \begin{pmatrix} 2 & 4 & 3 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}.$$

Observação. *Vamos denotar* $(f \circ g)$ *por* fg *e* $(f \circ f)$ *por* f^2.

Teorema 1.2.2. *Seja* $n \geq 1$. *O grupo das permutações* S_n *de grau* n *tem* $n!$ *elementos.* S_n *não abeliano para* $n \geq 3$.

Demonstração. Seja $f \in S_n$. Temos n possibilidades para a imagem $f(1)$, $(n-1)$ possibilidades para $f(2)$, $(n-2)$ possibilidades para $f(3)$, $\cdots$, 2 possibilidades para $f(n-1)$ e uma possibilidade para $f(n)$. Portanto pelo principio da multiplicação, f é uma das $n(-1)(n-2)\cdots 2\cdot 1 = n!$ bijeções possíveis. Portanto $|S_n| = n!$. ■

Exemplo 1.2.2 (O grupo S_3)**.** *Seja* S_3 *denota o conjunto das bijeções* $\{1,2,3\} \to \{1,2,3\}$. *Então* S_3 *é um grupo com 6 elementos, com operação composição de funções . Logo*

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

Sejam $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *e* $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. *Então*

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

$$\alpha^3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = id.$$

$$\beta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = id.$$

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

$$\beta\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \beta\alpha^2.$$

Portanto, S_3 pode ser escrito como

$$S_3 = \{id,\ \alpha,\ \alpha^2,\ \beta,\ \beta\alpha,\ \beta\alpha^2\} =< \alpha, \beta \mid \alpha^3 = id,\ \beta^2 = id >$$

e sua tabela de Cayley será:

$\cdot$	id	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
id	id	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
α	α	α^2	id	$\beta\alpha^2$	β	$\beta\alpha$
α^2	α^2	id	α	$\beta\alpha$	$\beta\alpha^2$	β
β	β	$\beta\alpha$	$\beta\alpha^2$	id	α	α^2
$\beta\alpha$	$\beta\alpha$	$\beta\alpha^2$	β	α^2	id	α
$\beta\alpha^2$	$\beta\alpha^2$	β	$\beta\alpha$	α	α^2	id

Ainda se nota, da tábua acima, que S_3 não abeliano nem cíclico (gerada pela permutações α e β).

1.2.2 Ciclos e Transposições

Definição 1.2.2. *Uma permutação $\sigma \in S_n$ é chamada de $k-$***ciclo** *se existem elementos distintos $a_1, a_2, \cdots, a_k \in \{1, 2, \cdots, n\}$ tais que*

$$\begin{cases} \sigma(a_1) = a_2 \\ \sigma(a_2) = a_3 \\ \vdots \\ \sigma(a_{k-1}) = a_k \\ \sigma(a_k) = a_1 \\ \sigma(a_j) = a_j, \ \forall j \in \{1, \cdots, n\} \setminus \{a_1, a_2, \cdots, a_k\}. \end{cases}$$

Tal $k-$ciclo será denotado por $(a_1\ a_2 \cdots a_k)$, k é chamado o **comprimento** *do ciclo. Os 2-ciclos são também chamados de* **transposições.**

Definimos o suporte de σ sendo o conjunto

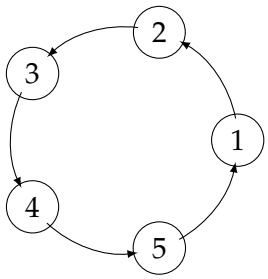
$$supp(\sigma) = \{j \in \{1, 2, \cdots, n\} \ : \ \sigma(j) \neq j\} = \{a_1,\ a_2, \cdots, a_k\}.$$

ou seja o $supp(\sigma)$ é o conjunto dos números que são movidos por σ.

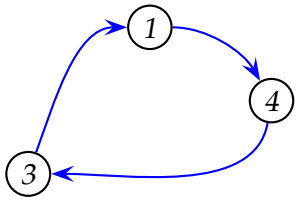
Observação. *Note-se que a notação $\sigma = (a_1\ a_2 \cdots a_k)$ é ambígua. Para ser precisa, é necessário indicar o grupo S_n ao qual σ pertence.*

Exemplo 1.2.3 (Exemplos em S_5)**.**

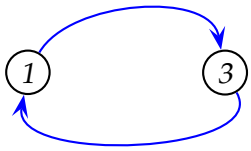
(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ *é um 5-ciclo, denotado por* (1 2 3 4 5)*; ele poderia também ser denotado por* (2 3 4 5 1)*, ou* (3 4 5 1 2)*, ou* (4 5 1 2 3)*, ou* (5 1 2 3 4).



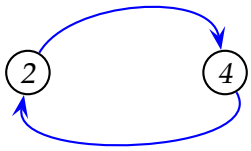
(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$ *é um 3-ciclo, denotado por* (1 4 3)*; ele poderia também ser denotado por* (4 3 1)*, ou* (3 1 4).



(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$ *é uma transposição, denotada por* (1 3)*; ela poderia também ser denotado por* (3 1).



(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$ *é uma transposição, denotada por* (2 4) *ou por* (4 2).



(e) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ *não é um $k-$ciclo, qualquer que seja k.*

Observação. *O único 1-ciclo é a identidade, que denotamos por* (1) *ou por* (a) *com* $a \in \{1, 2, 3, \cdots, n\}$.

Lema 1.2.3. *Se* $x \in supp(\sigma)$ *então* $\sigma(x) \in supp(\sigma)$.

Demonstração. Se $x \in \text{supp}(\sigma)$ então

$$\begin{aligned} \sigma(x) &\neq x \\ \sigma\big(\sigma(x)\big) &\neq \sigma(x) \neq x \quad \text{pois } \sigma \text{ é uma bijeção.} \end{aligned}$$

Portanto, $\sigma(x) \in \text{supp}(\sigma)$. ■

Definição 1.2.3. *Sejam* $\alpha \in S_n$ *um* $r-ciclo$ *e* $\beta \in S_n$ *um* $s-ciclo$. *Dizemos que* α *e* β *são* **disjuntos** *se* $supp(\alpha) \cap supp(\beta) = \emptyset$.

Exemplo 1.2.4 (Exemplos em S_5 :)**.**

(a) Os ciclos (1 3 4) *e* (2 5) *são disjuntos.*

(b) Os ciclos (1 4) *e* (2 5) *são disjuntos.*

(c) Os ciclos (1 3 5) *e* (2 5) *não são disjuntos, pois elemento 5 é movido por ambos.*

Lema 1.2.4. *Sejam* $\alpha,\ \beta \in S_n$ *dois ciclos disjuntos. Então* $\alpha\beta = \beta\alpha$.

Demonstração. Seja $x \in S_n$. Temos 3 casos a considerar:

1º caso: $x \notin \text{supp}(\beta)$ e $x \notin \text{supp}(\alpha)$ então

$$\alpha(\beta(x)) = \alpha(x) = x \quad \text{e} \quad \beta(\alpha(x)) = \beta(x) = x.$$

2º caso: $x \in \text{supp}(\alpha)$. Neste caso pelo Lema 1.2.3 temos que $\alpha(x) \in \text{supp}(\alpha)$.

Mas como $\text{supp}(\alpha) \cap \text{supp}(\beta) = \emptyset$ temos que $x \notin \text{supp}(\beta)$ e $\alpha(x) \notin \text{supp}(\beta)$. Então

$$\alpha(\beta(x)) = \alpha(x) \quad \text{e} \quad \beta(\alpha(x)) = \alpha(x).$$

3º caso: $x \in \text{supp}(\beta)$. Análoga ao 2º caso.

Assim $\alpha\beta(x) = \beta\alpha(x)$, $\forall x \in \{1, 2, \cdots, n\}$. Portanto $\alpha\beta = \beta\alpha$. ■

Proposição 1.2.5. *Toda a permutação de $\alpha \in S_n$ é um produto de ciclos disjuntos. Além disso, o produto é único a menos da permutação identidade e da ordem dos fatores.*

Demonstração. A demonstração desta será omitida, mas pode ser vista em [1]. ■

Exemplo 1.2.5. *Escreva a permutação* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 6 & 3 & 7 & 1 & 8 & 2 & 5 \end{pmatrix} \in S_9$ *como produto de ciclos disjuntos.*

Solução. *Começa com 1, e encontrar o ciclo que ela determina:*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & & \downarrow & \downarrow & & \downarrow & & & \\ 4 & 9 & 6 & 3 & 7 & 1 & 8 & 2 & 5 \end{pmatrix}$$

Portanto temos o ciclo

$$(1\ 4\ 3\ 6).$$

Agora vamos para o próximo inteiro menor, que é 2, e determinamos seu ciclo:

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

Portanto, temos o ciclo

$$(2\ 9\ 5\ 7\ 8).$$

Logo

$$\alpha = (1\ 4\ 3\ 6)(2\ 9\ 5\ 7\ 8).$$

1.2.3 Aplicações dos ciclos

O fato que podemos decompor qualquer $\alpha \in S_n$ como produto de ciclos disjuntos forneça muito informação sobre S_n e facilita bastante as simplificações.

Lema 1.2.6. *Seja $\alpha = (a_1\ a_2\ a_3 \cdots\ a_{k-1}\ a_k) \in S_n$ um k-ciclo. Então α^{-1} é um k-ciclo também e tem-se*

$$\alpha^{-1} = (a_1\ a_k\ a_{k-1} \cdots\ a_3\ a_2).$$

Demonstração. Temos que

$$(a_1\ a_2\ a_3 \cdots\ a_{k-1}\ a_k)(a_1\ a_k\ a_{k-1} \cdots\ a_3\ a_2) = (1) \text{ (identidade).}$$

■

Exemplo 1.2.6. *Sejam $\alpha = (1\ 3\ 5)(2\ 4)$, $\beta = (1\ 2\ 4)(3\ 5) \in S_5$. Calcular*

$(a)\ \alpha\beta \qquad (b)\ \beta\alpha \qquad (c)\ \alpha^{-1} \qquad (d)\ \beta^{-1}$.

Solução.

(a) $\alpha\beta = (1\ 3\ 5)\ (2\ 4)\ (1\ 2\ 4)\ (3\ 5) = (1\ 4\ 3)$.

(b) $\beta\alpha = (1\ 2\ 4)\ (3\ 5)\ (1\ 3\ 5)\ (2\ 4) = (1\ 5\ 2)$.

(c) $\alpha^{-1} = (2\ 4)^{-1}(1\ 3\ 5)^{-1} = (4\ 2)(1\ 5\ 3) = (1\ 5\ 3)(2\ 4)$.

(d) $\beta^{-1} = (3\ 5)^{-1}(1\ 2\ 4)^{-1} = (5\ 3)(1\ 4\ 2) = (1\ 4\ 2)(5\ 3)$.

Proposição 1.2.7 (Ordem de um ciclo). *A ordem de um k-ciclo é k, ou seja, a ordem de um ciclo é simplesmente o comprimento do ciclo.*

Demonstração. Seja $\alpha = (a_1\ a_2\ a_3 \cdots\ a_{k-1}\ a_k) \in S_n$ um k-ciclo. Seja $1 \leq m < k$. Tem-se

$$\alpha^m(a_1) = \alpha^{m-1}(a_2) = \alpha^{m-2}(a_3) = \cdots = \alpha^2(a_{m-1}) = \alpha(a_m) = a_{m+1}.$$

Então $\alpha^m(a_1) = a_{m+1} \neq a_1$ mostra que a ordem $\alpha \geq k$.

Temos

- $\alpha^k(a_1) = \alpha\left(\alpha^{k-1}(a_1)\right) = \alpha(a_{(k-1)+1}) = \alpha(a_k) = a_1$.
- Para qualquer $1 < i \leq k$ tem-se

$$\alpha^k(a_i) = \alpha^k\left(\alpha^{i-1}(a_1)\right) = \alpha^{i-1}\left(\alpha^k(a_1)\right) = \alpha^{i-1}(a_1) = a_i.$$

Portanto k é a ordem de α. ■

Exemplo 1.2.7. *Determine a ordem da permutação* $w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 1 & 4 & 2 & 6 & 3 & 8 \end{pmatrix} \in S_8$.

Solução. *Escrevendo w como um ciclo temos que*

$$w = (1\ 5\ 2\ 7\ 3)$$

ou seja, w é um 5-ciclo. Portanto ord$(w) = 5$.

Teorema 1.2.8. *Sejam* $\sigma \in S_n$ *e* $\sigma = \sigma_1\sigma_2\cdots\sigma_m$ *é um produto de ciclos disjuntos, onde cada* σ_j *tem comprimento* k_j. *Então*

$$ord(\sigma) = MMC(k_1, \cdots, k_m).$$

Demonstração. Seja ord$(\sigma) = s$. Como ciclos disjuntos comuta, temos que $\sigma^s = \sigma_1^s\sigma_2^s\cdots\sigma_m^s$. Mas

$$\sigma^s = (1) \iff \sigma_i^s = (1),\ \forall i = 1, \cdots, m.$$

Como cada σ_j tem ordem k_j, temos que $k_j \mid s$ para $j = 1, 2, \cdots, m$.

Portanto $MMC(k_1, \cdots, k_m) \mid s$.

Mas $M = MMC(k_1, \cdots, k_m)$ é o menor M tal que $\sigma_i^M = (1)$ para $i = 1, 2, \cdots, m$. Logo $M \mid s$. Portanto

$$\text{ord}(\sigma) = MMC(k_1, \cdots, k_m).$$

■

Exemplo 1.2.8. *Determine a ordem de* $\tau = (1\ 2\ 5\ 8\ 13)\ (3\ 4\ 9)\ (10\ 12) \in S_{13}$ *e expressa* τ^{245} *em ciclos.*

Solução.

$$ord(\tau) = MMC(5,3,2) = 30.\ \textit{Portanto}\ \ \tau^{30} = id.$$

$$\begin{aligned}\tau^{245} &= (\tau^{30})^8 \cdot \tau^5 = id^8 \cdot \tau^5 = \tau^5 \\ &= (1\ 2\ 5\ 8\ 13)^5\ (3\ 4\ 9)^5\ (10\ 12)^5 \\ &= (3\ 4\ 9)^2\ (10\ 12) \\ &= (3\ 9\ 4)\ (10\ 12).\end{aligned}$$

Exemplo 1.2.9. *Determine a ordem* $\alpha = (1\ 2\ 4)(3\ 4\ 5)$.

Solução. *Observe que* α *não é um produto de ciclos disjuntos. Portanto não podemos aplicar o Teorema 1.2.8. Então reescrevemos* α *como*

$$\alpha = (1\ 2\ 4)(3\ 4\ 5) = (1\ 2\ 4\ 5\ 3).$$

Portanto, a ordem de $\alpha = 5$.

1.2.4 Permutações pares e ímpares

Definição 1.2.4. *Um 2-ciclo diz-se uma transposição.*

Teorema 1.2.9. *Toda a permutação é produto de transposições.*

Demonstração. Seja $\alpha = (a_1\ a_2\ \cdots\ a_{m-1}\ a_m)$ um m-ciclo. Então

$$\alpha = (a_1\ a_m)\ (a_1\ a_{m-1}) \cdots (a_1\ a_2).$$

Logo α é produto de transposições. Pelo Proposição 1.2.5 toda a permutação é produto de ciclos. Como todo ciclo é produto de transposições também toda a permutação é produto de transposições. ■

Exemplo 1.2.10. *Escreva* $\alpha = (1\ 3\ 2\ 8)(4\ 6\ 5)$ *como produto de transposições.*

Solução. *Podemos escrever o primeiro ciclo como*

$$(1\ 3\ 2\ 8) = (1\ 8)\ (1\ 2)\ (1\ 3)$$

e o segundo ciclo é

$$(4\ 6\ 5) = (4\ 5)\ (4\ 6).$$

Portanto

$$\alpha = (1\ 8)\ (1\ 2)\ (1\ 3)\ (4\ 5)\ (4\ 6).$$

Observações.

(a) As transposições que compor uma permutação não precisam ser disjuntas.

(b) A fatorização em transposições não é única como podemos ver no exemplo no 3-ciclo $(1\ 3\ 2)$:

$$\begin{aligned}(1\ 3\ 2) &= (1\ 2)\ (1\ 3).\\ (1\ 3\ 2) &= (3\ 1)\ (3\ 2).\\ (1\ 3\ 2) &= (1\ 2)\ (1\ 3)\ (3\ 2)(3\ 2).\end{aligned}$$

Lema 1.2.10. *Se a permutação identidade e escrito como produto de r transposições: isto é se*

$$id = \sigma_1\sigma_2\cdots\sigma_r,$$

onde os σ*'s são transposições, então r é um número par.*

Demonstração. A demonstração desta será omitida, mas pode ser vista em [3]. ■

Teorema 1.2.11. *Seja $\alpha \in S_n$. Suponha que α pode ser escrito de duas maneiras como produto de transposições com k e com l fatores. Então k e l são ambos números pares ou ambos ímpares, ou seja, $k + l$ é par.*

Demonstração. Suponha que

$$\alpha = \beta_1\beta_2\cdots\beta_k = \gamma_1\gamma_2\cdots\gamma_{l-1}\gamma_l$$

onde os β's e γ's são transposições. Então

$$\begin{aligned} id &= \beta_1\beta_2\cdots\beta_k\gamma_l^{-1}\gamma_{l-1}^{-1}\cdots\gamma_2^{-1}\gamma_1^{-1} \\ &= \beta_1\beta_2\cdots\beta_k\gamma_l\gamma_{l-1}\cdots\gamma_2\gamma_1 \quad \text{pois cada transposição é seu proprio inverso.} \end{aligned}$$

Portanto escrevemos *id* como produto de $k + l$ transposições. Pela Lema 1.2.10, $(k + l)$ deve ser um número par. Portanto ou ambos k e l são números pares ou ambos são números impares. ■

Definição 1.2.5. *Uma permutação diz-se* **par** *se é produto de um número par de transposições e* **ímpar** *se é produto de um número ímpar de transposições.*
Definimos a função $sgn : S_n \to \{-1, 1\}$ com

$$sgn(\sigma) = \begin{cases} -1, & se\ \sigma\ é\ ìmpar \\ 1, & se\ \sigma\ é\ par \end{cases}$$

$sgn(\sigma)$ diz-se **o sinal** *de σ.*

Exemplo 1.2.11. *Seja $\sigma = (1\ 2\ 3\ 4\ 5) \in S_5$. Temos $\sigma = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$. Logo σ é uma permutação par e $sgn(\sigma) = 1$.*

Observação. *Se $\sigma = t_1\cdots t_k$ é produto de transposições então $sgn(\sigma) = (-1)^k$.*

Proposição 1.2.12. *Seja $n \geq 2$ e sejam $\sigma, \tau \in S_n$. Tem-se*

(i) $sgn(id) = 1$;

(ii) $sgn(\sigma\tau) = sgn(\sigma) \cdot sign(\tau)$;

(iii) $sgn(\sigma^{-1}) = sgn(\sigma)$;

(iv) se $\sigma = (a_1\ a_2 \cdots\ a_{m-1}\ a_m)$ *é um* $m-$*ciclo então* $sgn(\sigma) = (-1)^{m-1}$.

Demonstração.

(i) Pela Lema 1.2.10, a permutação identidade (1) ou *id* é uma permutação par, logo $sgn(id) = 1$.

(ii)Se σ, τ são ambos pares, então $\sigma\tau$ é par e

$$sgn(\sigma\tau) = 1 = 1 \cdot 1 = sgn(\sigma)sgn(\tau).$$

Se σ, τ são ambos impares, então $\sigma\tau$ é par e

$$sgn(\sigma\tau) = 1 = -1 \cdot -1 = sgn(\sigma)sgn(\tau).$$

Se σ é par e τ impar, então $\sigma\tau$ é impar e

$$sgn(\sigma\tau) = -1 = -1 \cdot 1 = sgn(\sigma)sgn(\tau).$$

(iii) Se $\sigma = \sigma_1\sigma_2 \cdots \sigma_{k-1}\sigma_k$ produto de k transposições então $\sigma^{-1} = \sigma_k\sigma_{k-1} \cdots \sigma_2\sigma_1$. Portanto, $sgn(\sigma) = sgn(\sigma^{-1})$.

(iv) Seja $\sigma = (a_1\ a_2 \cdots\ a_{m-1}\ a_m)$ um $m-$ciclo. Podemos escrever σ como $(m-1)$ transposições, isto é

$$\sigma = (a_1\ a_m)(a_1\ a_{m-1}) \cdots (a_1\ a_2).$$

Portanto,

- se m é par temos que $m-1$ é impar e $sgn(\sigma) = -1 = (-1)^{m-1}$.
- se m é impar temos que $m-1$ é par e $sgn(\sigma) = +1 = (-1)^{m-1}$.

Em ambos os casos temos que $sgn(\sigma) = (-1)^{m-1}$.

■

1.2.5 Grupo alternado

Definição 1.2.6. *Denotamos por A_n o subconjunto de S_n das permutações pares, ou seja,*

$$A_n = \{\alpha \in S_n \mid \alpha \text{ é uma permutação par}\}.$$

Teorema 1.2.13. *A_n é um subgrupo de S_n, chamado de* **grupo alternado de grau** *n.*

Demonstração. Da Proposição 1.2.12 decorre que

- Para duas permutações pares $\sigma, \tau \in A_n$ a composição $\sigma\tau$ pertence A_n.
- $id \in A_n$.
- Se $\sigma \in A_n$ então $\sigma^{-1} \in A_n$.

Portanto $A_n \leq S_n$. ■

Teorema 1.2.14. *Seja $n \geq 2$. Tem-se que A_n tem $\frac{n!}{2}$ elementos.*

Demonstração. A demonstração pode ser vista em [1]. ■

Exemplo 1.2.12.

(a) Se $n = 2$, então $|A_2| = 1$ e $A_2 = \{id\}$.

(b) Se $n = 3$, então $|A_3| = 3$ e $A_3 = \{id,\ (1\ 2\ 3),\ (1\ 32)\}$.

Os 3-ciclos são os ciclos de menor cumprimento que são permutações pares e, de fato, para $n \geq 3$, toda a permutação de A_n é produto de 3-ciclos.

Teorema 1.2.15. *Seja $n \geq 3$. Toda a permutação em A_n é produto de 3-ciclo. De fato temos que,*

- $(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d)$.
- $(a\ c)(a\ b) = (a\ b\ c)$.

Demonstração. Todos os 3-ciclos pertencem a A_3, pois são todas permutações pares. Agora seja $\sigma \in A_n$. Então $\sigma = \tau_1\tau_2\cdots\tau_{2r-1}\tau_{2r}$ é um produto de um número par de transposições. Portanto podemos escrever $\sigma = (\tau_1\tau_2)\cdots(t_{2r-1}\tau_{2r})$. Agora o produto de transposições $\tau\tau'$ tem a forma $(a\ b)(a\ b)$ ou $(a\ b)(a\ c)$ ou $(a,\ b)(c\ d)$, onde a, b, c, d são distintos. Calculando temos

$$(a\ b)(a\ b) = Id, \quad (a\ c)(a\ b) = (a\ b\ c) \text{ e } (a\ b)(c\ d) = (a\ c\ b)(a\ c\ d).$$

Isto mostra que σ é um produto de 3-ciclos. ■

Exemplo 1.2.13. *Seja $n = 5$ e seja $\alpha = (1\ 3)(2\ 4)(5\ 4)(2\ 4) \in A_5$. Escreva α como produto de triciclos.*

Solução. *Tem-se*

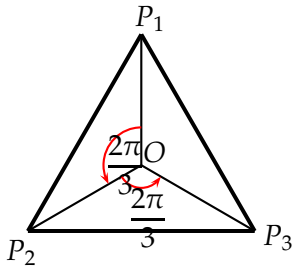
$$(1\ 3)(2\ 4) = (1\ 2\ 4)(1\ 3\ 4) \quad e \quad (5\ 4)(2\ 4) = (2\ 5\ 4).$$

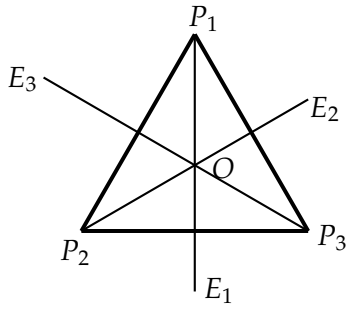
Logo

$$\alpha = (1\ 2\ 4)(1\ 3\ 4)(2\ 5\ 4).$$

1.2.6 O grupo, D_3, das simetrias do triângulo equilátero

Seja $P_1P_2P_3$ um triângulo equilátero. Sejam E_1, E_2, E_3 as mediatrizes do triângulo e O o baricentro. Vamos considerar o conjunto das transformações que preservam o triângulo, com a operação de composição.





Essa transformações consistem em:

- $id, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}$: *as rotações centradas em O, no sentido anti-horário, de ângulos zero,* $\frac{2\pi}{3}$ *e* $\frac{4\pi}{3}$ *respectivamente.*

- F_1, F_2, F_3 : *as reflexões em torno da reta mediatriz* E_1, E_2, E_3 *respectivamente.*

Denotamos por D_3*, o conjunto dessas seis simetrias do triângulo equilátero:*

$$D_3 = \{id, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, F_1, F_2, F_3\}.$$

D_3 *muindo da operação de composição de funções é um grupo não-abeliano finito de ordem 6.*

Sejam $r = R_{\frac{2\pi}{3}}$ *e* $s = F_1$*. Vamos mostrar a diante que* D_3 *é gerada por r e s. Observe que*

- $r^2 = R_{\frac{2\pi}{3}} \circ R_{\frac{2\pi}{3}} = R_{\frac{4\pi}{3}}$.

- $r^3 = r^2 \circ r = id$.

- $s^2 = F_1 \circ F_1 = id$.

- $sr = F_1 \circ R_{\frac{2\pi}{3}} = F_2$.

- $sr^2 = F_1 \circ R_{\frac{4\pi}{3}} = F_3$.

- $rs = R_{\frac{2\pi}{3}} \circ F_1 = F_3 = sr^2$.

Portanto, D_3 *pode ser escrito como*

$$\begin{aligned} D_3 &= \{id, r, r^2, s, sr, sr^2;\ \ r^3 = id,\ s^2 = id,\ rs = sr^2\} \\ &= \{s^i r^j;\ \ i = 0, 1,\ j = 0, 1, 2,\ r^3 = id,\ s^2 = id,\ rs = sr^2\} \\ &= < s, r \mid r^3 = id,\ s^2 = id,\ rs = sr^{-1} > . \end{aligned}$$

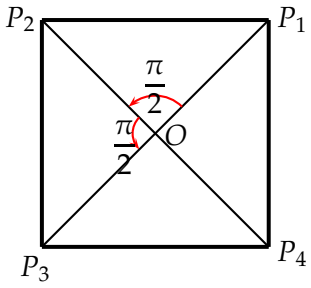
e sua tábua será:

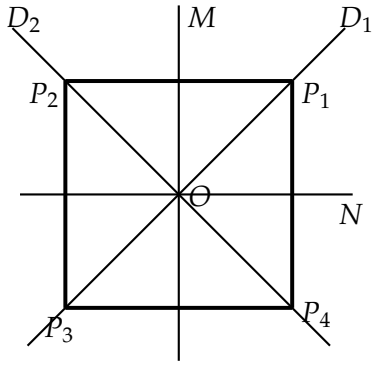
$\cdot$	id	r	r^2	s	sr	sr^2
id	id	r	r^2	s	sr	sr^2
r	r	r^2	id	sr^2	s	sr
r^2	r^2	id	r	sr	sr^2	s
s	s	sr	sr^2	id	r	r^2
sr	sr	sr^2	s	r^2	id	r
sr^2	sr^2	s	sr	r	r^2	id

Observe que esta tabua é a mesma que a de S_3. Isto essencialmente mostra que S_3 e D_3 são grupos isomorfos: "eles são o mesmo grupo vestida até em diferentes disfarces." Neste caso, não é difícil identificar D_3 com S_3, pois os elementos de D_3 podem ser visualizados como permutações dos vértices. Em geral, podemos visualizar os elementos de D_n como permutações dos vértices do polígono regular de n lados, mas não podemos fazer todas as permutações desta forma. Em outras palavras, veremos que D_n e S_n não são os mesmos. Uma forma de verifique este fato é observar que $D_n = 2n$ mas $S_n = n!$, e esses são apenas iguais quando $n = 3$.

1.2.7 O grupo, D_4, das simetrias do quadrado

Seja $P_1P_2P_3P_4$ um quadrado. Sejam D_1, D_2 as diagonais e M, N as mediatrizes do quadrado e O o baricentro. Vamos considerar o conjunto das transformações que preservam o quadrado, com a operação de composição.





Essa transformações consistem em:

- *$id, R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3\pi}{2}}$: as rotações centradas em O, no sentido anti-horário, de ângulos zero, $\frac{\pi}{2}$, π e $\frac{3\pi}{2}$ respectivamente.*

- *F_1, F_2, F_3, F_4 : as reflexões em torno das retas D_1, D_2, M, N respectivamente.*

Denotamos por D_4, o conjunto dessas oito simetrias do quadrado:

$$D_4 = \{id, R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3\pi}{2}}, F_1, F_2, F_3, F_4\}.$$

D_4 muindo da operação de composição de funções é um grupo não-abeliano finito de ordem 8 (faça a tabela de multiplicação e verifique os axiomas).

Sejam $r = R_{\frac{\pi}{2}}$ e $s = F_3$. Mostrar que D_4 é gerada por r e s, isto é, qualquer elemento de D_4 é um

produto de alguns r com alguns s. De fato,

$$\begin{aligned} D_4 &= \{id, r, r^2, r^3, s, sr, sr^2, sr^3;\ r^4 = id,\ s^2 = id,\ rs = sr^3\} \\ &= \{s^i r^j;\ \ i = 0, 1,\ j = 0, 1, 2, 3,\ r^4 = id,\ s^2 = id,\ rs = sr^3\} \\ &= < s, r \mid r^4 = id,\ s^2 = id,\ rs = sr^{-1} > . \end{aligned}$$

1.2.8 O grupo, D_n, das simetrias do polígono regular

Mais geral, seja $n \geq 3$ um inteiro, e seja P_n um polígono regular de n lados no plano $\mathbb{R}^2$. Então há exatamente $2n$ simetrias de P_n :

- *n rotações de angulo $\dfrac{2k\pi}{n}$ em torno do centro de P_n para $k = 0, 1, 2, \cdots n-1$, no sentido anti-horário;*
- *e n reflexões em torno dos eixos de simetria de P_n.*

Denotando por r a rotação de $\dfrac{2\pi}{n}$, o conjunto das rotações é:

$$\{id,\ r,\ r^2,\ \cdots, r^{n-1}\}.$$

Se s é a reflexão em torno de um eixo de simetria, de P_n, então todas as outras reflexões são da forma $sr^i,\ \ i = 1, \cdots, n-1$.

Assim, temos que:

$$D_n = \{id,\ r,\ r^2,\ \cdots, r^{n-1},\ s,\ sr,\ sr^2,\ sr^{n-1}\}$$

sendo $r^n = id,\ \ s^2 = id$ e $sr^{n-1} = rs$, ou seja

$$D_n =< s, r \mid r^n = id,\ s^2 = id,\ rs = sr^{-1} > .$$

Teorema 1.2.16. *O conjunto das simetrias de P_n forma um grupo para o composição de simetrias, denotado por D_n e chama-se o* **o grupo diedral** *de ordem $2n$.*

1.2.9 Teorema de Cayley

O Teorema de Cayley dá a importância dos grupos de permutação para Teoria do Grupos, pois permite representa qualquer grupo com um subgrupo conveniente do grupo de permutações.

Teorema 1.2.17 (Teorema de Cayley)**.** *Se G é um grupo então ele é isomorfo a um subgrupo de S_G. Em particular, se G tem ordem n então G é isomorfo a um subgrupo de S_n.*

Exemplo 1.2.14. *Seja $G = \mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. Então G é isomorfo ao subgrupo*

$$G' = \{id,\ (0\ 1\ 2\ 3),\ (0\ 2)(1\ 3),\ (0\ 3\ 2\ 1)\}$$

de S_4 (das permutações do conjunto $\{0,1,2,3\}$) pela isomorfismo:

$$\varphi : \mathbb{Z}_4 \to G'$$

definida por

$$\varphi(\overline{0}) = id$$

$$\varphi(\overline{1}) = (0\ 1\ 2\ 3)$$

$$\varphi(\overline{2}) = (0\ 2)(1\ 3)$$

$$\varphi(\overline{3}) = (0\ 3\ 2\ 1)$$

Observação. *À primeira vista, este teorema parece ser uma ferramenta para responder a todas as perguntas sobre grupos. No entanto, na prática examinando todos os grupos de permutação sobre conjuntos de todos os tamanhos seria uma tarefa enorme. Até mesmo os grupos finito de permutação S_n fica complicado para analisar quando n é suficiente grande. A importância do Teorema de Cayley é mais teórica do que prático. Ele mostra que é possível visualizar o teoria dos grupos como o estudo de grupos de permutação. Em outras palavras, grupos de permutação são um modelo universal para todos os grupos possíveis. O teorema de Cayley é um exemplo do que é conhecido como um teorema de representação - ele diz que cada grupo pode ser representado como (ou seja, é isomorfo) a algo razoavelmente concreto.*

1.2.10 Exercícios Resolvidos

Exercício 1.2.1. *Dadas as permutações em S_{10}*

$$\alpha = (1\ 2\ 6\ 9\ 4)(2\ 3\ 5\ 8)(2\ 4\ 10\ 5\ 3) \quad e \quad \beta = (1\ 2\ 7\ 5\ 8)(4\ 8\ 5\ 7)(3\ 10\ 7\ 2\ 4).$$

(a) Calcule $\alpha\beta$, $\alpha^{-1}\beta$ e $\beta^{-1}\alpha\beta$, deixando suas respostas como produtos de ciclos disjuntos, e determine as ordens destas permutações.

(b) Determine $m, n \geq 1$ tal que $\alpha^m = \beta^n$ sendo que nem α^m nem β^n são as permutações identidade.

Solução.

$$\begin{aligned}\alpha &= (1\ 2\ 6\ 9\ 4)(2\ 3\ 5\ 8)(2\ 4\ 10\ 5\ 3)\\ &= (1\ 2)(3)(4\ 10\ 8\ 6\ 9)(5)(7)\\ &= (1\ 2)(4\ 10\ 8\ 6\ 9)\end{aligned}$$

$ord(\alpha) = 10.$

$$\begin{aligned}\beta &= (1\ 2\ 7\ 5\ 8)(4\ 8\ 5\ 7)(3\ 10\ 7\ 2\ 4)\\ &= (1\ 2)(3\ 10\ 4)(5)(6)(7)(8)(9)\\ &= (1\ 2)(3\ 10\ 4)\end{aligned}$$

$ord(\beta) = 6.$

(a)

$$\begin{aligned}\alpha\beta &= (1\ 2)(4\ 10\ 8\ 6\ 9)(1\ 2)(3\ 10\ 4)\\ &= (1)(2)(3\ 8\ 6\ 9\ 4)\\ &= (3\ 8\ 6\ 9\ 4).\end{aligned}$$

Portanto, $ord(\alpha\beta) = 5.$

$$\begin{aligned}\alpha^{-1}\beta &= (4\ 9\ 6\ 8\ 10)(1\ 2)(1\ 2)(3\ 10\ 4)\\ &= (3\ 4)(6\ 8\ 10\ 9).\end{aligned}$$

Portanto, $ord(\alpha^{-1}\beta) = 4.$

$$\begin{aligned}\beta^{-1}\alpha\beta &= (3\ 4\ 10)(1\ 2)(3\ 8\ 6\ 9\ 4)\\ &= (1\ 2)(3\ 8\ 6\ 9\ 10).\end{aligned}$$

Portanto, $ord(\beta^{-1}\alpha\beta) = 10.$

(b) Queremos m, n tal que $\alpha^m = \beta^n$ sendo que $\alpha^m \neq Id$ e $\beta^n \neq Id$. Logo $m \neq 10$ e $n \neq 6$. Agora

$$\begin{aligned}\alpha^m &= \beta^n\\ \Rightarrow \alpha^m(\beta^{-1})^n &= Id\\ \Rightarrow (1\ 2)^m(4\ 10\ 8\ 6\ 9)^m(3\ 4\ 10)^n(1\ 2)^n &= Id\\ \Rightarrow (1\ 2)^{m+n}(4\ 10\ 8\ 6\ 9)^m(3\ 4\ 10)^n &= Id.\end{aligned}$$

Isso é possível se $m = 5 = ord(4\ 10\ 8\ 6\ 9)$ *e* $n = 3 = ord(3\ 4\ 10)$.

Portanto, a solução é $m = 5$ *e* $n = 3$.

Exercício 1.2.2. *No grupo* S_9 *seja* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 8 & 1 & 7 & 3 & 2 & 6 & 5 \end{pmatrix}$.

(a) Escreva α *como produto de ciclos disjuntos.*

(b) Determine a ordem de α.

(c) Calcule $\alpha(2\ 5\ 3\ 7\ 4)\alpha^{-1}$.

(d) Escreva α *como produto de transposições.*

(e) α *é par ou ímpar? Justifique.*

(f) Existe um elemento de ordem 16 *em* S_9*? Justifique.*

(g) Seja $\beta = \alpha^2$. *Escreva* β *como produto de ciclos disjuntos. Lista todos os elementos de* $< \beta >$.

Solução.

(a) $\alpha = (1\ 4\ )(2\ 9\ 5\ 7\ )(3\ 8\ 6\ )$.

(b) $ord(\alpha) = MMC(2, 4, 3) = 12$.

(c) $\alpha(2\ 5\ 3\ 7)\alpha^{-1} = (1\ 4\ )(2\ 9\ 5\ 7\ )(3\ 8\ 6\ )(2\ 5\ 3\ 7)(3\ 6\ 8)(2\ 7\ 5\ 9\ )(1\ 4) = (2\ 9\ 7\ 8)$.

(d) $\alpha = (1\ 4\ )(2\ 7\ )(2\ 5\ )(2\ 9\ )(3\ 6\ )(3\ 8\ )$.

(e) α *é par, pois* α *é produto de 6 transposições.*

(f) Não existe elemento de ordem 16 em S_9*, pois um elemento de ordem 16 deve ser um 16-ciclo, que não existe em* S_9. *O maior ciclo em* S_9 *é 9-ciclo.*

(g)

$$\begin{aligned} \beta &= \alpha^2 = (1\ 4\ )(2\ 9\ 5\ 7\ )(3\ 8\ 6\ )(1\ 4\ )(2\ 9\ 5\ 7\ )(3\ 8\ 6\ ) \\ &= (2\ 9\ 5\ 7\ )^2(3\ 8\ 6\ )^2 = (2\ 5\ )(7\ 9\ )(3\ 6\ 8\ ). \end{aligned}$$

$$\begin{aligned}\beta^2 &= (2\,5)(7\,9)(3\,6\,8)(2\,5)(7\,9)(3\,6\,8)\\ &= (3\,6\,8)^2 = (3\,8\,6).\end{aligned}$$

$$\begin{aligned}\beta^3 &= \beta\cdot\beta^2 = (2\,5)(7\,9)(3\,6\,8)(3\,8\,6)\\ &= (2\,5)(7\,9).\end{aligned}$$

$$\begin{aligned}\beta^4 &= \beta^2\cdot\beta^2 = (3\,8\,6)(3\,8\,6)\\ &= (3\,6\,8).\end{aligned}$$

$$\begin{aligned}\beta^5 &= \beta\cdot\beta^4 = (2\,5)(7\,9)(3\,6\,8)(3\,6\,8)\\ &= (2\,5)(7\,9)(3\,8\,6).\end{aligned}$$

$$\begin{aligned}\beta^6 &= \beta^3\cdot\beta^3 = (2\,5)(7\,9)(2\,5)(7\,9)\\ &= Id.\end{aligned}$$

Exercício 1.2.3. *Sejam* $\alpha=\begin{pmatrix}1&2&3&4&5&6&7&8\\6&8&1&7&5&3&4&2\end{pmatrix}$ *e* $\beta=\begin{pmatrix}1&2&3&4&5&6&7&8\\7&1&8&3&4&5&2&6\end{pmatrix}$.

(a) Expressa α *e* β *como produto de ciclos disjuntos e então como produto de transposições. Para cada um deles, diga que ele é uma permutação par ou ímpar.*

(b) Calcule α^{-1}, $\beta^{-1}\alpha$, $(\alpha\beta)^{-1}$.

(c) Determine a ordem de β *e calcule* β^{2010}.

Solução.

(a) $\alpha = (1\,6\,3)(2\,8)(4\,7) = (1\,3)(1\,6)(2\,8)(4\,7)$ *e*

$\beta = (1\,7\,2)(3\,8\,6\,5\,4) = (1\,2)(1\,7)(3\,4)(3\,5)(3\,6)(3\,8)$.

Portanto, α *e* β *são permutações pares.*

(b) $\alpha^{-1} = (4\,7)(2\,8)(1\,3\,6)$.

$\beta^{-1}\alpha = (3\ 4\ 5\ 6\ 8\ )(1\ 2\ 7\ )(1\ 6\ 3\ )(2\ 8\ )(4\ 7\ ) = (1\ 8\ 7\ 5\ 6\ 4\ )(2\ 3\ ).$

$(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1} = (3\ 4\ 5\ 6\ 8\ )(1\ 2\ 7\ )(4\ 7\ )(2\ 8\ )(1\ 3\ 6\ ) = (1\ 4\ )(2\ 3\ 8\ 7\ 5\ 6\ ).$

(c) $ord(\beta) = MMC(3,\ 5) = 15.$

Portanto, $\beta^{2010} = \left(\beta^{15}\right)^{134} = Id.$

Exercício 1.2.4. *Sejam* $\alpha = (1\ 2\ )(5\ 8\ )(3\ 4\ 6\ )(5\ 2\ )(4\ 1\ )(3\ 7\ )(6\ 7\ ) \in S_8.$

(a) Escreva α *como produto de ciclos disjuntos.*

(b) Determina a ordem de α.

(c) Será que $\alpha \in A_8$?

(d) Determine α^{-1}.

(e) Qual é a maior ordem possível de um elemento em S_8?

(f) Qual é a maior ordem possível de um elemento em A_8?

Solução.

(a) $\alpha = (\ 1\ 6\ 4\ 2\ 8\ 5\ )(\ 3\ 7\ ).$

(b) $ord(\alpha) = MMC(6, 2) = 6.$

(c) $\alpha = (\ 1\ 5\ )(\ 1\ 8\ )(1\ 2\ )(1\ 4\ )(\ 1\ 6\ )(\ 3\ 7\ )$. *Portanto* α *é uma permutação par, logo* $\alpha \in A_8$.

(d) $\alpha^{-1} = (\ 1\ 5\ 8\ 2\ 4\ 6\ )(\ 3\ 7\ ).$

(e) A maior ordem possível de um elemento em S_8 *é formado por um 3-ciclo e um 5-ciclo. Portanto a maior ordem de um elemento em* S_8 *é 15.*

(f) A maior ordem possível de um elemento em $\sigma \in A_8$ *é formado por um 3-ciclo e um 5-ciclo, pois tal elemento seu sinal é igual* $sgn(\sigma) = (-1)^2 \cdot (-1)^4 = +1$. *Logo* $\sigma \in A_8$. *Portanto a maior ordem de um elemento em* A_8 *é 15.*

1.2.11 Atividade

1. *Escreva as seguintes permutações na notação de ciclos:*

$$(a)\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} \qquad (b)\begin{pmatrix}1&2&3&4&5&6\\1&6&4&3&2&5\end{pmatrix} \qquad (c)\begin{pmatrix}1&2&3&4&5&6\\4&1&5&3&6&2\end{pmatrix}.$$

2. *Escreva as seguintes permutações em S_9 na notação matricial:*

(a) (1 2 3)(4 6 8); (b) (1 6)(4 2)(5 3); (c) (1 5 3); (d) (2 4)(3 5 7); (e) (1 9 3)(2 6)(7 8).

3. *Calcular $\sigma \circ \tau$ e $\tau \circ \sigma$ onde:*

$$(a)\ \sigma = \begin{pmatrix}1&2&3&4&5\\5&4&3&2&1\end{pmatrix}, \quad \tau = \begin{pmatrix}1&2&3&4&5\\1&3&5&4&2\end{pmatrix} \in S_5.$$

$(b)\ \sigma = (1\ 2)(5\ 6), \quad \tau = (1\ 3\ 4\ 6\ 2) \in S_6.$

$$(c)\ \sigma = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}, \quad \tau = (1\ 2)(3\ 4) \in S_4.$$

Em cada caso, dê sua resposta ambos na forma matricial e na forma de ciclos.

4. *Dadas as permutações*

$$f_1 = \begin{pmatrix}1&2&3&4&5\\3&4&2&1&5\end{pmatrix} \ e \ f_2 = \begin{pmatrix}1&2&3&4&5\\4&2&5&1&3\end{pmatrix}$$

calcule

$(a)\ f_1^2 = f_1 \circ f_1.$ $(b)\ f_1^3 = f_1^2 \circ f_1.$ $(c)\ f_1^4 = f_1^3 \circ f_1.$ $(d)\ f_2^{-1}.$ $(e)\ f_1 \circ f_2^{-1}.$ $(f)\ f_2^2.$

Em cada caso, dê sua resposta ambos na forma matricial e na forma de ciclos.

5. *Expresse como produto de ciclos disjuntos*

(a) (1 2 3)(4 5)(1 6 7 8 9)(1 5) $\in S_9$. (b) (1 2)(1 2 3)(1 2) $\in S_3$.

6. *Calcule* $a^{-1}ba$ *sendo que* $a = (1\ 3\ 5)(1\ 2) \in S_9$ *e* $b = (1\ 5\ 7\ 9) \in S_9$.

7. *Determine quantos elementos de* S_3 *são ciclos de comprimento 2 e de comprimento 3.*

8. *Encontre no* S_3 *dois elementos a e b tais que* $(ab)^2 \neq a^2b^2$.

9. *Mostre que o conjunto constituído das três permutações*

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\ e\ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

munido da operação de composição, constitui um grupo.

10. *(a) Mostre que* S_4 *contém exatamente 6 ciclos de comprimento 2, 8 de comprimento 3 e 6 de comprimento 4.*

    (b) Mostre que os elementos restantes de S_4 *forma um subgrupo H de* S_4.

    (c) Qual é a ordem de H? H é ciclo?

11. *Considere a permutação* $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 3 & 2 & 5 & 9 & 6 & 1 & 4 \end{pmatrix}$

    (a) Escreva s como produto de transposições.

    (b) s é uma permutação par ou ímpar?

    (c) É possível escrever s como produto de 10 transposições?

    (d) Complete com transposições de maneira conveniente para obter a igualdade

$$s = - - - - - - - - - - - -(2\ 5)(2\ 3)(1\ 4)(7\ 9).$$

12. *Escreva a transposição* $(4\ 8) \in S_{10}$ *como produto de transposições de números consecutivos.*

13. *Considere a permutação* $s = (1\ 4\ 7)(3\ 7)(2\ 5\ 8\ 1\ 3\ 9) \in S_9$.

    (a) Escreva s como produto de ciclos disjuntos.

    (b) $s \in A_9$?

14. *Determine a ordem da permutação* $w = (1\ 5\ 2\ 7\ 3) \in S_8$.

15. *Mostre que nenhum elemento de* S_5 *têm ordem maior do que 6.*

16. *Considere a permutação* $\sigma = (1\ 5\ 3\ 2)(6\ 2\ 7\ 3)(1\ 3\ 4)(1\ 6\ 8)(5\ 8)$.

    (a) Escreva σ *como produto de ciclos disjuntos.*

    (b) Utilize a resposta do item anterior para dizer a ordem de σ*. Justifique a resposta.*

17. *Determine quais das seguintes permutações são pares e quais são ímpares:*

$$(a)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}. \qquad (b)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}.$$

$$(c)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}. \qquad (d)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 6 & 9 & 8 & 5 & 4 & 7 \end{pmatrix}.$$

18. *Determine todas as possibilidades dos símbolos* $*$ *restantes para que tenhamos uma permutação par:*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & * & * & 3 & * & \end{pmatrix}$$

19. *Determine* $(1\ 2\ 3\ 4)^{30} \in S_5$.

20. *Determine* $(1\ 2\ 3\ 4)(2\ 4\ 5)^{-1}$ *expressando sua resposta como produto de ciclos disjuntos em* S_6.

21. *Determine a ordem do subgrupo cíclico*

$$< (1\ 2), (3\ 4), (5\ 6\ 7) > \ \ de\ \ S_{10}.$$

22. *Sejam* σ *e* τ *as permutações em* S_7 *dado por*

$$\sigma = (1\ 5\ 2\ 4\ 3)(6\ 7) \quad e \quad \tau = (1\ 6)(2\ 3\ 4\ 5\ 7).$$

    (a) Calcule $\sigma\tau \quad e \quad \tau\sigma$.

    (b) Escreve σ *como produto de transposições.*

    (c) Determine a permutação ρ *tal que* $\rho\sigma\rho^{-1} = \tau$.

23. *Mostre que o produto de dois r-ciclos é uma permutação par.*

24. *Escreva a permutação* $(1\ 5\ 3\ 7)(2\ 4\ 6\ 9)$ *como produto de triciclos.*

25. *Determine as ordens possíveis para os elementos de* S_5. *Para cada ordem, dê exemplo de um elemento com esta ordem.*

26. *Mostre que* $(a_1\ a_2\ \cdots a_k)^{-1} = (a_k\ \cdots a_2\ a_1)$.

27. *Mostre que se* a, i, j *são inteiros distintos então* $(i\ j) = (a\ i)(a\ j)(a\ i)$.

28. *Mostre que se k é número ímpar, então* $(a_1\ a_2\ \cdots\ a_k)^2$ *é um ciclo e que se k é par, então* $(a_1\ a_2\ \cdots\ a_k)^2$ *é o produto de dois ciclos disjuntos.*

29. *Seja* $H = \{(1),\ (1\ 2\ 3\ 4),\ (1\ 3)(2\ 4),\ (4\ 3\ 2\ 1)\} \subset S_4$.

    (a) Construa a tabela de multiplicação de H.

    (b) H é um subgrupo de S_4?

    (c) H é um subgrupo de A_4?

30. *Determine o subgrupo* $A_3 < S_3$.

31. *Faça a tabela de multiplicação do grupo* D_4. *Determine os subgrupos cíclicos de* D_4. *Quantos são eles? Determine a ordem e o inverso de cada elemento de* D_4.

32. *O grupo alternado* A_4 *possui um subgrupo de ordem 9?*

33. *No grupo diedral*

$$D_7 =< r, s \mid r^7 = id,\ s^2 = id, rs = sr^{-1} >,$$

simplifique $r^9 s^7 r^{-4} srsr^2 sr^3 r^{12} sr$.

Aula 1.3

Homomorfismo de Grupos

Nesta aula vamos definir os conceitos de homomorfismo e isomorfismo de grupos e determinar quando dois grupos são "iguais", no sentido que eles possui a mesma estrutura algébrica.

Definição 1.3.1. *Sejam G_1 e G_2 grupos. Uma função $\varphi : G_1 \to G_2$ é chamada de um* **homomorfismo** *(de grupos) se*

$$\varphi(ab) = \varphi(a)\varphi(b) \quad \text{para todo } a, b \in G_1.$$

Exemplo 1.3.1. *Sejam $n, m \in \mathbb{Z}_+$, já vimos que os espaços vetoriais $\mathbb{R}^n$ e $\mathbb{R}^m$ são grupos abelianos com a operação a soma. Seja $T : \mathbb{R}^n \to \mathbb{R}^m$ uma transformação linear. Então T é um homomorfismo de grupo, pois*

$$T(v + w) = T(v) + T(w) \quad \text{para todo } v, w \in \mathbb{R}^n.$$

Exemplo 1.3.2. *Define $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ por*

$$\varphi(a) = a \bmod n = [\overline{a}]_n$$

Ou seja, $\varphi(a)$ é o resto da divisão de a por n. Então φ é um homomorfismo, pois

$$\varphi(a + b) = [\overline{a} + \overline{b}]_n = [\overline{a}]_n +_n [\overline{b}]_n = \varphi(a) +_n \varphi(b)$$

onde definimos $\varphi(a) +_n \varphi(b)$ *por* $[\overline{a} + \overline{b}]_n$. *Este homomorfismo chama-se* **redução mod** n.

Exemplo 1.3.3. *Se* G_1 *e* G_2 *são grupos quaisquer, há sempre um homomorfismo* $\varphi : G_1 \to G_2$ *dado por*

$$\varphi(a) = e_2 \quad \text{para todo } a \in G_1,$$

onde e_2 *é o elemento neutro de* G_2. *Este é um homomorfismo, pois*

$$\varphi(ab) = e = e \cdot e = \varphi(a)\varphi(b) \quad \text{para todo } a, b \in G_1.$$

Este homomorfismo é chamada o **homomorfismo trivial**.

Exemplo 1.3.4. *Seja* G *um grupo e considere a aplicação identidade* $id : G \to G$. *Este é um homomorfismo, pois*

$$id(ab) = ab = id(a) \cdot id(b) \quad \text{para todo } a, b \in G.$$

Este homomorfismo é chamada o **homomorfismo identidade**

Exemplo 1.3.5. *Define* $\varphi : GL(n, \mathbb{R}) \to \mathbb{R}^\times$ *por* $\varphi(A) = \det(A)$. *Este é um homomorfismo: se* $A, B \in GL(n, \mathbb{R})$, *então*

$$\varphi(AB) = \det(AB) = \det(A)\det(B) = \varphi(A)\varphi(B).$$

Definição 1.3.2. *Seja* $\varphi : G_1 \to G_2$ *um homomorfismo.*

- *Se* φ *é injetora, dizemos que ela é um* **monomorfismo**.
- *Se* φ *é sobrejetora, dizemos que ela é um* **epimorfismo**.
- *Se* φ *é bijetora, dizemos que ela é um* **isomorfismo**.
- *Um isomorfismo de um grupo para ele mesmo é chamado um* **automorfismo**.

Definição 1.3.3. *2 grupos G_1 e G_2 são* **isomorfos**, *denotamos por*

$$G_1 \cong G_2,$$

se existe um isomorfismo $\varphi : G_1 \to G_2$.

Exemplo 1.3.6. *Considere os grupos $(\mathbb{R}, +)$ e $(\mathbb{R}^+, \cdot)$. Define a função $\varphi : \mathbb{R} \to \mathbb{R}^+$ por*

$$\varphi(a) = e^a.$$

- *φ é um homomorfismo, pois $\varphi(a + b) = e^{a+b} = e^a e^b = \varphi(a)\varphi(b)$.*
- *φ é injetora, pois $\varphi(a) = \varphi(b) \Rightarrow a = b$.*
- *φ é sobrejetora, pois dado qualquer numero real positivo c, pode define $a = \log c$. Então*

$$\varphi(a) = e^a = e^{\log c} = c.$$

Portanto, φ é um isomorfismo, e $\mathbb{R} \cong \mathbb{R}^+$.

Teorema 1.3.1. *Seja G um grupo cíclico.*

1. *Se G é infinito, então $G \cong \mathbb{Z}$.*
2. *Se G é finito com $|G| = n$, então $G \cong \mathbb{Z}_n$.*

Como qualquer grupo de ordem primo é cíclico, temos os seguinte:

Teorema 1.3.2. *Seja p um número primo. Se G é um grupo de ordem p, então $G \cong \mathbb{Z}_p$.*

1.3.1 Propriedades Básicas de Homomorfismos

Proposição 1.3.3. *Sejam $\varphi : G_1 \to G_2$ um homomorfismo.*

(a) Se e_1 e e_2 são os elementos neutros de G_1 e G_2 respectivamente, então

$$\varphi(e_1) = e_2.$$

(b) Para todo $a \in G_1$,

$$\varphi(a^{-1}) = \varphi(a)^{-1}.$$

(c) Mais geral, se $a \in G_1$, então

$$\varphi(a^n) = \varphi(a)^n \quad \text{para todo } n \in \mathbb{Z}.$$

Demonstração.

(a) Para qualquer $a \in G_1$, temos que

$$\varphi(a)\varphi(e_1) = \varphi(ae_1) = \varphi(a) = \varphi(a)e_2.$$

Portanto, pela lei da cancelamento temos que $\varphi(e_1) = e_2$.

(b) Se $a \in G_1$, temos que

$$\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e_1) = e_2.$$

Portanto, $\varphi(a^{-1}) = \varphi(a)^{-1}$.

(c) Para $n = 0$, o resultado vale pelo (a).

Suponha que $n \in \mathbb{Z}^+$. Provamos por indução. O resultado é valido para $n = 1$, pois

$$\varphi(a^1) = \varphi(a) = [\varphi(a)]^1.$$

Suponhamos que o resultado é valido para $n-1$. Então

$$\varphi(a^n) = \varphi(aa^{n-1}) = \varphi(a)\varphi(a^{n-1}) = \varphi(a)[\varphi(a)]^{n-1} = [\varphi(a)]^n$$

pelo hipótese de indução.

Agora para $n < 0$, isto é $n = -m,\ m \in \mathbb{Z}^+$. Observe primeiramente se $a \in G$, temos que

$$\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e) = e_H.$$

Portanto $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Agora

$$\varphi(a^n) = \varphi(a^{-m}) = \varphi\left((a^{-1})^m\right) = [\varphi(a^{-1})]^m = [\varphi(a)^{-1}]^m = [\varphi(a)]^{-m} = [\varphi(a)]^n.$$

Logo o resultado é valido para todo $n \in \mathbb{Z}$.

■

Proposição 1.3.4. *Sejam G_1 e G_2 grupos e seja $\varphi : G_1 \to G_2$ um homomorfismo. Se $a \in G_1$ tem ordem finito, então ord$(\varphi(a))$ divide ord(a).*

Demonstração. Seja $n = \text{ord}(a)$. Então $a^n = e_1$, logo

$$\varphi(a)^n = \varphi(a^n) = \varphi(e_1) = e_2.$$

Portanto $\varphi(a)^n = e_2$, logo temos que ord$\big(\varphi(a)\big)$ divide ord(a). ■

Proposição 1.3.5. *Sejam G_1, G_2 e G_3 grupos e seja $\varphi : G_1 \to G_2$ e $\psi : G_2 \to G_3$ homomorfismos.*

(a) A composição $\psi \circ \varphi$ é um homomorfismo.

(b) Se φ e ψ são ambos isomorfismos, então $\psi \circ \varphi$ é um isomorfismo.

(c) Se φ é um isomorfismo, então φ^{-1} é um isomorfismo.

Demonstração.

(a) Seja $a, b \in G_1$. Então

$$\psi \circ \varphi(ab) = \psi\Big(\varphi(ab)\Big) = \psi\Big(\varphi(a)\varphi(b)\Big) = \psi\Big(\varphi(a)\Big)\psi\Big(\varphi(b)\Big),$$

pois ψ e φ são ambos homomorfismos.

(b) Se φ e ψ são isomorfismos, então $\psi \circ \varphi$ é um homomorfismo pelo (a), e ela é uma bijeção pois ambos φ e ψ também são. Portanto $\psi \circ \varphi$ é um isomorfismo.

(c) Suponha que $x, y \in G_2$. Então $x = \varphi(a)$ e $y = \varphi(b)$ para alguns $a, b \in G_1$. Portanto

$$\varphi^{-1}(xy) = \varphi^{-1}\Big(\varphi(a)\varphi(b)\Big) = \varphi^{-1}\Big(\varphi(ab)\Big) = ab = \varphi^{-1}(x)\varphi^{-1}(y).$$

Portanto φ^{-1} é também um isomorfismo.

■

Proposição 1.3.6. *Se $\varphi : G_1 \to G_2$ é um isomorfismo, então $ord(\varphi(a)) = ord(a)$.*

Demonstração. Suponha que $a \in G_1$ tem ordem finita. Então da Proposição 1.3.4 que

$$\text{ord}(\varphi(a)) \,\Big|\, \text{ord}(a). \tag{1}$$

Mas como φ^{-1} é também um homomorfismo, temos que

$$\text{ord}(a) = \text{ord}\Big(\varphi^{-1}(\varphi(a))\Big) \,\Big|\, \text{ord}(\varphi(a)). \tag{2}$$

De (1) e (2) temos que $\text{ord}(\varphi(a)) = \text{ord}(a)$.
Observe a Proposição 1.3.4 também implica que a tem ordem finita se e somente se $\varphi(a)$ também tem ordem finita. Logo seguir que se a tem ordem infinta se e somente se $\varphi(a)$ também tem. Portanto a demonstração. ■

1.3.2 A imagem e núcleo de um homomorfismo

Definição 1.3.4. *Sejam $(G_1, *)$ e $(G_2, \circ)$ grupos e $f : G_1 \to G_2$ um homomorfismo. A imagem de f é o subconjunto*

$$Im(f) := \{f(a) : a \in G\}$$

de G_2.

Exemplo 1.3.7. *Seja $f : \mathbb{R} \to \mathbb{R}^*$, a exponencial. Então*

$$Im(f) = \mathbb{R}_+ = \{x \in \mathbb{R}, x > 0\}.$$

Lema 1.3.7. *$Im(f)$ é um subgrupo de $(G_2, \circ)$.*

Demonstração. Usando o critério de subgrupo:

- Se $x = f(a), y = f(b) \in Im(f)$ então

  $$x \circ y = f(a) \circ f(b) = f(a * b) \text{ pois } f \text{ é um homomorfismo.}$$

  Portanto, $Im(f)$ é fechado em relação ao $\circ$.

- Se e_{G_1} e e_{G_2} são os elementos neutros de G_1, G_2 respectivamente, então $f(e_{G_1}) = e_{g_2}$ pois f é um homomorfismo. Portanto $e_{G_2} \in Im(f)$.

- Se $x = f(a) \in Im(f)$ então

  $$x^{-1} = f(a)^{-1} = f(a^{-1}).$$

  Portanto $x^{-1} \in Im(f)$.

Portanto $Im(f)$ é um grupo. ■

Lema 1.3.8. *Seja $f : G_1 \to G_2$ um homomorfismo injetora. Então f define uma isomorfismo de G em $Im(f)$.*

Demonstração. $f : G_1 \to Im(f)$ é uma bijeção. ■

Definição 1.3.5. *Sejam $(G_1, *)$ e $(G_2, \circ)$ grupos e $f : G_1 \to G_2$ um homomorfismo. Então o núcleo de f é o subconjunto*

$$Nuc(f) := \{x \in G_1 | \ f(x) = e_{G_2}\}$$

de G_1, onde e_{G_2} é o elemento neutro do grupo G_2.

Exemplo 1.3.8. *Seja $f : (\mathbb{Z}, +) \to (\mathbb{Z}_3, +)$ o homomorfismo $f(n) = n \bmod 3$. Então $Nuc(f)$ é o conjunto de inteiros congruente a 9 modulo 3, ou seja $Nuc(f) = 3\mathbb{Z}$.*

Lema 1.3.9. *Seja $f : G_1 \to G_2$ um homomorfismo. Então $Nuc(f)$ é um subgrupo de G_1.*

Demonstração. Usando o critério de subgrupo:

- Se $x, y \in Nuc(f)$. Então

$$f(x * y) = f(x) \circ f(y) = e_{G_2} \circ e_{G_2} = e_{G_2}.$$

  Portanto $x * y \in Nuc(f)$, ou seja $Nuc(f)$ é fechado com respeito a $*$.

- Claro que $e_{G_1} \in Nuc(f)$, pois $f(e_{G_1}) = e_{G_2}$.

- Se $x \in Nuc(f)$, então

$$f(x^{-1}) = f(x)^{-1} = e_{G_2}^{-1} = e_{G_2}.$$

  Portanto $x^{-1} \in Nuc(f)$.

Portanto $Nuc(f)$ é um grupo. ■

Exemplo 1.3.9.

(a) A função $sgn : S_n \to \{-1, 1\}$ *definido por*

$$sgn(\sigma) = \begin{cases} 1, & \text{se } \sigma \text{ é par} \\ -1, & \text{se } \sigma \text{ é ímpar} \end{cases}$$

é um homomorfismo com núcleo

$$Nuc(f) = \{\sigma \in S_n : \ sgn(\sigma) = 1\} = A_n,$$

o grupo alternado de grau n.

(b) A função determinante $\det : GL(n, \mathbb{R}) \to \mathbb{R}^*$ *é um homomorfismo com núcleo*

$$Nuc(\det) = \{A \in GL(n, \mathbb{R}) : \ \det(A) = 1\} = SL(n, \mathbb{R}).$$

Teorema 1.3.10. *Um homomorfismo* $f : G_1 \to G_2$ *é injetora se, e somente se* $Nuc(f) = \{e_{G_1}\}$.

Demonstração. Suponha que f é injetora, então é claro que $Nuc(f) = \{e_1\}$.
Suponha que $Nuc(f) = \{e_{G_1}\})$ e $a, b \in G_1$ com $f(a) = f(b)$. Então

$$e_{G_2} = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}),$$

logo $ab^{-1} \in Nuc(f)$. Portanto $ab^{-1} = e_{G_1}$ Ou seja $a = b$. Logo f é injetora. ■

1.3.3 Exercícios Resolvidos

Exercício 1.3.1. *Seja* $f : \mathbb{Z}_{12} \to \mathbb{Z}_{24}$ *um homomorfismo com* $f(\overline{7}) = \overline{18}$.

(a) Determine $f(\overline{x})$.

(b) Determine a imagem de f.

(c) Determine a núcleo de f.

(d) Determine $f^{-1}(\overline{3})$.

Solução.

(a) Seja $f(\overline{1}) = \overline{k}$. *Como* $f(\overline{7}) = \overline{18}$ *temos que*

$$f(\overline{1}) +_{24} f(\overline{1}) +_{24} f(\overline{1}) +_{24} f(\overline{1}) +_{24} f(\overline{1}) +_{24} f(\overline{1}) +_{24} f(\overline{1}) = f(\overline{7}) = \overline{18}.$$

Logo $7\overline{k} = \overline{18}\ (mod)\ 24 \Rightarrow \overline{k} = \overline{6}$.

Dado $\overline{x} \in \mathbb{Z}_{12}$ *temos que*

$$\overline{x} = \underbrace{(\overline{1}) +_{12} (\overline{1}) +_{12} (\overline{1}) +_{12} \cdots +_{12} (\overline{1})}_{x \text{ vezes}}.$$

Portanto $f(\overline{x}) = xf(\overline{1}) = \overline{6}x$.

(b) Seja $Im(f)$ *a imagem de* f *então*

$$Im(f) = \{\overline{y} \in \mathbb{Z}_{24} : \ \exists\, \overline{x} \in \mathbb{Z}_{12} \text{ com } \ f(\overline{x}) = \overline{y}\} = \{\overline{0},\ \overline{6},\ \overline{12},\ \overline{18}\}.$$

(c) Seja $Nuc(f)$ *o núcleo de* f *então*

$$Nuc(f) = \{\overline{x} \in \mathbb{Z}_{12} : \ f(\overline{x}) = \overline{0}\} = \{\overline{0},\ \overline{4},\ \overline{8}\}.$$

(d) $f^{-1}(\overline{3}) = \emptyset$ *pois* $\overline{3} \notin Im(f)$.

1.3.4 Atividade

1. *Verifique quais das aplicações abaixo são homomorfismo de grupos. Para aquelas que são homomorfismo determine seu núcleo.*

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

   (b) $f : (\mathbb{R}^*, \cdot) \to (\mathbb{R}^*, \cdot)$ *dada por* $f(x) = x^2$.

   (c) $f : (\mathbb{R}^*, \cdot) \to (\mathbb{R}^*, \cdot)$ *dada por* $f(x) = 2^x$.

   (d) $f : \Big(M(2, \mathbb{Z}), +\Big) \to \Big(M(2, \mathbb{Z}), +\Big)$ *dada por* $f(A) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} A$.

   (e) $f : (\mathbb{R}, +) \to \Big(GL(2, \mathbb{R}), \cdot\Big)$ *dada por* $f(x) = \begin{pmatrix} \cos x & \text{sen } x \\ -\text{sen } x & \cos x \end{pmatrix}$.

2. *Seja* $H = \{2^a 3^b, \mid a, b \in \mathbb{Z}\}$ *um subgrupo de* $\mathbb{R}^+$. *Mostre que* $H \simeq \mathbb{Z} \times \mathbb{Z}$.

3. *Sejam G e G' grupos, $f : G \to G'$ um homomorfismo e $H < G'$. Mostre que $f^{-1}(H) = \{x \in G;\ f(x) \in H\}$ é um subgrupo de G.*

4. *Seja G um grupo com 3 elementos. Mostre que $G \simeq \mathbb{Z}_3$.*

5. *Sejam G, H grupos e $f : G \to H$ um homomorfismo sobrejetora. Prove que se G é abeliano então H também é abeliano.*

6. *Sejam G, H grupos e $f : G \to H$ um homomorfismo sobrejetora. Prove que se G é cíclico então H também é cíclico.*

7. *Verifique se os grupos G e H são isomorfos:*

   (a) $G = \mathbb{Z}_6$ *e* $H = S_3$.

   (b) $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ *e* $H = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

   (c) $G = \mathbb{Z}_4$ *e* $H = \mathbb{Z}_2 \times \mathbb{Z}_2$.

   (d) $G = D_4$ *e* $H = \mathbb{Z}_8$.

   (e) $G = D_4$ *e* $H = \mathbb{Z}_4 \times \mathbb{Z}_2$.

   (f) $G = D_4$ *e* $H = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

   (g) $G = \mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_3$ *e* $H = \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_{15}$.

8. *Determine o núcleo das seguintes homomorfismos*

   (a) $f : \mathbb{Z} \to \mathbb{Z}_8$ *tal que* $f(1) = \overline{6}$.

   (b) $f : \mathbb{Z}_{40} \to \mathbb{Z}_5 \times \mathbb{Z}_8$ *tal que* $f(\overline{1}) = \left([\overline{1}]_5,\ [\overline{4}]_8\right)$.

9. *Existe um único homomorfismo $f : \mathbb{Z}_6 \to S_3$ tal que $f(\overline{1}) = (1\ 2\ 3)$. Determine $f(\overline{k})$ para cada $\overline{k} \in \mathbb{Z}_6$. Quais são os elementos do núcleo de f?*

10. *Mostre que $f : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ dada por $f\left([\overline{a}]_6\right) = \left([\overline{a}]_2,\ [\overline{a}]_3\right)$ é um homomorfismo. E deduza que $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.*

11. *Considere o homomorfismo do grupo $f : \mathbb{Z}_{12} \to \mathbb{Z}_4 \times \mathbb{Z}_3$ dado por $f\left([\overline{a}]_{12}\right) = \left([\overline{a}]_4,\ [\overline{0}]_3\right)$.*

    (a) Describa $Nuc(f)$. Escreva todos seus elementos.

    (b) Describa $Im(f)$. Escreva todos seus elementos.

12. *Considere o homomorfismo do grupo* $f : \mathbb{Z}_{12} \to \mathbb{Z}_{24}$ *dado por* $f\left([\overline{a}]_{12}\right) = [2\overline{a}]_{24}$.

    (a) Describa $Nuc(f)$. *Escreva todos seus elementos.*

    (b) Describa $Im(f)$. *Escreva todos seus elementos.*

13. *Considere o homomorfismo do grupo* $f : \mathbb{Z}_{12} \to \mathbb{Z}_{24}$ *dado por* $f\left([\overline{a}]_{12}\right) = [4\overline{a}]_{24}$.

    (a) Describa $Nuc(f)$. *Escreva todos seus elementos.*

    (b) Describa $Im(f)$. *Escreva todos seus elementos.*

14. *Considere o homomorfismo do grupo* $f : \mathbb{Z}_{12} \to \mathbb{Z}_{24}$ *dado por* $f\left([\overline{a}]_{12}\right) = [6\overline{a}]_{24}$.

    (a) Describa $Nuc(f)$. *Escreva todos seus elementos.*

    (b) Describa $Im(f)$. *Escreva todos seus elementos.*

15. *Prove que não existe um homomorfismo* $f : \mathbb{Z}_{12} \to \mathbb{Z}_{24}$ *tal que* $f\left([\overline{a}]_{12}\right) = [\overline{a}]_{24}$.

16. *Seja* H *um subgrupo de* $GL(2, \mathbb{R})$ *gerado por*

$$A_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \; e \; B_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

    Prove que H *é um grupo não abeliano de 8 elementos e que é isomorfo a* D_4.

17. *O grupo* G *das matrizes reais* $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, *com* $a \neq 0$ *é um subgrupo de* $GL(2, \mathbb{R})$. *Prove que* G *é isomorfo ao grupo*

$$A = \{\alpha_{a,b} : \mathbb{R} \to \mathbb{R} : \; \alpha_{a,b}(x) = ax + b, \; a \neq 0\}.$$

18. *Seja* $f : \mathbb{Z}_{50} \to \mathbb{Z}_{15}$ *um homomorfismo com* $f(\overline{7}) = \overline{6}$.

    (i) Determine $f(\overline{x})$.

    (ii) Determine a imagem de f.

    (iii) Determine a núcleo de f.

    (iv) Determine $f^{-1}(\overline{3})$.

Aula 1.4

Classes Laterais e o Teorema de Lagrange

Sejam G um grupo finito e $H \leq G$. O nosso objetivo nessa aula é obter uma relação entre o número dos elementos de H e o número dos elementos de G, o Teorema de Lagrange.

1.4.1 Classes Laterais

Primeiro definiremos as classes laterias e estudaremos as suas propriedades básicas. Vale a pena observar que estas definições e propriedades não dependem da finitude de G.

Definição 1.4.1 (Classe Lateral). *Sejam $(G, \cdot)$ um grupo e $H \leq G$. Para cada $a \in G$, chamamos de uma* **classe lateral à esquerda de G com respeito a H** *ao conjunto*

$$a \cdot H := \{a \cdot h \mid h \in H\}.$$

De modo análogo, chamamos de **classe lateral à direita de G com respeito a H** *ao conjunto*

$$H \cdot a := \{h \cdot a \mid h \in H\}.$$

Observações.

1. *Como o elemento neutro $e \in G$, para cada elemento fixo $a \in G$, $a = ae \in aH$. Portanto, dizemos que o conjunto aH é classe lateral à esquerda de H contendo a. De modo análogo, $a \in Ha$ e portanto Ha*

é a classe lateral à direita de H contendo a.

2. *Se G é um grupo aditivo, então denotamos a classes aH e Ha por*

$$a + H = \{a + h \mid h \in H\}$$

e

$$H + a = \{h + a \mid h \in H\}$$

respectivamente.

Exemplo 1.4.1. *Considere o grupo,* $D_4 = \{id, r, r^2, r^3, s, sr, sr^2, sr^3;\ r^4 = id,\ s^2 = id,\ rs = sr^3\}$ *das simetrias do quadrado e sejam* $H = \{id, s\}$ *e* $K = \{id, r^2\}$*, 2 subgrupos de* D_4*. Calcular as classes laterais à esquerda e a direita de G com respeito a H e K.*

Solução.

- *Classes laterais à esquerda e a direita de G com respeito a H*

$$\begin{cases} H = \{id, s\} = sH \\ rH = \{r, rs\} = rsH = sr^3H \\ r^2H = \{r^2, r^2s\} = r^2sH = sr^2H \\ r^3H = \{r^3, r^3s\} = r^3sH = srH. \end{cases} \qquad \begin{cases} H = \{id, s\} = Hs \\ Hr = \{r, sr\} = Hsr \\ Hr^2 = \{r^2, sr^2\} = Hsr^2 \\ Hr^3 = \{r^3, sr^3\} = Hsr^3. \end{cases}$$

- *Classes laterais à esquerda e a direita de G com respeito a K.*

$$\begin{cases} K = \{id, r^2\} = r^2K = Kr^2 \\ rK = \{r, r^3\} = Kr = r^3K = Kr^3 \\ sK = \{s, sr^2\} = Ks = sr^2K = Ksr^2 \\ srK = \{sr, sr^3\} = Ksr = sr^3K = Ksr^3. \end{cases}$$

Observação. *Observamos da Exemplo 1.4.1 que em geral* $Ha \neq aH$*, para cada* $a \in D_4$*, entretanto,* $Ka = aK$*, para cada* $a \in D_4$*. O subgrupo K de* D_4 *chama-se subgrupo normal, que será estudadas na Aula 6.*

Se G é um grupo abeliano e se H é um subgrupo de G, então

$$H \cdot a = a \cdot H, \ \forall a \in G.$$

Exemplo 1.4.2. *Considere o grupo aditivo $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$ e os 3 subgrupos*

$H_1 = \{(x, y) \in \mathbb{R}^2 : \ y = 0\}$ *(o eixo x),*

$H_2 = \{(x, y) \in \mathbb{R}^2 : \ x = 0\}$ *(o eixo y),*

$H_3 = \{(x, y) \in \mathbb{R}^2 : \ y = 3x\}$ *(a reta que passa pela origem de coeficiente angular 3).*

Dê uma descrição geométrica das classes laterais de H_j $(j = 1, 2, 3)$ em G.

Solução. *Como $(\mathbb{R}^2, +)$ é abeliano, para cada $(x, y) \in \mathbb{R}^2$ temos que $(x, y+)H = H + (x, y)$.*
Seja $(x_0, y_0) \in \mathbb{R}^2$ arbitrário. Então

- $(x_0, y_o) + H_1 = \{(x_0, y_0) + (x, y) : \ y = 0\} = \{(x_0 + x, y_0) : \ x \in \mathbb{R}\}$ *representa a equação da reta que passa pelo ponto (x_0, y_0) e é paralelo ao eixo x,*

- $(x_0, y_o) + H_2 = \{(x_0, y_0) + (x, y) : \ x = 0\} = \{(x_0, y_0 + y) : \ y \in \mathbb{R}\}$ *representa a equação da reta que passa pelo ponto (x_0, y_0) e é paralelo ao eixo y,*

- $(x_0, y_o) + H_3 = \{(x_0, y_0) + (x, y) : \ y = 3x\} = \{(x_0 + x, y_0 + 3x) : \ x \in \mathbb{R}\}$ *representa a equação da reta que passa pelo ponto (x_0, y_0) de coeficiente angular 3.*

Portanto se fixamos um subgrupo H de $\mathbb{R}^2$, (todos os subgrupos de $\mathbb{R}^2$ são retas que passam pela origem), e escolher qualquer ponto $(x_0, y_0) \in \mathbb{R}^2$, então o conjunto $(x_0, y_0) + H$ representa a reta que é uma translação paralela da reta que representada por H e $(x_0, y_0) + H$ contem o ponto (x_0, y_0).

Exemplo 1.4.3. *Considere o grupo $G = \mathbb{U}_{28}$ e $H = \{\overline{1}, \overline{13}, \overline{15}, \overline{27}\}$ o subgrupo de ordem 4 de G. Calcular as classes laterais à esquerda e a direita de G com respeito a H.*

Solução. *Como $\mathbb{U}_{28} = \{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}, \overline{15}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{27}\}$ é abeliano, as classes laterais à esquerda e a direta são iguais. As classes à esquerda de G com respeito a H são:*

- $H = \{\overline{1}, \overline{13}, \overline{15}, \overline{27}\}$.

- $3H = \{\overline{3}, \overline{11}, \overline{17}, \overline{25}\}$.

- $5H = \{\overline{5}, \overline{9}, \overline{19}, \overline{23}\}$.

1.4.2 Propriedades das Classes Laterais

Proposição 1.4.1. *Sejam $(G, \cdot)$ um grupo, $H \leq G$ e $a, b \in G$.*

(a) $aH = bH$ se, e somente se, $b^{-1}a \in H$. Em particular $aH = H \Leftrightarrow a \in H$.

(b) $aH = bH \Leftrightarrow a \in bH$.

(c) Se $aH \cap bH \neq \emptyset$, então $aH = bH$, ou, equivalentemente, se $aH \neq bH$, então $aH \cap bH = \emptyset$.

(d) $f_a : H \to aH$ definida por $f_a(h) = ah$ é bijetora. Em particular se G é um grupo finito, então todas as classes laterais têm $|H|$ elementos, isto é, $|aH| = |H|$ para todo $a \in G$.

(e) Se G é um grupo finito, então existem elementos $a_1, a_2, \cdots, a_k \in G$, com $a_1 = e_G$, tal que

$$G = a_1H \cup a_2H \cup \cdots \cup a_kH,$$

e a união é disjunta.

Demonstração.

(a) ($\Rightarrow$) Vamos supor, primeiramente, que $aH = bH$. Queremos provar que $b^{-1}a \in H$.
Como $a \in aH = bH$, logo, existe $h \in H$, tal que $a = bh$. Portanto,

$$\begin{aligned} b^{-1}a &= b^{-1}(bh) \\ &= (b^{-1}b)h \\ &= h \in H. \end{aligned}$$

($\Leftarrow$) Vamos, agora, supor que $b^{-1}a \in H$. Queremos provar que $aH = bH$, ou seja $aH \subseteq bH$ e $bH \subseteq aH$.
Vamos provar, inicialmente, a inclusão $aH \subseteq bH$. Como $b^{-1}a \in H$, então existe $h_1 \in H$, tal que $b^{-1}a = h_1$. Portanto, $a = bh_1$. Seja, agora, $ah \in aH$, um elemento genérico de aH, com

$h \in H$. Então, temos

$$\begin{aligned} ah &= (bh_1)h \\ &= b(h_1h). \end{aligned}$$

Como H é subgrupo de G e $h, h_1 \in H$, então $h_1h \in H$ e portanto,

$$ah = b(h_1h) \in bH.$$

Daí, segue que $ah \in bH$, para todo $h \in H$, ou seja $aH \subseteq bH$.

A inclusão contrária, $bH \subseteq aH$, é análoga.

(b) ($\Rightarrow$) Suponha que $aH = bH$. Então

$$a = ae \in aH = bH.$$

($\Leftarrow$) Suponha que $a \in bH$. Então temos que $a = bh$, com $h \in H$. Portanto

$$aH = (bh)H = b(hH) = bH.$$

(c) Propriedade 3 seguir diretamente da propriedade 2, pois se existe $c \in aH \cap bH$ então $cH = aH$ e $cH = bH$. Portanto, $aH = bH$.

(d) Vamos provar que a função $f_a : H \to aH$, $f_a(h) = ah$ é uma bijeção.

Pela própria definição de aH, já vemos que $Im(f_a) = aH$, ou seja f_a é sobrejetora.

Para provar que f_a é injetora, sejam $h_1, h_2 \in H$ tais que $f_a(h_1) = f_a(h_2)$. Queremos concluir que $h_1 = h_2$. Assim temos

$$\begin{aligned} f_a(h_1) = f_a(h_2) &\Rightarrow ah_1 = ah_2 \\ &\Rightarrow a^{-1}(ah_1) = a^{-1}(ah_2) \\ &\Rightarrow h_1 = h_2. \end{aligned}$$

Portanto f_a é injetora. Portanto, como f_a é uma bijeção, então aH e H têm o mesmo número de elementos, isto é $|aH| = |H|$.

(e) Como G é um grupo finito, o número de classes laterais a esquerda de H em G é finito. Sejam $a_1H,\ a_2H, \cdots, a_kH$ a coleção de todas as classes laterais esquerda de H em G. Então pelo propriedade 2, como duas classes laterais coincidem ou são disjuntas, a união

$$G = a_1H \cup a_2H \cup \cdots \cup a_kH$$

pode ser considerada uma união disjunta.

Uma propriedade idêntica, com uma demonstração análoga, vale para as classes laterais à direta.

Lema 1.4.2. *Considere a aplicação*

$$\begin{array}{rcl} \varphi : \{\textit{classes laterais à esquerda}\} & \to & \{\textit{classes laterais à direta}\} \\ aH & \mapsto & Ha^{-1} \end{array}$$

Então φ é bijetora.

Definição 1.4.2. *O número de classes laterais à esquerda que é igual ao número de classes laterais à direta, pelo Lema 1.4.2 se chama o* **índice** *de H em G e é denotado por $(G : H)$.*

Exemplo 1.4.4. *Dado o subgrupo $H = \{id,\ (2\ 3)\}$ de $S_3 = \{id,\ (1\ 2\ 3),\ (1\ 3\ 2),\ (2\ 3),\ (1\ 3),\ (1\ 2)\}$, obter elementos $a_1, a_2, \cdots, a_k \in S_3$ tal que*

$$S_3 = a_1H \cup a_2H \cup \cdots \cup a_kH$$

seja uma união disjunta.

Solução. *As classes laterais distintas são*

- $H = \{id,\ (2\ 3)\}$
- $(1\ 2\ 3)H = \{(1\ 2\ 3),\ (1\ 3)\}$
- $(1\ 3\ 2)H = \{(1\ 3\ 2),\ (1\ 2)\}$.

Então, podemos escolher $a_1 = id,\ a_2 = (1\ 2\ 3)$ e $a_3 = (1\ 3\ 2)$, e temos que

$$S_3 = a_1H \cup a_2H \cup a_3H$$

é uma união disjunta. Portanto $(S_3 : H) = 3$.

Exemplo 1.4.5. *Como o subgrupo* $H = \{id, s\}$ *de* D_4 *tem 4 classes laterais esquerda, pelo Exemplo 1.4.1,*

$$H, rH = \{r, rs\},\ r^2H = \{r^2, r^2s\},\ r^3H = \{r^3s\}$$

temos que $(D_4 : H) = 4$ *e* $D_4 = H \cup rH \cup r^2H \cup r^3H$.

1.4.3 O Teorema de Lagrange

Teorema 1.4.3 (Teorema de Lagrange)**.** *Sejam G um grupo finito e H um subgrupo de G. Então vale*

$$|G| = |H| \cdot (G : H).$$

Em particular, a ordem e o índice de um subgrupo dividem a ordem do grupo.

Demonstração. Pela Proposição 1.4.1(e), sabemos que existem $a_1, a_2, \cdots, a_k \in G$ tal que

$$G = a_1H \cup a_2H \cup \cdots \cup a_kH,$$

e a união é disjunta. Temos que $k = (G : H)$ pela definição. Como a união é disjunta, o número de elementos de G é igual à soma do número de elementos de cada classe lateral da união, ou seja,

$$|G| = |a_1H| + |a_2H| + \cdots + |a_kH|.$$

De novo pela Proposição 1.4.1(d), sabemos que

$$|a_iH| = |H| \text{ para todo } i = 1, 2, \cdots, k.$$

Fazendo as devidas substituições na equação anterior, temos

$$\begin{aligned} |G| &= |a_1H| + |a_2H| + \cdots + |a_kH| \\ &= |H| + |H| + \cdots + |H|, \ (k \text{ parcelas}) \\ &= k\,|H|. \end{aligned}$$

Portanto, $|G| = (G : H)|H|$, ou seja, $|H|$ divide $|G|$.

Exemplo 1.4.6. *Procure todos os subgrupos de S_3 com suas ordens.*

Solução. *O grupo S_3 tem 6 elementos. Um subgrupo H de S_3, pelo Teorema de Lagrange, só pode ter $|H| \in \{1, 2, 3\}$, que são os divisores de 6.*

- *O único subgrupo de ordem 1 é* $\{id\}$.
- *Os subgrupos de ordem 2 são:*

  $< (2\ 3) >= \{id,\ (2\ 3)\}$,

  $< (1\ 3) >= \{id,\ (1\ 3)\}$,

  $< (1\ 2) >= \{id,\ (1\ 2)\}$.

- *O único subgrupo de ordem 3 é* $< (1\ 2\ 3) >= \{id,\ (1\ 2\ 3),\ (1\ 3\ 2)\} =< (1\ 3\ 2) >$.

Observação. *A reciproca do Teorema de Lagrange é verdadeira para alguns grupos (por exemplo todos os grupos cíclicos), mas ela é* **falsa** *em geral: dada um divisor n da ordem de um grupo, não existe necessariamente um subgrupo de ordem n como mostramos em Exemplo 1.4.8.*

1.4.4 Algumas Consequências do Teorema de Lagrange

Corolário 4. *Sejam G um grupo finito e K, H subgrupos de G, com $K \subset H$. Então*

$$(G : K) = (G : H) \cdot (H : K)$$

Demonstração. Teorema 1.4.3 implica

$$(G : H) \cdot (H : K) = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = \frac{|G|}{|K|} = (G : K)$$

■

Corolário 5. *Sejam G um grupo finito e $a \in G$, então a ordem de a divide a ordem de G, isto é, $ord(a) \Big| |G|$.*

Demonstração. O subgrupo gerado por a, $< a >$, é um subgrupo do grupo finito G. Logo, pelo Teorema de Lagrange, temos que $| < a > |$ divide $|G|$. Mas, como por definição, a ordem do elemento a é a ordem do subgrupo $< a >$, ou seja, $ord(a) \Big| |G|$. ■

Observação. *Corolário 5 implica que se G é um grupo de ordem n então os possíveis ordens de seus elementos são divisores de n. Por exemplo, se $|G| = 30$ então para cada $a \in G$, $ord(a) \in \{1, 2, 3, 5, 6, 10, 15, 30\}$.*

Corolário 6. *Sejam G um grupo finito de ordem n e $a \in G$, então $a^n = e$.*

Demonstração. Seja m a ordem do elemento $a \in G$, ou seja, $a^m = e$. De acordo como o Corolário 5, $m|n$, ou seja, existe um inteiro k, tal que $n = km$. Portanto

$$a^n = a^{mk} = (a^m)^k = e^k = e$$

■

Corolário 7. *Todo grupo de ordem primo é cíclico.*

Demonstração. Seja G um grupo de ordem primo p. Como $p > 1$, então existe $a \in G$ com $a \neq e$. Agora, como $a \neq e$, então $\text{ord}(a) > 1$. Por outro lado, pelo Corolário 5, $\text{ord}(a) \Big| |G|$, ou seja, $\text{ord}(a) \mid p$. mas, como p é primo, então seus únicos divisores positivos são 1 e p, e como $\text{ord}(a) > 1$. Assim, só resta a possibilidade $\text{ord}(a) = p$. Isto significa que o subgrupo $< a >$ gerado por a tem o mesmo número de elementos que G e, como $< a > \subset G$, segue que $< a >= G$, ou seja, G é um grupo cíclico. ■

1.4.5 Classificação de grupos finitos

Um dos principais problemas na teoria dos grupos é a classificação de todos os grupos finitos. Neste seção enunciamos alguns resultados básicos para a classificação de alguns grupos finitos.

Teorema 1.4.4. *Se G é um grupo finito de ordem p, primo, então G é cíclico e isomorfo a $\mathbb{Z}_p$.*

Demonstração. Segue do Corolário 7. ■

Teorema 1.4.5 (Teorema de Cauchy)**.** *Seja p primo e G um grupo finito de ordem n. Suponha que p divide n. Então G possui pelo menos um elemento de ordem p, ou seja, um subgrupo de ordem p.*

Proposição 1.4.6. *Se G é um grupo de ordem 2p, p primo então G é isomorfo ao grupo cíclico $\mathbb{Z}_{2p}$ ou isomorfo ao grupo diedral D_{2p}.*

Demonstração. A demonstração desta será omitida, mas pode ser vista em [3]. ■

Exemplo 1.4.7.

(a) Existe somente 2 grupos de ordem $6 = 2 \cdot 3$. São eles $\mathbb{Z}_6$ e $D_3 \cong S_3$.

(b) Existe somente 2 grupos de ordem $10 = 2 \cdot 5$. São eles $\mathbb{Z}_{10}$ e D_5.

Exemplo 1.4.8. *Mostre que o grupo A_4, das permutações pares não possui um subgrupo de ordem 6.*

Solução. *O grupo*

$A_4 = \{id, (1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (2\,3\,4), (2\,4\,3), (1\,3\,4), (1\,4,3), (1\,2)(3\,4), (1\,3)(2\,4), (2\,3)(1\,4)\}$.

Suponha que existe um subgrupo H de A_4 de ordem 6.
Então H é isomorfo a $\mathbb{Z}_6$ ou S_3 (Exemplo 1.4.7 (a)).

- *Como A_4 não tem elemento de ordem 6, H não pode ser isomorfo ao $\mathbb{Z}_6$.*
- *Agora suponha $H \cong S_3$.*
  Em $S_3 = \{id, (1\ 2\ 3), (1\ 3\ 2), (2\ 3), (1\ 3), (1\ 2)\}$, existem 3 elementos de ordem 2. O grupo A_4 possuem 3 elementos de ordem 2, que são $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, $(2\ 3)(1\ 4)$. Portanto, estes elementos devem pertencem H.
  Então $K = \{id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (2\ 3)(1\ 4)\}$ é um subgrupo de ordem 4 de H, contradição , pois um grupo de ordem 6 não possui um subgrupo de ordem 4 (Teorema de Lagrange).

Portanto não existe um subgrupo de ordem 6 de A_4.

Proposição 1.4.7. *Se G é um grupo finito de ordem pq, com p e q primos, $p < q$ e $p \nmid (q-1)$ então G é cíclico e isomorfo a $\mathbb{Z}_{pq}$.*

Exemplo 1.4.9. *Exemplos satisfazendo a condição $p \nmid (q-1)$ são*

$$15 = 3 \cdot 5,\ \ 33 = 3 \cdot 11,\ \ 35 = 5 \cdot 7,\ \ 51 = 3 \cdot 17,\ \ 65 = 5 \cdot 13,\ \ \textit{etc.}.$$

Qualquer grupo com estes ordens é cíclico.

1.4.6 Classificação de Grupos Abelianos Finitos

Agora consideramos a classificação de grupos abelianos finitos:

Proposição 1.4.8. *Se G é um grupo abeliano finito de ordem pq, com p e q relativamente primos, então G é cíclico e isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_q$.*

Exemplo 1.4.10. $\mathbb{Z}_{120} \cong \mathbb{Z}_{24} \times \mathbb{Z}_5 \cong \mathbb{Z}_8 \times \mathbb{Z}_{15}$

Teorema 1.4.9 (Teorema Fundamental de Grupos Abelianos Finitos). *Todo grupo abeliano finito G é isomorfo ao produto direto de grupos cíclicos de ordem potências de primos:*

$$G \cong \mathbb{Z}_{{p_1}^{r_1}} \times \mathbb{Z}_{{p_2}^{r_2}} \times \cdots \times \mathbb{Z}_{{p_k}^{r_k}}$$

onde os p_i não são necessariamente distintos. Além disto, o número dos termos no produto e as ordens dos grupos cíclicos são unicamente determinados pelo grupo.

Exemplo 1.4.11. *Classifique todos os grupos G de ordem ≤ 5, a menos de isomorfismo.*

Solução. *Como todos os grupos de ordem ≤ 5 são abelianos temos que*

- *Se $|G| = 2$, então $G \cong \mathbb{Z}_2$.*

- *Se* $|G| = 3$ *então* $G \cong \mathbb{Z}_3$.
- *Se* $|G| = 4 = 2 \cdot 2$, *então* $G \cong \mathbb{Z}_4$ *ou* $\mathbb{Z}_2 \times \mathbb{Z}_2$. *Observando que* $\mathbb{Z}_4$ *possui um elemento de ordem 4, mas* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *não tem elemento de ordem 4.*
- $|G| = 5$ *então* $G \cong \mathbb{Z}_5$.

Exemplo 1.4.12. *Quais são os grupos abelianos de ordem 120, a menos de isomorfismo.*

Solução. *Temos a decomposição em produtos de primos*

$$120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$$

Para cada primo distinto (ou potência dele) consideremos todos os possíveis grupos abelianos de tal ordem:

- *Para* $8 = 2^3$ *temos os seguintes grupos* $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
- *Para 3 temos o grupo* $\mathbb{Z}_3$.
- *Para 5 temos o grupo* $\mathbb{Z}_5$.

Agora os possíveis grupos de ordem 120 consiste de produtos de grupos - exatamente tomado 1 grupo de cada uma das 3 listas acima. Portanto a menos de isomorfismo, existem 3 grupos abelianos de ordem 120:

(1) $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{120} \cong \mathbb{Z}_{24} \times \mathbb{Z}_5 \cong \mathbb{Z}_8 \times \mathbb{Z}_{15}$

(2) $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

(3) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

Exemplo 1.4.13. *Quais são os grupos abelianos de ordem 108, a menos de isomorfismo.*

Solução. *Temos a decomposição em produtos de primos*

$$108 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3$$

Para cada primo distinto (ou potência dele) consideremos todos os possíveis grupos abelianos de tal ordem:

- *Para* $4 = 2^2$ *temos os seguintes grupos* $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$
- *Para* $27 = 3^3$ *temos o grupo* $\mathbb{Z}_{27}$, $\mathbb{Z}_9 \times \mathbb{Z}_3$, $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

Agora os possíveis grupos de ordem 108 consiste de produtos de grupos - exatamente tomado 1 grupo de cada uma das 2 listas acima. Portanto a menos de isomorfismo, existem 6 grupos abelianos de ordem 108:

(1) $\mathbb{Z}_4 \times \mathbb{Z}_{27} \cong \mathbb{Z}_{108}$

(2) $\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_3$

(3) $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

(4) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27}$

(5) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_3$

(6) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

1.4.7 Exercícios Resolvidos

Exercício 1.4.1. *Determine todos as classes laterais distintos do subgrupo* $H =< (1,2) >$ *de* $\mathbb{Z}_4 \times \mathbb{Z}_8$.

Solução. $H = \{(0,0),\ (1,2),\ (2,4),\ (3,6)\}$. *Como G é abeliano e* $|G| = 32$ *e* $|H| = 4$ *temos 8 classes laterais distintas de H que são:*

$$H = \{(0,0),\ (1,2),\ (2,4),\ (3,6)\}$$
$$(0,1)H = \{(0,1),\ (1,3),\ (2,5),\ (3,7)\ \}$$
$$(0,2)H = \{(0,2),\ (1,4),\ (2,6),\ (3,0)\ \}$$
$$(0,3)H = \{(0,3),\ (1,5),\ (2,7),\ (3,1)\ \}$$
$$(0,4)H = \{(0,4),\ (1,6),\ (2,0),\ (3,2)\ \}$$
$$(0,5)H = \{(0,5),\ (1,7),\ (2,1),\ (3,3)\ \}$$
$$(0,6)H = \{(0,6),\ (1,0),\ (2,2),\ (3,4)\ \}$$
$$(0,7)H = \{(0,7),\ (1,1),\ (2,3),\ (3,5)\ \}$$

Exercício 1.4.2. *Suponha que* $G =< a >$ *é um grupo cíclico de ordem 15. Determine todos as classes laterais distintos de* $K =< a^3 >$ *em G.*

Solução. $K = \{e,\ a^3,\ a^6,\ a^9, a^12\}$. *Como G é abeliano e* $|G| = 15$ *e* $|K| = 5$ *temos 3 classes laterais distintas de K que são:*

$$K = \{e,\ a^3,\ a^6,\ a^9, a^{12}\}$$
$$aK = \{a,\ a^4,\ a^7,\ a^{10},\ a^{13}\ \}$$
$$a^2K = \{a^2,\ a^5,\ a^8,\ a^{11},\ a^{14}\ \}$$

Exercício 1.4.3. *Determine todas as classes laterais esquerda do subgrupo* $H =< \overline{4} >$ *do grupo multiplicativo* $\mathbb{U}_{17}$.

Solução. $G = \{\overline{1}, \overline{2}, \cdots, \overline{16}\}$ *e* $H =< \overline{4} >= \{\overline{1}, \overline{4}, \overline{13}, \overline{16}\}$

Como $|G| = 16$ *e* $|H| = 4$ *temos 4 classes laterais esquerda de H que são:*

$$\begin{aligned} 1H = \{\overline{1}, \overline{4}, \overline{13}, \overline{16}\} &= 4H = 13H = 16H = H \\ 2H = \{\overline{2}, \overline{8}, \overline{9}, \overline{15}\} &= 8H = 9H = 15H \\ 3H = \{\overline{3}, \overline{12}, \overline{5}, \overline{14}\} &= 12H = 5H = 14H \\ 6H = \{\overline{6}, \overline{7}, \overline{10}, \overline{11}\} &= 7H = 10H = 11H \end{aligned}$$

Exercício 1.4.4. *Determine a ordem de um subgrupo* **próprio** *e* **não abeliano** *H, de um grupo G de ordem 52.*

Solução.

- *Pelo Teorema de Lagrange,* $|H|$ *divide 52.*
- *Portanto* $|H|$ *pode ser 1, 2, 4, 13, 26 ou 52.*
- *Mas* $|H| \neq 52$, *pois H é um subgrupo proprio de G.*
- *Como H não é abeliano ela não é cíclico.*
- *Como grupos de ordem primos são cíclicos,* $|H|$ *não é primo, ou seja* $|H| \neq 2$ *ou* 13.
- *Do mesmo modo* $|H| \neq 1$, *(pois grupos de ordem 1 contem somente o elemento neutro e portanto são cíclicos)*
- *Além disso* $|H| \neq 4$ *pois grupos de ordem 4 são abelianos.*
- *Portanto* $|H| = 26$.

Exercício 1.4.5. *Seja G um grupo de ordem* 21. *Mostre que qualquer subgrupo próprio de G é cíclico.*

Solução. *Sejam G um grupo com* $|G| = 21$. *Queremos mostrar que qualquer subgrupo próprio de G é cíclico.*

Seja H um subgrupo proprio de G. Então pelo Teorema de Lagrange, $|H|$ *divide* $|G| = 21$.

Como H é próprio, $|H| < 21$ *então temos que* $|H| = 1, 3, 7$.

Se $|H| = 1$, então $H = \{e\}$, que é cíclico.
Caso contrario, $|H| = p$ é primo sendo $p = 3, 7$. Mas, como qualquer grupo de ordem primo é cíclico, H é cíclico.

Exercício 1.4.6. *Seja G um grupo de ordem 36 com elemento neutro e. Se G possui um elemento $a \in G$ tal que $a^{12} \neq e$ e $a^{18} \neq e$, mostre que G é cíclico.*

Solução. *Vamos provar que*

$$G =< a >=< e,\ a,\ a^2,\ a^3,\ \cdots,\ a^{35} > \quad \text{sendo que } a^{36} = e.$$

Como $|G| = 36$, pelo Teorema de Lagrange, todos os elementos de G deve ter ordem que divide 36, ou seja, todos os elementos de G deve ter ordem 1, 2, 3, 4, 6, 9, 12, 18 ou 36.
Mas, como $a^{12} \neq e$ e $a^{18} \neq e$, temos que que a não tem ordem 1, 2, 3, 4, 6, 9, 12 ou 18.
Portanto $ord(a) = 36$, ou seja, $a^{36} = e$. Portanto, $G =< a >$ e portanto é cilício.

Exercício 1.4.7. *Determine a ordem de um subgrupo H que tem as seguintes condições:*

(a) H é um subgrupo próprio de um grupo G de ordem 68.

(b) H não é abeliano.

Solução.

- *Pelo Teorema de Lagrange, $|H|$ divide 68.*
- *Portanto $|H|$ pode ser 1, 2, 4, 17, 34 ou 68.*
- *Mas $|H| \neq 68$, pois H é um subgrupo proprio de G.*
- *Como H não é abeliano ela não é cíclico.*
- *Como grupos de ordem primos são cíclicos, $|H|$ não é primo, ou seja $|H| \neq 2$ ou 17.*
- *Do mesmo modo $|H| \neq 1$, (pois grupos de ordem 1 contem somente o elemento neutro e portanto são cíclicos)*
- *Além disso $|H| \neq 4$ pois grupos de ordem 4 são abelianos.*
- *Portanto $|H| = 34$.*

Exercício 1.4.8. *Determine a ordem de um subgrupo H que tem as seguintes condições:*

(a) H é um subgrupo de algum grupo G de ordem 100.

(b) H contem nenhum elemento de ordem 2.

(c) H não é cíclico.

Solução.

- *Pelo Teorema de Lagrange, $|H|$ divide 100.*
- *Portanto $|H|$ pode ser 1, 2, 4, 5, 10, 20, 25 ou 100.*
- *Como grupos de ordem primos são cíclicos, $|H|$ não é primo, ou seja $|H| \neq 1,\ 2$ ou 5.*
- *Agora grupos de ordem pares deve ter um elemento de ordem 2. Como H não contem um elemento de ordem 2, temos que a ordem de H deve ser ímpar.*
- *Portanto $|H| = 25$.*

1.4.8 Atividade

1. *Dados os grupos G e seus subgrupos H abaixo, determine as classes laterais à direta e à esquerda determinados pelos elementos de G e escreva G como a união das classes laterais à direta e à esquerda distintas:*

   (a) $G = \mathbb{Z}_{12}$ *e* $H = \{\ \overline{0},\ \overline{4},\ \overline{8}\ \}$.

   (b) $G = S_3$ *e* $H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$.

   (c) $G = \mathbb{Z}$ *e* $H = 6\mathbb{Z}$.

   (d) $G = \mathbb{Z}_{13}^*$ *e* $H = <\overline{5}>$.

2. *Seja $m \in \mathbb{N}, m \geq 2$. Seja $m\mathbb{Z} = \{mz;\ z \in \mathbb{Z}\}$.*

   (a) Mostre que $m\mathbb{Z}$ é um subgrupo de $\mathbb{Z}$.

   (b) Determine $(\mathbb{Z} : m\mathbb{Z})$ e todas as classes laterais de $m\mathbb{Z}$ em $\mathbb{Z}$.

   (c) Determine o subgrupo $m\mathbb{Z} \cap n\mathbb{Z}$.

3. *Determine as classes laterais esquerda e a direta de* $\{1, s\}$ *do grupo diedral*

$$D_{12} =< r,\ s\ | r^6 = id,\ s^2 = id,\ rs = sr^{-1} > .$$

4. *Seja G um grupo de ordem* p^n*, em que p é primo e* $n > 1$*. Mostre que a ordem de um elemento qualquer de G é potência de p.*

5. *Sejam H e K subgrupos de um grupo finito G com* $|H| = p,\ |K| = q,\ p$ *e q primos distintos. Prove que* $H \cap K = \{e\}$.

6. *Determine a ordem de um subgrupo* **próprio** *e* **não abeliano não isomorfo ao um grupo diedral** *H, de um grupo G de ordem 78.*

7. *Determine a ordem de grupo H com as seguintes propriedades:*

   (a) H é um subgrupo de um grupo G de ordem 168.

   (b) H é um subgrupo de um outro grupo K de ordem 112.

   (c) H não é cíclico nem isomorfo ao um grupo diedral.

   (d) H contém um elemento de ordem 7

   (e) H tem mais de 2 classes laterais esquerda em K.

8. *Determine a ordem de um grupo H com as seguintes propriedades:*

   (a) H é um subgrupo de um grupo G de ordem 100.

   (b) H é um subgrupo de um outro grupo K de ordem 40.

   (c) H não é cíclico nem isomorfo a um grupo diedral.

9. *Determine a ordem de um grupo H com as seguintes propriedades:*

   (a) H é um subgrupo de um grupo G de ordem 20.

   (b) H é não abeliano.

   (c) G contem um elemento g de ordem 2 e um elemento h de ordem 5.

   (d) h pertence a H mas g não

10. *Sejam H e K subgrupos de um grupo G. Se* $|H| = 14$ *e* $|K| = 35$*, mostre que* $H \cap K$ *é cíclico.*

11. *Seja G um grupo de ordem 22, quais são os possíveis ordens de cada elemento em G.*

12. *Seja G um grupo com $|G| < 300$. Se G possuem um subgrupo H de ordem 24 e um subgrupo K de ordem 54, determine a ordem $|G|$ de G.*

13. *Determine todos os grupos abelianos de ordens 64, 212, 600, 1000, 1250 a menos de isomorfismo.*

Aula 1.5

Subgrupos Normais e Grupos Quocientes

Vimos na Aula 1.4 que dado um grupo G, podemos encontrar uma partição de G em classes laterais do subgrupo H. Cada partição tem o mesmo número de elementos. Nesta aula vamos estudar a estrutura das classes laterais e a relação entre eles. O conceito do subgrupo normais vai ser apresentado e vamos formar um grupo das classes laterais, o grupo quociente.

1.5.1 Subgrupo normal

1.5.1.1 Motivação

Exemplo 1.5.1. *Considere o grupo* $G = S_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$.

(a) Seja o subgrupo $K = \{(1), (1\ 2)\}$ *de G. Determine as classes laterais à esquerda e à direta de K em G.*

(b) Seja o subgrupo $H = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ *de G. Determine as classes laterais à esquerda e à direta de H em G.*

Solução:

(a) Classes laterais à esquerda de K são

- $(1)K = (1\ 2)K = K = \{(1), (1\ 2)\}$
- $(1\ 3)K = (1\ 2\ 3)K = \{(1\ 3), (1\ 2\ 3)\}$
- $(2\ 3)K = (1\ 3\ 2)K = \{(2\ 3), (1\ 3\ 2)\}$

(a) Classes laterais à direta de K são

- $K(1) = K(1\ 2) = K = \{(1), (1\ 2)\}$
- $K(1\ 3) = K(1\ 3\ 2) = \{(1\ 3), (1\ 3\ 2)\}$
- $K(2\ 3) = K(1\ 2\ 3) = \{(2\ 3), (1\ 2\ 3)\}$

Observamos que a classe $(1\ 3)K \neq K(1\ 3)$ *e* $(2\ 3)K \neq K(2\ 3)$.

(b) Classes laterais à esquerda de H são

- $(1)H = (1\ 2\ 3)H = (1\ 3\ 2)H = H = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$
- $(1\ 2)H = (1\ 3)H = (2\ 3)H = \{(1\ 2), (1\ 3), (2\ 3)\}$

(b) Classes laterais à direta de H são

- $H(1) = H(1\ 2\ 3) = H(1\ 3\ 2) = H = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$
- $H(1\ 2) = H(1\ 3) = H(2\ 3) = \{(1\ 2), (1\ 3), (2\ 3)\}$

Observamos que a classes laterais esquerda de H são iguais às respectivas classes laterais à direta de H.

Os subgrupos H de G nas quais as classes laterais esquerda são iguais às respectivas classes laterais à direta recebe uma denominação especial. São chamados subgrupos normais.

Definição 1.5.1. *Seja H um subgrupo G. Dizemos que H é um* **subgrupo normal** *de G (e denotamos* $H \trianglelefteq G$*) se* $aH = Ha$ *para todo* $a \in G$.

Observação. *O significado de* $H \trianglelefteq G$*, é que dado* $a \in G$ *e* $h \in H$*, existem* $h', h'' \in H$ *tal que*

$$ah = h'a \quad e \quad ha = ah''$$

Note que $H \trianglelefteq G$ **não** *implica que* $ah = ha$, $\forall\ h \in H$.
Vimos no Exemplo 1.5.1 que $H = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ *é normal em* S_3. *Seja* $a = (1, 2) \in S_3$ *e* $h = (1\ 3\ 2) \in H$. *Então existe* $h' = (1\ 2\ 3) \in H$ *tal que*

$$\overbrace{(1\ 2)}^{a}\overbrace{(1\ 3\ 2)}^{h} = \overbrace{(1\ 2\ 3)}^{h'}\overbrace{(1\ 2)}^{a} = (1\ 3).$$

Exemplo 1.5.2. *Seja G um grupo. Então os subgrupos triviais de G,* $H_1 = \{e\}$ *e* $H_2 = G$*, são subgrupos normais de G.*

Exemplo 1.5.3. *Seja G um grupo abeliano, então todo subgrupo H de G é normal pois* $ah = ha$, $\forall a \in G$ *e* $\forall h \in H$.

Exemplo 1.5.4. *O centro* $Z(G)$ *de um grupo é sempre normal pois* $ah = ha$ $\forall a \in G$ *e* $\forall h \in Z(G)$.

Definição 1.5.2. *Um grupo $G \neq \{e\}$ é dito simples se $\{e\}$ e G são seus únicos subgrupos normais.*

Exemplo 1.5.5. *Seja p um número primo. Então $\mathbb{Z}_p$ é um grupo simples. De fato $\mathbb{Z}_p$ são os únicos abeliano simples grupos.*

Teorema 1.5.1. *Se $H \leq G$ e $(G : H) = 2$ então $H \trianglelefteq G$.*

Demonstração. Seja $a \in G$.

- Se $a \in H$, então
$$H = aH = Ha$$
- Se $a \notin H$ então a classe lateral esquerda aH e a classe lateral a direta Ha de H são diferente de H.

Como $(G : H) = 2$, ou seja temos somente 2 distintos classes laterais esquerda (ou a direta) de H em G.
Portanto
$$G = H \cup aH = H \cup Ha \quad \text{e} \quad H \cap aH = \emptyset = H \cap Ha$$
Logo temos que $aH = Ha, \ \forall a \in G$. Portanto $H \trianglelefteq G$. ■

Exemplo 1.5.6. *Considere S_n, o grupo de permutação de $\{1, 2, 3 \cdots, n\}$ e A_n o subgrupo de permutações pares. $|S_n| = n!$ e $|A_n| = \frac{n!}{2}$. Logo*
$$(S_n : A_n) = \frac{|S_n|}{|A_n|} = 2$$
Portanto pelo teorema acima temos A_n é normal em S_n.

Teorema 1.5.2. *(Teste para Subgrupos Normais)*
Se $H \leq G$, $H \trianglelefteq G \Leftrightarrow \ xHx^{-1} \subseteq H$ para todo $x \in G$.

Demonstração.

($\Rightarrow$) : Suponha que H é normal em G. Então $\forall x \in G$ e $\forall h \in H$, existe $h' \in H$ tal que
$$xh = h'x \Rightarrow xhx^{-1} = h' \in H.$$
Portanto $xHx^{-1} \subseteq H$.

($\Rightarrow$) : Suponha que $xHx^{-1} \subseteq H$ para todo $x \in G$.

- Seja $x = a$. Então

$$aHa^{-1} \subseteq H \Rightarrow aH \subseteq Ha \tag{1}$$

- Seja $x = a^{-1}$. Então

$$a^{-1}H(a^{-1})^{-1} = a^{-1}Ha \subseteq H \Rightarrow Ha \subseteq aH \tag{2}$$

De (1) e (2) temos que $Ha = aH \Rightarrow H \trianglelefteq G$.

■

Exemplo 1.5.7. *Considere o grupo $G = \mathbb{R}^* \times \mathbb{R}$ cuja operação $*$ é definida por*

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

Prove que

(a) $H = \{(1, b) |\ b \in \mathbb{R}\} \trianglelefteq G$

(b) $K = \{(a, 0) |\ a \in \mathbb{R}^*\}$ *não é subgrupo normal de* G.

Solução.

(a) Inicialmente, vamos determinar o elemento neutro de G e o inverso de $(a, b) \in G$ para a operação $*$.

Seja (x, y) o elemento neutro de G, temos

$$(a, b) = (ab) * (x, y) = (ax, ay + b) \Rightarrow ax = a \Rightarrow x = 1 \text{ e } ay + b = b \Rightarrow ay = 0 \Rightarrow y = 0,$$

pois $a \neq 0$. Como $(1, 0) * (a, b) = (a, b)$, vemos que $(1, 0)$ é o elemento neutro de G.

Dado $(a, b) \in G$ seja (c, d) seu inverso para a operação $*$, temos

$$(1, 0) = (a, b) * (c, d) = (ac, ad + b) \Rightarrow ac = 1 \Rightarrow c = \frac{1}{a} \text{ e } ad + b = 0 \Rightarrow d = -\frac{b}{a}.$$

Como $\left(\frac{1}{a}, -\frac{b}{a}\right) * (a, b) = (1, 0)$, temos que $(a, b)^{-1} = \left(\frac{1}{a}, -\frac{b}{a}\right)$

Agora provamos que H é normal em G. Seja $(1, c) \in H$, para cada $(a, b) \in G$ temos:

$$(a, b) * (1, c) * (a, b)^{-1} = (a, b) * (1, c) * \left(\frac{1}{a}, -\frac{b}{a}\right) = (a, ac + b) * \left(\frac{1}{a}, -\frac{b}{a}\right) = (1, ac) \in H.$$

Portanto, $H = \{(1, b) | \ b \in \mathbb{R}\} \trianglelefteq G$

(b) Seja $(c, 0) \in K$*, para cada* $(a, b) \in G$ *temos:*

$$(a, b) * (c, 0) * (a, b)^{-1} = (a, b) * (c; 0) * \left(\frac{1}{a}, -\frac{b}{a}\right) = (ac, b) * \left(\frac{1}{a}, -\frac{b}{a}\right) = (c, -bc + b).$$

Se $0 \neq -bc + b = b(1 - c)$*, então* $(a, b) * (c, 0) * (a, b)^{-1} \notin K$ *e* K *não será subgrupo normal de* G*. Podemos, por exemplo, tomar* $a = b = 1$ *e* $c = 2$*. Neste caso* $(1, 1)*(2, 0)*(1, 1)^{-1} = (2, -1) \notin K \Rightarrow K$ *não é subgrupo normal de* G*.*

O resultado a seguir mostra outras caracterização de subgrupo normal muito usada.

Proposição 1.5.3. *Sejam* G *um grupo e* $N \trianglelefteq G$*. Então as seguintes afirmações são equivalentes:*

1. $N \trianglelefteq G$
2. *Para todo* $a \in G$, $aNa^{-1} = N$.
3. *As classes laterais à esquerda e à direta coincidem, ou seja* $Na = aN$ *para todo* $a \in G$.

Exemplo 1.5.8. *Seja* $G = GL(2, \mathbb{R})$ *e* $H = SL(2, \mathbb{R})$*. Mostre que* H *é um subgrupo normal de* G*.*

Solução: *Seja* $x \in GL(2, \mathbb{R})$*. Então para todo* $h \in SL(2, \mathbb{R})$*, temos que*

$$\det(xhx^{-1}) = (\det(x))\,(\det(h))\,(\det(x))^{-1} = (\det(x))\,(\det(h))\left(\frac{1}{\det(x)}\right) = 1,$$

portanto $xhx^{-1} \in SL(2, \mathbb{R}) \Rightarrow xSL(2, \mathbb{R})x^{-1} \subseteq SL(2, \mathbb{R})$.

Portanto $SL(2, \mathbb{R})$ *é normal em* $GL(2, \mathbb{R})$.

1.5.2 O Grupo Quociente

Definição 1.5.3. *Sejam G um grupo e H um subgrupo normal de G. Denotamos por*

$$G/H = \{aH \mid a \in G\}$$

o **conjunto das classes laterais** *à esquerda com respeito a H.*

Vamos construir uma operação binária no conjunto das classes laterais G/H de modo a torná-lo um grupo. Definimos a seguinte operação no conjunto das classes laterais G/H :

$$\psi : G/H \times G/H \to G/H$$

dada por

$$aH \cdot bH \mapsto (ab)H.$$

O problema é verificar que ψ está bem definida, ou seja, se ela não depender da escolha dos representantes de a e b das classes laterais aH e bH respectivamente.

Suponha que $a, a', b, b' \in G$ tais que $aH = a'H$ e $bH = b'H$. Então $a' = ah_1$ e $b' = bh_2$ para algum $h_1, h_2 \in H$. Então

$$\begin{aligned}
\psi(a'H,\ b'H) &= (a'b')H \qquad \text{pela definição de } \psi \\
&= ah_1bh_2H \\
&= ah_1bH \qquad \text{pois } h_2 \in H \\
&= ah_1Hb \qquad \text{pois } H \text{ é normal} \\
&= aHb \qquad \text{pois } h_1 \in H \\
&= abH \qquad \text{pois } H \text{ é normal} \\
\psi(aH,\ bH)
\end{aligned}$$

Portanto ψ é bem definida.

Teorema 1.5.4. *Se G é um grupo e $H \trianglelefteq G$, então G/H é um grupo com respeito da operação*

$$aH \cdot bH = (ab)H.$$

Chamamos este grupo de **grupo quociente de** G **módulo** H.

Demonstração. Vamos provar que a operação $\cdot$ é associativa, possui elemento neutro e que todo elemento de G/H possui elemento inverso para $\cdot$

(i) Associatividade: sejam $aH,\ bH$ e $cH \in G/H$. Como G é um grupo temos $(ab)c = a(bc)$, logo $(aH \cdot bH) \cdot cH = abH \cdot cH = (ab)cH = a(bc)H = aH \cdot (bH \cdot cH)$

(ii) Como G é grupo, G possui elemento neutro e e, evidentemente, $N = eN$. Temos

$$aH \cdot H = aH \cdot eH = aeH = aH = eaH = eH \cdot aH = H \cdot aH,\ \forall a \in G.$$

Logo, H é o elemento neutro de $\cdot$.

(iii) Como G é grupo, todo $a \in G$ possui elemento inverso a^{-1}. Temos

$$aH \cdot a^{-1}H = aa^{-1}H = eH = H = a^{-1}aH = a^{-1}H \cdot aH.$$

Logo, $a^{-1}H$ é o elemento inverso de aH para a operação $\cdot$.

Resulta de (i), (ii) e (iii) que G/H munido da operação $\cdot$ é um grupo. ■

Exemplo 1.5.9. *Seja $G = \mathbb{U}_{14}$ (com operação multiplicação) e considere o subconjunto $H = \{1,\ 13\}$ de G. Prove que H é um subgrupo normal de G. Listar todos os elementos de G/H e construa a tabela de Cayley para G/H e mostrar que $G/H \cong \mathbb{Z}_3$.*

Solução. $G = \mathbb{U}_{14} = \{1,\ 3,\ 5,\ 9,\ 11,\ 13\}$ *e* $N = \{1,\ 13\}$

- $H = 1H = \{1,\ 13\} = H1$
- $3H = \{3,\ 11\} = H3$
- $5H = \{5,\ 9\} = H5$

Portanto $H \trianglelefteq G$ *e* $G/H = \{H,\ 3H,\ 5H\}$

$\cdot$	H	$3H$	$5H$
H	H	$3H$	$5H$
$3H$	$3H$	$5H$	H
$5H$	$5H$	H	$3H$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Vimos que a tabela de Cayley de G/H *coincide com a tabela de Cayley de* $(\mathbb{Z}_3, +)$*, pela isomorfismo* $H \mapsto 0,\ 3H \mapsto 1,\ 5H \mapsto 2$*. Em particular, o grupo quociente* G/H *é isomorfo a* $\mathbb{Z}_3$*.*

Exemplo 1.5.10. *Describa todos os grupos quocientes de* S_3*.*

Solução. *Os subgrupos de* S_3 *são:*

- $\{id\}$: *Normal, e o grupo quociente é* $S_3/\{id\} \cong S_3$*.*
- $\{id, (123), (321)\}$: *Normal, e o grupo quociente é* $S_3/\{id, (123), (321)\} \cong \mathbb{Z}_2$*.*
- $\{id, (12)\},\ \{id, (23)\},\ \{id, (13)\}$: *Nenhum deste são normais*
- S_3 : *Normal, é o grupo quociente é* $S_3/S_3 \cong \{id\}$

Exemplo 1.5.11. *Seja* $G = \mathbb{Z}$ *(com operação adição) e* $H = 4\mathbb{Z}$*. Listar todos os elementos de* G/H *e construa a tabela de Cayley para* G/H*. Mostre que* $G/H \cong \mathbb{Z}_4$*.*

Solução. *Seja* $4\mathbb{Z} = \{0,\ \pm 4,\ \pm 8, \cdots\}$*. Para construir* $\mathbb{Z}/4\mathbb{Z}$ *determinamos as classes laterais a esquerda de* $4\mathbb{Z}$ *em* $\mathbb{Z}$*. Considere os seguintes 4 classes:*

$$0 + 4\mathbb{Z} = 4\mathbb{Z} = \{0,\ \pm 4,\ \pm 8,\ \cdots\},$$

$$1 + 4\mathbb{Z} = \{1, 5, 9, \cdots; -3, -7, -11, \cdots\},$$

$$2 + 4\mathbb{Z} = \{2, 6, 10, \cdots; -2, -6, -10, \cdots\},$$

$$3 + 4\mathbb{Z} = \{3, 7, 11, \cdots; -1, -5, -9, \cdots\}.$$

Afirmamos que não há outros classes. Pois, se $k \in \mathbb{Z}$*, então* $k = 4q + r$*, onde* $0 \leq r < 4$*; e, portanto,* $k + 4\mathbb{Z} = r + 4q + 4\mathbb{Z} = r + 4\mathbb{Z}$*. A tabela de Cayley é*

+	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$0+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

Vimos que a tabela de Cayley de $\mathbb{Z}/4\mathbb{Z}$ *coincide com a tabela de Cayley de* $(\mathbb{Z}_4, +)$*, pela isomorfismo* $i + 4\mathbb{Z} \mapsto [i]_4$*. Em particular, o grupo quociente* $\mathbb{Z}/4\mathbb{Z}$ *é isomorfo a* $\mathbb{Z}_4$*.*

Proposição 1.5.5. *Seja* $n \geq 2$ *inteiro.O grupo quociente* $\mathbb{Z}/n\mathbb{Z}$ *é isomorfo a* $\mathbb{Z}_n$ *pela isomorfismo* $(i + n\mathbb{Z}) \mapsto [i]_n$*.*

1.5.3 Ordem de G/H

Proposição 1.5.6. *Sejam G é um grupo finito e* $H \trianglelefteq G$*. Então*

$$\left|G/H\right| = \frac{|G|}{|H|}.$$

Demonstração. O número de elementos em G/H, é o índice do subgrupo H do grupo G, que é o número de classes laterais à direita distintas de H em G. Portanto $\left|G/H\right| = [G : H]$.
Mas pelo Teorema de Lagrange,

$$[G : H] = \frac{|G|}{|H|}$$

Portanto

$$\left|G/H\right| = \frac{|G|}{|H|}.$$

■

Exemplo 1.5.12.

(a) Determine a ordem de $\mathbb{Z}_6/_{< 3 >}$

(b) Determine a ordem de $\mathbb{Z}_4 \times \mathbb{Z}_2/_{< (2,1) >}$

Solução.

(a) $|\mathbb{Z}_6| = 6$ *e* $| < 3 > | = 2$. *Portanto* $\left| \mathbb{Z}_6/_{< 3 >} \right| = 3$.

(b) $|\mathbb{Z}_4 \times \mathbb{Z}_2| = 8$ *e* $| < (2,1) > | = 2$. *Portanto* $\left| \mathbb{Z}_4 \times \mathbb{Z}_2/_{< (2,1) >} \right| = 4$.

1.5.4 Ordem de um elemento em $G/_H$

Podemos definir a ordem $|aH|$, de duas maneiras:

(a) a ordem de aH como elemento de $G/_H$

(b) o comprimento do conjunto aH

A interpretação correta será claro em cada contexto.

Proposição 1.5.7. *Sejam $H \trianglelefteq G$ e $a \in G$ Então a ordem de aH em $G/_H$ é o menor inteiro positivo n tal que $a^n \in H$.*

Demonstração. Suponha que aH é um elemento de $G/_H$ (portanto $a \in G$) e queremos calcular sua ordem como elemento de $G/_H$. Em outras palavras, queremos determinar um inteiro positivo n tais que

$$(aH)^n = eH = H \quad \text{e se} \quad 1 \leq m < n, \ (aH)^m \neq H.$$

Pela definição da multiplicação no grupo quociente, precisamos encontrar n tais que

$$a^n H = H \quad \text{e se} \quad 1 \leq m < n, \ a^m H \neq H$$

Pelo Proposição 1.4.1

$$a^n H = H \Leftrightarrow a^n \in H, \ \text{e} \ a^m H \neq H \Leftrightarrow a^m \neq H.$$

Portanto, $|aH| = n$ em $G/_H \Leftrightarrow n$ é o menor inteiro positivo para que $a^n \in H$. ■

Exemplo 1.5.13.

(a) Determine a ordem de $5 + < 4 >$ *em* $\mathbb{Z}_{12}/_{< 4 >}$

(b) Determine a ordem de $(2,1) + < (1,1) >$ *em* $\mathbb{Z}_3 \times \mathbb{Z}_6/_{< (1,1) >}$

(c) Determine a ordem de $(2,0) + < (4,4) >$ *em* $\mathbb{Z}_6 \times \mathbb{Z}_8/_{< (4,4) >}$

Solução.

(a) $< 4 >= \{0,\ 4,\ 8\}$ *e* $5 * 4 = 8$, *que é a primeira vez que um múltiplo de 5 em* $< 4 >$ *. Portanto a ordem do elemento dado é 4.*

(b) $< (1,1) >= \{(1,1),\ (2,2),\ (0,3),\ (1,4),\ (2,5),\ (0,0)\}$ *e* $(2,1) * 3 = (0,3)$, *que é a primeira vez que um múltiplo de* $(2,1)$ *em* $< (1,1) >$ *. Portanto a ordem do elemento dado é 3.*

(c) $< (4,4) >= \{(4,4),\ (2,0),\ (0,4),\ (4,0),\ (2,4),\ (0,0)\}$ *e* $(2,0) \in < (4,4)$, *é portanto a ordem do elemento dado é 1.*

Exemplo 1.5.14. *Considere o grupo diedral*

$$D_6 = \{id,\ r,\ r^2,\ r^3,\ r^4,\ r^5,\ s,\ sr,\ sr^2,\ sr^3,\ sr^4, sr^5\},\ \ r^6 = id,\ s^2 = id,\ sr^5 = rs$$

e $H = Z(D_6) = \{id,\ r^3\}$ *o centro de* D_6. *Determine as ordens de* rH e $(sr^3)H$ *em* $D_6/_H$.

Solução.

- *A ordem de* rH *em* $D_6/_H$ *é o menor inteiro positivo* n *tal que* $r^n \in H = \{1,\ r^3\}$. *Logo* $n = 3$ *e a ordem de* rH *em* $D_6/_H$ *é igual 3.*

- *A ordem de* $(sr^3)H$ *em* $D_6/_H$ *é o menor inteiro positivo* n *tal que* $(sr^3)^n \in H = \{1,\ r^3\}$. *Agora*

$$(sr^3)^2 = sr^3 \cdot sr^3 = sr^3 \cdot r^3 s = s^2 r^6 = id \in H.$$

Logo $n = 2$ *e a ordem de* $(sr^3)H$ *em* $D_6/_H$ *é igual 2.*

Apresentamos alguns resultados sobre o grupo quociente.

Proposição 1.5.8. *Sejam G um grupo e $N \trianglelefteq G$. Então:*

(a) Se G é um grupo abeliano, então o grupo quociente G/N é um grupo abeliano.

(b) Se G é um grupo cíclico, então o grupo quociente G/N é um grupo cíclico.

Demonstração.

(a) Sejam $aN,\ bN \in G/N$. Como G é abeliano temos $ab = ba$ o que implica

$$aN \cdot bN = abN = baN = bN \cdot aN$$

e completa a prova de que G/N é abeliano.

(b) Suponha que G é um grupo cíclico gerado pelo elemento $x \in G$. Isto é, qualquer elemento de G é uma potência de x. Afirmamos que a classe lateral xN é gerador do grupo G/N. De fato, seja $aN \in G/N$ com $a \in G$, então podemos escrever $a = x^k$ para algum $k \in \mathbb{Z}$. Assim,

$$aN = x^kN = (xN)^k \ \text{ para algum } \ k \in \mathbb{Z}$$

o que mostra que G/N é um grupo cíclico.

■

Lema 1.5.9. *Se G é um grupo tal que $G/Z(G)$ é cíclico então G é abeliano.*

Demonstração. Seja $gZ(G)$ o gerador do grupo quociente $G/Z(G)$, e seja $a, b \in G$. Então existe inteiros i e j tais que

$$aZ(G) = (gZ(G))^i = g^iZ(G)$$

e

$$bZ(G) = (gZ(G))^j = g^jZ(G).$$

Portanto, $a \in g^i x$ para algum $x \in Z(G)$ e $b \in g^j y$ para algum $y \in Z(G)$. Portanto temos que

$$\begin{aligned} ab &= (g^i x)(g^j y) = g^i(xg^j)y = g^i(g^j x)y \\ &= (g^i g^j)(xy) = (g^j g^i)(yx) = (g^j y)(g^i x) = ba. \end{aligned}$$

■

1.5.5 Grupos quocientes e Homomorfismos de grupos

Nossa próximo objetivo é mostrar que grupos quocientes são relacionadas com homomorfismos. Vamos mostrar que cada grupo quociente G/H naturalmente dar um homomorfismo $\pi : G \to G/H$, chamado a projeção natural de G para G/H.

Teorema 1.5.10. *Sejam G_1 e G_2 grupos e $\varphi : G_1 \to G_2$ um homomorfismo. Então o núcleo, $Nuc(\varphi)$, de φ é um subgrupo normal de G_1.*

Demonstração. Seja $H = Nuc(\varphi)$. Já vimos que em Lema 1.3.9 que H é um subgrupo de G_1, então basta provar que ela é normal. Escolhe $h \in H$ e $g \in G_1$. Pela definição do núcleo de φ temos que $\varphi(h) = e_{G_2}$ (o elemento neutro de G_2.). Portanto

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)e_2\varphi(g)^{-1} = e_{G_2}$$

Portanto $ghg^{-1} \in Nuc(\varphi) = H$. Portanto H é normal em G. ■

Exemplo 1.5.15. *Podemos deduzir do Exemplo 1.3.9 que*

(a) $A_n \trianglelefteq S_n$, pois $A_n = Nuc(sgn)$

(b) $SL(n.\mathbb{R}) \trianglelefteq GL(n, \mathbb{R})$ pois $SL(n, \mathbb{R}) = Nuc(\det)$

Teorema 1.5.11. *Seja G um grupo e $H \trianglelefteq G$. Define a aplicação $\pi : G \to {}^{G}\!/_{H}$ por*

$$\pi(g) = gH \text{ para todo } g \in G.$$

Então π é um homomorfismo sobrejetora e $Nuc(\pi) = H$.

Demonstração.

- π é um homomorfismo pois

$$\pi(xy) = xyH = (xH)(yH) = \pi(x)\pi(y)$$

- π é sobrejetora diretamente pela definição de G/H pois cada elemento de G/H tem a forma $gH = \pi(g)$ para todo $g \in G$.

- $Nuc(\pi) = \{x \in G : \pi(x) = e_G H\} = \{x \in G : xH = e_G H\} = H$

■

1.5.6 Teoremas de Isomorfismos

Teorema 1.5.12. ***[Primeiro Teorema de Isomorfismo] Sejam $\varphi : G \to G'$ um homomorfismo de grupos. Então***

$${}^{G}\!/_{Nuc(\varphi)} \simeq Im(\varphi)$$

Demonstração. Seja $N = Nuc(\varphi)$. Defina o homomorfismo $\widetilde{\varphi} : {}^{G}\!/_{N} \to Im(\varphi)$ por

$$\widetilde{\varphi}(Na) = \varphi(a).$$

- Vamos provar primeiramente que $\widetilde{\varphi}$ é bem-definida, ou seja, precisamos verifique que se

$$a' \in Na, \text{ então } \widetilde{\varphi}(Na) = \widetilde{\varphi}(Na')$$

Mas, observe que $a' \in Na \Rightarrow a' = na$ para algum $n \in N$. Portanto

$$\widetilde{\varphi}(Na') = \varphi(a') = \varphi(na) = \varphi(n)\varphi(a) = e' \cdot \varphi(a) = \varphi(a) = \widetilde{\varphi}(Na)$$

- Vamos provar agora que $\widetilde{\varphi}$ é um homomorfismo:
  Considere $Na, Na' \in G/N$. Então

$$\begin{aligned}
\widetilde{\varphi}(aN \cdot a'N) &= \widetilde{\varphi}(aa'N) && \text{pela definição de multplicação de classes laterais} \\
&= \varphi(aa') && \text{pela definição de } \widetilde{\varphi} \\
&= \varphi(a)\varphi(a') && \text{pois } \varphi \text{ é um homomorfismo} \\
&= \widetilde{\varphi}(aN)\widetilde{\varphi}(a'N) && \text{pela definição de } \widetilde{\varphi}
\end{aligned}$$

  Portanto φ é um homomorfismo.

- Vamos provar agora que $\widetilde{\varphi}$ é injetora, ou seja, basta provar que $Nuc(\widetilde{\varphi}) = N$. Para isto, observe que

$$\widetilde{\varphi}(aN) = e' \Leftrightarrow \varphi(a) = e' \Leftrightarrow a \in Nuc(\varphi) \Leftrightarrow a \in N \Leftrightarrow aN = N.$$

  Portanto $Nuc(\widetilde{\varphi}) = N$.

- Finalmente precisamos ver que $\widetilde{\varphi}$ é sobrejetora. De fato se $\varphi(a) \in Im(\varphi)$, então $\varphi(a)$ tem a preimagem aN.

■

Exemplo 1.5.16.

(a) Seja $\varphi : \mathbb{Z} \to \mathbb{Z}_n, \ a \mapsto [\overline{a}]_n$ *(redução modulo n).*

- φ *é um homomorfismo*
- φ *é sobrejetora, pois se* $a \in \mathbb{Z}_n = \{0, 1, \cdots n-1\}$ *então* $\varphi(a) = a$. *Portanto* $Im(\varphi) = \mathbb{Z}_n$.
- $Nuc(f) = \{a \in \mathbb{Z} : \varphi(a) = [\overline{a}]_n\} = \{na, a \in \mathbb{Z}\} = n\mathbb{Z}$

Portanto pelo 1^o *Teorema de Isomorfismo (Teorema 1.5.12)*

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/Nuc(\varphi) \cong \mathbb{Z}_n$$

(b) Vimos no Exemplo 1.3.9 que $sgn : S_n \to \{-1, 1\}$

- *é um homomorfismo com*
- $Nuc(sgn) = A_n$
- *Além disto* sgn *é sobrejetora*

Portanto pelo 1^o *Teorema de Isomorfismo (Teorema 1.5.12)*

$$S_n/A_n \cong \{-1, 1\}$$

(c) Vimos no Exemplo 1.3.9 que $\det : GL(n, \mathbb{R}) \to \mathbb{R}^*$

- *é um homomorfismo com*
- $Nuc(\varphi) = SL(n, \mathbb{R})$

Teorema 1.5.13 (Segundo Teorema de Isomorfismo). *Sejam H e K subgrupos de G. Se K é um subgrupo normal, então*

- *HK é subgrupo de G,*
- *$H \cap K$ é subgrupo normal de H,*
- *$\varphi : H \to HK/K$, definido por $\varphi(x) = xK$ é um homomorfismo sobrejetivo de núcleo $H \cap K$*

portanto, $H/H \cap K \cong HK/K$.

Teorema 1.5.14 (Terceiro Teorema de Isomorfismo). *Se $H \subseteq K$ são subgrupos normais de G então K/H é subgrupo normal de G/H e a função $\varphi : G/H \to G/K$ definida por $\varphi(xH) = xK$ é um homomorfismo de grupos com núcleo K/H, portanto*

$$\left(G/H\right)\Big/\left(H/K\right) \cong G/K.$$

1.5.7 Classificação do grupo quociente

Problema: Dado o grupo quociente G/H***, queremos determinar um grupo*** G' ***isomorfo a*** G/H.

Alguns resultados simples

(1) $G/_{\{e\}}$ ***é isomorfo a*** G.

(2) $G/_{G}$ ***é isomorfo a*** $\{e\}$.

(3) Se G ***é cíclico então*** $G/_{H}$ ***é também cíclico.***

(4) Se $G = G_1 \times G_2$, ***então*** $G/_{(\{e\} \times G_2)}$ ***é isomorfo a*** G_1.

(5) Se $G = G_1 \times G_2$, $H \lhd G_1$ ***e*** $H \lhd G_2$, ***então*** $G/_{(H_1 \times H_2)}$ ***é isomorfo a*** $G_1/_{H_1} \times G_2/_{H_2}$.

Exemplo 1.5.17. *Classifique o grupo quociente*

$$(\mathbb{Z}_4 \times \mathbb{Z}_6) \Big/ (< 2 > \times < 3 >)$$

Solução. *Usando o fato que*

$$G/_{(H_1 \times H_2)} \cong G_1/_{H_1} \times G_2/_{H_2}$$

temos que

$$(\mathbb{Z}_4 \times \mathbb{Z}_6) \Big/ (< 2 > \times < 3 >) \cong \mathbb{Z}_4/_{< 2 >} \times \mathbb{Z}_6/_{< 3 >} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Método mais geral I

Se $G/_{H}$ *é um grupo finito, podemos usar a classificação de grupos finito para classificar* $G/_{H}$.
Por exemplo:

(1) Se $\left|G/_{H}\right| = p$, *p primo, então* $G/_{H}$ *é isomorfo a* $\mathbb{Z}_p$.

(2) Se $\left|G/_{H}\right| = 4$, *então* $G/_{H}$ *é isomorfo a* $\mathbb{Z}_4$ *ou* $\mathbb{Z}_2 \times \mathbb{Z}_2$. *A primeiro tem elemento de ordem 4 enquanto a segunda não tem.*

(3) Se $\left|G/_{H}\right| = 2p$, *p primo, então* $G/_{H}$ *é isomorfo a* $\mathbb{Z}_{2p}$ *ou* D_p.

(4) Se $G/_{H}$ *é abeliano e* $\left|G/_{H}\right| = 8$, *então* $G/_{H}$ *é isomorfo a* $\mathbb{Z}_8$, $Z_4 \times \mathbb{Z}_2$ *ou* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Exemplo 1.5.18. *Seja* $G = \mathbb{U}_{30} = \{n \in \mathbb{Z},\ 1 \leq n < 30,\ mdc(n, 30) = 1\}$ *e* $H = \{1, 11\}$. *Quais dos conjuntos* $\mathbb{Z}_4$, *ou* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *é isomorfo a* $G/_{H}$?

Solução. *A ordem de* $\mathbb{U}_{30}$ *é* $\varphi(30) = \varphi(2)\cdot\varphi(3)\cdot\varphi(5) = 8$. *Portanto* G/H *é abeliano de ordem* $8/2 = 4$. *Para determinar quais dos conjuntos* $\mathbb{Z}_4$ *ou* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *é isomorfo a* G/H *usamos a propriedade que* $\mathbb{Z}_4$ *possui um elemento de ordem 4, mas* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *não tem elemento de ordem 4.*

Portanto vamos calcular as ordens dos elementos de $G/H = \{H,\ 7H,\ 13H,\ 19H\}$. *A ordem de um elemento* $aH \in G/H$ *é o menor inteiro positivo n tal que* $a^n \in H$.

- $ord(7H) = 4$ *pois*
  - $7^2 = 49 \equiv_{30} 19$
  - $7^4 \equiv_{30} 19^2 = 361 \equiv_{30} 1 \in H$
- $ord(13H) = 4$ *pois*
  - $13^2 = 169 \equiv_{30} 19$
  - $13^4 \equiv_{30} 19^2 = 361 \equiv_{30} 1 \in H$
- $ord(19H) = 2$ *pois*
  - $19^2 = 361 \equiv_{30} 1 \in H$

Portanto G/H possui um elemento de ordem 4. Logo G/H é isomorfo a $\mathbb{Z}_4$.

Observação: *As ordens dos elementos de* $\mathbb{Z}_4$ *são* $ord(1) = 4$, $ord(2) = 2$ *e* $ord(3) = 4$. *E podemos definir o isomorfismo* $G/H \mapsto \mathbb{Z}_4$ *por*

$$H \mapsto 0,\ \ 7H \mapsto 1,\ \ 13H \mapsto 3,\ \ 19H \mapsto 2.$$

Exemplo 1.5.19. *Seja* $G = \mathbb{U}_{32} = \{n \in \mathbb{Z},\ 1 \le n < 32,\ mdc(n, 32) = 1\}$ *e* $H = \{1, 31\}$. *Quais dos conjuntos* $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, *ou* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ *é isomorfo a* G/H?

Solução. *A ordem de* $\mathbb{U}_{32}$ *é* $\varphi(32) = \varphi(2^5) = 2^4 = 16$. *Portanto G/H é abeliano de ordem* $16/2 = 8$. *Para determinar quais dos conjuntos* $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ *ou* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ *é isomorfo a* G/H *usamos a propriedade que* $\mathbb{Z}_8$ *possui um elemento de ordem 8,* $\mathbb{Z}_4 \times \mathbb{Z}_2$ *possui um elemento de ordem 4 mas nenhum elemento de ordem 8 e* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ *possui elementos somente de ordens menores ou iguais a 2.*

Para determinar quais dos conjuntos $\mathbb{Z}_4$ *ou* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *é isomorfo a* G/H *usamos a propriedade que* $\mathbb{Z}_4$ *possui um elemento de ordem 4, mas* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *não tem elemento de ordem 4.*

Portanto vamos calcular as ordens dos elementos de $G/H = \{H,\ 3H,\ 5H,\ 7H,\ 9H,\ 11H,\ 13H,\ 15H\}$. *A ordem de um elemento* $aH \in G/H$ *é o menor inteiro positivo n tal que* $a^n \in H$.

- $ord(3H) = 8$ *pois*
  - $3^4 = 81 \equiv_{32} 17$
  - $3^8 \equiv_{32} 17^2 = 289 \equiv_{32} 1 \in H$
- $ord(5H) = 8$ *pois*
  - $5^4 = 625 \equiv_{32} 17$
  - $5^8 \equiv_{32} 17^2 = 289 \equiv_{32} 1 \in H$
- $ord(7H) = 4$ *pois*
  - $7^2 = 49 \equiv_{32} 17$
  - $7^4 \equiv_{32} 17^2 = 289 \equiv_{32} 1 \in H$
- $ord(9H) = 4$ *pois*
  - $9^2 = 81 \equiv_{32} 17$
  - $9^4 \equiv_{32} 17^2 = 289 \equiv_{32} 1 \in H$
- $ord(11H) = 8$ *pois*
  - $11^2 = 121 \equiv_{32} 25$
  - $11^4 \equiv_{32} 25^2 = 625 \equiv_{32} 17$
  - $11^8 \equiv_{32} 17^2 = 289 \equiv_{32} 1 \in H$
- $ord(13H) = 8$ *pois*
  - $13^2 = 169 \equiv_{32} 9$
  - $13^4 \equiv_{32} 9^2 = 81 \equiv_{32} 17$
  - $13^8 \equiv_{32} 17^2 = 289 \equiv_{32} 1 \in H$
- $ord(15H) = 2$ *pois*
  - $15^2 = 225 \equiv_{32} \in H$

Portanto G/H *possui um elemento de ordem 8. Logo* G/H *é isomorfo a* $\mathbb{Z}_8$.

Observação: *As ordens dos elementos de* $\mathbb{Z}_8$ *são*

$$ord(1) = 8, \quad ord(2) = 4, \quad ord(3) = 8, \quad ord(4) = 2, \quad ord(5) = 8, \quad ord(6) = 4 \ \ e \ \ ord(7) = 8.$$

E podemos definir o isomorfismo $G/H \mapsto \mathbb{Z}_8$ *por*

$$H \mapsto 0,\ \ 3H \mapsto 1,\ \ 5H \mapsto 3,\ \ 7H \mapsto 2,\ \ 9H \mapsto 6,\ \ 11H \mapsto 7,\ \ 13H \mapsto 5,\ \ 15H \mapsto 4.$$

Exemplo 1.5.20. *Classifique o grupo quociente*

$$(\mathbb{Z}_4 \times \mathbb{Z}_6) \Big/ (< (2,3) >)$$

Solução. *A ordem de* $< (2,3) >$ *em* $\mathbb{Z}_4 \times \mathbb{Z}_6$ *é 2. Portanto* $(\mathbb{Z}_4 \times \mathbb{Z}_6) \Big/ (< (2,3) >)$ *é abeliano de ordem* $24/2 = 12$.

Existe 2 grupos abeliano de ordem 12 (a menos de isomorfismo) que são $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ *e* $\mathbb{Z}_4 \times \mathbb{Z}_3$.

Para determinar quais dos conjuntos $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ *ou* $\mathbb{Z}_4 \times \mathbb{Z}_3$ *é isomorfo a* $(\mathbb{Z}_4 \times \mathbb{Z}_6) \Big/ (< (2,3) >)$, *usamos a propriedade que* $\mathbb{Z}_4 \times \mathbb{Z}_3$ *possui um elemento de ordem 4, mas* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ *não tem elemento de ordem 4.*

Considere o elemento $(1,0) + < (2,3) >$ *em* $(\mathbb{Z}_4 \times \mathbb{Z}_6) \Big/ (< (2,3) >)$. *A ordem de* $(1,0) + < (2,3) >$ *é o menor inteiro positivo n tal que*

$$n(1,0) \in < (2,3) > = \{(0,0),\ (2,3)\}.$$

O menor inteiro positivo que satisfazer isto é 4. Portanto, a ordem de $(1,0) + < (2,3) >$ *é 4 e*

$$(\mathbb{Z}_4 \times \mathbb{Z}_6) \Big/ (< (2,3) >) \cong \mathbb{Z}_4 \times \mathbb{Z}_3.$$

Método mais geral II

Podemos classificar G/H *pelo* 1^o *Teorema de Isomorfismo (Teorema 1.5.12). Construímos um homomorfismo de grupos* $\phi : G \to G'$ *tal que o núcleo* ϕ *é H. Determine a imagem de* ϕ *e aplicar o* 1^o *Teorema de Isomorfismo (Teorema 1.5.12).*

Exemplo 1.5.21. *Classifique o grupo quociente* $(\mathbb{Z} \times \mathbb{Z}) \Big/ (< (1,1) >)$

Solução. *Seja*

$$\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \quad \textit{definida por} \quad \phi(a,b) = a - b.$$

Verificamos que

- ϕ *é um homomorfismo*

$$\begin{aligned}\phi\Big((a_1,b_1)+(a_2,b_2)\Big) &= \phi(a_1+a_2,\ b_1+b_2)\\ &= (a_1+a_2)-(b_1+b_2)\\ &= (a_1-b_1)+(a_2-b_2)\\ &= \phi(a_1,b_1)+\phi(a_2,b_2)\end{aligned}$$

- $Nuc(\phi) =< (1,1) >$

$$\begin{aligned}Nuc(\phi) &= \{(a,b)\in\mathbb{Z}\times\mathbb{Z} : a-b=0\}\\ &= \{(a,a) : a\in\mathbb{Z}\}\\ &= < (1,1) >\end{aligned}$$

- $Im(\phi) = \mathbb{Z}$

  Para todo $n\in\mathbb{Z},\quad n=\phi(n,0)\in Im(\phi)$

Então 1^o *Teorema de Isomorfismo (Teorema 1.5.12)*

$$(\mathbb{Z}\times\mathbb{Z})\Big/(< (1,1) >)\cong\mathbb{Z}.$$

Exemplo 1.5.22. *Classifique o grupo quociente* $(\mathbb{Z}\times\mathbb{Z})\Big/(< (2,2) >)$.

Solução. *O conjunto*

$$< (2,2) >= \{(2,2),\ (4,4),\ (6,6),\ (8,8),\cdots\}$$

tem a propriedade que

$$(a,b)\in< (2,2) > \iff\ a-b=0\ \ e\ \ a\equiv 0\ mod\ 2$$

Portanto definimos

$$\phi:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}_2\ \ por\ \ \phi(a,b)=(a-b,\ a\ mod\ 2).$$

ϕ *é um homomorfismo de grupos com núcleo* $< (2,2) >$ *e* $Im(\phi)=\mathbb{Z}\times\mathbb{Z}_2$. *Então* 1^o *Teorema de Isomorfismo (Teorema 1.5.12)*

$$(\mathbb{Z}\times\mathbb{Z})\Big/(< (2,2) >)\cong\mathbb{Z}\times\mathbb{Z}_2.$$

1.5.8 Exercícios Resolvidos

Exercício 1.5.1. *Sejam $H \trianglelefteq G$ e $K \trianglelefteq G$ tais que $H \cap K = \{e\}$, onde e é o elemento neutro de G. Prove que $hk = kh$, $\forall h \in H$, $\forall k \in K$.*

Solução. *Considere $g = hkh^{-1}k^{-1}$, $h \in H$ e $k \in K$.*

- $g = \underbrace{hkh^{-1}}_{\in K} \cdot \underbrace{k^{-1}}_{\in K}$. *Portanto $g \in K$.*
- $g = \underbrace{h}_{\in H} \cdot \underbrace{kh^{-1}k^{-1}}_{\in H}$. *Portanto $g \in H$.*

Logo $g \in H \cap K$. Mas $H \cap K = \{e\}$. Logo

$$g = e \Longrightarrow hkh^{-1}k^{-1} = e \Longrightarrow hk = kh, \quad \forall h \in H, \ \forall k \in K.$$

Exercício 1.5.2. *Se $H \trianglelefteq G$ e $K \trianglelefteq G$, prove que $H \cap K \trianglelefteq G$.*

Solução. *Sabemos já que $H \cap K$ é um subgrupo de G. Logo vamos provar que $H \cap K$ é normal em G. Seja $x \in H \cap K$. Então $x \in H$ e $x \in K$.*

- *Como H é normal em G temos que $gxg^{-1} \in H$ para todo $g \in G$*
- *Na mesma forma como K é normal em G temos que $gxg^{-1} \in K$ para todo $g \in G$*

Logo $gxg^{-1} \in H \cap K$ para todo $g \in G$. Portanto $H \cap K$ é normal em G.

Exercício 1.5.3. *Seja G um grupo, $H \lhd G$ e $K < G$. Mostre que $HK < G$.*

Solução.

$$HK = \{hk : \ h \in H, \ k \in K\}$$

Vamos provar que HK é um subgrupo de G.

- *$e = e \cdot e \in HK$. Portanto HK não é vazio e contém o elemento neutro.*

- *Seja* $a,\ b \in HK$ *então* $a = hk\ \ e\ \ b = h_1k_1\ \ para\ alguns\ h,\ h_1 \in H\ \ e\ \ k,\ k_1 \in K.$
  Portanto

$$\begin{aligned} ab &= hkh_1k_1 \\ &= hkh_1k^{-1}kk_1 && pois\ \ k^{-1}k = e \\ &= h \cdot \underbrace{kh_1k^{-1}}_{\in H} \cdot \underbrace{kk_1}_{\in K} && pois\ \ H \lhd G\ \ e\ \ K < G \\ &= hh_2k_2 && onde\ \ h_2 = kh_1k^{-1}\ \ e\ \ k_2 = kk_1 \\ &= \underbrace{hh_2}_{\in H} \cdot \underbrace{k_2}_{\in K} \end{aligned}$$

  Logo $ab \in HK$. *Portanto* HK *é fechado em relação a operação em* G

- *Seja* $a \in HK,\quad a = hk$ *para algum* $h \in H$ *e* $k \in K$. *Portanto*

$$\begin{aligned} a^{-1} &= (hk)^{-1} \\ &= k^{-1}h^{-1} \\ &= k^{-1}h^{-1}kk^{-1} && pois\ \ kk^{-1} = e \\ &= k_1h^{-1}k_1^{-1}k^{-1} && onde\ \ k^{-1} = k_1 \\ &= \underbrace{k_1h^{-1}k_1^{-1}}_{\in H} \cdot \underbrace{k^{-1}}_{\in K} && pois\ \ H \lhd G \end{aligned}$$

  Logo $a^{-1} \in HK$.

Portanto HK *é um subgrupo de* G.

Exercício 1.5.4. *Dar exemplo de dois subgrupos* H *e* K *do* S_3 *tais que* HK *não é um subgrupo do* S_3.

Solução. *Em* $S_3 = \{id,\ (1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2),\ (1\ 3),\ (2\ 3)\}$, *considere os subgrupos*

$$H = \{id,\ (1\ 2)\} \quad e \quad K = \{id,\ (2\ 3)\}$$

Então

$$HK = \{id,\ (2\ 3),\ (1\ 2),\ (1\ 2\ 3)\} \quad e \quad KH = \{id,\ (1\ 2),\ (2\ 3),\ (1\ 3\ 2)\}$$

Observe que nem HK e KH são subgrupos de S_3 pois cada um tem ordem 4 que não divide $|S_3| = 6$.

Exercício 1.5.5. *Seja G um grupo, $H \lhd G$ e $K \lhd G$. Mostre que $HK \lhd G$.*

Solução. *Seja $g \in G$ e $x = HK$. Então $x = hk$ para algum $h \in H$ e $k \in K$. Portanto*

$$\begin{aligned} gxg^{-1} &= g(hk)g^{-1} \\ &= gh(g^{-1}g)kg^{-1} \quad \text{pois } g^{-1}g = e \\ &= \underbrace{(ghg^{-1})}_{\in H}\underbrace{(gkg^{-1})}_{\in K} \quad \text{pois } H \text{ e } K \text{ são normais em } G. \end{aligned}$$

Logo $gxg^{-1} \in HK$. Portanto HK é normal em G.

1.5.9 Atividade

1. *Seja G um grupo. Prove que o centro de G, $Z(G)$, é um subgrupo normal de G.*
2. *Suponha que H é um subgrupo de G. Defina o normalizador de H em G por:*

$$N(H) = \{g \in G : gHg^{-1} = H\}.$$

mostre

   (a) $N(H)$ é um subgrupo de G e H é um subgrupo normal de $N(H)$.

   (b) Se H é normal em um subgrupo K de G, então K é um subconjunto de $N(H)$.

   (c) H é normal em G se e somente se $N(H) = G$.

3. *Se H é um subgrupo do grupo G e $K \trianglelefteq G$, prove que $H \cap K \trianglelefteq H$.*
4. *Sejam G um grupo e H um subgrupo de G. Prove que se o índice, $(G : H) = 2$ então $H \trianglelefteq G$.*
5. *Determine todos os subgrupos normais de S_4.*
6. *Prove que se um grupo G de ordem 28 possui um subgrupo normal de ordem 4, então G é abeliano.*
7. *Determine a ordem de $\mathbb{Z}_2 \times \mathbb{Z}_4 / < (1,1) >$*
8. *Determine a ordem de $(3,1) + < (0,2) >$ em $\mathbb{Z}_4 \times \mathbb{Z}_8 / < (0,2) >$*
9. *Determine o grupo quociente $\mathbb{Z}_6/H$, onde $H = \{\overline{0}, \overline{3}\}$. Construa sua tabela.*

10. *Determine os elementos e a tabela da operação + do grupo quociente* $\mathbb{Z}_{24}/ < \overline{4} >$

11. *Sejam G um grupo e H um subgrupo de G. Suponha que H possui a seguinte propriedade: o produto de quaisquer duas classes laterais à direita de H é também uma classe lateral à direita de H. Prove que* $Hg = gH, \ \forall g \in H$.
Sugestão: Se $g \in G$ *e* g^{-1} *e o seu inverso, considere o produto das classes* Hg *e* Hg^{-1}.

12. *Suponha que G é um grupo e* $H < G$. *Mostre que se o índice de H em G,* $(G : H) = 2$ *então* $H \lhd G$.

13. *Sejam* $i^2 = -1$ *e* $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$
Se em $Q = \{1, -1, I, -I, J, -J, K, -K\}$ *definimos como o operação o produto usual de matrizes, obtemos um grupo chamado* ***Quatérnios***

    (a) Construa a tabela da operação dos Quatérnios.

    (b) Prove que Q é não-abeliano e que se H é um subgrupo de Q, então $Hg = gH, \ \forall g \in Q$.

    (c) Seja $H = \{1, -1\}$. *Construa a tabela do grupo quociente* Q/H. $H \lhd G$?

    (d) Seja $K = \{1, -1, I, -I\}$. *Construa a tabela do grupo quociente* Q/K. $K \lhd G$?

14. *Seja G um grupo e seja G′ o subgrupo de G gerado pelo seguinte conjunto:*

$$\{aba^{-1}b^{-1} : \ a, b \in G\}$$

(chamado de subgrupo dos comutadores (ou derivado) de G)

    (a) Mostre que G′ é normal em G.

    (b) Mostre que G/G′ é abeliano.

    (c) Seja N um subgrupo normal de G. Mostre que se G/N for abeliano, então $G' \subseteq N$.

    (d) Mostre que se H é um subgrupo de G tal que $G' \subseteq H$, *então H é normal em G.*

15. *Prove que se G é um grupo abeliano, então G/H é abeliano.*

16. *Prove que se G é um grupo cíclico, então G/H é cíclico.*

17. *Prove que se G/Z(G) é cíclico então G é abeliano*

18. *Considere o grupo quociente* $\mathbb{Q}/\mathbb{Z}$. *Prove que, dado* $g \in \mathbb{Q}$, *existe um inteiro positivo n tal que* $(g + \mathbb{Z})^n = \mathbb{Z}$.

19. *Considere o produto direto $G_1 \times G_2$ dos grupos G_1 e G_2. Sejam $H_1 \lhd G_1$ e $H_2 \lhd G_2$. Mostre que $H_1 \times H_2 \lhd G_1 \times G_2$.*

20. *Seja G um grupo e $H < G$ tais que $|G| = 50$ e $|H| = 25$. Decida se $H \lhd G$. Se fizer sentido falar no grupo quociente G/H, descreva seus elementos.*

21. *Seja $f : G \to H$ um homomorfismo sobrejetora e N um subgrupo normal de G. Prove que $f(N)$ é normal em H.*

22. *Seja $G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},\ a, b \in \mathbb{R} \text{ e } a > 0 \right\}$ um subgrupo de $GL(2, \mathbb{R})$. Prove que $f : G \to \mathbb{R}^*,\ f \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = a$ é um homomorfismo. Prove que $N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},\ b \in \mathbb{R} \right\}$ é um subgrupo normal de G.*

23. *Sejam G, K grupos e suponha que $\varphi : G \to K$ é um homomorfismo com núcleo H e a um elemento fixo de G. Seja $X = \{x \in G \mid \varphi(x) = \varphi(a)\}$. Mostre que $X = Ha$*

24. *Mostre que $\mathbb{Z}_6/H \simeq \mathbb{Z}_3$, onde H é o subgrupo $\{0, 3\}$.*

25. *Sejam $G = \mathbb{Z}_4 \times \mathbb{Z}_4$ e $H =< (3, 2) >$, o grupo cíclico gerado por $(3, 2)$. Mostre que $G/H \simeq \mathbb{Z}_4$.*

26. *Use o primeiro teorema de isomorfismo para mostrar que $\mathbb{Z}_{30}/ < 5 > \simeq \mathbb{Z}_5$*

27. *(a) Mostre que $f : 4\mathbb{Z} \to \mathbb{Z}_6$, dado por $f(x) = 4x$ é um homomorfismo*

    (b) Mostre que $Im(f) = \{\overline{0}, \overline{2}, \overline{4}\}$ e $Nuc(f) = 12\mathbb{Z}$

    (c) Conclua que $\{\overline{0}, \overline{2}, \overline{4}\} \lhd \mathbb{Z}_6$, $12\mathbb{Z} \lhd 4\mathbb{Z}$ e $4\mathbb{Z}/12\mathbb{Z} \cong \{\overline{0}, \overline{2}, \overline{4}\}$.

    (d) Mostre que $Im(f) \cong \mathbb{Z}_3$.

28. *Sejam $G = D_4$ e $H = \{e, a, a^2, a^3\}$. Descreva o homomorfismo projeção canônica $f : G \to G/H$, e explicite $Nuc(f)$ e $Im(f)$.*

29. *Identifique, via isomorfismo, os grupos abaixo:*

    (a) $(\mathbb{Z}/15\mathbb{Z}) / (3\mathbb{Z}/15\mathbb{Z})$ *(b)* $3\mathbb{Z}/15\mathbb{Z}$ *(c)* $(3\mathbb{Z} + 15\mathbb{Z})/5\mathbb{Z}$

30. *Prove que $(\mathbb{Z}_4 \times \mathbb{Z}_6)/ < (2, 3) > \cong \mathbb{Z}_{12}$.*

31. *Prove que $(\mathbb{Z} \times D_n)/(m\mathbb{Z} \times D_n) \cong \mathbb{Z}_m$.*

32. *Classifique os seguintes grupos quocientes:*

(a) $(\mathbb{Z} \times \mathbb{Z}) \Big/ (< (1,2) >)$;

(b) $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_4) \Big/ (< (3,0,0) >)$.

UNIDADE 2

ANÉIS

Aula 2.1

Anéis

Nesta aula vamos definir o conceito de anéil e identificar as propriedades que caracterizam um anel. Apresentar as estruturas algébricas de domínio de integridade e corpos.

2.1.1 Definição de anel, exemplos e propriedades básicas

Definição 2.1.1. *Um conjunto não vazio R, juntamente com duas operações binárias $+, \cdot$ é dito ser um* **anel** *se:*

(a) $(R, +)$ *é um grupo abeliano, ou seja*

(A1): $a + (b + c) = (a + b) + c$, *para todo* $a, b, c \in R$;

(A2): $a + b = b + a$; *para todo* $a, b \in R$.

(A3): $\exists\, 0 \in R; a + 0 = 0 + a = a$, *para todo* $a \in R$;

(A4): Para todo $a \in R$, $\exists - a \in R$; $a + (-a) = 0 = (-a) + a$;

(b) $\cdot$ *é associativa, ou seja,*

(A5): $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, *para todo* $a, b, c \in R$.

(c) Valem as leis distributivas, ou seja,

(A6): $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ *para todo* $a, b, c \in R$;

(A7): $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ *para todo* $a, b, c \in R$.

Notação: $(R, +, \cdot)$ *denotará um anel* R *com as operações* $+$ *e* $\cdot$.

Observação. *Observe que a multiplicação não necessita ser comutativa, isto é,* $ab \neq ba$ *para alguns* $a, b \in R$. *Quando temos* $a \cdot b = b \cdot a$ *para todo* $a, b \in R$, *dizemos que* R *é um* **anel comutativo**. *Caso contrario* R *é* ***não comutativa***.

Definição 2.1.2. *Se existe um elemento* $1 \in R$ *tal que* $a \cdot 1 = 1 \cdot a = a$ *para todo* $a \in R$, *então chamamos* 1 *a* **unidade ou identidade** *do anel* R.
Quando um anel R *possui o elemento identidade dizemos que* R *é um anel com unidade, ou simplesmente um anel com* 1.

Lema 2.1.1. *Se* R *é um anel com* 1, *então* 1 *é única.*

Demonstração. Mesmo demonstração feito para grupos, isto é

$$1 = 1 \cdot 1' = 1'.$$

■

Notação (Subtração) *Em qualquer anel* R, *para todo* $a \in R$ *escrevemos o inverso aditivo por* $(-a)$. *Pela definição temos que* $a + (-a) = (-a) + a = 0$. *Para qualquer* $a, b \in R$ *denotamos* $a + (-b)$ *por* $a - b$.

Exemplo 2.1.1. $(\mathbb{Z}, +, \cdot)$ *é um* **anel comutativo com unidade,** *onde* $+$ *e* $\cdot$ *são a adição e a multiplicação usuais dos inteiros.*

Exemplo 2.1.2. *O conjunto* $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$ *com as operações* $+_n$ *(adição modulo* n*)* $e \cdot_n$ *(multiplicação modulo* n*) é um* **anel comutativo com unidade.** *Este anel é chamado o anel dos inteiros módulo* n.

Exemplo 2.1.3. *(Anéis de polinômios). Sejam* $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *ou* $\mathbb{C}$ *e seja* $R[x]$ *denota todos os polinômios na variável* x *com coeficientes em* R, *ou seja,*

$$R[x] = \{f(x) = a_0 + a_1 x + \cdots + a_n x^n : a_j \in R\}.$$

$R[x]$ muindo com a multiplicação e adição usuais, isto é, se

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \ \text{ e } \ g(x) = b_0 + b_1x + \cdots + b_mx^m \in R[x]$$

então

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_k + b_k)x^k, \quad \text{onde } k = \max\{n, m\}$$

e

$$f(x) \cdot g(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}, \ \text{ onde } c_j = a_jb_0 + a_{j-1}b_1 + \cdots + a_0b_j$$

é um **anel comutativo e sua unidade** *é* $f(x) = 1$.

Exemplo 2.1.4. *(Matrizes). O conjunto $M_{2\times2}(F)$ das matrizes 2×2 com entradas em F, onde $F = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, ou $\mathbb{C}$ com a soma e produto usuais de matrizes, é* **um anel não comutativo com unidade** $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Exemplo 2.1.5. *O conjunto dos inteiros pares $2\mathbb{Z}$, com a soma e produto usuais é um anel comutativo sem unidade.*

Exemplo 2.1.6. *(Anéis de funções). Se X é um conjunto não vazio, então o conjunto*

$$R = \{f : X \to \mathbb{R}; \ f \text{ é continua}\}$$

muindo com a soma e multiplicação usuais de funções, isto é

$$(f + g)(x) = f(x) + g(x) \ \text{ e } \ (f \cdot g) = f(x)g(x) \ \text{ para todo } \ x \in X$$

então R é **um anel comutativo com unidade** $f(x) \equiv 1$.

Exemplo 2.1.7. *(**Anel dos Inteiros de Gauss**). O conjunto $\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1}, \ a, b \in \mathbb{Z}\}$ com operações*

$$(a_1 + b_1\sqrt{-1}) + (a_2 + b_2\sqrt{-1}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{-1}$$

$$(a_1 + b_1\sqrt{-1}) \cdot (a_2 + b_2\sqrt{-1}) = (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{-1}$$

é um anel comutativo com unidade 1 chamado de anel dos inteiros de Gauss.

Em geral se $d \in \mathbb{Z}$ *não é um quadrado então*

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

é um anel comutativo com unidade, com operações

$$(m + n\sqrt{d}) - (a + b\sqrt{d}) = (m - a) + (n - b)\sqrt{d}$$

$$(m + n\sqrt{d})(a + b\sqrt{d}) = (ma + nbd) + (mb + na)\sqrt{d}$$

Além disto, se $m + n\sqrt{d} = m' + n'\sqrt{d}$ *então* $m = m'$ *e* $n = n'$.

Lema 2.1.2. (Alguns propriedades básicas de anéis). *Seja R um anel. Então*

(a) $a0 = 0 = 0a$ *para todo* $a \in R$.

(b) $(-a)b = -(ab) = a(-b)$ *para todo* $a, b \in R$.

(c) $(-a)(-b) = ab$ *para todo* $a, b \in R$. *Em particular, se R é um anel com* 1, *então*

$$(-1)(-1) = 1 \quad e$$

$$(-1)a = -a \quad \text{para todo} \quad a \in R.$$

(d) Se $a, b, c \in R$, *então* $a(b - c) = ab - ac \quad e \quad (b - c)a = ba - ca$.

Demonstração. Para todo $a, b \in R$;

(a) $a0 + 0 = a0 = a(0 + 0) = a0 + a0$, e portanto pela lei do cancelamento do grupo aditivo $(R, +)$, concluímos que $0 = a0$. Analogamente podemos provar que $0 = 0a$.

(b) $(-a)b + ab = (-a + a)b = 0b = 0$, portanto $(-a)b = -(ab)$. Analogamente $a(-b) = -ab$.

(c) $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$, sendo que na última igualdade usamos o fato se tomar a inversa de um elemento duas vezes obtemos o elemento.

(d) $a(b - c) := a(b + (-c)) = ab + a(-c) = ab + (-ac) = ab - ac$.

■

2.1.2 Subanéis e Ideais

Vamos define o conceito de um subanel da forma semelhante ao conceito de um subgrupo.

Definição 2.1.3. (Subanel). *Um subconjunto não vazio S de um anel R é dito ser um* **subanel** *de R se, com as operações induzidas pelas operações de R (restrições), S é um anel.*

Lema 2.1.3. (Teste para Subanel).

Um subconjunto $S \neq \emptyset$ de um anel R é um subanel de R se, e somente se valem as seguinte afirmações:

(i) Para todo $a, b \in S \Rightarrow a - b = a + (-b) \in S$

(ii) Para todo $a, b \in S \Rightarrow ab \in S$.

Demonstração. Exercício

■

Exemplo 2.1.8. *Mostre que o conjunto $D_7 = \left\{ \frac{a}{7^k};\ a \text{ é inteiro e } k \in \{1, 2, 3 \cdots\} \right\}$ é um subanel de $(\mathbb{Q}, +, \cdot)$.*

Solução. *Tomando $a = 0 \Rightarrow 0 \in D_7$. Portanto $D_7 \neq \emptyset$.*

- *Sejam $x = \frac{a_1}{7^{k_1}}$ e $y = \frac{a_2}{7^{k_2}} \in D_7$*
  Suponhamos, sem perda de generalidade, que $k_1 \leq k_2$. Temos

  (i) $x - y = \frac{a_1}{7^{k_1}} - \frac{a_2}{7^{k_2}} = \frac{a_1 7^{k_2 - k_1} - a_2}{7^{k_2}} \in D_7$

  (ii) $x \cdot y = \frac{a_1}{7^{k_1}} \cdot \frac{a_2}{7^{k_2}} = \frac{a_1 a_2}{7^{k_1 + k_2}} \in D_7$

Resulta de (i) e (ii) que D_7 é subanel de $\mathbb{Q}$.

Definição 2.1.4. (Ideais). *Um subanel I de um anel R é*

- *um* **ideal** *de R, se $\forall\ a \in I$ e $r \in R \Rightarrow a \cdot r \in I$ e $r \cdot a \in I$.*
- *um* **ideal à direta** *de R, se $\forall\ a \in I$ e $r \in R \Rightarrow a \cdot r \in I$.*
- *um* **ideal à esquerda** *de R, se $\forall\ a \in I$ e $r \in R \Rightarrow r \cdot a \in I$.*

Observação. *Note que num anel comutativa, os ideais à direta e à esquerda são iguais.*

O próximo teorema caracteriza um ideal.

Teorema 2.1.4. *Sejam R um anel e $I \neq \emptyset$ um subconjunto de R. I é um ideal de R se, e somente se para todo $a, b \in I$ e $r \in R$, temos:*

(i) $a - b \in I$

(ii) $a \cdot r \in I$ e $r \cdot a \in I$.

Demonstração. Segue diretamente da definição do ideal e do Lema 2.1.3 (Teste para Subanel) ■

Exemplo 2.1.9.

(a) Dado um anel R, então R e $\{0\}$ são sempre ideais de R, chamados ideais triviais.

(b) Para qualquer inteiro positivo n, $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \cdots\}$ é um ideal de $\mathbb{Z}$.

Definição 2.1.5. *Um anel com 1 é chamada de* **simples** *se R e $\{0\}$ são os únicos ideais de R.*

Observação. *Um ideal (subanel) $I \subset R$ tal que $I \neq R$ é chamado de ideal (subanel) próprio.*

Proposição 2.1.5. *Suponha que R é um anel com 1 e I é um ideal de R. Se $1 \in I$, então $I = R$.*

Demonstração. Temos que $I \subset R$. Falta provar que $R \subset I$. Seja r qualquer elemento de R, então $r = r \cdot 1 = 1 \cdot r \in I$. Portanto $R \subset I$, logo $R = I$. ■

Exemplo 2.1.10. *Seja* $T = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$

(a) Prove que T é um subanel de $M_2(\mathbb{R})$.

(b) Mostre que $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \;\middle|\; b \in \mathbb{R} \right\}$ *é um ideal de T.*

Solução.

(a) Sejam $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \in T$. *Então*

- $T \neq \emptyset$ *pois* $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in T$
- $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ 0 & a+c \end{pmatrix} \in T$
- $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix} \in T$

Então T é um subanel de $M_2(\mathbb{R})$

(b) Seja $\begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} \in I$ *e* $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in T$. *Então*

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

Portanto I é um ideal de T.

Definição 2.1.6. (Ideais gerados por conjuntos). *Seja R um anel comutativo com unidade e seja $X = \{x_1, x_2, \cdots, x_n\}$ um subconjunto de R. Então definimos* **ideal gerado por X de R, por**

$$\langle X \rangle = \langle x_1, x_2, \cdots, x_n \rangle = \{r_1x_1 + r_2x_2 + \cdots r_nx_n \mid r_i \in R\}$$

É fácil verificar que $\langle X \rangle$ é o menor ideal de R que contêm X.

Definição 2.1.7. (Ideais Principais). *Sejam R um anel comutativo com unidade.*

- *Um ideal I de R é dito* **finitamente gerado** *se $I =< X >$, para algum conjunto X com $|X| < \infty$.*
- *Um ideal I de R é dito* **principal** *se $I =< a >$, para algum elemento $a \in R$.*
  Note que $< a >= \{ra \mid r \in R\}$

Teorema 2.1.6. (Ideais de $\mathbb{Z}$ e $\mathbb{Z}_n$). *Seja $R = \mathbb{Z}$ ou $\mathbb{Z}_m$ para algum $m \in \mathbb{Z}_+$. Então*

$$\text{os subgrupos de } (R, +) = \text{ os subaneis de } R = \text{os ideais de } R.$$

Além disto, todo ideal de R é principal.

Demonstração.

- Se $R = \mathbb{Z}$, então $< m >= m\mathbb{Z} \subset \mathbb{Z}$ é o principal ideal gerado por m. Como cada subanéis, $S \subset \mathbb{Z}$ é também um subgrupo e todos os subgrupos de $\mathbb{Z}$ são da forma $m\mathbb{Z}$ para algum $m \in \mathbb{Z}$, (Corolário 2 de Aula 1) seguir que todos os subgrupos de $(\mathbb{Z}, +)$ são de fato os ideais principais.

- Suponha agora que $R = \mathbb{Z}_n$. Então para qualquer $m \in \mathbb{Z}_n$,

$$< m >= \{km : k \in \mathbb{Z}\} = m\mathbb{Z}_n \qquad (*)$$

é o ideal principal em $\mathbb{Z}_n$ gerado por m.

Reciprocamente se $S \subset \mathbb{Z}_n$ é um subanel então em particular S é um subgrupo de $\mathbb{Z}_n$. De Corolário 3 de Aula 1 sabemos que $S =< m >=< \text{mdc}(n, m) >$ para algum $m \in \mathbb{Z}_n$. Portanto todo subgrupo de $(\mathbb{Z}_n, +)$ é um ideal principal como em Eq. $(*)$

■

Exemplo 2.1.11. *Determine os ideais do anel $\mathbb{Z}_{12}$.*

Solução. *Como $\mathbb{Z}_{12}$ é comutativa, não há diferença entre ideais à esquerda e à direta. Os ideais de $\mathbb{Z}_{12}$ são:*

- $I_1 = \{0\}$
- $I_2 =< 1 >=< 5 >=< 7 >=< 11 >= \mathbb{Z}_{12}$
- $I_3 =< 2 >=< 10 >= \{0, 2, 4, 6, 8, 10\}$
- $I_4 =< 3 >=< 9 >= \{0, 3, 6, 9\}$
- $I_5 =< 4 >=< 8 >= \{0, 4, 8\}$
- $I_6 =< 6 >= \{0, 6, \}$

2.1.3 Unidades de um anel

Os elementos não nulos de um anel com unidade não necessitam ter inversos multiplicativos (isto é, y inverso multiplicativo de x se e somente se $xy = yx = 1$). Os elementos de um anel R que possuem inverso multiplicativo são chamados de invertíveis de R ou unidades de R.

Definição 2.1.8. *Seja R um anel com unidade. Uma unidade do anel é um elemento $a \in R$ tal que existe um elemento $b \in R$ com $ab = ba = 1$. Este elemento será denotado por a^{-1}.*
Usaremos a notação $\mathbb{U}(R) = \{x \in R;\ x \text{ é uma unidade de } R\}$ para denotar as unidades de R.

Lema 2.1.7. *Seja R é um anel com 1. Se um elemento $a \in R$ tem inverso multiplicativo b, então b é único, e escrevemos $b = a^{-1}$.*

Demonstração. Mesmo demonstração feito para grupos, isto é se b, b' são inversos multiplicativos de a, então

$$b = b \cdot 1 = b(a \cdot b') = (b \cdot a)b' = 1 \cdot b' = b'$$

■

Proposição 2.1.8. *O conjunto $\mathbb{U}(R)$ muindo com a operação de multiplicação em R é um grupo, chamado de o* **grupo das unidades de** *R.*

Demonstração.

- $\mathbb{U}(R)$ é fechado em relação ao multiplicação em R :
  seja $a, b \in \mathbb{U}(R)$ e a^{-1}, b^{-1} seus inversos multiplicativos respectivamente em R. Então

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} \\ &= a1a^{-1} \\ &= aa^{-1} \\ &= 1\end{aligned}$$

  Analogamente $(b^{-1}a^{-1})(ab) = 1$. e portanto $b^{-1}a^{-1}$ é o inverso multiplicativo de ab e portanto $ab \in \mathbb{U}(R)$.

- $\mathbb{U}(R)$ possui elemento neutro para a multiplicação pois $1 \in \mathbb{U}(R)$.

- Cada elemento de $\mathbb{U}(R)$ possui inverso:
  seja $a \in \mathbb{U}(R)$ e a^{-1} seu inverso em R. Então $aa^{-1} = 1$ e $a^{-1}a = 1$. Portanto $a^{-1} \in \mathbb{U}(R)$.

Portanto $\mathbb{U}(R)$ é um grupo.

■

Exemplo 2.1.12.

(a) Em $\mathbb{Z}$, as unidades são 1 *e* -1. *Logo* $\mathbb{U}(\mathbb{Z}) = \{-1, 1\}$.

(b) Em $M_2(\mathbb{R})$, *as unidades são os elementos de* $GL(2, \mathbb{R})$, *isto é*

$$\mathbb{U}(M_2(\mathbb{R})) = GL(2, \mathbb{R}) = \{A \in M_2(\mathbb{R}) : \det(A) \neq 0\}$$

(c) Em $\mathbb{R}$, *as unidades são os elementos em* $\mathbb{R}^* := \mathbb{R}\backslash\{0\}$, *ou seja* $\mathbb{U}(\mathbb{R}) = \mathbb{R}^*$.

(d) Em $\mathbb{Z}_m$, $m \geq 2$, *temos que* $\mathbb{U}(\mathbb{Z}_m) = \mathbb{U}(m) = \{a \in \mathbb{Z}_m;\ mdc(a, m) = 1\}$

Demonstração. Se $a \in \mathbb{U}(\mathbb{Z}_m)$, então existe $r \in \mathbb{Z}_m$ tal que

$$1 = r \cdot a = ra \bmod m$$

ou seja existe $t \in \mathbb{Z}$ tal que $ra - 1 = tm$. Como $1 = ra - tm$ seguir que $\text{mdc}(a, n) = 1$, ou seja $a \in \mathbb{U}(m)$.

Reciprocamente, se $a \in \mathbb{U}(m) \Leftrightarrow \text{mdc}(a, m) = 1$ que implica que existem $s, t \in \mathbb{Z}$ tal que $sa + tm = 1$. Tomando mod m deste equação e fazendo $b := s \bmod m \in \mathbb{Z}_m$, temos que $b \cdot a = 1$ em $\mathbb{Z}_m$, ou seja $a \in \mathbb{U}(\mathbb{Z}_m)$. ■

(e) Em $\mathbb{Z}[i]$, *temos que* $\mathbb{U}(\mathbb{Z}[i]) = \{1, -1, i, -i\}$. *De fato suponha que* $a + bi \in \mathbb{U}(\mathbb{Z}[i])$ *é uma unidade, então*

$$(a + bi)(c + di) = 1 \ \textit{para alguns}\ c, d \in \mathbb{Z}.$$

Então $(a - bi)(c - di) = 1$. *Portanto*

$$\begin{aligned} (a + bi)(c + di)(a - bi)(c - di) &= 1 \\ \Rightarrow (a^2 + b^2)(c^2 + d^2) &= 1 \end{aligned}$$

Portanto $a^2 + b^2 = 1$, *logo* $a + bi \in \{1, -1, i, -i\}$.

(f) Em $\mathbb{Z}[\sqrt{d}]$, $d < -1$, *então* $\mathbb{U}(\mathbb{Z}[\sqrt{d}]) = \{\pm 1\}$

2.1.4 Divisores de zero e Domínios de Integridade

Definição 2.1.9. (Divisores de zero). *Sejam R um anel. Um elemento $a \in R$, $a \neq 0$ é chamado de* **divisor de zero** *se existe outro elemento $b \in R, b \neq 0$ tal que $ab = 0$.*

Definição 2.1.10. (Domínio de integridade). *Um anel R é chamado* ***domínio de integridade,*** *se*

(a) R é comutativa,

(b) R possui o elemento identidade 1,

(c) R não possui divisores de zero, ou seja, $ab \neq 0$ para todo $a, b \in R$ com $a \neq 0 \neq b$,

(d) $0 \neq 1$.

Observação. *Se* $0 = 1$, *então* $x = x \cdot 1 = x \cdot 0 = 0$. *Portanto se* $0 = 1$ *então* $R = \{0\}$.

Exemplo 2.1.13. *Os anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[\sqrt{d}]$ não tem divisores de zero e portanto são domínios de integridade. Neste sistemas sabemos que*

$$ab = 0 \Rightarrow \text{ ou } a = 0 \text{ ou } b = 0.$$

Exemplo 2.1.14. *O anel $\mathbb{Z}_6$* **não** *um domínio de integridade. Por exemplo,* $2 \cdot 3 = 0$ *com* $\neq 0 \neq 3$, *portanto ambos 2 e 3 são divisores de zero.*

Lema 2.1.9. *O anel $\mathbb{Z}_m$ é um domínio de integridade se e somente se m é primo.*

Demonstração. Suponha que m é primo. Sabemos que $U(\mathbb{Z}_m) = U(m) = \mathbb{Z}_m \backslash \{0\}$. Portanto se $a, b \in \mathbb{Z}_m$ com $a \neq 0$ e $ab = 0$ então $b = a^{-1}ab = a^{-1}0 = 0$. Portanto $\mathbb{Z}_m$ é um domínio de integridade.
Agora suponha que m não é primo, ou seja, $m = a \cdot b$ com $a, b \in \mathbb{Z}_m \backslash \{0\}$, então $ab = 0 \bmod m$, logo a e b são divisores de zero, portanto $\mathbb{Z}_m$ não é domínio de integridade. ■

Proposição 2.1.10. *Se R é um domínio de integridade, então $R[x]$ também é.*

Demonstração. Seja $f, g \in R[x]$ dois polinômios não nulos. Então $f(x) = a_n x^n + \cdots + a_1 x + a_0$ e $g(x) = b_m x^m + \cdots + b_1 x + b_0 \in R[x]$ com $a_n \neq 0 \neq b_n$ e portanto,

$$f(x)g(x) = a_n b_m x^{m+n} + \cdots a_0 b_0 \neq 0 \text{ pois } a_n b_m \neq 0.$$

■

Proposição 2.1.11. ***(Cancelamento).*** *Se R é um domínio de integridade e $ab = ac$, com $a \neq 0$ então $b = c$.*
Reciprocamente se R é um anel comutativa com 1 satisfazendo a a propriedade de cancelamento então R não possui divisores de xeros e portanto R é um domínio de integridade.

Demonstração. Se $ab = ac$, então $a(b-c) = 0$. Portanto com $a \neq 0$ e R é um domínio de integridade, então $b - c = 0$, ou seja $b = c$.
Reciprocamente, suponha que R satisfaz a lei do cancelamento e $ab = 0$. Se $a \neq 0$, então $ab = a \cdot 0$ e pela lei do cancelamento $b = 0$. Mostrando que R não possui divisores de zero. ■

Exemplo 2.1.15. *O anel $M_2(\mathbb{R})$ possui muitos divisores de zero. Por exemplo*

$$\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Portanto, em $M_2(\mathbb{R})$ não podemos concluir que $B = 0$ se $AB = 0$ com $A \neq 0$, ou seja não vale a lei do cancelamento.

2.1.5 Corpos

Definição 2.1.11. (Corpos). *Um anel R é chamado* ***um corpo,*** *se*

(a) R é comutativa,

(b) R possui o elemento identidade 1,

(c) Todo os elementos não nulo de R são unidades, isto é, $\forall a \in R,\ \exists\, b \in R :\ ab = ba = 1$.

Exemplo 2.1.16.

(a) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$ são corpos. $\mathbb{Z}$ não é um corpo pois por exemplo $2 \neq 0$ tem não inverso multiplicativo.

(b) $\mathbb{Z}[\sqrt{d}]$ não é um corpo, pois $\frac{1}{2} \notin \mathbb{Z}[\sqrt{d}]$.

(c) $\mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\}$ é um corpo. De fato, se $x \neq 0, y \neq 0$ temos que

$$\begin{aligned} \frac{1}{x + y\sqrt{d}} &= \frac{x - y\sqrt{d}}{(x - y\sqrt{d})(x + y\sqrt{d})} \\ &= \frac{x - y\sqrt{d}}{x^2 - y^2 d} \end{aligned}$$

Note $x^2 - y^2 d \neq 0$ pois d não é quadrado de um racional.

Proposição 2.1.12. *Seja R um anel comutativo com 1. Então R é simples se e somente se R é um corpo.*

Demonstração. ($\Rightarrow$:) Suponha que R é simples e comutativo e seja $0 \neq a \in R$. Então $Ra = \{ra|\ r \in R\}$ um ideal de R. Como $Ra \neq 0$ (pois $a \in Ra$) e R é simples, $Ra = R$. Portanto $1 \in Ra$, logo existe algum elemento $r \in R$ tal que $ra = 1$, ou seja, a é inversível em R. Portanto todo elemento diferente de zero em R é inversível. Logo R é um corpo.
($\Leftarrow$:) Suponha que R é um corpo. Seja $I \neq 0$ um ideal de R. Se $0 \neq r \in I$, então r é um unidade (pois R é um corpo). Portanto $r = r \cdot 1 \in I,\ \forall r \in R$. Portanto $R = I$. ■

Lema 2.1.13. (Corpos são domínios). *Todo corpo R é um domínio de integridade.*

Demonstração. Basta provar que não existe divisores de zero. Suponha que $ab = 0,\ a \neq 0, b \neq 0$. Então a^{-1} existe, e

$$0 = a^{-1}0 = a^{-1}ab = b$$

Contradição. ■

Lema 2.1.14. *Todo domínio de integridade **finito** R é um corpo.*

Demonstração. Basta provar que todo elemento não nulo é inversível. Seja $R = \{r_1, \cdots, r_n\}$ (todos distintos) um domínio de integridade. Tomar $r \in R,\ r \neq 0$ qualquer. Considere $\{rr_1, rr_2, \cdots, rr_n\}$. Se para algum i e j temos que $rr_i = rr_j$ então $r_i = r_j$ pela lei do cancelamento.
Portanto $\{rr_1, rr_2, \cdots, rr_n\}$ é um conjunto de n elementos distintos de R. Como R tem n elementos,

$$\{rr_1, rr_2, \cdots, rr_n\} = R = \{r_1, r_2, \cdots, r_n\}.$$

Portanto qualquer r_i pode ser escrito como rr_j para algum j. Em particular, $1 = rr_j$ para algum j, portanto $r_j = r^{-1}$. ■

Corolário 8. *O anel $\mathbb{Z}_m$ é um corpo se e somente se m é prime.*

Demonstração.

(⇒) Se m não é primo sabemos do Lema 2.1.9 que $\mathbb{Z}_m$ não é um domínio de integridade, portanto não é um corpo.

(⇐) Se m é primo, então $\mathbb{Z}_m$ é um domínio de integridade finito, portanto é um corpo pela Lema 2.1.14.

■

Observação. *Quando p é primo, denotamos $\mathbb{Z}_p$ por $\mathbb{F}_p$ para indicar que estamos olhando $\mathbb{Z}_p$ como um corpo.*

Proposição 2.1.15. *Seja R um corpo. Então as únicas ideais de R são triviais, ou seja, as únicas ideais são $\{0\}$ e R.*

Demonstração. Suponha que $I \subset R$ é um ideal tal que $I = \{0\}$. Então existe $x \in I, x \neq 0$. Como R é um corpo, $x^{-1} \in R$. Mas I é um ideal, portanto $1 = x^{-1}x \in I$. Portanto pelo Proposição 2.1.5 temos que $I = R$. ■

2.1.6 Caraterística de um anel

Notação. *Sejam que R um anel e $a \in R$. Então para cada $n \in \mathbb{Z}$ definimos*

$$na := \begin{cases} \overbrace{a + a + \cdots + a}^{n \text{ vezes}} & \text{se } n \geq 1 \\ 0 & \text{se } n = 0 \\ \overbrace{-(a + a + \cdots + a)}^{|n| \text{ vezes}} = |n| \cdot (-a) & \text{se } n \leq -1 \end{cases}$$

Se $n \in \mathbb{N}$ definimos

$$a^n := \underbrace{a \cdot a \cdots a}_{n \text{ fatores}}$$

(Aqui $a^0 = 1$) Se a é uma unidade, então a^n é definida por todo $n \in \mathbb{Z}$. Para $n \in \mathbb{Z}^-$, definimos

$$a^n := \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{|n| \text{ fatores}}$$

Lema 2.1.16. *Sejam R um anel e $a, b \in R$. Então para todo $m \in \mathbb{Z}$ temos*

$$(ma)b = m(ab) = a(mb)$$

Demonstração. Exercício ■

Corolário 9. *Sejam R um anel e $a, b \in R$. Então para todo $m, n \in \mathbb{Z}$ temos*

$$(ma)(nb) = (mn)(ab)$$

Demonstração. Usando o lema anterior temos

$$(ma)(nb) = m(a(nb)) = m(n(ab)) = (mn)(ab).$$

■

Definição 2.1.12. (Característica de um anel). *Seja R um anel com $1 \in R$. Definimos a* **característica** *de R, denotado por* **car(**R**)**, *como sendo a ordem do elemento 1 no grupo $(R, +)$. Portanto* **car(**R**)** *é o menor inteiro em $\mathbb{Z}_+$ tal que $n \cdot 1 = 0$. Caso não existe tal $n \in \mathbb{Z}_+$ dizemos que* **car(**R**)** *é igual 0.*

Lema 2.1.17. *Seja R um anel com 1 e $car(R) = n \geq 1$. Então $nx = 0$ para todo $x \in R$.*

Demonstração. Para qualquer $x \in R$, $nx = n(1x) = (n1)x = 0x = 0$. ■

Lema 2.1.18. *Seja R um domínio de integridade. Então $car(R) = 0$ ou $car(R)$ é primo.*

Demonstração. Suponha que $n = \text{car}(R)$ não é primo, ou seja $n = pq$ com $1 < p < n$ e $1 < q < n$. Então

$$(p1)(q1) = (pq)(1 \cdot 1) = (pq)1 = n1 = 0$$

Como $p1 \neq 0$ e $q1 \neq 0$ concluímos que ambos $p1$ e $q1$ são divisores de zero contradizendo o fato que R é um domínio de integridade. ■

Corolário 10. *Todo corpo tem característica zero ou primo. Em particular, todo corpo finito tem característica primo.*

Exemplo 2.1.17. *Os anéis* $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}, \mathbb{Q}[\sqrt{d}]$, $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ *tem caraterística 0.*
Para cada $m \in \mathbb{Z}_+$, $\mathbb{Z}_m$ *e* $\mathbb{Z}[m]$ *são anéis com caraterística* m.

2.1.7 Exercícios Resolvidos

Exercício 2.1.1. *Verifique se os seguintes conjuntos com as operações indicadas são anéis. Dos anéis, decida se é anel com unidade e se tem divisores de zero. Algum deles é corpo? Algum deles é anel de integridade?*

(a) $\left(M_{2\times 2}(\mathbb{R}),\ +,\ \cdot\right)$, *onde* $M_{2\times 2}(\mathbb{R})$ *é o conjunto das matrizes quadradas* 2×2 *de números reais,* $+$ *e* $\cdot$ *as operações de adição e multiplicação usuais de matrizes respectivamente.*

(b) $\left(\mathbb{Z}\times\mathbb{Z},\ \oplus,\ \odot\right)$, *em que as operações* $\oplus$ *e* $\odot$ *são definidas por*

$$(a,b)\oplus(c,d) = (a+c,\ b+d) \qquad (a,b)\odot(c,d) = (a.c,\ b.d)$$

com $a,\ b,\ c,\ d \in \mathbb{Z}$ *e* $+$ *e* $\cdot$ *as operações de adição e multiplicação usuais em* $\mathbb{Z}$.

(c) $\left(\mathcal{P}(X),\ \triangle,\ \cap\right)$, *onde* $\mathcal{P}(X)$ *é o conjunto das partes de um conjunto não vazio* X *e* $A\triangle B = (A\cup B) - (A\cap B),\quad \forall\ A,B\in\mathcal{P}(X)$

(d) $\left(\mathbb{R},\ \oplus,\ \odot\right)$, *em que as operações* $\oplus$ *e* $\odot$ *são definidas por*

$$a\oplus b = a+b+1 \qquad a\odot b = a+b+a\cdot b$$

com $a,\ b,\ c,\ d \in \mathbb{R}$ *e* $+$ *e* $\cdot$ *as operações de adição e multiplicação usuais em* $\mathbb{R}$.

(e) $\left(\mathbb{Z}[\sqrt{-2}], +,\ \cdot\right)$, *onde* $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2};\ \ a,b\in\mathbb{Z}\}$ *e* $+$ *e* $\cdot$ *as operações de adição e multiplicação usuais em* $\mathbb{Z}$.

Solução.

(a) $\left(M_{2\times 2}(\mathbb{R}),\ +,\ \cdot\right)$:

- $\left(M_{2\times 2}(\mathbb{R}),\ +,\ \cdot\right)$ *é um anel pois*

(A1):

$$\left(\left[\begin{array}{cc} a & b \\ c & d \end{array}\right]+\left[\begin{array}{cc} a' & b' \\ c' & d' \end{array}\right]\right)+\left[\begin{array}{cc} a'' & b'' \\ c'' & d'' \end{array}\right]=\left[\begin{array}{cc} a+a' & b+b' \\ c+c' & d+d' \end{array}\right]+\left[\begin{array}{cc} a'' & b'' \\ c'' & d'' \end{array}\right]=$$

$$=\left[\begin{array}{cc} (a+a')+a'' & (b+b')+b'' \\ (c+c')+c'' & (d+d')+d'' \end{array}\right]=\left[\begin{array}{cc} a+(a'+a'') & b+(b'+b'') \\ c+(c'+c'') & d+(d'+d'') \end{array}\right]=$$

$$=\left[\begin{array}{cc} a & b \\ c & d \end{array}\right]+\left[\begin{array}{cc} a'+a'' & b'+b'' \\ c'+c'' & d+d'' \end{array}\right]=\left[\begin{array}{cc} a & b \\ c & d \end{array}\right]+\left(\left[\begin{array}{cc} a' & b' \\ c' & d' \end{array}\right]+\left[\begin{array}{cc} a'' & b'' \\ c'' & d'' \end{array}\right]\right).$$

(A2):

$$\left[\begin{array}{cc} a & b \\ c & d \end{array}\right]+\left[\begin{array}{cc} a' & b' \\ c' & d' \end{array}\right]=\left[\begin{array}{cc} a+a' & b+b' \\ c+c' & d+d' \end{array}\right]=\left[\begin{array}{cc} a'+a & b'+b \\ c'+c & d'+d \end{array}\right]=\left[\begin{array}{cc} a' & b' \\ c' & d' \end{array}\right]+\left[\begin{array}{cc} a & b \\ c & d \end{array}\right].$$

(A3):

O elemento neutro da adição é a matriz $\left[\begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array}\right]$*, pois* $\left[\begin{array}{cc} a & b \\ c & d \end{array}\right]+\left[\begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array}\right]=\left[\begin{array}{cc} a & b \\ c & d \end{array}\right].$

(A4):

O simétrico da matriz $\left[\begin{array}{cc} a & b \\ c & d \end{array}\right]$ *é a matriz* $\left[\begin{array}{cc} -a & -b \\ -c & -d \end{array}\right]$*, pois*

$$\left[\begin{array}{cc} a & b \\ c & d \end{array}\right]+\left[\begin{array}{cc} -a & -b \\ -c & -d \end{array}\right]=\left[\begin{array}{cc} 0 & 0 \\ 0 & 0 \end{array}\right].$$

(A5):

$$=\left[\left(\begin{array}{cc} a & b \\ c & d \end{array}\right)\cdot\left(\begin{array}{cc} a' & b' \\ c' & d' \end{array}\right)\right]\cdot\left(\begin{array}{cc} a'' & b'' \\ c'' & d'' \end{array}\right)=\left(\begin{array}{cc} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{array}\right)\cdot\left(\begin{array}{cc} a'' & b'' \\ c'' & d'' \end{array}\right)=$$

$$=\left(\begin{array}{cc} (aa'+bc')a''+(ab'+bd')c'' & (aa'+bc')b''+(ab'+bd')d'' \\ (ca'+dc')a''+(cb'+dd')c'' & (ca'+dc')b''+cb'+dd')d'' \end{array}\right)=$$

$$=\left(\begin{array}{cc} a(a'a'')+b(c'a'')+a(b'c'')+b(d'c'') & a(a'b'')+b(c'b'')+a(b'd'')+b(d'd'') \\ c(a'a'')+d(c'a'')+c(b'c'')+d(d'c'') & c(a'b'')+d(c'b'')+c(b'd'')+d(d'd'') \end{array}\right)=$$

$$=\left(\begin{array}{cc} a(a'a''+b'c'')+b(c'a''+d'c'') & a(a'b''+b'd'')+b(c'b''+d'd'') \\ c(a'a''+b'c'')+d(c'a''+d'c'') & c(a'b''+b'd'')+d(c'b''+d'd'') \end{array}\right)=$$

$$=\left(\begin{array}{cc} a & b \\ c & d \end{array}\right)\cdot\left(\begin{array}{cc} a'a''+b'c'' & a'b''+b'd'' \\ c'a''+d'c'' & c'b''+d'd'' \end{array}\right)=\left(\begin{array}{cc} a & b \\ c & d \end{array}\right)\cdot\left[\left(\begin{array}{cc} a' & b' \\ c' & d' \end{array}\right)\cdot\left(\begin{array}{cc} a'' & b'' \\ c'' & d'' \end{array}\right)\right]$$

(A6):

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \left(\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} + \begin{bmatrix} a'' & b'' \\ c'' & d'' \end{bmatrix} \right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a'+a'' & b'+b'' \\ c'+c'' & d'+d'' \end{bmatrix} =$$

$$= \begin{bmatrix} a(a'+a'')+b(c'+c'') & a(b'+b'')+b(d'+d'') \\ c(a'+a'')+d(c'+c'') & c(b'+b'')+d(d'+d'') \end{bmatrix}$$

$$= \begin{bmatrix} aa'+aa''+bc'+bc'' & ab'+ab''+bd'+bd'' \\ ca'+ca''+dc'+dc'' & cb'+cb''+dd'+dd'' \end{bmatrix}$$

$$= \begin{bmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{bmatrix} + \begin{bmatrix} aa''+bc'' & ab''+bd'' \\ ca''+dc'' & cb''+dd'' \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a'' & b'' \\ c'' & d'' \end{bmatrix}$$

A outra lei distributiva (A7) é mostrada de forma análoga.

- $\left(M_{2\times 2}(\mathbb{R}),\ +,\ \cdot\right)$ *é um anel não comutativo, pois por exemplo*

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \text{ mas } \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}.$$

- $\left(M_{2\times 2}(\mathbb{R}),\ +,\ \cdot\right)$ *é um anel com unidade* $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, *pois*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \text{ para todo } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times 2}(\mathbb{R}).$$

- $\left(M_{2\times 2}(\mathbb{R}),\ +,\ \cdot\right)$ *não é um domínio de integridade pois possui divisores de zero, por exemplo*

$$\begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}$$

logo $\begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}$ *é um divisor de zero.*

- $\left(M_{2\times 2}(\mathbb{R}),\ +,\ \cdot\right)$ *não é um corpo, pois* $\begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}$ *não possui elemento inverso multiplicativo.*

(b) $\Big(\mathbb{Z}\times\mathbb{Z},\ \oplus,\ \odot\Big)$:

- $\Big(\mathbb{Z}\times\mathbb{Z},\ \oplus,\ \odot\Big)$ *é um anel pois*

  (A1):

  $$\Big((a,b)\oplus(c,d)\Big)\oplus(e,f) = (a+c,b+d)\oplus(e,f) = \Big((a+c)+e,(b+d)+f\Big) =$$
  $$= \Big(a+(c+e),b+(d+f)\Big) = (a,b)+(c+e,d+f) =$$
  $$= (a,b)\oplus\Big((c,d)\oplus(e,f)\Big).$$

  (A2):

  $$(a,b)\oplus(c,d) = (a+c,b+d) = (c+a,d+b) = (c,d)\oplus(a,b).$$

  (A3):

  O elemento neutro da adição é o par $(0,0)$*, pois* $(a,b)\oplus(0,0) = (a,b)$.

  (A4)

  O simétrico do elemento (a,b) *é o par* $(-a,-b)$*, pois*
  $$(a,b)\oplus(-a,-b) = \Big(a+(-a),b+(-b)\Big) = (0,0)$$

  (A5):

  $$\Big((a,b)\odot(c,d)\Big)\odot(e,f) = (a\cdot c,\ b\cdot d)\odot(e,f) = \Big((a\cdot c)\cdot e,\ (b\cdot d)\cdot f\Big) =$$
  $$= \Big(a\cdot(c\cdot e),\ b\cdot(d\cdot f)\Big) = (a,b)\odot(c\cdot e,\ d\cdot f) =$$
  $$= (a,b)\odot\Big((c,d)\odot(e,f)\Big).$$

  (A6):

  $$(a,b)\odot\Big((c,d)\oplus(e,f)\Big) = (a,b)\odot(c+e,\ d+f) = \Big(a\cdot(c+e),\ b\cdot(d+f)\Big) =$$
  $$= \Big(a\cdot c+a\cdot e,\ b\cdot d+b\cdot f\Big) = (a\cdot c,b\cdot d)\oplus(a\cdot e,\ b\cdot f) =$$
  $$= \Big((a,b)\odot(c,d)\Big)\oplus\Big((a,b)\odot(e,f)\Big).$$

  A outra lei distributiva é mostrada de forma análoga.

- $\Big(\mathbb{Z}\times\mathbb{Z},\ \oplus,\ \odot\Big)$ *é um anel comutativo, pois*
  $(a,b)\odot(c,d) = (a\cdot c,\ b\cdot d) = (c\cdot a,\ d\cdot b) = (c,d)\odot(a,b)$ *para todo* $(a,b),\ (c,d)\in\mathbb{Z}\times\mathbb{Z}$.

- $\Big(\mathbb{Z}\times\mathbb{Z},\ \oplus,\ \odot\Big)$ *é um anel com unidade* $(1,1)$*, pois*
  $(a,b)\odot(1,1) = (a\cdot 1,\ b\cdot 1) = (a,b)$ *para todo* $(a,b),\ (c,d)\in\mathbb{Z}\times\mathbb{Z}$.

- $\left(\mathbb{Z}\times\mathbb{Z},\ \oplus,\ \odot\right)$ *é um domínio de integridade, pois não possui divisores de zero. De fato,* $(a,b)\odot(c,d)=(0,0)\Leftrightarrow\ (a,b)=(0,0)$ *ou* $(c,d)=(0,0)$.

- $\left(\mathbb{Z}\times\mathbb{Z},\ \oplus,\ \odot\right)$ *não é um corpo, pois* $(2,2)$ *não possui um inverso multiplicativo.*

(c) $\left(\mathcal{P}(X),\ \triangle,\ \cap\right)$:

- $\left(\mathcal{P}(X),\ \triangle,\ \cap\right)$ *é um anel pois*

(A2):

$A\triangle B=(A\cup B)-(A\cap B)=(B\cup A)-(B\cap A)=B\triangle A$

pois $\cap$ *e* $\cup$ *são operações comutativos.*

(A1):

Para provar a lei da associatividade, vamos usar os seguintes fatos:

- *Se* A,B *são conjuntos e* X *o conjunto universo. Então* $A-B=A\cap\overline{B}$.
- *Leis de Morgan:* $\overline{(A\cap B)}=\overline{A}\cup\overline{B}\ \ e\ \ \overline{(A\cup B)}=\overline{A}\cap\overline{B}$
- *Portanto, podemos reescrever* $A\triangle B=(A\cap\overline{B})\cup(B\cap\overline{A})$

$$
\begin{aligned}
A\triangle(B\triangle C) &= \left[A\cap\overline{(B\triangle C)}\right]\cup\left[(B\triangle C)\cap\overline{A}\right]\\
&= \left[A\cap\overline{\left((B\cap\overline{C})\cup(C\cap\overline{B})\right)}\right]\cup\left[\left((B\cap\overline{C})\cup(C\cap\overline{B})\right)\cap\overline{A}\right]\\
&= \left[A\cap\overline{\left(B\cap\overline{C}\right)}\cap\overline{\left(C\cap\overline{B}\right)}\right]\cup\left[\left((B\cap\overline{C})\cap\overline{A}\right)\cup\left((C\cap\overline{B})\cap\overline{A}\right)\right]\\
&= \left[A\cap\left(\overline{B}\cup C\right)\cap\left(\overline{C}\cup B\right)\right]\cup\left((B\cap\overline{C})\cap\overline{A}\right)\cup\left((C\cap\overline{B})\cap\overline{A}\right)\\
&= A\cap\left[\left(\overline{B}\cap(\overline{C}\cup B)\right)\cup\left(C\cap(\overline{C}\cup B)\right)\right]\cup\left(B\cap\overline{C}\cap\overline{A}\right)\cup\left(C\cap\overline{B}\cap\overline{A}\right)\\
&= A\cap\left[(\overline{B}\cap\overline{C})\cup(\overline{B}\cap B)\cup(C\cap\overline{C})\cup(C\cap B)\right]\cup\left(B\cap\overline{C}\cap\overline{A}\right)\cup\left(C\cap\overline{B}\cap\overline{A}\right)\\
&= A\cap\left[(\overline{B}\cap\overline{C})\cup\emptyset\cup\emptyset\cup(C\cap B)\right]\cup\left(B\cap\overline{C}\cap\overline{A}\right)\cup\left(C\cap\overline{B}\cap\overline{A}\right)\\
&= A\cap\left[(\overline{B}\cap\overline{C})\cup(C\cap B)\right]\cup\left(B\cap\overline{C}\cap\overline{A}\right)\cup\left(C\cap\overline{B}\cap\overline{A}\right)\\
&= \left(A\cap\overline{B}\cap\overline{C}\right)\cup\left(A\cap C\cap B\right)\cup\left(B\cap\overline{C}\cap\overline{A}\right)\cup\left(C\cap\overline{B}\cap\overline{A}\right)
\end{aligned}
$$

Agora usando o fato que $\triangle$ é comutativa (A1) e se trocamos conjuntos na expressão original $A\triangle(B\triangle C)$ no seguinte maneira: $A\leftrightarrow C$; $B\leftrightarrow A$; $C\leftrightarrow B$ temos que

$$
\begin{aligned}
(A\triangle B)\triangle C &= C\triangle(A\triangle B) \quad por \quad A1\\
&= \left(C\cap\overline{A}\cap\overline{B}\right)\cup\left(C\cap B\cap A\right)\cup\left(A\cap\overline{B}\cap\overline{C}\right)\cup\left(B\cap\overline{A}\cap\overline{C}\right)
\end{aligned}
$$

Agora com $\cap$ e $\cup$ são comutativos temos,

$$
\begin{aligned}
(A\triangle B)\triangle C &= \left(A\cap\overline{B}\cap\overline{C}\right)\cup\left(A\cap C\cap B\right)\cup\left(B\cap\overline{C}\cap\overline{A}\right)\cup\left(C\cap\overline{B}\cap\overline{A}\right)\\
&= \left(C\cap\overline{A}\cap\overline{B}\right)\cup\left(C\cap B\cap A\right)\cup\left(A\cap\overline{B}\cap\overline{C}\right)\cup\left(B\cap\overline{A}\cap\overline{C}\right)\\
&= C\triangle(A\triangle B)
\end{aligned}
$$

(A3):

O elemento neutro da adição é o conjunto $\emptyset$, pois $A\triangle\emptyset = A$.

(A4):

O simétrico do elemento A é o conjunto A pois $A\triangle A = \emptyset$

(A5):

$(A \cap B) \cap C = A \cap (B \cap C)$.

(A6):

$$A \cap (B \triangle C) = A \cap \Big((B - C) \cup (C - B)\Big) = \Big(A \cap (B - C)\Big) \cup \Big(A \cap (C - B)\Big) =$$
$$= \Big((A \cap B) - (A \cap C)\Big) \cup \Big((A \cap C) - (A \cap B)\Big) =$$
$$= (A \cap B) \triangle (A \cap C).$$

A outra lei distributiva é mostrada de forma análoga.

- $\Big(\mathcal{P}(X),\ \triangle,\ \cap\Big)$ *é um anel comutativo, pois* $A \cap B = B \cap A$ *para todo* $A, B \in \mathcal{P}$.

- $\Big(\mathcal{P}(X),\ \triangle,\ \cap\Big)$ *é um anel com unidade X, pois* $A \cap X = A$.

- $\Big(\mathcal{P}(X),\ \triangle,\ \cap\Big)$ *não é um domínio de integridade, pois possui divisores de zero. Por exemplo* $A \cap \overline{A} = \overline{A} \cap A = \emptyset$.

- $\Big(\mathcal{P}(X),\ \triangle,\ \cap\Big)$ *não é um corpo pois, se A e B são subconjuntos de X não temos em geral que* $A \cap B = X$.

(d) $\Big(\mathbb{R},\ \oplus,\ \odot\Big)$:

- $\Big(\mathbb{R},\ \oplus,\ \odot\Big)$ *é um anel pois*

  (A1)

  $$\Big(a \oplus b\Big) \oplus c = a + b + 1 \oplus c = (a + b + 1) + c + 1 = a + (b + c + 1) + 1 = a \oplus (b \oplus c).$$

  (A2)

  $$a \oplus b = a + b + 1 = b + a + 1 = b \oplus a.$$

  (A3)

  O elemento neutro da adição é (-1), *pois* $a \oplus (-1) = a + (-1) + 1 = a - 1 + 1 = a$.

  (A4)

  O simétrico do elemento a é $(-2 - a)$, *pois*

  $a \oplus (-2 - a) = a + (-2 - a) + 1 = a - 2 - a + 1 = -1$

  (A5)

$$\Big(a \odot b\Big) \odot c = (a + b + a \cdot b) \odot c = (a + b + a \cdot b) + c - (a + b + a \cdot b) \cdot c =$$
$$= a + b + a \cdot b + c + a \cdot c + b \cdot c + a \cdot b \cdot c = a + (b + c + bc) + \cdot(a \cdot b + a \cdot c + a \cdot b \cdot c) =$$
$$= a + (b + c + bc) + a \cdot (b + c + b \cdot c) = a \odot \Big(b \odot c\Big).$$

(A6)

$$a \odot \Big(b \oplus c\Big) = a \odot (b + c + 1) = a + (b + c + 1) + a \cdot (b + c + 1) =$$
$$= a + b + c + 1 + a \cdot b + a \cdot c + a = (a + b + a \cdot b) + (a + c + a \cdot c) + 1 =$$
$$= (a \odot b) + (a \odot c) + 1 = (a \odot b) \oplus (a \odot c).$$

A outra lei distributiva é mostrada de forma análoga.

- $\Big(\mathbb{R}, \oplus, \odot\Big)$ *é um anel comutativo pois* $a \odot b = a + b + a \cdot b = b + a + b \cdot a = b \odot a$ *para todo* $a, b \in \mathbb{R}$.

- $\Big(\mathbb{R}, \oplus, \odot\Big)$ *é um anel com unidade* -1, *pois* $a \odot -1 = a - 1 + 1 = a$ *para todo* $a \in R$.

- $\Big(\mathbb{R}, \oplus, \odot\Big)$ *é domínio de integridade pois não possui divisores de zero. De fato se* $a \odot b = -1 \Leftrightarrow\ a = -1\ \ ou\ \ b = -1$.

- $\Big(\mathbb{R}, \oplus, \odot\Big)$ *é um corpo, pois cada elemento* $a \neq (-1)$, *possui inverso multiplicativo* $b = \dfrac{-a}{1 + a}$.

(e) $\Big(\mathbb{Z}[\sqrt{-2}], +, \cdot\Big)$

- $\Big(\mathbb{Z}[\sqrt{-2}], +, \cdot\Big)$ *é um anel pois*

  (A1)

  $$\Big((a + b\sqrt{-2}) + (c + d\sqrt{-2})\Big) + (e + f\sqrt{-2}) = (a + c) + (b + d)\sqrt{-2} + (e + f\sqrt{-2}) =$$
  $$= (a + c + e) + (b + d + f)\sqrt{-2} = (a + b\sqrt{-2}) + (c + e) + (d + f)\sqrt{-2} =$$
  $$= (a + b\sqrt{-2}) + \Big((c + d\sqrt{-2}) + (e + f\sqrt{-2})\Big).$$

  (A2)

  $$(a + b\sqrt{-2}) + (c + d\sqrt{-2}) = (a + c) + (b + d)\sqrt{-2} = (c + a) + (d + b)\sqrt{-2} =$$
  $$= (c + d\sqrt{-2}) + (a + b\sqrt{-2})$$

  (A3)

  O elemento neutro da adição é $(0 + 0\sqrt{-2})$, *pois*
  $(a + b\sqrt{-2}) + (0 + 0\sqrt{-2}) = a + b\sqrt{-2}$.

(A4)

O simétrico do elemento $(a + b\sqrt{-2})$ *é* $(-a - b\sqrt{-2})$, *pois*

$(a + b\sqrt{-2}) + (-a - b\sqrt{-2}) = (a - a) + (b - b)\sqrt{-2} = 0 + 0\sqrt{-2}.$

(A5)

$\Big((a + b\sqrt{-2}) \cdot (c + d\sqrt{-2})\Big) \cdot (e + f\sqrt{-2}) = \Big((ac - 2bd) + (ad + bc)\sqrt{-2}\Big) \cdot (e + f\sqrt{-2}) =$

$= \Big(e(ac - 2bd) - 2f(ad + bc)\Big) + \Big(f(ac - 2bd) + e(ad + bc)\Big)\sqrt{-2} =$

$= \Big(eac - 2ebd - 2fad - 2fbc\Big) + \Big(fac - 2fbd + ead + ebc\Big)\sqrt{-2}.$

Por outro lado,

$(a + b\sqrt{-2}) \cdot \Big((c + d\sqrt{-2}) \cdot (e + f\sqrt{-2})\Big) = (a + b\sqrt{-2}) \cdot \Big((ce - 2fd) + (cf + de)\sqrt{-2}\Big) =$

$= \Big(a(ce - 2fd) - 2b(cf + de)\Big) + \Big(a(cf + de) + b(ce - 2fd)\Big)\sqrt{-2} =$

$= \Big(ace - 2afd - 2bcf - 2bde\Big) + \Big(acf + ade + bce - 2bfd\Big)\sqrt{-2}.$

Portanto

$\Big((a + b\sqrt{-2}) \cdot (c + d\sqrt{-2})\Big) \cdot (e + f\sqrt{-2}) = (a + b\sqrt{-2}) \cdot \Big((c + d\sqrt{-2}) \cdot (e + f\sqrt{-2})\Big)$

(A6)

$(a + b\sqrt{-2}) \cdot \Big((c + d\sqrt{-2}) + (e + f\sqrt{-2})\Big) = (a + b\sqrt{-2}) \cdot \Big((c + e) + (d + f)\sqrt{-2}\Big) =$

$= \Big(a(c + e) - 2b(d + f)\Big) + \Big(a(d + f) + b(c + e)\Big)\sqrt{-2} =$

$= \Big(ac + ae - 2bd - 2bf\Big) + \Big(ad + af + bc + be\Big)\sqrt{-2}.$

Por outro lado,

$(a + b\sqrt{-2}) \cdot (c + d\sqrt{-2}) + (a + b\sqrt{2}) \cdot (e + f\sqrt{-2}) =$

$= \Big((ac - 2bd) + (ad + bc)\sqrt{-2}\Big) + \Big((ae - 2bf) + (af + be)\sqrt{-2}\Big) =$

$= \Big((ac - 2bd) + (ae - 2bf)\Big) + \Big((ad + bc) + (af + be)\Big)\sqrt{-2} =$

$= \Big(ac - 2bd + ae - 2bf\Big) + \Big(ad + bc + af + be\Big)\sqrt{-2}.$

Portanto

$(a + b\sqrt{-2}) \cdot \Big((c + d\sqrt{-2}) + (e + f\sqrt{-2})\Big) = (a + b\sqrt{-2}) \cdot (c + d\sqrt{-2}) + (a + b\sqrt{2}) \cdot (e + f\sqrt{-2})$

A outra lei distributiva é mostrada de forma análoga.

- $\Big(\mathbb{Z}[\sqrt{-2}], +, \cdot\Big)$ *é um anel comutativo pois*

  $(a + b\sqrt{-2}) \cdot (c + d\sqrt{-2}) = (ac - 2bd) + (ad + bc)\sqrt{-2}$

  Por outro lado,

  $(c + d\sqrt{-2}) \cdot (a + b\sqrt{-2}) = (ca - 2db) + (cb + da)\sqrt{-2}.$

Portanto

$(a + b\sqrt{-2}) \cdot (c + d\sqrt{-2}) = (c + d\sqrt{-2}) \cdot (a + b\sqrt{-2})$

- $\left(\mathbb{Z}[\sqrt{-2}], +, \cdot\right)$ *um anel com unidade* $(1 + 0\sqrt{-2})$*, pois* $(a + b\sqrt{-2}) \cdot (1 + 0\sqrt{-2}) = a + b\sqrt{-2}$.

- $\left(\mathbb{Z}[\sqrt{-2}], +, \cdot\right)$ *é um domínio de integridade pois não possui divisores de zero. De fato* $(a+b\sqrt{-2})\cdot(c+d\sqrt{-2}) = 0+0\sqrt{-2} \Leftrightarrow (a+b\sqrt{-2}) = 0+0\sqrt{-2}$ *ou* $(c+d\sqrt{-2}) = 0+0\sqrt{-2}$.

- $\left(\mathbb{Z}[\sqrt{-2}], +, \cdot\right)$ *não é um corpo. De fato se* $(c + d\sqrt{-2})$ *é o inverso de* $(a + b\sqrt{-2})$ *então* $c = \dfrac{a}{a^2 + 2b^2} \notin \mathbb{Z}$ *e* $d = \dfrac{-b}{a^2 + 2b^2} \notin \mathbb{Z}$.

Exercício 2.1.2. *Seja* $(A, +, \cdot)$ *um anel comutativo com identidade. Prove que:*

(a) Se $u \in A$ *é unidade (invertível) então* u *não é divisor de zero.*

(b) O produto de um divisor de zero por qualquer elemento de A *é nulo ou é um divisor de zero.*

(c) Se o produto de dois elementos de A *é um divisor de zero então algum dos fatores o é.*

(d) A soma de dois divisores de zero pode não ser um divisor de zero.

Solução.

(a) Se u *é unidade em* A*, então existe* $t \in A$ *tal que* $u \cdot t = t \cdot u = 1$.

Agora suponha que u *é um divisor de zero em* A*. Então existe* $\widetilde{u} \neq 0$ *tal que* $u \cdot \widetilde{u} = 0$

Agora $0 \neq \widetilde{u} = \widetilde{u} \cdot 1 = \widetilde{u} \cdot (u \cdot t) = (\widetilde{u} \cdot u) \cdot t = 0 \cdot t = 0$

Contradição, logo u *não é um divisor de zero.*

(b) Seja a *um divisor de zero de* A*. Então existe* $\widetilde{a} \neq 0$ *tal que* $a \cdot \widetilde{a} = 0$.

Seja $c = a \cdot b$, $b \in A$ *qualquer.*

- *Se* $b = 0$ *ou* $b = \widetilde{a}$*, então* $c = 0$.
- *Suponha que* $b \neq 0$ *e* $b \neq \widetilde{a}$*. Portanto* $c \neq 0$.

  Multiplicando c *por* $\widetilde{a}$ *temos*

$$\widetilde{a} \cdot c = \widetilde{a} \cdot (ab) = (\widetilde{a} \cdot a) \cdot b = 0 \cdot b = 0$$

Logo c é um divisor de zero de A.

(c) Sejam $a, b \in A$ tal que $(a \cdot b)$ é um divisor. Então existe $c \neq 0$ tal que $c \cdot (a \cdot b) = 0$.

Pela lei da associatividade, temos que

$$c \cdot (a \cdot b) = (c \cdot a) \cdot b = 0 \Rightarrow \begin{cases} ou\ (c \cdot a) \neq 0 \Rightarrow b\ \text{é divisor de zero} \\ ou\ (c \cdot a) = 0 \Rightarrow a\ \text{é divisor de zero} \end{cases}$$

(d) Em $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ temos que 3 e 4 são divisores de zero. Mas $3 + 4 = 1$ não é um divisor zero.

Exercício 2.1.3. *Estabeleça uma relação de inclusão entre anel, corpo e domínio de integridade e justifique.*

Solução.

$$corpo \ \subset \ domínio\ de\ integridade \ \subset \ anel$$

- *Seja A um corpo e considere $a, b \in A$ tais que $a \cdot b = 0$. Para garantir que A é um domínio de integridade precisamos mostrar que $a = 0$ ou $b = 0$.*

  Se $a = 0$, conclui-se não há o que fazer.

  Se $a \neq 0$, então a é inversível (pois A é um corpo) e, portanto

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

  Logo, A é um domínio de integridade e, assim, tem-se a primeira inclusão.

- *A segunda inclusão segue diretamente da definição de domínio de integridade.*

Exercício 2.1.4. *Quais dos seguintes conjuntos são subanéis e/ou ideais dos anéis indicados.*

(a) $\mathbb{P} = \{2k,\ k \in \mathbb{Z}\}$ *em* $\left(\mathbb{Z}, +, \cdot\right)$

(b) $\mathbb{I} = \{2k - 1,\ k \in \mathbb{Z}\}$ *em* $\left(\mathbb{Z}, +, \cdot\right)$

(c) $\mathbb{Z}$ *em* $\mathbb{Q}$

(d) $\{a + b\sqrt{2},\ a, b \in \mathbb{Z}\}$ *em* $\left(\mathbb{R}, +, \cdot\right)$

(e) $\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix};\ a, b \in \mathbb{Z}\right\}$ *em* $\left(M_{2\times 2}(\mathbb{Z}),\ +,\ \cdot\right)$

(f) $\left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix};\ a \in \mathbb{Z} \right\}$ *em* $\left(M_{2\times 2}(\mathbb{Z}),\ +,\ \cdot\right)$,

Solução.

(a) $\mathbb{P} = \{2k,\ k \in \mathbb{Z}\}$

(a1) Sejam $a, b \in \mathbb{P}$ *quaisquer. Ou seja,* $a = 2k_1$ *e* $b = 2k_2$, *onde* $k_1, k_2 \in \mathbb{Z}$. *Assim*

- $a - b = 2k_1 - 2k_2 = 2(k_1 - k_2) = 2\overline{k} \Rightarrow a - b \in \mathbb{P}$.
- $a \cdot b = 2k_1 2k_2 = 2(2k_1k_2) = 2\overline{k} \Rightarrow a \cdot b \in \mathbb{P}$

Como $a - b \in \mathbb{P}$ *e* $a \cdot b \in \mathbb{P}$, *temos que* $\mathbb{P}$ *é um* **subanel** *em* $\left(\mathbb{Z}, +, \cdot\right)$.

(a2) Sejam $a, b \in \mathbb{P}$ *e* $n \in \mathbb{Z}$ *quaisquer. Assim*

- $a + b = 2k_1 + 2k_2 = 2(k_1 + k_2) = 2\overline{k} \Rightarrow a + b \in \mathbb{P}$.
- $a \cdot n = 2k_1 n = 2(k_1 n) = 2\overline{k} \Rightarrow a \cdot n \in \mathbb{P}$

Como $a - b \in \mathbb{P}$ *e* $a \cdot b \in \mathbb{P}$, *temos que* $\mathbb{P}$ *é um* **ideal** *em* $\left(\mathbb{Z}, +, \cdot\right)$.

(b) $\mathbb{I} = \{2k - 1,\ k \in \mathbb{Z}\}$ *em* $\left(\mathbb{Z}, +, \cdot\right)$

O conjunto $\mathbb{I}$ *dos inteiros ímpares* **não é um subanel nem ideal** *de* $\mathbb{Z}$, *pois para*

$$a = 3 \ \ e\ b = 1,\ a - b = 2 \notin \mathbb{I}.$$

(c) $\mathbb{Z}$ *em* $\mathbb{Q}$

(c1) Sejam $a, b \in \mathbb{Z}$ *quaisquer. Então* $a - b \in \mathbb{Z}$ *e* $a \cdot b \in \mathbb{Z}$. *Portanto* $\mathbb{Z}$ *é um* **subanel** *em* $\mathbb{Q}$.

(c2) $\mathbb{Z}$ **não é ideal** *em* $\mathbb{Q}$ *pois* $a = 3 \in \mathbb{Z}$ *e* $b = \dfrac{1}{2} \in \mathbb{Q}$, *mas* $a \cdot b = \dfrac{3}{2} \notin \mathbb{Z}$.

(d) $\mathcal{A} = \{a + b\sqrt{2},\ a, b \in \mathbb{Z}\}$ *em* $\left(\mathbb{R}, +, \cdot\right)$

(d1) Sejam $x, y \in \mathcal{A}$ *quaisquer. Ou seja,* $x = a_1 + b_1\sqrt{2}$ *e* $y = a_2 + b_2\sqrt{2}$, *onde* $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. *Assim*

- $x - y = (a_1 + b_1\sqrt{2}) - (a_2 + b_2\sqrt{2}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{2} \Rightarrow x - y \in \mathcal{A}$
- $x \cdot y = (a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2} \Rightarrow x \cdot y \in \mathcal{A}$

Como $x - y \in \mathcal{A}$ *e* $a \cdot b \in \mathcal{A}$, *temos que* $\mathcal{A}$ *é um* **subanel** *em* $\mathbb{R}$.

(d2) $\mathcal{A}$ **não é ideal** *em* $\mathbb{R}$ *pois* $a = 3 + 4\sqrt{2} \in \mathcal{A}$ *e* $b = \dfrac{1}{5} \in \mathbb{R}$, *mas* $a \cdot b = \dfrac{3}{5} + \dfrac{4}{5}\sqrt{2} \notin \mathcal{A}$.

(e) $M = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix};\ a, b \in \mathbb{Z} \right\}$ *em* $\left(M_{2\times 2}(\mathbb{Z}),\ +,\ \cdot\right)$

(e1) Sejam $A, B \in M$ *quaisquer. Ou seja,* $A = \begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix}$ *e* $B = \begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix}$. *Assim*

- $A - B = \begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & 0 \end{bmatrix} \Rightarrow A - B \in M.$
- $A \cdot B = \begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1a_2 & a_1b_2 \\ 0 & 0 \end{bmatrix} \Rightarrow A \cdot B \in M$

Como $A - B \in M$ *e* $A \cdot B \in M$, *temos que* M *é um* **subanel** *em* $M_{2\times 2}(\mathbb{Z})$.

(e2) Sejam $A, B \in M$ *e* $C \in M_{2\times 2}$ *quaisquer. Assim*

- $A + B = \begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ 0 & 0 \end{bmatrix} \Rightarrow A + B \in M.$
- $A \cdot C = \begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} = \begin{bmatrix} a_1c_1 + b_1c_3 & a_1c_2 + b_1c_4 \\ 0 & 0 \end{bmatrix} \Rightarrow A \cdot B \in M.$

Como $A - B \in \mathbb{P}$ *e* $A \cdot B \in M$, *temos que* M *é um* **ideal a esquerda** *de* $M_{2\times 2}$.

(f) $M_1 = \left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix};\ a \in \mathbb{Z} \right\}$ *em* $\left(M_{2\times 2}(\mathbb{Z}),\ +,\ \cdot\right)$,

Sejam $A, B \in M_1$ *quaisquer. Ou seja,* $A = \begin{bmatrix} a_1 & 0 \\ 0 & 1 \end{bmatrix}$ *e* $B = \begin{bmatrix} a_2 & 0 \\ 0 & 1 \end{bmatrix}$. *Assim*

$$A - B = \begin{bmatrix} a_1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} a_2 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1 - a_2 & 0 \\ 0 & 0 \end{bmatrix} \Rightarrow A - B \notin M.$$

O conjunto M_1 **não é um subanel nem ideal** *de* $M_{2\times 2}(\mathbb{Z})$

Exercício 2.1.5. *Sejam* A *um anel e* $I,\ J$ *ideais de* A. *Mostre que*

(a) $I + J$ *é ideal de* A

(b) $I \cap J$ *é ideal de* A

(c) IJ *é ideal de* A *contido em* $I \cap J$.

Solução.

(a) $I + J = \{x + y \in A \mid x \in I \text{ e } y \in J\}$ *é ideal de* A *pois*

- *Sejam* $x, y \in I + J$*, ou seja ,* $x = x_1 + x_2$ *e* $y = y_1 + y_2$ *com* $x_1, y_1 \in I$ *e* $x_2, y_2 \in J$*. Temos que*

$$\begin{aligned} x + y &= (x_1 + x_2) + (y_1 + y_2) \\ &= (x_1 + y_1) + (x_2 + y_2) \end{aligned}$$

  Como I *e* J *são ideais de* A*, vale* $(x_1 + y_1) \in I$ *e* $(x_2 + y_2) \in J$*.*
  Logo, $x + y \in I + J$

- *Seja* $x \in I + J$*, ou seja* $x = x_1 + x_2$ *com* $x_1 \in I$ *e* $x_2 \in J$ *e seja* $r \in A$*. Temos que*

$$\begin{aligned} x \cdot r &= (x_1 + x_2) \cdot r \\ &= x_1 \cdot r + x_2 \cdot r \end{aligned}$$

  Como I *e* J *são ideais de* A*, vale que* $x_1 \cdot r \in I$ *e* $x_2 \cdot r \in J$
  Logo $x \cdot r \in I + J$*.*

Concluímos, assim, que $I + J$ *é um ideal de* A*.*

(b) $I \cap J = \{x \in A \mid x \in I \text{ e } x \in J\}$ *é ideal de* A *pois*

- *Sejam* $x, y \in I \cap J$*, então* $x, y \in I$ *e* $x, y \in J$*. Como* I *e* J *são ideais de* A*, vale que*

$$x + y \in I \text{ e } x + y \in J$$

  Logo $x + y \in I \cap J$*.*

- *Seja* $x \in I \cap J$ *e* $r \in A$*. Assim* $x \in I$ *e* $x \in J$*. Como* I *e* J *são ideais de* A*, vale que*

$$x \cdot r \in I \text{ e } x \cdot r \in J$$

  Logo $x \cdot r \in I \cap J$*.*

Concluímos, assim, que $I \cap J$ *é um ideal de* A*.*

(c) $IJ = \left\{ \sum_{i=1}^{n} a_i b_i; \;\; a_i \in I, \; b_i \in J, \; n \in \mathbb{N} \right\}$ *é ideal de* A *pois*

- *Sejam* $x, y \in IJ$, *então* $x = \sum_{i=1}^{n} a_i b_i$ *e* $y = \sum_{j=1}^{m} c_j d_j$ *com* $a_i, c_j \in I$ *e* $b_i, d_j \in J$.
  Portanto $x + y = \sum_{i=1}^{n} a_i b_i + \sum_{j=1}^{m} c_j d_j \in IJ$
  pois ela é uma soma finita $(n + m$ *termos) com os termos obtidos de produtos de elementos de* I *com elementos de* J.
- *Seja* $x \in IJ$ *e* $r \in A$. *Assim* $x = \sum_{i=1}^{n} a_i b_i$ *e temos que* $x \cdot r = \sum_{i=1}^{n} (ra_i) b_i \in IJ$ *pois* $ra_i \in I$. *Logo* $x \cdot r \in I \cap J$.
- *Além disto, observe que* $x = \sum_{i=1}^{n} a_i b_i \in I$ *pois* $a_i \in I,\ b_i \in A$ *e* I *é ideal de* A.
  Da mesma forma, $x \in J$ *pois* $a_i \in A,\ b_i \in J$ *e* J *é ideal de* A.
  Portanto, temos que $IJ \subseteq I \cap J$.

Concluímos, assim, que IJ *é um ideal de* A *contido em* $I \cap J$.

Exercício 2.1.6. *Em cada um dos casos abaixo diga se o elemento* r *é uma unidade no anel* R. *Justifique suas respostas.*

$(a)\ R = \mathbb{Z}_{11},\quad r = 5, \qquad (b)\ R = \mathbb{Z}_{12},\ \ r = 4 \qquad (c)\ R = \mathbb{Z}[i],\quad r = 2 + i$

Solução.

(a) $r = 5$ *é uma unidade em* $\mathbb{Z}_{11}$ *pois* $\mathbb{Z}_{11}$ *é um corpo. De fato,* $5 \cdot 9 = 45 \equiv 1$ *em* $\mathbb{Z}_{11}$

(b) $r = 4$ *não é uma unidade pois* $r = 4$ *é um divisor de zero, isto é* $3 \cdot 4 \equiv 0$ *em* $\mathbb{Z}_{12}$.

(c) $2 + i$ *não é uma unidade de* $\mathbb{Z}[i]$ *pois as únicas unidades de* $\mathbb{Z}[i]$ *são* $\{1, -1, i, -i\}$.
De fato se existe $a + ib \in \mathbb{Z}[i]$ *tal que*

$$(2 - i)(a + ib) = 1$$

então teremos os sistema

$$\begin{cases} 2a + b = 1 \\ -a + 2b = 0 \end{cases} \Rightarrow a = \frac{2}{5},\ b = \frac{1}{5}.$$

Mas $\frac{2}{5} + i\frac{1}{5} \notin \mathbb{Z}[i]$.

Exercício 2.1.7. *Seja R um anel comutativo com característica p, número primo.*

(a) Mostre que $(x+y)^p = x^p + y^p$

(b) Mostre que, para todo n inteiro positivo, $(x+y)^{p^n} = x^{p^n} + y^{p^n}$.

(c) Determine os elementos x, y um anel comutativo de caraterística 4 tal que $(x+y)^4 \neq x^4 + y^4$.

Solução.

(a) Usando a expansão binômio e o fato que R é comutativo, temos que

$$\begin{aligned}(x+y)^p &= x^p + px^{p-1}y + \frac{p(p-1)}{2}x^{p-2}y^2 + \frac{p(p-1)(p-2)}{3!}x^{p-3}y^3 + \cdots + pxy^{p-1} + y^p \\ &= x^p + \cancelto{0}{px^{p-1}y} + \frac{(p-1)}{2}\cancelto{0}{\left(px^{p-2}y^2\right)} + \frac{(p-1)(p-2)}{3!}\cancelto{0}{\left(px^{p-3}y^3\right)} + \cdots + \cancelto{0}{pxy^{p-1}} + y^p \\ &= x^p + y^p\end{aligned}$$

sendo que na segunda igualdade, usamos o fato que se R é uma anel comutativo com característica p, temos do Lema 2.1.17 que $px = 0$ para todo $x \in R$.

(b) Provamos por indução:

Consideremos a condição

$$P(n): \quad (x+y)^{p^n} = x^{p^n} + y^{p^n}. \qquad (*)$$

Pretendemos mostrar que $P(n)$ é válida para todo o número natural n.

- *Para $n = 1$ a condição reduz-se a*

$$(x+y)^p = x^p + y^p,$$

logo $P(1)$ é verdadeira pelo parte (a).

- *Suponha que, para algum $n \in N$, se tenha que $P(n)$ é verdadeira, isto é, $(*)$ é válida. Pretendemos provar que $P(n+1)$ também é verdadeira, ou seja*

$$(x+y)^{p^{n+1}} = x^{p^{n+1}} + y^{p^{n+1}}$$

Para isto, note que

$$\begin{aligned}
(x+y)^{p^{n+1}} &= (x+y)^{p^n \cdot p} \\
&= \left((x+y)^{p^n}\right)^p \\
&= \left(x^{p^n} + y^{p^n}\right)^p \quad \textit{usando } (*) \\
&= x^{p^{n+1}} + px^{p^{n+1}-1}y + \frac{p(p-1)}{2}x^{p^{n+1}-2}y^2 + \cdots + pxy^{p^{n+1}-1} + y^{p^{n+1}} \\
&= x^{p^{n+1}} + \cancelto{0}{px^{p^{n+1}-1}}y + \frac{(p-1)}{2}\cancelto{0}{\left(px^{p^{n+1}-2}y^2\right)} + \cdots + \cancelto{0}{pxy^{p^{n+1}-1}} + y^{p^{n+1}} \\
&= x^{p^{n+1}} + y^{p^{n+1}}
\end{aligned}$$

Isso mostra que $P(n+1)$ é verdadeira, toda vez que $P(n)$ é verdadeira. Portanto, pelo princípio de indução matemática, a fórmula é válida para todo número natural n.

(c) Considere $\mathbb{Z}_4 = \{0,\ 1,\ 2,\ 3\}$. Temos que a característica de $\mathbb{Z}_4$ é 4. Tomamos $x = y = 1$ temos que

$$(x+y)^4 = (1+1)^4 = 2^4 = 16 = 0 \quad \textit{mas } x^4 + y^4 = 1^4 + 1^4 = 2$$

Logo $(x+y)^4 \neq x^4 + y^4$.

Aula 2.2

Homomorfismo de Anéis e Anel Quociente

Nesta aula definimos homomorfismo entre anéis e apresentamos suas principais propriedades.

2.2.1 Homomorfismo de Anéis

Definição 2.2.1. *Sejam $(R, +, \cdot)$ e $(S, +, \cdot)$ anéis com unidades e $\varphi : R \to S$ função. Dizemos que φ é* **homomorfismo de anéis (com unidade)** *se*

(1) $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$

(2) $\varphi(r_1 \cdot r_2) = \varphi(r_1)\varphi(r_2)$

(3) $\varphi(1_R) = 1_S$

para todo $r_1, r_2 \in R$.

Se a condição (3) não é satisfeito, dizemos que φ é simplesmente um **homomorfismo de anéis**.

Dizemos que $\varphi : R \to S$ é **isomorfismo** *se φ for homomorfismo que é injetora e tal que $Im(\varphi) = S$. Neste caso dizemos que R e S são* **isomorfos.**

Observação. *Se $\varphi : (R, +, \cdot) \to (S, +, \cdot)$ é um homomorfismo de anéis então $\varphi : (R, +) \to (S, +)$ é um homomorfismo de grupos.*

Exemplo 2.2.1.

(a) Seja $\varphi : \mathbb{Z} \to \mathbb{Z}_m$, $\varphi(x) = \overline{x}$, classe de x mod m. Então φ é um homomorfismo de anéis com unidade.

(b) Seja $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $\varphi(x, y) = x$. Então φ é um homomorfismo de anéis com unidade.

(c) Seja $\varphi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$, $\varphi\left(a + b\sqrt{2}\right) = a - b\sqrt{2}$ para todo $a, b \in \mathbb{Q}$. Então φ é um isomorfismo de anéis.

(e) Seja $g \in M_2(\mathbb{R})$ tal que g^{-1} existe. Então $M_2(\mathbb{R}) \to M_2(\mathbb{R})$, $\varphi(A) = gAg^{-1}$ para todo $A \in M_2(\mathbb{R})$, então φ é um isomorfismo de anéis.

(f) Seja $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $\varphi(x, y) = x - y$ para todo $x, y \in \mathbb{Z}$. Então φ não é um homomorfismo de anéis, pois, por exemplo,

$$\varphi((1,1)(1,2)) = \varphi(1,2) = 1 + 2 = 3 \quad \textit{mas} \quad \varphi(1,1)\varphi(1,2) = (1+1)(1+2) = 6.$$

(g) Seja $\varphi : \mathbb{Z}_2 \to \mathbb{Z}_{10}$, $\varphi(0) = 0$, $\varphi(1) = 5$. Então φ é um homomorfismo de anéis, mas não é um homomorfismo de anéis com unidade pois $\varphi(1) \neq 1$.

Proposição 2.2.1. *Seja $\varphi : R \to S$ um homomorfismo de anéis com unidade. Então*

(a) $\varphi(0_R) = 0_S$,

(b) $\varphi(-r) = -\varphi(r)$ para todo $r \in R$,

(c) $\varphi(r_1 - r_2) = \varphi(r_1) - \varphi(r_2)$ para todo $r_1, r_2 \in R$,

(d) se $r \in \mathbb{U}(R)$ então $\varphi(r) \in \mathbb{U}(S)$ e $\varphi(r^{-1}) = [\varphi(r)]^{-1}$

(e) Se $\varphi : R \to S$ é um isomorfismo de anéis, então $\varphi^{-1} : S \to R$ é também um isomorfismo.

Demonstração.

(a) Como $0_R + 0_R = 0_R$, $\varphi(0_R) + \varphi(0_R) = \varphi(0_R)$. Então como S é um anel, $\exists\, -\varphi(0_R) \in S$. Somando $-\varphi(0_R)$ em cada lado temos que

$$\begin{aligned} \varphi(0_R) + \varphi(0_R) + (-\varphi(0_R)) &= \varphi(0_R) + (-\varphi(0_R)) \\ \varphi(0_R) + 0_S &= 0_S \\ \varphi(0_R) &= 0_S \end{aligned}$$

(b) Seja $r \in R$. Então $r + (-r) = -r + r = 0_R$, temos que

$$\varphi(r) + \varphi(-r) = \varphi(-r) + \varphi(r) = \varphi(0_R) = 0_S$$

(c) Sejam $r_1, r_2 \in R$. Então

$$\varphi(r_1 - r_2) = \varphi(r_1 + (-r_2)) = \varphi(r_1) + \varphi(-r_2) = \varphi(r_1) - \varphi(r_2).$$

(d) Seja $r \in \mathbb{U}(R)$. Então existe $r^{-1} \in R$ tal que $r \cdot r^{-1} = r^{-1} \cdot r = 1_R$. Então como φ é um homomorfismo de anéis temos que

$$\varphi(r) \cdot \varphi(r^{-1}) = \varphi(r^{-1}) \cdot \varphi(r) = \varphi(1_R) = 1_S.$$

Portanto $\varphi(r)$ possui um inverso multiplicativo e ele é $\varphi(r^{-1})$.

(e) Suponha que $s_1, s_2 \in S$. Então $s_1 = \varphi(r_1)$ e $s_2 = \varphi(r_2)$ para alguns $r_1, r_2 \in R$. Portanto

$\varphi^{-1}(s_1 + s_2) = \varphi^{-1}\Big(\varphi(r_1) + \varphi(r_2)\Big) = \varphi^{-1}\Big(\varphi(r_1 + r_2)\Big) = r_1 + r_2 = \varphi^{-1}(s_1) + \varphi^{-1}(s_2)$

e

$\varphi^{-1}(s_1 s_2) = \varphi^{-1}\Big(\varphi(r_1)\varphi(r_2)\Big) = \varphi^{-1}\Big(\varphi(r_1 r_2)\Big) = r_1 r_2 = \varphi^{-1}(s_1)\varphi^{-1}(s_2)$.

Portanto φ^{-1} é também um isomorfismo de anéis.

■

Definição 2.2.2. (Núcleo e imagem). *Seja $\varphi : R_1 \to R_2$ um homomorfismo de anéis. Definimos o* **núcleo** *de φ por*

$$Nuc(\varphi) := \{x \in R_1 : \varphi(x) = 0\}$$

e a **imagem** *de φ por*

$$Im(\varphi) = \{f(x) \mid x \in R_1\}$$

Teorema 2.2.2. *Seja $\varphi : R \to S$ um homomorfismo de anéis com unidade. Então*

(a) $Im(\varphi)$ é um subanel de S.

(b) $Nuc(\varphi)$ é um ideal de R.

Demonstração.

(a) Como $\varphi(0) = 0$, temos que $0 \in Im(\varphi)$.

Agora sejam $x, y \in Im(\varphi)$. Então existem $x', y' \in R$ tais que $\varphi(x') = x$ e $\varphi(y') = y$. Portanto

$$x - y = \varphi(x') - \varphi(y') = \varphi(x' - y') \in Im(\varphi),$$

$$xy = \varphi(x')\varphi(y') = \varphi(x'y') \in Im(\varphi).$$

Portanto $Im(\varphi)$ é um subanel de S.

(b) Sabemos que $Nuc(\varphi)$ é um subgrupo de $(R, +)$. Agora, se $r \in R$ e $n \in Nuc(\varphi)$, então

$$\varphi(rn) = \varphi(r)\varphi(n) = \varphi(r)\varphi(0) = 0 \quad \text{e}$$

$$\varphi(nr) = \varphi(n)\varphi(r) = 0\varphi(r) = 0$$

que mostra que rn e $nr \in Nuc(\varphi)$ para todo $r \in R$ e $n \in Nuc(\varphi)$.

■

2.2.2 Anel quociente

Definição 2.2.3. *Seja I um ideal de um anel R. Seja $a \in R$. Definimos a classe lateral de a sendo o conjunto*

$$r + I = \{a + x,\ x \in I\}$$

Proposição 2.2.3. *Seja I um ideal de um anel R. Para qualquer $a, b \in R$ temos que*

$$(a + I) \cap (b + I) = \emptyset \quad ou \quad a + I = b + I$$

Além disto $a + I = b + I \Leftrightarrow a - b \in I$.

Demonstração. Mesmo no caso de grupos.

■

Definição 2.2.4. *Sejam R um anel e I um ideal. O anel quociente R/I é definido por*

$$R/I := \{a + I :\ a \in R\}$$

com as operações

$$(a + I) + (b + I) := (a + b) + I \quad e$$

$$(a + I) \cdot (b + I) := (ab) + I.$$

Teorema 2.2.4. *O anel quociente R/I é de fato um anel.*

Demonstração. Observe que com $(R, +)$ é um grupo abeliano, temos que $I \subset R$ é um subgrupo normal de $(R, +)$. Logo $\left(R/I, +\right)$ é um grupo abeliano.
Portanto precisamos provar que a definição do produto $\cdot$ em R/I é bem definida. Isto é o

resultado do produto não depende das escolhas de a e b nas respectivas classes laterais. Isto é vamos provar que : se $a, b, a', b' \in R$ com

$$a + I = a' + I \quad \text{e} \quad b + I = b' + I \text{ então } ab + I = a'b' + I.$$

Pelo Proposição 2.2.3 temos que

$$i := a - a' \in I \quad \text{e} \quad j := b - b' \in I.$$

Portanto,

$$\begin{aligned} ab &= (a' + i)(b' + j) \\ &= a'b' + \underbrace{ib' + a'j + ij}_{\in I} \end{aligned}$$

Agora $i, j \in I$ e portanto $ib',\ a'j,\ ij \in I$, pois I é um ideal. Portanto $ab - a'b' \in I \Rightarrow ab + I = a'b' + I$.
Portanto o produto $\cdot$ é bem definida.
Deixamos como exercício a provar da associatividade do produto $\cdot$ e das leis distributivas. ■

Teorema 2.2.5. (Primeiro Teorema do Isomorfismo). *Sejam R e S anéis e $\varphi : R \to S$ um homomorfismo. Então a aplicação*

$$\overline{\varphi} : R/(Nuc(\varphi)) \to Im(\varphi), \quad \overline{\varphi}\Big(r + Nuc(\varphi)\Big) = \varphi(r)$$

é um isomorfismo de anéis. Em particular,

$$R/(Nuc(\varphi)) \cong Im(\varphi).$$

Demonstração. Já vimos que $\overline{\varphi} : R/(Nuc(\varphi)) \to Im(\varphi)$ é um isomorfismo de grupos (aditivo).

Portanto só faltar provar que $\overline{\varphi}$ preserva o produto. Suponha que $r_1, r_2 \in R$. Agora

$$\begin{aligned}\overline{\varphi}\Big(r_1 + Nuc(\varphi)\Big)\,\overline{\varphi}\Big(r_2 + Nuc(\varphi)\Big) &= \varphi(r_1)\varphi(r_2)\\ &= \varphi(r_1 r_2)\\ &= \overline{\varphi}\Big(r_1 r_2 + Nuc(\varphi)\Big)\\ &= \overline{\varphi}\Big(((r_1 + Nuc(\varphi))\,((r_2 + Nuc(\varphi))\Big)\end{aligned}$$

Portanto $\overline{\varphi}$ é um homomorfismo de anéis. Como aplicação é uma bijeção, temos uma isomorfismo de anéis.

■

2.2.3 Exercícios Resolvidos

Exercício 2.2.1. *Considere o anel de inteiros de Gauss*

$$\mathbb{Z}[i] = \{a + bi,\ \ i = \sqrt{-1},\ \ a, b \in \mathbb{Z}\}\ \ e\ \ I\ \ o\ ideal\ \ I =< 1 + 2i >= (1 + 2i)\mathbb{Z}[i].$$

Mostre que

$$\varphi : \mathbb{Z}[i] \to \mathbb{Z}_5 \quad \varphi(a + ib) = [a + 2b]_5$$

é um homomorfismo de anéis com unidade. Deduza que o anel quociente $\mathbb{Z}[i]/I$ *é isomorfo a* $\mathbb{Z}_5$.

Solução.

- *Vamos provar que φ é um homomorfismo de anéis. Sejam $a + ib,\ \ c + id \in \mathbb{Z}[i]$. Então*

$$\begin{aligned}\varphi\Big((a + ib) + (c + id)\Big) &= \varphi\Big((a + c) + i(b + d)\Big)\\ &= [a + c + 2(b + d)]_5\\ &= [a + 2b]_5 + [c + 2d]_5\\ &= \varphi(a + ib) + \varphi(c + id)\end{aligned}$$

$$\begin{aligned}\varphi\Big((a+ib)(c+id)\Big) &= \varphi\Big((ac-bd)+i(ad+bc)\Big)\\ &= [ac-bd+2(ad+bc)]_5\\ &= [c(a+2b)+2d(a-\frac{1}{2}b)]_5\end{aligned}$$

Em $\mathbb{Z}_5$, temos que o inverso multiplicativo de 2 é 3 cujo inverso aditivo é 2, ou seja $-\frac{1}{2}=2$. Portanto,

$$\begin{aligned}\varphi\Big((a+ib)(c+id)\Big) &= \varphi\Big((ac-bd)+i(ad+bc)\Big)\\ &= [ac-bd+2(ad+bc)]_5\\ &= [c(a+2b)+2d(a-\frac{1}{2}b)]_5\\ &= [c(a+2b)+2d(a+2b)]_5\\ &= [(a+2b)(c+2d)]_5\\ &= [(a+2b)]_5[(c+2d)]_5\\ &= \varphi(a+ib)\cdot\varphi(c+id)\end{aligned}$$

E temos que $\varphi(1)=\varphi(1+0i)=1$
Portanto φ é um homomorfismo de anéis com unidade.

- *Vamos provar que φ é sobrejetora com $Nuc(\varphi)=I$.*

  Dado $d\in\mathbb{Z}_5$, temos que $d+5di\in\mathbb{Z}[i]$ e $\varphi(d+5di)=[d+2(5d)]_5=[11d]_5=d$. Portanto φ é sobrejetora.

  Seja $a+ib\in Nuc(\varphi)$. Então $a+2b=5k$ para algum $k\in\mathbb{Z}$, ou $a=5k-2b$. Temos que

$$\begin{aligned}a+ib &= (5k-2b+ib)\\ &= 5k+ib(1+2i)\\ &= (1+2i)(1-2i)k+ib(1+2i)\\ &= \Big(1+i(b-2k)\Big)(1+2i)\in<1+2i>\end{aligned}$$

Portanto $Nuc(\varphi)=<1+2i>=I$. Portanto pelo 1^o teorema de isomorfismo

$$\mathbb{Z}[i]/Nuc(\varphi)=\mathbb{Z}[i]/_I\cong\mathbb{Z}_5.$$

Exercício 2.2.2. *Seja $R = \mathbb{Z}[\sqrt{n}]$ e I o ideal $I =< \sqrt{n} >$. Mostre que $R/I \cong \mathbb{Z}_n$.*

Solução. *Defina $\varphi : \mathbb{Z}[\sqrt{n}] \to \mathbb{Z}_n$ por*

$$\varphi(a + b\sqrt{n}) = a \ (mod\ n)$$

- *φ é um homomorfismo de anéis (verifique)*
- *φ é sobrejetora, isto é $Im(\varphi) = \mathbb{Z}_n$*
- *$a + b\sqrt{n} \in Nuc(\varphi) \Leftrightarrow a \equiv 0 \ \ (mod\ n) \Leftrightarrow a = qn,\ q \in \mathbb{Z}$. Portanto*

$$Nuc(\varphi) = \{qn + b\sqrt{n},\ \ q, b \in \mathbb{Z}\} = \{\sqrt{n}(b + q\sqrt{n})\} =< \sqrt{n} >= I.$$

Portanto pelo 1^o teorema de isomorfismo

$$\mathbb{Z}[\sqrt{n}]/Nuc(\varphi) = \mathbb{Z}[\sqrt{n}]/I \cong \mathbb{Z}_n.$$

Exercício 2.2.3. *Considere o anel $\mathbb{Z}_6 \times \mathbb{Z}_6 = \{(\overline{a}, \overline{b});\ \overline{a},\ \overline{b} \in \mathbb{Z}_6\}$, cujas operações $+$ e $\cdot$ são definidas por:*

$$(\overline{a_1},\ \overline{b_1}) + (\overline{a_2},\ \overline{b_2}) = (\overline{a_1 + a_2},\ \overline{b_1 + b_2})$$
$$(\overline{a_1},\ \overline{b_1}) \cdot (\overline{a_2},\ \overline{b_2}) = (\overline{a_1 \cdot a_2},\ \overline{b_1 \cdot b_2})$$

(a) Prove que a função

$$\begin{array}{rccc} \varphi & : & \mathbb{Z}_6 \times \mathbb{Z}_6 & \longrightarrow & \mathbb{Z}_6 \times \mathbb{Z}_6 \\ & & (\overline{a},\ \overline{b}) & \longmapsto & (3\overline{a},\ 4\overline{b}) \end{array}$$

é um homomorfismo de anéis.

(b) Determine o núcleo $N(\varphi)$, e a imagem, $Im(\varphi)$, de φ.

(c) Construa a tabela da operação $\cdot$ de $Im(\varphi)$ e determine as unidades (elementos invertíveis) e os divisores de zero desse anel.

(d) Determine o número de elementos do anel quociente $(\mathbb{Z}_6 \times \mathbb{Z}_6)/N(\varphi)$
(Sugestão: aplique o Teorema Fundamental do Homomorfismo)

Solução.

(a) Sejam $(\overline{a}, \overline{b}),\ (\overline{c}, \overline{d}) \in \mathbb{Z}_6 \times \mathbb{Z}_6$. Temos

- $\varphi\Big((\overline{a},\overline{b})+(\overline{c},\overline{d})\Big)=\varphi\Big((\overline{a+c},\ \overline{b+d})\Big)=\Big(\overline{3(a+c)},\ \overline{4(b+d)}\Big)=(\overline{3a}+\overline{3c},\ \overline{4b}+\overline{4d})=$
  $=(\overline{3a},\overline{4b})+(\overline{3c},\ \overline{4d})=\varphi\Big((\overline{a},\overline{b})\Big)+\varphi\Big((\overline{c},\overline{d})\Big)$
- $\varphi\Big((\overline{a},\overline{b})\cdot(\overline{c},\overline{d})\Big)=\varphi\Big((\overline{a\cdot c},\ \overline{b\cdot d})\Big)=\Big(\overline{3(a\cdot c)},\ \overline{4(b\cdot d)}\Big)=\Big(\overline{9(a\cdot c)},\ \overline{16(b\cdot d)}\Big)=(\overline{3a}\cdot\overline{3c},\ \overline{4b}\cdot\overline{4d})=$
  $=(\overline{3a},\overline{4b})\cdot(\overline{3c},\ \overline{4d})=\varphi\Big((\overline{a},\overline{b})\Big)\cdot\varphi\Big((\overline{c},\overline{d})\Big)$
  pois $9\equiv 3\ (mod\ 6)$ *e* $16\equiv 4\ (mod\ 6)$

Portanto φ *é homomorfismo de anéis.*

(b)

- *Temos que* $3a\equiv 4b\equiv 0\ (mod\ 6)\Leftrightarrow a\in\{0,2,4\}$ *e* $b=\{0,3\}$. *Logo*

$$(\overline{3a},\overline{4b})=(\overline{0},\overline{0})\Leftrightarrow\{\overline{a},\overline{b}\}=\{(\overline{0},\overline{0}),(\overline{0},\overline{3}),(\overline{2},\overline{0}),(\overline{2},\overline{3}),(\overline{4},\overline{0}),(\overline{4},\overline{3})\}=N(\varphi)$$

- *Se* $a,b\in\{0,1,2,3,4,5\}$ *então* $\overline{3a}\in\{\overline{0},\overline{3}\}$ *e* $\overline{4b}\in\{\overline{0},\overline{2},\overline{4}\}$. *Portanto*

$$Im(\varphi)=\{(\overline{0},\overline{0}),(\overline{3},\overline{0}),(\overline{0},\overline{2}),(\overline{3},\overline{2}),(\overline{0},\overline{4}),(\overline{3},\overline{4})\}$$

(c) A tabela da operação $\cdot$ *de* $Im(\varphi)$ *é:*

$\cdot$	$(\overline{0},\overline{0})$	$(\overline{3},\overline{0})$	$(\overline{0},\overline{2})$	$(\overline{3},\overline{2})$	$(\overline{0},\overline{4})$	$(\overline{3},\overline{4})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$
$(\overline{3},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{3},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{3},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{3},\overline{0})$
$(\overline{0},\overline{2})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{4})$	$(\overline{0},\overline{4})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{2})$
$(\overline{3},\overline{2})$	$(\overline{0},\overline{0})$	$(\overline{3},\overline{0})$	$(\overline{0},\overline{4})$	$(\overline{3},\overline{4})$	$(\overline{0},\overline{2})$	$(\overline{3},\overline{2})$
$(\overline{0},\overline{4})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{4})$	$(\overline{0},\overline{4})$
$(\overline{3},\overline{4})$	$(\overline{0},\overline{0})$	$(\overline{3},\overline{0})$	$(\overline{0},\overline{2})$	$(\overline{3},\overline{2})$	$(\overline{0},\overline{4})$	$(\overline{3},\overline{4})$

Observando a tabela acima verificamos que as unidades (os elementos inversíveis) de $Im(\varphi)$ *são* $(\overline{3},\overline{4})$ *e* $(\overline{3},\overline{2})$ *pois* $(\overline{3},\overline{4})\cdot(\overline{3},\overline{4})=(\overline{3},\overline{4})$ *e* $(\overline{3},\overline{2})\cdot(\overline{3},\overline{2})=(\overline{3},\overline{4})$ *e* $(\overline{0},\overline{4}),(\overline{3},\overline{0})$ *são divisores de zero.*

(d) Aplicando o Teorema Fundamental do Homomorfismo obtemos

$$(\mathbb{Z}_6\times\mathbb{Z}_6)\Big/_{N(\varphi)}\approx Im(\varphi)=Im(\varphi)=\{(\overline{0},\overline{0}),(\overline{3},\overline{0}),(\overline{0},\overline{2}),(\overline{3},\overline{2}),(\overline{0},\overline{4}),(\overline{3},\overline{4})\}$$

Como um isomorfismo é uma função bijetora e $Im(\varphi)$ tem 6 elementos $\mathbb{Z}_6 \times \mathbb{Z}_6$ também possui 6 elementos.

Exercício 2.2.4. *(a) Prove que a função*

$$\begin{array}{rccc} \varphi & : & \mathbb{Z}_{30} & \longrightarrow & \mathbb{Z}_{30} \\ & & \overline{k} & \longmapsto & \overline{6k} \end{array}$$

é um homomorfismo de anéis.

(b) Determine o núcleo $N(\varphi)$, e a imagem, $Im(\varphi)$, de φ.

(c) Determine os elementos do anel quociente $\mathbb{Z}_{30}/N(\varphi)$

(d) Prove que o anel $\mathbb{Z}_{30}/N(\varphi)$ é isomorfo ao ideal $I = \{\overline{0},\ \overline{6},\ \overline{12},\ \overline{18},\ \overline{24}\}$ de $\mathbb{Z}_{30}$. (Sugestão: aplique o Teorema Fundamental do Homomorfismo)

Solução.

(a) Sejam $\overline{m},\ \overline{n} \in \mathbb{Z}_{30}$. Temos

- $\varphi(\overline{m} + \overline{n}) = \overline{6(m+n)} = \overline{6m + 6n} = \overline{6m} + \overline{6n} = \varphi(\overline{m}) + \varphi(\overline{n})$
- $\varphi(\overline{m} \cdot \overline{n}) = \overline{6(m \cdot n)} = \overline{36(m \cdot n)} = \overline{6m \cdot 6n} = \overline{6m} \cdot \overline{6n} = \varphi(\overline{m}) \cdot \varphi(\overline{n})$
  pois $36 \equiv 6$ (*mod* 30)

Portanto φ é homomorfismo de anéis.

(b) Seja $\overline{m} \in N(\varphi)$. Temos

$\varphi(m) = \overline{6m} = \overline{0} \Rightarrow 6m \equiv 0$ (*mod* 30)

$\Rightarrow m \equiv 0$ (*mod* 5) $\Rightarrow m = 0, 5, 10, 15, 20, 25$

Logo, $N(\varphi) = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}, \overline{25}\}$

(c) $\varphi(\overline{1}) = \varphi(\overline{6}) = \varphi(\overline{11}) = \varphi(\overline{16}) = \varphi(\overline{21}) = \varphi(\overline{26}) = \overline{6}$

$\varphi(\overline{2}) = \varphi(\overline{7}) = \varphi(\overline{12}) = \varphi(\overline{17}) = \varphi(\overline{22}) = \varphi(\overline{27}) = \overline{6}$

$\varphi(\overline{3}) = \varphi(\overline{8}) = \varphi(\overline{13}) = \varphi(\overline{18}) = \varphi(\overline{23}) = \varphi(\overline{28}) = \overline{6}$

$\varphi(\overline{4}) = \varphi(\overline{9}) = \varphi(\overline{14}) = \varphi(\overline{19}) = \varphi(\overline{24}) = \varphi(\overline{29}) = \overline{6}$

Portanto , $Im(\varphi) = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}\}$

(d) Há 5 classes de equivalência determinadas por $\equiv$ (*mod* $N(\varphi)$)

$\overline{v} = \overline{0} + N(\varphi),\quad \overline{w} = \overline{1} + N(\varphi),\quad \overline{x} = \overline{2} + N(\varphi),\quad \overline{y} = \overline{3} + N(\varphi),\quad \overline{z} = \overline{4} + N(\varphi)$

(e) Aplicando o Teorema Fundamental do Homomorfismo obtemos

$$\mathbb{Z}_{30}\Big/_{N(\varphi)} \approx Im(\varphi) = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}\}$$

Exercício 2.2.5. *Considere o anel $(\mathbb{Z}\times\mathbb{Z},\ \oplus,\ \odot)$ cujas operações $\oplus$ e $\odot$ são definidas por:*

$$(a,\ b)\oplus(c,\ d) = (a+c,\ b+d)$$
$$(a,\ b)\odot(c,\ d) = (0,\ bd)$$

(a) Prove que a função

$$\begin{array}{rccc} \varphi & : & \mathbb{Z}\times\mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & & (a,\ b) & \longmapsto & b \end{array}$$

é um homomorfismo de anéis.

(b) Determine o núcleo $N(\varphi)$, e a imagem, $Im(\varphi)$, de φ.

(c) Prove que $(\mathbb{Z}\times\mathbb{Z})\Big/_{\{(a,0),\ a\in\mathbb{Z}\}} \approx \mathbb{Z}$

(Sugestão: aplique o Teorema Fundamental do Homomorfismo)

Solução.

(a) Sejam $(a,b),\ (c,d)\in\mathbb{Z}\times\mathbb{Z}$. Temos

- $\varphi\Big((a,b)\oplus(c,d)\Big) = \varphi(a+c, b+d) = b+d = \varphi(a,b)+\varphi(c,d)$
- $\varphi\Big((a,b)\odot(c,d)\Big) = \varphi(0,bd) = bd = \varphi(a,b)\odot\varphi(c,d)$

Portanto φ é homomorfismo de anéis.

(b)

- *Seja $(a,b)\in N(\varphi)$. Então $\varphi(a,b) = b = 0$*
  Logo, $N(\varphi) = \{(a,0)|\ a\in\mathbb{Z}\}$
- *Seja $b\in\mathbb{Z}$. Temos que $\varphi(0,b) = b$. Portanto φ é sobrejetora, isto é a imagem de φ é $\mathbb{Z}$.*

(c) Vimos nos ítens b) e c) que $N(\varphi) = \{(a,0)|a\in\mathbb{Z}\}$ e que φ é um homomorfismo sobrejetora, isto é $Im(\varphi) = \mathbb{Z}$. Assim, o resulta do Teorema Fundamental do Homomorfismo que

$$(\mathbb{Z}\times\mathbb{Z})\Big/_{\{(a,0),\ a\in\mathbb{Z}\}} \approx \mathbb{Z}$$

Exercício 2.2.6.

(a) Se $\varphi : \mathbb{Q} \longrightarrow \mathbb{Q}$ *é um homomorfismo, prove que ou* $\varphi(1) = 0$ *e* $\varphi(x) = 0 \ \ \forall x \in \mathbb{Q}$ *(homomorfismo trivial) ou* $\varphi(1) = 1$ *e* φ *é injetivo.*

(b) Se $\varphi : \mathbb{Q} \longrightarrow \mathbb{Q}$ *é um homomorfismo não trivial e* $n \in \{1, 2, \cdots\}$*, prove que* $\varphi\left(\frac{1}{n}\right) = \frac{1}{n}$.

Solução.

(a) Temos $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) \Rightarrow \varphi(1)\Big(\varphi(1) - 1\Big) = 0 \Rightarrow \varphi(1) = 0$ *ou* $\varphi(1) = 1$.

- $\varphi(1) = 0$ *temos* $\varphi(x) = \varphi(x \cdot 1) = \varphi(x) \cdot \varphi(1) = \varphi(x) \cdot 0 = 0 \ \ \forall\, x \in \mathbb{Q}$.
- $\varphi(1) = 1$, *seja* $N(\varphi)$, *o núcleo de* φ. *Se mostrarmos que* $N(\varphi) = \{0\}$ *concluiremos que* φ *é injetora. Suponha que exista* $a \in N(\varphi) - \{0\}$. *Temos*
  $0 = \varphi(a)$ *e* $1 = \varphi(1) = \varphi\Big(a \cdot \frac{1}{a}\Big) = \varphi(a) \cdot \varphi\Big(\frac{1}{a}\Big) = 0 \cdot \varphi\Big(\frac{1}{a}\Big) = 0$ *absurdo!!!!*
  Portanto $N(\varphi) = \{0\}$

(b) Se φ *não é trivial, vimos no item (a) que* $\varphi(1) = 1$. *Temos*

$$1 = \varphi(1) = \varphi\Big(\underbrace{\frac{1}{n} + \frac{1}{n} + \cdots \frac{1}{n}}_{n \text{ vezes}}\Big) = \underbrace{\varphi\Big(\frac{1}{n}\Big) + \varphi\Big(\frac{1}{n}\Big) + \cdots \varphi\Big(\frac{1}{n}\Big)}_{n \text{ vezes}} = n\varphi\Big(\frac{1}{n}\Big)$$

Portanto $\varphi\Big(\frac{1}{n}\Big) = \frac{1}{n}$.

Exercício 2.2.7.

(a) Determine todos os homomorfismos $\varphi : 3\mathbb{Z} \longrightarrow 5\mathbb{Z}$

(b) Determine todos os homomorfismos $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$

Solução.

(a) Sejam $\varphi : 3\mathbb{Z} \longrightarrow 5\mathbb{Z}$ *e* $\varphi(3) = k \in 5\mathbb{Z}$. *Temos que*

$\varphi(9) = \varphi(3 + 3 + 3) = \varphi(3) + \varphi(3) + \varphi(3) = k + k + k = 3k$ *e*

$\varphi(9) = \varphi(3 \cdot 3) = \varphi(3) \cdot \varphi(3) = k \cdot k = k^2$ *o que implica que*

$$3k = k^2 \Rightarrow k = 0 \ \ ou \ \ k = 3.$$

Como $3 \notin 5\mathbb{Z}$, *segue que* $k = 0$, *ou seja* $\varphi(3) = 0 \Rightarrow \varphi(3k) = \varphi(3) \cdot \varphi(k) = 0$.

Assim, o único homomorfismo $\varphi : 3\mathbb{Z} \longrightarrow 5\mathbb{Z}$ *é o homomorfismo trivial,*

$$\varphi(k) = 0, \ \ \forall\, k \in 3\mathbb{Z}.$$

(b) Sejam $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ *e* $\varphi(1) = a \in \mathbb{Z}$. *Temos que*
$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) = a \cdot a = a^2$ *o que implica que*

$$a^2 = a \Rightarrow a = 0 \ \ ou \ \ a = 1.$$

- *Se* $a = 0$, *então* $\varphi(k) = \varphi(k \cdot 1) = \varphi(k) \cdot \varphi(1) = 0 \ \forall k \in \mathbb{Z}$.

- *Se* $\varphi(1) = 1$, *obtemos*

$$\varphi(2) = \varphi(1 + 1) = \varphi(1) + \varphi(1) = 1 + 1 = 2$$

$$\varphi(3) = \varphi(2 + 1) = \varphi(2) + \varphi(1) = 2 + 1 = 3$$

$$\varphi(4) = \varphi(3 + 1) = \varphi(3) + \varphi(1) = 3 + 1 = 4$$

Isto nos surge que $\varphi(k) = k \in \{0, 1, 2, 3 \cdots\}$

Vamos provar isto por indução sobre k.

- *Resultado valido para* $k = 0, 1, 2$ *como vimos acima*
- *Suponha que o resultado é valido para k, isto é* $\varphi(k) = k$.
- *Vamos provar que o resultado é valido para* $k + 1$: *Temos que*
  $\varphi(k + 1) = \varphi(k) + \varphi(1) = k + 1$ *por hipótese de indução*
  Portanto $\varphi(k) = k \in \{0, 1, 2, \cdots\}$

$k < 0$, *podemos escrever*
$k = -|k| \Rightarrow 0 = \varphi(0) = \varphi(k + |k|) = \varphi(k) + \varphi(|k|) \Rightarrow \varphi(k) = -\varphi(|k|) = -k$
ou seja $\varphi(k) = k \ \forall k < 0$
Isto implica que $\varphi(k) = k \ \ \forall \ k \in \mathbb{Z}$. *Portanto, os homomorfismos* $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ *são o trivial,* $\varphi(k) = 0$ *e* $\varphi(k) = k$, *identidade em* $\mathbb{Z}$.

Aula 2.3

Ideais primos e Ideais Máximos

Seja R um anel e I um ideal. Queremos saber quando o anel quociente R/I é um domínio de integridade ou um corpo? Vamos ver que isto não depende de R, mas sim depende apenas das propriedades do ideal I.

Definição 2.3.1. (Ideal primo). *Sejam R um anel comutativo e $I \subset R$ um ideal. Dizemos que I é um* ***ideal primo*** *se $I \neq R$ e,*

$$\forall\, a, b \in R,\ ab \in I \Rightarrow a \in I \text{ ou } b \in I$$

Exemplo 2.3.1.

(a) Se R é um domínio de integridade, então $\{0\}$ é um ideal primo.

De fato seja $a, b \in R$ tal que $ab \in \{0\}$. Então

$$ab = 0 \Longrightarrow a = 0 \ \text{ ou } \ b = 0 \quad \text{pois } R \text{ é domínio de integridade}$$

Logo $a \in \{0\}$ ou $b \in \{0\}$. Portanto $\{0\}$ é um ideal primo.

(b) $\mathbb{Z} \times \{0\}$ é um ideal primo de $\mathbb{Z} \times \mathbb{Z}$.

De fato seja $(a, b),\ (c, d) \in \mathbb{Z} \times \mathbb{Z}$ tal que $(a, b)(c, d) \in \mathbb{Z} \times \{0\}$. Então

$$ac \in \mathbb{Z} \quad e \quad bd \in \{0\}$$

Como $\mathbb{Z}$ é um domínio de integridade temos que ou $(a, b) \in \mathbb{Z} \times \{0\}$ ou $(c, d) \in \mathbb{Z} \times \{0\}$.

Portanto $\mathbb{Z} \times \{0\}$ *é um ideal primo.*

(c) $2\mathbb{Z} \times \{0\}$ *e* $\{0\} \times \{0\}$ *não são ideais primos de* $\mathbb{Z} \times \mathbb{Z}$.

De fato

- $(1,0)$ *e* $(2,2) \in \mathbb{Z} \times \mathbb{Z}$ *e* $(1,0)(2,2) = (2,0) \in 2\mathbb{Z} \times \{0\}$. *Mas* $(1,0) \notin \mathbb{Z} \times \{0\}$ *nem* $(2,2) \notin \mathbb{Z} \times \{0\}$.
- *Da mesma forma* $(1,0)$ *e* $(0,1) \in \mathbb{Z} \times \mathbb{Z}$ *e* $(1,0)(0,1) = (0,0) \in \{0\} \times \{0\}$. *Mas* $(1,0) \notin \{0\} \times \{0\}$ *nem* $(0,1) \notin \{0\} \times \{0\}$.

(d) Em Z, o ideal

$$< m >= m\mathbb{Z} = \begin{cases} \text{é ideal primo,} & \text{se } m \text{ é um número primo} \\ \\ \text{não é ideal primo,} & \text{se } m \text{ não foi um número primo} \end{cases}$$

De fato se $m = ab$ *com* $a, b > 1$ *então* $ab = m \in m\mathbb{Z}$, *mas* $a, b \notin m\mathbb{Z}$ *e* $m\mathbb{Z}$ *não é ideal primo. Por exemplo,* $< 6 >$ *não é primo, pois*

$$2 \cdot 3 = 6 \in < 6 >, \text{ mas } 2 \notin < 6 >, \text{ e } 3 \notin < 6 > .$$

se $m = p$ *é primo e* $ab \in p\mathbb{Z}$, *então* $p|ab$ *que implica que* $p|a$ *ou* $p|b$. *Então* $ab \in p\mathbb{Z}$ *implica que* $a \in p\mathbb{Z}$ *e* $b \in p\mathbb{Z}$. *Portanto* $p\mathbb{Z}$ *é um ideal primo de* $\mathbb{Z}$.

(e) Em $\mathbb{Z}_{18}$, *os ideais primos são os ideais da forma* $m\mathbb{Z}_{18}$ *onde* m *é um divisor primo de 18. Portanto os ideais primos são* $2\mathbb{Z}_{18}$ *e* $3\mathbb{Z}_{18}$.

Teorema 2.3.1. *Seja R um anel comutativo com unidade e* $I \subsetneq R$ *um ideal.Então*

$$R/I \text{ é um domínio de integridade } \Leftrightarrow I \text{ é primo.}$$

Demonstração. Suponha que I seja um ideal primo de R.
Sejam $(a + I), (b + I) \in R/I$ tais que

$$(a + I)(b + I) = ab + I = I$$

Então temos que $ab \in I$. Como I é primo, temos que $a \in I$ ou $b \in I$, isto é, $a + I = I$ ou $b + I = I$.
Portanto R/I é um domínio de integridade.
Reciprocamente, suponha que R/I seja um domínio de integridade.
Sejam $a, b \in R$ tais que $ab \in I$, isto é

$$(ab) + I = (a + I)(b + I) = I.$$

Por hipótese, $a + I = I$ ou $b + I = I$, ou seja $a \in I$ ou $b \in I$.

■

Exemplo 2.3.2.

(a) Seja R um domínio de integridade. Então $\{0\}$ é um ideal primo. Vimos que $R/\{0\} \cong R$ que é de fato um domínio de integridade.

(b) Seja $\mathbb{Z} \times \{0\}$ um ideal primo de $\mathbb{Z} \times \mathbb{Z}$. Então temos que $(\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times \{0\}) \cong \mathbb{Z}$ que de fato é um domínio de integridade.

(c) Seja n um número composto, então $n\mathbb{Z}$ não é ideal primo e $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ não é um domínio de integridade.

(d) Seja p um primo, então $p\mathbb{Z}$ é um ideal primo e $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ é um domínio de integridade(de fato um corpo)

Definição 2.3.2. (Ideal maximal). *Sejam R um anel comutativo e $M \subset R$ um ideal. Dizemos que M é um **ideal maximal** se $M \neq R$ e não existe ideal N de R tal que $M \subsetneq N \subsetneq R$.*

Vale observar que $M \neq R$ é ideal maximal se, e somente se, para todo ideal N, tal que $M \subset N \subset R$, tenhamos $M = N$ ou $N = R$.

Exemplo 2.3.3.

(a) $\{0\}$ não é ideal maximal de $\mathbb{Z}$, por exemplo

$$\{0\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}.$$

(b) Seja p primo. Então $p\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$. Por exemplo, $5\mathbb{Z} \subset \mathbb{Z}$ é um ideal maximal. De fato se J é um ideal tal que $5\mathbb{Z} \subsetneq J \subset \mathbb{Z}$ então $J = \mathbb{Z}$: vamos mostrar que $1 \in J$. Como $5\mathbb{Z} \subsetneq J$, existe $a \in J$ não divisível por 5. Portanto a e 5 são coprimos e $5n + am = 1$ para alguns $n, m \in \mathbb{Z}$. Portanto $1 \in J$.

(c) Seja m um inteiro positivo composto. Então $m\mathbb{Z}$ não é ideal maximal de $\mathbb{Z}$. Por exemplo $6\mathbb{Z}$ não é maximal pois

$$6\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z} \text{ e também } 6\mathbb{Z} \subset 3\mathbb{Z} \subset \mathbb{Z}.$$

Teorema 2.3.2. *Seja R um anel comutativo com unidade e $M \subsetneq R$ um ideal.Então*

$$R/M \text{ é um corpo } \Leftrightarrow M \text{ é maximal.}$$

Demonstração. Suponha que M seja um ideal maximal de R. Seja $a + M \neq M$ um classe em R/M. Isto equivale a $a \in I$. Considere

$$M + aR = \{x + ay \mid x \in M, y \in R\}$$

Então $M + aR$ é um ideal de R. De fato para qualquer $z \in R$, temos que

$$z(x + ay) = \underbrace{xz}_{\in M} + \underbrace{ayz}_{\in R} \in M + aR.$$

Como M é maximal e $M \subset M + aR$ temos que $M + aR = R$, em particular $1 = x + ay$ para alguns $x \in M, y \in R$. Afirmamos que $M + y$ é o inverso de $M + a$. De fato

$$(a + M)(y + M) = ay + M = 1 - x + M = 1 + M$$

pois $x \in I$. Portanto $a + M$ admite inverso multiplicativo.

Reciprocamente, suponha que R/M seja um corpo. Então $M \neq R$ (pois $0 \neq 1$ in R/M). Suponha que existe um ideal J tal que $M \subseteq J \subsetneq R$. Escolhe $a \in J$, $a \notin I$. Então $a + M \neq M$. Como R/M é um corpo, todo elemento diferente de M tem inverso multiplicativo, ou seja $a + M$ é

inversível. Portanto para todo $b \in R$, temos

$$(a + M)(b + M) = ab + M = 1 + M$$

Portanto $ab - 1 \in M \subset J$ e portanto $1 = ab + x$ para algum $x \in J$. Mas $ab \in J$, pois $a \in J$. Portanto $1 \in J$ e logo pelo Proposição 2.1.5 temos que $J = R$ e M é maximal. ■

2.3.1 Exercícios Resolvidos

Exercício 2.3.1. *Quais dos ideais I são maximal no anel R?*

(a) $I = 7\mathbb{Z}$, $R = \mathbb{Z}$;

(b) $I =< 6 >$, $R = \mathbb{Z}$;

(c) $I =< \sqrt{5} >$, $R = \mathbb{Z}[\sqrt{5}]$;

(d) $I =< \sqrt{6} >$, $R = \mathbb{Z}[\sqrt{6}]$.

Solução.

(a) Como $\mathbb{Z}/_{7\mathbb{Z}} \cong \mathbb{Z}_7$, *que é um corpo, temos que* $7\mathbb{Z} \subset \mathbb{Z}$ *é um ideal maximal.*

(b) Como $\mathbb{Z}/_{< 6 >} \cong \mathbb{Z}_6$, *que não é um corpo, temos que* $< 6 > \subset \mathbb{Z}$ *não é um ideal maximal.*

(c) Como $\mathbb{Z}[\sqrt{5}]/_{< \sqrt{5} >} \cong \mathbb{Z}_5$, *que é um corpo, temos que* $< \sqrt{5} > \subset \mathbb{Z}[\sqrt{5}]$ *é um ideal maximal.*

(d) Como $\mathbb{Z}[\sqrt{6}]/_{< \sqrt{6} >} \cong \mathbb{Z}_6$, *que não é um corpo, temos que* $< \sqrt{6} > \subset \mathbb{Z}[\sqrt{6}]$ *não é um ideal maximal.*

Aula 2.4

Atividade

2.4.1 Atividade das Aulas 2.1, 2.2 e 2.3

1. *Quais dos seguintes conjuntos são subanéis e/ou ideais doa anéis indicados:*

   (a) $A = \{3k : \ k \in \mathbb{Z}\}$ *em* $(\mathbb{Z}, +, \cdot)$

   (b) $B = \{75a + 30b : \ a, b \in \mathbb{Z}\}$ *em* $(\mathbb{Z}, +, \cdot)$

   (c) o conjunto de todos os divisores de zero de $\mathbb{Z}_{14}$ *em* $(\mathbb{Z}_{16}, +, \cdot)$

   (d) Seja $p \in \mathbb{Z}$ *primo e seja* $S = \left\{\frac{a}{b} : \ a, b \in \mathbb{Z}, p \nmid b\right\}$

2. *Definimos em* $\mathbb{R}^2 = \{(a, b) : \ a, b \in \mathbb{R}\}$ *duas novas operações dadas por*

$$(a, b) \oplus (c, d) = (a + c, b + d)$$
$$(a, b) \odot (c, d) = (ac - bd, ad + bc)$$

   (a) Mostre que $\left(\mathbb{R}^2, \ \oplus, \ \odot\right)$ *é um corpo. Qual o zero e qual a identidade? Qual o simétrico de* (a, b)*? Qual o inverso de* (a, b) *quando* (a, b) *não é o zero?*

   (b) Calcule $(0, 1) \odot (0, 1)$*. Mostre que a equação* $x^2 = (0, 1)$ *tem 2 soluções? Quais?*

   (c) Verifique que $(a, b) = (a, 0) \oplus (0, 1) \odot (b, 0)$ *para* $(a, b) \in \mathbb{R}^2$*.*

3. *Seja* $T = \left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \ \middle| \ a, b \in \mathbb{R}\right\} \subset M_2(\mathbb{R})$

   (a) Prove que T é um subanel de $M_2(\mathbb{R})$*.*

   (b) Mostre que $I = \left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \ \middle| \ b \in \mathbb{R}\right\}$ *é um ideal de T.*

4. *(a) Mostre que o conjunto* $I = \{(k, 0);\ k \in \mathbb{Z}\}$ *é um ideal do anel de* $\mathbb{Z} \times \mathbb{Z}$.

   (b) Mostre que o conjunto $T = \{(k, k);\ k \in \mathbb{Z}\}$ *não é um ideal do anel de* $\mathbb{Z} \times \mathbb{Z}$.

   (c) Sejam A, B *anéis. Mostre que se* I *é um ideal de* A *e* J *é um ideal de* B, *então* $I \times J = \{(a, b);\ a \in I, b \in J\}$ *é um ideal de* $A \times B$.

5. *Seja* $B = \{(1 + \sqrt{2})a,\ a \in \mathbb{Z}[\sqrt{2}]\}$, *onde* $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathbb{Z}\}$

   (a) Verifique que $\mathbb{Z}[\sqrt{2}]$ *é um subanel com unidade de* $\mathbb{R}$.

   (b) Verifique se B *é um ideal de* $\mathbb{Z}[\sqrt{2}]$.

6. *Seja* $R = \mathbb{Z}[\sqrt{2}]$. *Determine quais dos subconjuntos de* R *abaixo são subanéis e quais são ideais.*

   (a) $S = \{n\sqrt{2}\ : n \in \mathbb{Z}\}$

   (b) $S = \{2x\ : x \in \mathbb{Z}[\sqrt{2}]\}$

   (c) $S = \{m + n\sqrt{2}\ : m, n \in \mathbb{Z},\ m \text{ é ímpar}\}$

   (d) $S = \{m + n\sqrt{2}\ : m, n \in \mathbb{Z},\ m \text{ é par}\}$

7. *O conjunto* $\left(\mathbb{R}_+, \oplus, \otimes\right)$, *onde*

$$a \oplus b = ab \ \text{ e } \ a \otimes b = a^{\ln b}$$

   é um anel comutativo. Encontre o elemento neutro da soma e da multiplicação e determine o inverso multiplicativo do número $a \neq 1 \in \mathbb{R}_+$.

8. *Considere o anel* $\mathbb{Z} \times \mathbb{Z}$. *Mostre que* $\mathbb{Z} \times \mathbb{Z}$ **não** *é um domínio de integridade apesar de cada fator* $\mathbb{Z}$ *é um domínio de integridade.*

9. *Sejam* A *um anel (comutativo e com unidade) e* $a \in A$.

   (a) Verifique que $I(a) = \{x \in A | x \cdot a = 0_A\}$ *um ideal de* A.

   (b) Calcule $I(a)$ *no caso em que* $A = \mathbb{Z}_{18}$ *e* $a = \overline{3} \in \mathbb{Z}_{18}$.

10. *Sejam* R *um anel e* $a \in R$. *Seja* $S = \{x \in \mathbb{R} \mid ax = 0\}$. *Mostre que* S *é um subanel de* R.

11. *Sejam* R *um anel. O* ***centro*** *de* R *é o conjunto* $Z(R) = \{x \in R \mid ax = xa,\ \forall a \in R\}$. *Prove que* $Z(R)$ *é um subanel de* R.

12. *Mostre que uma unidade num anel* R *divide qualquer elemento de* R.

13. *Seja R um anel com 1 e seja $a, b \in R$. Se a é uma unidade de R e $b^2 = 0$, mostre que $a + b$ é uma unidade de R. (Dica: Considere $(a - b)(a + b)$)*

14. *Seja R um anel. Prove que $a^2 - b^2 = (a+b)(a-b)$ para todo $a, b \in R$ se, e somente se R é comutativa.*

15. *Prove que não existe um domínio de integridade com 4 elementos.*

16. *Um elemento a de um anel é chamado **idempotente** se $a^2 = a$. Prove que os únicos elementos idempotentes num domínio de integridade são 0 e 1.*

17. *Um anel R é dito **booleano,** se todo elemento seu é idempotente. Mostre que todo anel booleano é comutativo.*

18. *Um elemento a de um anel é chamado **nilpotente** se $a^n = 0$, para algum inteiro positiva n. Prove $(1 - a)$ é uma unidade em R. (Dica: Considere $(1 - a)(1 + a + a^2 + \cdots + a^{n-1})$)*

19. *Mostre que os elementos nilpotentes de um anel comutativo forma um subanel.*

20. *Mostre que 0 é o único elemento nilpotente num domínio de integridade.*

21. *Encontre todos os elementos idempotentes, nilpotentes, divisores de zero e unidades de $\mathbb{Z}_6 \times \mathbb{Z}_{12}$.*

22. *Sejam R um domínio de integridade e $a, b \in R$.*

    (a) Se $a^5 = b^5$ e $a^3 = b^3$, prove que $a = b$.

    (b) Se $a^m = b^m$ e $a^n = b^m$, com $mdc(m, n) = 1$ prove que $a = b$.

23. *Determine todos ideais maximal em* (*a*) $\mathbb{Z}_8$ (*b*) $\mathbb{Z}_{10}$ (*c*) $\mathbb{Z}_{12}$ (*d*) $\mathbb{Z}_n$

24. *Em $\mathbb{Z}_m$, determine um inteiro positivo a tal que*

    (a) $< a >=< 2 > + < 3 >$

    (b) $< a >=< 6 > + < 8 >$

    (c) $< a >=< m > + < n >$

    (d) $< a >=< 3 >< 4 >$

    (e) $< a >=< 6 >< 8 >$

    (f) $< a >=< m >< n >$

25. *Seja R um anel comutativo e $|R| = 30$. Se I é um ideal de R e $|I| = 10$, prove que I é ideal maximal.*

26. *Para cada função φ abaixo decida se ela é um homomorfismo de anéis com unidade. Justifique brevemente suas respostas e no caso em que φ é um homomorfismo de anéis, determine o núcleo de φ.*

    (a) $\varphi : \mathbb{Z} \to \mathbb{Z}_6 : \quad m \mapsto m \ (mod\ 6)$,

    (b) $\varphi : \mathbb{Z} \to \mathbb{Z} : \quad m \mapsto m^2$,

    (c) $\varphi : \mathbb{Q}[x] \to \mathbb{Q} : \quad p(x) \mapsto p(3)$,

    (d) $\varphi : \mathbb{Z}_2[x] \to \mathbb{Z}_2[x] : \quad p(x) \mapsto (p(x))^2$.

27. *Defina* $\varphi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}_2$ *por*

$$\varphi(m + n\sqrt{2}) = m \ (mod\ 2)$$

    Assumindo que φ é um homomorfismo com unidade, determine o núcleo $Nuc(\varphi)$, de φ.

28. *(a) Mostre que $R = \{0, 3, 6, 9\}$ é um subanel de $\mathbb{Z}_{12}$. (Dica: use tabelas)*
    R é isomorfo a $\mathbb{Z}_4$?

    (b) Seja $\varphi : A \to \mathbb{R}$ um homomorfismo de anéis, e seja $A' = \{a \in A; \varphi(a) \in \mathbb{Q}(\sqrt{2})\}$. Prove que A' é um subanel de A.

    (c) Seja $f : R \to S$ um homomorfismo de anéis. Se r é um divisor de zero em R, será que $f(r)$ é um divisor de zero em S?

29. *Seja $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ e $H = \{\overline{0}, \overline{3}\}$. Determine o anel quociente $\mathbb{Z}_6/H$ e construa sua tabela.*

30. *Considere a função*

$$\begin{array}{rccc} \varphi & : & \mathbb{Z}_{12} & \longrightarrow & \mathbb{Z}_2 \times \mathbb{Z}_4 \\ & & \overline{n} & \longmapsto & (\overline{n}, \overline{n}) \end{array}$$

    Por exemplo $\varphi(\overline{7}) = (\overline{1}, \overline{3})$.

    (a) Prove que φ é um homomorfismo de anéis.

    (b) Determine o núcleo $N(\varphi)$, e a imagem $Im(\varphi)$, de φ.

    (c) Prove que os anéis $\mathbb{Z}_{12}\big/\{\overline{0}, \overline{4}, \overline{8}\}$ *e* $\left\{(\overline{0}, \overline{0}), (\overline{0}, \overline{2}), (\overline{1}, \overline{1}), (\overline{1}, \overline{3})\right\} \subset \mathbb{Z}_2 \times \mathbb{Z}_4$ *são isomorfos. (Sugestão: aplique o Teorema Fundamental do Homomorfismo)*

31. *Mostre que* $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_{10} \quad \varphi(a + ib) = [a + 3b]_{10}$ *é um homomorfismo de anéis. Deduza que o anel quociente $\mathbb{Z}[i]/ < 1 + 3i >$ é isomorfo a $\mathbb{Z}_{10}$.*

32. *Seja o anel $\mathbb{Z}_{12}$, dos inteiros modulo 12 e considere o ideal*
$H = \{\overline{0},\ \overline{3},\ \overline{6},\ \overline{9}\}$. *Determine o anel quociente $\mathbb{Z}_{12}/H$. Que anel é isomorfo a $\mathbb{Z}_{12}/H$?*

33. *Considere a função*

$$\begin{array}{rccc} \varphi & : & \mathbb{Z}_7 & \longrightarrow & \mathbb{Z}_{28} \\ & & [\overline{a}]_7 & \longmapsto & [8\overline{a}]_{28} \end{array}$$

(a) Prove que φ é um homomorfismo de anéis.

(b) Prove que os anéis $\mathbb{Z}_7$ e $\left\{\overline{0},\ \overline{4},\ \overline{8},\ \overline{12},\ \overline{16},\ \overline{20},\ \overline{24}\right\} \subset \mathbb{Z}_{28}$ são isomorfos.
(Sugestão: aplique o Teorema Fundamental do Homomorfismo)

34. *Considere a função*

$$\begin{array}{rccc} \varphi & : & \mathbb{Z}_{24} & \longrightarrow & \mathbb{Z}_8 \\ & & [\overline{a}]_{24} & \longmapsto & [\overline{a}]_8 \end{array}$$

(a) Prove que φ é um homomorfismo de anéis.

(b) Determine o núcleo de φ, $N(\varphi)$

(c) Prove que φ é sobrejetora

(d) Aplicando o Teorema Fundamental do Homomorfismo, conclua que $\mathbb{Z}_{24}\Big/[\ \overline{0}, \overline{8}, \overline{16}\ ]$ é isomorfo a $\mathbb{Z}_8$.

Aula 2.5

Anéis de Polinômios

Nesta aula apresentamos a estrutura de anel para o conjunto dos polinômios com coeficientes num anel A. Apresentamos algoritmo da divisão para polinômios em $A[x]$, onde A é um corpo. Estudamos irredutibilidade de polinômios.

Definição 2.5.1. *Seja R um anel comutativo e seja $R[x]$ denota todos os polinômios na variável x com coeficientes em R, ou seja,*

$$R[x] = \{f(x) = a_0 + a_1x + \cdots + a_nx^n \mid n \geq 0,\ a_j \in R,\ \forall j\}.$$

Em $R[x]$ definimos duas operações $+$ e $\cdot$ por: se

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \ \text{ e } \ g(x) = b_0 + b_1x + \cdots + b_mx^m \in R[x]$$

então

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_k + b_k)x^k, \quad \text{onde } k = \max\{n, m\}$$

e

$$f(x) \cdot g(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}, \ \text{ onde } c_j = a_jb_0 + a_{j-1}b_1 + \cdots + a_0b_j$$

Proposição 2.5.1. $(R[x], +, \cdot)$ *é um anel, chamado o* **anel de polinômios** *em uma variável com coeficientes no anel R.*

Demonstração. Exercício

■

Definição 2.5.2. (Grau) *Sejam R um anel e $R[x]$ o anel de polinômios com coeficientes em R. Se $f \in R[x]$, $f \neq 0$, $f = a_0 + a_1x + \cdots + a_nx^n$, com $a_n \neq 0$, então o* **grau** *de f é definido por $\text{grau}(f) = n$ e a_n é dito ser o* **coeficiente dominante ou líder** *de f.*
Em particular, quando o coeficiente líder for igual 1,

$$f(x) = a_0 + a_1x + \cdots + x^n, \quad a_n = 1,$$

dizemos que $f(x)$ é um **polinômio mônico.**

Observação.

(a) O elemento neutro de $R[x]$ é o **polinômio nulo** *(polinômio cujos coeficientes são todos iguais a zero)*

$$0 = 0 + 0x + 0x^2 + \cdots$$

(b) Um polinômio é chamado de **polinômio constante** *se ele é da forma*

$$f(x) = a_0 \quad (com \ \ a_i = 0 \ \ para\ todo \ \ i > 0).$$

(c) R é um subanel de $R[x]$. Os elementos do anel anel R, em $R[x]$, fazem o papel dos polinômios constantes.

(d) Se R_1 e R_2 são anéis e $R_1 \subset R_2$, então $R_1[x] \subset R_2[x]$.

Teorema 2.5.2. *Seja R um anel. Se $f(x), g(x) \in R[x]\backslash\{0\}$, então temos*

(a) $grau(f(x) + g(x)) \leq \max\{grau(f(x)),\ grau(g(x))\}$

(b) $grau(f(x)g(x)) \leq grau(f(x)) + grau(g(x))$

(c) Se R é um domínio de integridade, então $grau(f(x)g(x)) = grau(f(x)) + grau(g(x))$

(d) Se R é um domínio de integridade, então $R[x]$ é também um domínio de integridade.

(e) Se R é um domínio de integridade, então as unidades de $R[x]$ são as unidades de R, ou seja $U(R[x]) = U(R)$. Em particular se $R = K$ um corpo então $U(K[x]) = K\backslash\{0\} \neq K[x]\backslash\{0\}$. Isto é, se K é um corpo, não necessariamente que $K[x]$ seria um corpo.

Demonstração. Se $f = a_0 + a_1x + \cdots + a_nx^n$, com $a_n \neq 0$, e $g = b_0 + b_1x + \cdots + b_mx^m$, com $b_m \neq 0$ e $n \leq m$, então

(a) $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \cdots + b_mx^m$,
o que implica que $\text{grau}(f + g) \leq m = \max\{n, m\}$

(b) $f(x) \cdot g(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$, onde $c_j = a_jb_0 + a_{j-1}b_1 + \cdots + a_0b_j$
ou seja, $\text{grau}(fg) \leq n + m$.

(c) Se R é um domínio de integridade, como $a_n \neq 0$ e $b_m \neq 0$, temos que $c_{n+m} = a_nb_m \neq 0$, o que mostra que $\text{grau}(fg) = n + m = \text{grau}(f) + \text{grau}(g)$.

(d) Em particular, da demonstração do item (c) temos que se $f \neq 0$ e $g \neq 0$, então $fg \neq 0$.

(e) Se $f(x) \in U(R[x])$ então existe $g(x) \in R[x]$ tal que $f(x)g(x) = 1$. Note que neste caso, o lado esquerdo da equação tem grau (n+m) e o lado direto tem grau 0, logo $n = m = 0$ o que implica que $f, g \in R$. Como $fg = 1$, temos que $f \in U(R)$ o que mostra que $U(R[x]) \subseteq U(R)$. A outra inclusão é imediata, portanto $U(R[x]) = U(R)$.

■

Exemplo 2.5.1. *Em $\mathbb{Z}_6[x]$ considere os polinômios $f(x) = 2x^2 + 1$ e $g(x) = 3x^5 + 1$ então o*

produto

$$\begin{aligned} fg &= (2x^2+1)(3x^5+1) \\ &= 6x^6+3x^4+2x^2+1 \\ &= 3x^4+2x^2+1 \end{aligned}$$

Portanto $grau(fg) < grau(f) + grau(g)$.

2.5.1 Divisão de polinômios

Definição 2.5.3. *Seja A um anel comutativo com identidade. Dados $f(x),\ g(x) \in R[x]$, dizemos que $g(x)$ divide $f(x)$ se existe $h(x) \in R[x]$ tal que $f(x) = g(x)h(x)$.*

Teorema 2.5.3. (Algoritmo da Divisão de Euclides). *Sejam K um corpo e $f, g \in K[x],\ g \neq 0$, então existem únicos $q(x), r(x) \in K[x]$ tais que*

$$f(x) = q(x)g(x) + r(x)$$

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

Demonstração. A demonstração pode ser vista em [1].

■

Observação. *Observe que o resultado do Teorema 2.5.3 pode não ser verdadeiro se K não é corpo. Por exemplo*

(a) Em $Z[x]$ não existem polinômios $q(x),\ r(x) \in \mathbb{Z}[x]$ tal que $1 + 3x^2 = q(x)(1 + 2x) + r(x)$.

(b) Em $\mathbb{Z}_4[x]$ temos que

$$2x^3 + 2x^2 + 3x + 3 = q_1(x)(2x^2 + 3) + r_1(x) \quad \text{onde } q_1(x) = x + 1,\ r_1(x) = 0$$

e também

$$2x^3 + 2x^2 + 3x + 3 = q_2(x)(2x^2 + 3) + r_2(x) \quad \textit{onde } q_2(x) = 3x + 1,\ r_2(x) = 2x$$

Logo os $q(x)$ e $r(x)$ não são únicas.

Exemplo 2.5.2. *Determine polinômios $q(x)$ e $r(x)$ tais que $f(x) = g(x)q(x) + r(x)$, e $r(x) = 0$ ou grau $r(x) <$ grau $g(x)$:*

(a) $f(x) = x^4 - 7x + 1, \quad g(x) = 2x^2 + 1 \in \mathbb{Q}[x]$

(b) $f(x) = \overline{4}x^4 + \overline{2}x^3 + \overline{6}x^2 + \overline{4}x + \overline{5}, \quad g(x) = \overline{3}x^2 + \overline{2} \in \mathbb{Z}_7[x]$

(c) $f(x) = \overline{3}x^6 + \overline{2}x^5 + \overline{2}x^4 + \overline{4}x^3 + x^2 - x + \overline{4}, \quad g(x) = \overline{2}x^3 + \overline{4}x^2 - x + \overline{3} \in \mathbb{Z}_5[x]$

(d) $f(x) = \overline{2}x^2 - \overline{4}x + \overline{3}, \quad g(x) = \overline{7}x - \overline{5} \in \mathbb{Z}_8[x]$

Solução. *(a)*

$$\begin{array}{rrl|l}
x^4 & & -7x+1 & 2x^2+1 \\
\cline{4-4}
-x^4 & -\frac{1}{2}x^2 & & \frac{1}{2}x^2 - \frac{1}{4} \\
\cline{1-2}
 & -\frac{1}{2}x^2 & -7x+1 & \\
 & \frac{1}{2}x^2 & +\frac{1}{4} & \\
\cline{2-3}
 & & -7x+\frac{5}{4} &
\end{array}$$

Portanto, $q(x) = \frac{1}{2}x^2 - \frac{1}{4},\ r(x) = -7x + \frac{5}{4}$ *e* $f(x) = q(x)g(x) + r(x)$

(b)

$$\begin{array}{rrrl|l}
4x^4 & +2x^3 & +6x^2 & +4x+5 & 3x^2+2 \\
\cline{5-5}
-4x^4 & & -5x^2 & & 6x^2+3x+5 \\
\cline{1-3}
 & 2x^3 & +x^2 & +4x & \\
 & -2x^3 & & -6x & \\
\cline{2-4}
 & & x^2 & -2x+5 & \\
 & & -x^2 & -3 & \\
\cline{3-4}
 & & & -2x+2 &
\end{array}$$

Portanto, $q(x) = \overline{6}x^2 + \overline{3}x + \overline{5},\ r(x) = \overline{5}x + \overline{2}$ *e* $f(x) = q(x)g(x) + r(x)$

(c)

$$
\begin{array}{rrrrrrr|l}
3x^6 & +2x^5 & +2x^4 & +4x^3 & +x^2 & -x & +4 & 2x^3+4x^2-x+3 \\
\cline{8-8}
-3x^6 & -x^5 & +4x^4 & -2x^3 & & & & 4x^3+3x^2+2x+1 \\
\cline{1-4}
 & x^5 & +x^4 & +2x^3 & +x^2 & & & \\
 & -x^5 & -2x^4 & +3x^3 & -4x^2 & & & \\
\cline{2-5}
 & & 4x^4 & & -3x^2 & -x & & \\
 & & -4x^4 & -3x^3 & +2x^2 & -x & & \\
\cline{3-6}
 & & & 2x^3 & -x^2 & -2x & +4 & \\
 & & & -2x^3 & -4x^2 & +x & -3 & \\
\cline{4-7}
 & & & & & -x & +1 &
\end{array}
$$

Portanto, $q(x) = \overline{4}x^3 + \overline{3}x^2 + \overline{2}x + \overline{1}$, $r(x) = \overline{4}x + \overline{1}$ *e* $f(x) = q(x)g(x) + r(x)$

(d)

$$
\begin{array}{rrr|l}
2x^2 & -4x & +3 & 7x-5 \\
\cline{4-4}
-2x^2 & -2x & & 6x+6 \\
\cline{1-2}
 & 2x & +3 & \\
 & -2x & -2 & \\
\cline{2-3}
 & & 1 &
\end{array}
$$

Portanto, $q(x) = 6x + 6$, $r(x) = 1$ *e* $f(x) = q(x)g(x) + r(x)$

2.5.2 Máximo divisor comum

Definição 2.5.4. *Seja R um anel comutativo com identidade. Dados $f(x), g(x) \in R[x]$, um polinômio $d(x) \in R[x]$ diz-se o máximo divisor comum, MDC($f(x)$, $g(x)$) se*

(1) $d(x)$ divide $f(x)$ e divide $g(x)$

(2) se o polinômio $q(x) \in R[x]$ é outro divisor comum de $f(x)$ e $g(x)$ então $q(x)$ também divide $d(x)$.

Teorema 2.5.4. *Sejam K um corpo e $f(x)$, $g(x) \in K[x]$. Então existe MDC$\big(f(x), g(x)\big)$.*

Demonstração. Exercício ■

Observação. *O MDC quando existe não é único. De fato se $d(x)$ satisfazer as condições (1) e (2) na Definição 2.5.4 e $\lambda \neq 0$ um elemento em K então $\lambda d(x)$ também satisfaz as 2 condições. Muito vezes escolhemos o MDC com $\lambda = c^{-1}$, sendo c o coeficiente dominante ou líder de $d(x)$. Então $c^{-1}d(x)$ é um polinômio mônico.*

Teorema 2.5.5. (Algoritmo do MDC). *Sejam K um corpo, $f(x), g(x) \in K[x]\backslash\{0\}$ tais que $g(x)$ não divide $f(x)$. Seja $r_k(x)$ o ultimo resto não nulo que se obtém aplicando sucessivamente o algoritmo da divisão do modo seguinte:*

$$\begin{cases} f(x) = q(x)g(x) + r(x), & \text{com grau } r(x) < \text{grau } g(x); \\ g(x) = q_1(x)r(x) + r_1(x), & \text{com grau } r_1(x) < \text{grau } r(x); \\ r(x) = q_2(x)r_1(x) + r_2(x), & \text{com grau } r_2(x) < \text{grau } r_1(x); \\ \vdots & \vdots \\ r_{k-2}(x) = q_k(x)r_{k-1}(x) + r_k(x), & \text{com grau } r_k(x) < \text{grau } r_{k-1}(x); \\ r_{k-1}(x) = q_{k+1}(x)r_k(x). & \end{cases}$$

Seja $c \in K$ o coeficiente dominante de $r_k(x)$. Então

$$MDC\Big(f(x), g(x)\Big) = c^{-1}r_k(x).$$

Demonstração. Exercício ■

Exemplo 2.5.3. *Calcule $MDC\Big(f(x), g(x)\Big)$, onde*
$f(x) = \overline{3}x^6 + \overline{2}x^5 + \overline{2}x^4 + \overline{4}x^3 + x^2 - x + \overline{4}$, $g(x) = \overline{2}x^3 + \overline{4}x^2 - x + \overline{3} \in \mathbb{Z}_5[x]$

Solução. *Vamos efetuar as divisões em* $\mathbb{Z}_5[x]$:

$$\begin{array}{r|l}
3x^6 + 2x^5 + 2x^4 + 4x^3 + x^2 - x + 4 & 2x^3 + 4x^2 - x + 3 \\
\cline{2-2}
-3x^6 - x^5 + 4x^4 - 2x^3 & 4x^3 + 3x^2 + 2x + 1 \\
\cline{1-1}
x^5 + x^4 + 2x^3 + x^2 & \\
-x^5 - 2x^4 + 3x^3 - 4x^2 & \\
\cline{1-1}
4x^4 - 3x^2 - x & \\
-4x^4 - 3x^3 + 2x^2 - x & \\
\cline{1-1}
2x^3 - x^2 - 2x + 4 & \\
-2x^3 - 4x^2 + x - 3 & \\
\cline{1-1}
4x + 1 &
\end{array}$$

Portanto

$$f(x) = (4x^3 + 3x^2 + 2x + 1)g(x) + r(x)$$

onde $r(x) = 4x + 1$. *Vamos fazer a divisão de* $g(x)$ *por* $r(x)$.

$$\begin{array}{r|l}
2x^3 + 4x^2 - x + 3 & 4x + 1 \\
\cline{2-2}
-2x^3 - 3x^2 & 3x^2 + 4x \\
\cline{1-1}
+x^2 - x + 3 & \\
-x^2 - 4x & \\
\cline{1-1}
3 &
\end{array}$$

Nota: Observamos que ao atingirmos um resto que é uma constante não nula, alcançamos o último resto não nulo.

Portanto $r_k(x) = 3$. *Logo*

$$MDC\Big(f(x), g(x)\Big) = 3^{-1} \cdot 3 = 1.$$

Teorema 2.5.6. *Seja K um corpo. Dados* $f(x), g(x) \in K[x]\backslash\{0\}$, *o polinômio* $MDC\Big(f(x), g(x)\Big)$ *pode ser escrito na forma* $a(x)f(x) + b(x)g(x)$, *com* $a(x), b(x) \in K[x]$.

Demonstração. Exercício ■

Exemplo 2.5.4. *Em* $\mathbb{Z}_3[x]$, *determine o* $MDC\Big(f(x),\ g(x)\Big)$, *onde* $g(x) = x^3+2x^2+2x+1$, $f(x) = x^4+2$

e expressa sua resposta como uma combinação linear dos polinômios $f(x)$ e $g(x)$.

Solução. *Vamos efetuar as divisões em $\mathbb{Z}_3[x]$:*

$$\begin{array}{r|l} x^4 + 0x^3 + 0x^2 + 0x + 2 & x^3 + 2x^2 + 2x + 1 \\ \hline -x^4 - 2x^3 - 2x - x & x + 1 \\ \hline x^3 + x^2 + 2x + 2 & \\ -x^3 - 2x^2 - 2x - 1 & \\ \hline 2x^2 + 1 & \end{array}$$

Portanto

$$f(x) = (x+1)g(x) + (2x^2+1) \tag{1}$$

Vamos fazer a divisão de $g(x)$ por $2x^2 + 1$.

$$\begin{array}{r|l} x^3 + 2x^2 + 2x + 1 & 2x^2 + 1 \\ \hline -x^3 - 2x & 2x + 1 \\ \hline 2x^2 + 1 & \\ -2x^2 - 1 & \\ \hline 0 & \end{array}$$

Portanto

$$g(x) = (2x+1)(2x^2+1) + 0 \tag{2}$$

Logo

$$MDC\Big(f(x), g(x)\Big) = 2x^2 + 1 \quad e \quad 2x^2 + 1 = f(x) - (x+1)g(x).$$

2.5.3 Raízes de polinômios

Teorema 2.5.7. (Teorema do Resto). *Seja R um domínio de integridade. Se $f(x) \in R[x]$ e $a \in R$, então o resto da divisão de $f(x)$ pelo polinômio $g(x) = x - a$, é $f(a)$.*

Demonstração. Pelo Algoritmo da Divisão, podemos escrever

$$f(x) = q(x)(x-a) + r(x)$$

onde $r(x) = 0$ ou grau$r(x) < 1$. Portanto temos que $r(x)$ é um polinômio constante. Isto é , $r(x) = r$ para algum $r \in R$. Então

$$f(a) = q(a) \cdot (a - a) + r = r.$$

■

Exemplo 2.5.5. *Seja $f(x) = x^3 + 5x - 5 \in \mathbb{R}[x]$. Então*

- *o resto da divisão de $f(x)$ por $x - 2$ é $f(2) = 13$*
- *o resto da divisão de $f(x)$ por $x + 2$ é $f(-2) = -23$.*

Corolário 11. *Se R um domínio de integridade, $f(x) \in R[x]$ e $a \in R$, então $(x - a)$ divide $f(x)$ se e somente se o resto da divisão de $f(x)$ por $(x - a)$ é $f(a) = 0$ isto é $(x - a)$ divide $f(x)$ se, e somente se, $f(x) = (x - a)q(x)$ para algum $q(x) \in R[x]$.*

Demonstração. Dividindo $f(x)$ por $(x - a)$, do teorema do resto, temos que existe $q(x) \in R[x]$ tal que $f(x) = q(x) \cdot (x - a) + f(a)$. Assim, $f(a) = 0$ se, e somente se $f(x) = (x - a)q(x)$. ■

Definição 2.5.5. (Raiz de um polinômio). *Seja R um anel comutativo e $f(x) \in R[x]\backslash\{0\}$. Um elemento $a \in R$ é chamado de **raiz** de $f(x)$ se $f(a) = 0$.*

Exemplo 2.5.6. *As raízes de $x^2 - \overline{1} \in \mathbb{Z}_8$ são $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$.*

Exemplo 2.5.7. *Se $f(x) = x^2 + 5$ então f não tem raízes em $\mathbb{R}$ mas tem 2 raízes em $\mathbb{C}$. De fato*

$$f(x) = (x - i\sqrt{5})(x + i\sqrt{5})$$

portanto $f(\pm i\sqrt{5}) = 0$.

Definição 2.5.6. (Multiplicidade de uma raiz). *Seja R um anel comutativo e $f(x) \in R[x]\backslash\{0\}$. Se $a \in R$ é uma raiz de $f(x)$, dizemos que a tem multiplicidade $m \geq 0$ se $f(x) = (x - a)^m g(x)$ com $g(a) \neq 0$.*

Exemplo 2.5.8. *Determine todas as raízes e suas multiplicidades da* $f(x) = x^3 + \overline{3}x + \overline{4} \in \mathbb{Z}_5[x]$.

Solução. *Determinamos todos os raízes:*

x	0	1	2	3	4
$f(x)$	4	3	3	0	0

Temos que $f(\overline{3}) = \overline{0}$. *Dividendo* $f(x)$ *por* $x - \overline{3}$ *temos que*

$$f(x) = (x - \overline{3})g(x), \quad com \quad g(x) = x^3 + \overline{3}x + \overline{2}.$$

Como $g(\overline{3}) = \overline{0}$, *podemos divide de novo para obtêm*

$$g(x) = (x - \overline{3})(x + \overline{1}).$$

portanto temos que $f(x) = (x - \overline{3})^2(x - \overline{4})$. *Como* $\overline{3}$ *não é raiz de* $x - \overline{4}$, *concluímos que a raiz* $\overline{3}$ *tem multiplicidade 2 e a raiz* $\overline{4}$ *multiplicidade 1.*

Teorema 2.5.8. *Seja* R *um domínio de integridade e* $f(x) \in R[x]\backslash\{0\}$. *Se* $n = grau f(x)$, *então* $f(x)$ *tem no máximo* n *raízes em* R.

Demonstração. Provamos por indução sobre n, os casos $n = 0, 1$ são triviais.
Suponha que grau$f(x) = n+1$. Então, se $f(a) = 0$, temos que $f(x) = (x-a)g(x)$ com grau$g(x) = n$. Se f tem mais do que $(n+1)$ raízes, então temos que $f(a_1) = f(a_2) = \cdots = f(a_{n+1}) = 0$ para algum $a_1, \cdots, a_{n+1} \neq a$ distintos. Então, para $i = 1, \cdots (n+1)$, temos $0 = f(a_i) = (a_i - a)g(a_i)$ e $a_i - a \neq 0$, que implica que $g(a_i) = 0$. Portanto $g(x)$ tem (n+1) raízes, que contradiz o hipótese de indução pois grau $g(x) = n$.

■

Teorema 2.5.9. (Teorema Fundamental da Álgebra). *Sejam* $\mathbb{C}$ *o corpo dos números complexos e* $f(x) \in \mathbb{C}[x]$ *um polinômio não-constante. Então, existe um valor* $\alpha \in \mathbb{C}$ *tal que* $f(\alpha) = 0$, *ou seja,* $f(x)$ *admite raiz complexa.*

Um resultado importante é como determinar as possíveis raízes racionais de um polinômio com coeficientes inteiros.

Teorema 2.5.10. (Teorema das Raízes Racionais). *Sejam* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x]$ *um polinômio de grau* $n \geq 1$ *e* $r = \dfrac{p}{q}$ *uma raiz racional de* $f(x)$ *com* $p, q \in \mathbb{Z}$, $q > 0$ *e* $mdc(p, q) = 1$.
Então, $p \mid a_0$ *e* $q \mid a_n$.

Demonstração. Como $f(p/q) = 0$ temos que

$$a_0 + a_1\left(\frac{p}{q}\right) + a_2\left(\frac{p}{q}\right)^2 + a_3\left(\frac{p}{q}\right)^3 + \cdots + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + a_n\left(\frac{p}{q}\right)^n = 0$$

Multiplicando esta equação por q^n, obtemos

$$a_0q^n + a_1pq^{n-1} + a_2p^2q^{n-2} + \cdots + a_{n-1}p^{n-1}q + a_np^n = 0$$

Portanto

$$\begin{cases} a_0q^n = -p(a_1q^{n-1} + a_2pq^{n-2} + \cdots + a_{n-1}p^{n-2}q + a_np^{n-1}) \\ a_np^n = -q(a_0q^{n-1} + a_1pq^{n-2} + a_2p^2q^{n-3} + \cdots + a_{n-1}p^{n-2}) \end{cases}$$

Portanto $p \mid a_0q^n$ e $q \mid a_np^n$. Como $\text{mdc}(p, q) = 1$ isto implica que $p \mid a_0$ e $q \mid a_n$. ■

Exemplo 2.5.9. *Fatorize o polinômio* $f(x) = 3x^3 - x^2 - x - 4 \in \mathbb{Q}[x]$.

Solução. *Aplicando o Teorema das Raízes Racionais, se* $\alpha = \dfrac{p}{q}$ *for uma raiz racional de* $f(x)$ *com* $mdc(p, q) = 1$, *então*

$$p \mid 4 \ \ e \ \ q \mid 3.$$

Portanto, $p \in \{-4, -2, -1, 1, 2, 4\}$ *e* $q \in \{1, 3\}$. *Logo, os candidatos a raiz racional de* $f(x)$ *são*

$$\alpha = \frac{p}{q} \in \left\{1, -1, -2, 2, 4, -4, \frac{4}{3}, -\frac{4}{3}, \frac{1}{3}, -\frac{1}{3}, \frac{1}{2}, -\frac{1}{2}\right\}.$$

Verificando temos que $x = \dfrac{4}{3}$ *é uma raiz. Pelo divisão de polinômios temos que*

$$f(x) = \left(x - \frac{4}{3}\right)(3x^2 + 3x + 3) = (3x - 4)(x^2 + x + 1).$$

Usando de novo o Teorema das Raízes Racionais, vamos ver que $x^2 + x + 1$ *não tem raízes racionais e portanto não podemos fatoriza mais ele.*

Exemplo 2.5.10. *Fatorize o polinômio* $f(x) = x^4 + 25x + 24 \in \mathbb{Q}[x]$.

Solução. *Como* $f(-1) = 0$, *temos que* $(x + 1)$ *é um fator de* $f(x)$. *Pelo divisão de polinômios temos que*

$$f(x) = (x + 1)(x^3 - x^2 + x - 24).$$

Aplicando o Teorema das Raízes Racionais, qualquer raiz racional de $x^3 - x^2 + x + 24$ *deve pertencer o conjunto*

$$\{\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 8,\ \pm 12,\ \pm 24\}.$$

Verificando temos que nenhum deste números é uma raiz e não podemos fatoriza mais $f(x)$.

Exemplo 2.5.11. *Fatorize o polinômio* $f(x) = 2x^4 - 5x^3 - 2x^2 - 4x + 3 \in \mathbb{C}[x]$.

Solução. *Aplicando o Teorema das Raízes Racionais, se* $\alpha = \dfrac{p}{q}$ *for uma raiz racional de* $f(x)$ *com* $mdc(p, q) = 1$, *então*

$$p \mid 3 \ \ e \ \ q \mid 2.$$

Portanto, $p \in \{-3, -1, 1, 3\}$ *e* $q \in \{1, 2\}$. *Logo, os candidatos a raiz racional de* $f(x)$ *são*

$$\alpha = \frac{p}{q} \in \left\{1, -1, 3, -3, \frac{1}{2}, -\frac{1}{2}, \frac{3}{2}, -\frac{3}{2}\right\}.$$

Agora verificamos estas possibilidades:

$$f(1) = -6 \neq 0, \ \ f(-1) = 12 \neq 0, \ \ f(-3) = 294 \neq 0, \ \ f(3) = 0 \ \ e \ \ f(1/2) = 0.$$

Como 3 *e* $1/2$ *são raízes de* $f(x)$, *temos pelo algoritmo da divisão*

$$\begin{aligned} f(x) &= (2x^2 + 2x + 2)(x - 3)(x - \frac{1}{2}) \\ &= 2\left(x - \frac{-1 - \sqrt{3}i}{2}\right)\left(x - \frac{-1 + \sqrt{3}i}{2}\right)\left(x - 3\right)\left(x - \frac{1}{2}\right) \end{aligned}$$

$$f(x) = (2x^2 + 2x + 2)(x - 3)(x - \frac{1}{2}).$$

2.5.4 Polinômios irredutíveis

Definição 2.5.7. (Polinômio irredutível). *Seja R um domínio de integridade. Um polinômio $f(x) \in R[x]$ é dito* **irredutível sobre** *R, ou* **irredutível em** *$R[x]$ se*

(a) $f(x) \neq 0$ e grau $f(x) \geq 1$ (isto é, $f(x)$ é um polinômio não constante) e

(b) se $f(x) = p(x)q(x)$ em $R[x]$, então ou $p(x)$ é unidade ou $q(x)$ é unidade.

Dizemos que $f(x)$ é **redutível** *em $R[x]$, quando ele não for irredutível, ou seja, se $f(x) = p(x)q(x)$ com $p(x)$ e $q(x)$ não unidades, (isto é f admite fatorização não trivial). Neste caso $p(x)$ e $s(x)$ são chamados de* **fatores** *de f.*

Observação. *Seja K um corpo e pelo Teorema 2.5.2(e) temos que as unidades de $K[x]$ é*

$$U(K[x]) = K - \{0\}.$$

Portanto os elementos associados a $f(x) \in K[x]$ são $\{af(x) : a \in K - \{0\}\}$. Portanto

$$f(x) = ah(x) \quad com \quad a \in K - \{0\} \quad e \quad h(x) \in K[x]$$

é uma fatorização trivial.

Exemplo 2.5.12. *Se $p(x) = 2x + 4 = 2(x + 2)$. Então*

- *$p(x)$ é irredutível sobre $\mathbb{Q}$ pois 2 é uma unidade em $\mathbb{Q}$ mas*
- *$p(x)$ é redutível sobre $\mathbb{Z}$ pois 2 não é uma unidade em $\mathbb{Z}$.*

Definição 2.5.8. *Se K é um corpo, então $f(x) \in K[x]$ é redutível se e somente se existe uma fatorização da forma*

$$f(x) = p(x)q(x) \quad com \quad p(x), q(x) \in K[x], \quad grau\, p(x) \geq 1 \quad e \quad grau\, q(x) \geq 1.$$

Exemplo 2.5.13. *(Irredutibilidade depende do anel R)*

- x^2-2 *é irredutível sobre* $\mathbb{Z}$ *e sobre* $\mathbb{Q}$*, mas redutível sobre* $\mathbb{R}$*, pois* $(x^2-2) = (x-\sqrt{2})(x+\sqrt{2})$ *em* $\mathbb{R}[x]$.
- x^2+2 *é irredutível sobre* $\mathbb{R}$*, mas é irredutível sobre* $\mathbb{C}$ *pois* $x^2+2 = (x-i\sqrt{2})(x+i\sqrt{2})$ *em* $\mathbb{C}[x]$.

Teorema 2.5.11. *Seja K um corpo e seja* $p(x) \in K[x]$*. Se grau* $p(x) = 1$*, então* $p(x)$ *é irredutível sobre K.*

Demonstração. Se $p(x) = a(x)b(x)$ para alguns $a(x), b(x) \in K[x]$, então

$$1 = \text{grau } p(x) = \text{grau } [a(x)b(x)] = \text{grau } a(x) + \text{grau } b(x),$$

pois K é um domínio de integridade.
Como grau $a(x) \geq 0$ e grau $b(x) \geq 0$ temos uns dos graus deve ser 0. Portanto $a(x)$ ou $b(x)$ é um constante não nulo, logo uma unidade pois K é um corpo. Portanto $p(x)$ é irredutível sobre K. ■

Observação. *Note que o resultado acima é falsa se K não é um corpo.*
Por exemplo, $p(x) = 2x + 4 \in \mathbb{Z}[x]$ *é de grau 1, mas* $p(x) = 2(x + 2)$ *e nem* 2 *e* $x + 2$ *é uma unidade em* $\mathbb{Z}$*. Portanto* $p(x)$ *é redutível sobre* $\mathbb{Z}$*.*

De fato, se R é um domínio de integridade que não é um corpo, então existe um elemento $r \neq 0$ *em R que não é uma unidade, e portanto* $f(x) = rx$ *é redutível sobre R.*

Teorema 2.5.12. *Seja K é um corpo e* $f(x) \in K[x]$ *com grau* $f(x) \geq 2$*. Então* $f(x)$ *é irredutível sobre K se* $f(x)$ *não tem raízes em K.*

Demonstração. Se $f(x)$ tem uma raiz $a \in K$, então $f(x) = (x - a)p(x)$ para algum $p(x) \in K[x]$ com grau $p(x) \geq 1$. Como ambos $(x - a)$ e $p(x)$ não são unidades de K, segue que f é redutível. Portanto, se $f(x)$ é irredutível sobre K, então $f(x)$ não tem raízes em K. ■

Teorema 2.5.13. (Teste de redutibilidade para graus 2 e 3). *Se K é um corpo e $f(x) \in K[x]$ com grau $f(x) = 2$ ou 3, então $f(x)$ é irredutível sobre K se, e somente se, $f(x)$ não tem raízes em K.*

Demonstração.

($\Rightarrow$) Segue do teorema acima.

($\Leftarrow$) Se $f(x)$ é redutível, então $f(x) = a(x)b(x)$, onde $a(x),\ b(x) \in K[x]$ não são unidades em K. Como K é um corpo, isto implica que $a(x),\ b(x) \notin K$, e cada um tem grau pelo menos 1. Mas

$$\text{grau } a(x) + \text{grau } b(x) = \text{grau } f(x) = 2 \text{ ou } 3,$$

logo um dos grau $a(x)$, grau $b(x)$ é igual 1.
Portanto, $f(x)$ tem um fator $sx + t \in K[x]$ de grau 1, e a raiz $x = -\dfrac{t}{s} \in K$, pois K é um corpo.
Portanto, se $f(x)$ não tem raízes em F, então $f(x)$ é irredutível sobre K.

■

Exemplo 2.5.14.

(a) O polinômio $x^2 - 2$ é irredutível sobre $\mathbb{Q}$ mas redutível sobre $\mathbb{R}$ pois ele tem uma raiz em $\mathbb{R}$ mas não em $\mathbb{Q}$.

(b) O polinômio $x^2 + 1$ é irredutível sobre $\mathbb{R}$ mas redutível sobre $\mathbb{C}$ pois ele tem uma raiz em $\mathbb{C}$ mas não em $\mathbb{R}$.

(c) O polinômio $x^3 + \overline{2}x^2 + x + \overline{2}$ é irredutível em $\mathbb{Z}_5[x]$ pois ele não tem raízes em $\mathbb{Z}_5$.

(d) O polinômio $x^2 - 2$ é redutível em $\mathbb{R}[x]$ mas irredutível em $\mathbb{Z}_3[x]$.

(e) O polinômio $x^2 + 2$ é irredutível em $\mathbb{R}[x]$ mas redutível em $\mathbb{Z}_3[x]$ (em particular, $x^2 + 2 = (x + 2)(x + 1) \in \mathbb{Z}_3[x]$)

Observação.

- *Se K não é um corpo, então $f(x)$ pode tem um fator de grau 1 mas nenhuma raiz. Por exemplo,*

$$f(x) = 6x^2 - 13x + 6 = (2x - 3)(3x - 2)$$

não tem raízes em $\mathbb{Z}$ mas ela não é irredutível sobre $\mathbb{Z}$.

- *Se grau $f(x) \geq 4$, então $f(x)$ pode ter fatores não constantes mas sem raízes. Por exemplo,*

$$f(x) = x^4 + 3x^2 + 2 = (x^2 + 1)(x^2 + 2)$$

não tem raízes em $\mathbb{Q}$, mas não é irredutível sobre $\mathbb{Q}$.

Exemplo 2.5.15. *Determinar todos os polinômios irredutíveis de grau 2 em $\mathbb{Z}_2[x]$.*

Solução. *Estes polinômios são da forma*

$$x^2 + ax + b, \quad com \;\; a, b \in \mathbb{Z}_2.$$

Como $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ só tem dois elementos, podemos escrever todos estes polinômios:

$$x^2, \quad x^2 + x, \quad x^2 + \overline{1} \quad e \quad x^2 + x + \overline{1}.$$

Isto é só existem 4 polinômios de grau 2 em $\mathbb{Z}_2[x]$. Destes, o unico que não possui raiz em $\mathbb{Z}_2$ é $x^2 + x + \overline{1}$. Assim, $x^2 + x + \overline{1}$ é o único polinômio irredutível de grau 2 em $\mathbb{Z}_2[x]$.

Teorema 2.5.14. *Suponha que $f(x) \in \mathbb{C}[x]$ com grau $f(x) \geq 1$. Se escrever $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_n \neq 0$, então $f(x)$ fatoriza como $f(x) = a_n(x - z_1)(x - z_2)\cdots(x - z_n)$, onde $z_1, \cdots, z_n$ são raízes de $f(x)$. Em particular, as únicas polinômios irredutíveis em $\mathbb{C}[x]$ são lineares.*

Demonstração. Por indução sobre o grau de $f(x)$, usando a Teorema Fundamental da Álgebra. ■

Teorema 2.5.15. *Se $f(x) \in \mathbb{R}[x]$ é um polinômio não constante, então $f(x)$ fatoriza (em $\mathbb{R}[x]$) como produto de polinômios de grau no máximo 2. Em particular, os polinômios irredutíveis em $\mathbb{R}[x]$ são lineares ou quadráticos.*

Demonstração. Por indução sobre o grau de $f(x)$. O caso grau $f(x) \leq 2$ é imediato. Assume que o resultado valido por polinômios de grau $\leq n$ e considere $f(x)$ com grau $f(x) = n + 1$. Existe 2

casos:

(a) Se $f(z) = 0$ para algum $z \in \mathbb{R}$, então $f(x) = (x - z)g(x)$ e grau $g(x) = n$. O resultado então seguir do hipótese de indução aplicado $g(x)$.

(b) Caso contrario, $f(x)$ não tem raízes reais. Pelo Teorema Fundamental da Álgebra, ela tem raiz complexo z. Então $f(z) = 0$ e portanto $f(\overline{z}) = \overline{f(z)} = \overline{0} = 0$. Portanto,

$$f(x) = (x - z)(x - \overline{z})g(x) = \underbrace{\left(x^2 - (z + \overline{z})x + z\overline{z}\right)}_{\in \mathbb{R}[x]} g(x),$$

e o resultados de novo seguir do hipótese de indução para a $g(x)$.

■

Teorema 2.5.16. (Redutibilidade sobre $\mathbb{Q} \Rightarrow$ Redutibilidade sobre $\mathbb{Z}$). *Seja $f \in \mathbb{Z}[x]$. Se f for redutível sobre $\mathbb{Q}$ então ele vai ser redutível sobre $\mathbb{Z}$.*

Demonstração. Exercício ■

Existe uma espécie de recíproca do teorema acima:

Definição 2.5.9. *Um polinômio $a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ é dito* **primitivo** *se*

$$mdc(a_n, \cdots, a_0) = 1.$$

Exemplo 2.5.16.

(a) $2x + 1$ *é primitivo pois* $mdc(2, 1) = 1$.

(b) $4x^3 + 2$ *não é primitivo pois* $mdc(4, 2) = 2$.

Teorema 2.5.17. (Lema de Gauss). *O produto de 2 polinômios primitivos é um polinômio primitivo.*

Demonstração. Exercício

■

Proposição 2.5.18. *Se $f \in \mathbb{Z}[x]$ é primitivo de grau ≥ 1, então*

f é irredutível em $\mathbb{Z}[x]$ se e somente se f é irredutível em $\mathbb{Q}[x]$.

Demonstração. Exercício ■

Teorema 2.5.19. (Teste de Irredutibilidade mod p). *Seja p um número primo e suponha $f(x) \in \mathbb{Z}[x]$ com grau $f \geq 1$. Seja $\bar{f}$ é o polinômio obtido de f reduzindo todos os coeficientes mod p. Se $\bar{f}$ é irredutível mod p, isto é, sobre $\mathbb{Z}_p$ e grau$(\bar{f})$ = grau(f) então f não se escreve como produto de polinômios de grau ≥ 1 em $\mathbb{Z}[x]$. Em particular, f é irredutível sobre $\mathbb{Q}[x]$.*

Exemplo 2.5.17. *Mostre que $q(x) = x^4 - 7x^3 + 5x^2 - 3x - 9$ é irredutível em $\mathbb{Q}[x]$.*

Solução. *Para mostrar que $g(x) = x^4 - 7x^3 + 5x^2 - 3x - 9$ é irredutível em $\mathbb{Q}[x]$, usamos o Teste de Irredutibilidade mod p*
Seja $\bar{g}$ é o polinômio obtido de g reduzindo todos os coeficientes mod 2. Então $\bar{g}(x) = x^4 + x^3 + x^2 + x + 1$. Portanto basta provar que $\bar{g}(x)$ é irredutível em $\mathbb{Z}_2[x]$

Observamos primeiro que $\bar{g}(x)$ não tem raízes em $\mathbb{Z}_2$ pois $\bar{g}(0) = 1$ e $\bar{g}(1) = 1$. Portanto pelo Teorema do Fator $\bar{g}(x)$ não tem fatores lineares. Além disto, $\bar{g}(x)$ não tem polinômios de grau 3.

Portanto precisa verificar fatores irredutíveis de grau 2. De Exemplo 2.5.15, sabemos que $x^2 + x + 1$ é o único polinômio irredutível de grau 2 em $\mathbb{Z}_2[x]$, portanto vamos divide $\bar{g}(x)$ por $x^2 + x + 1$:

$$\begin{array}{r|l} x^4 + x^3 + x^2 + x + 1 & x^2 + x + 1 \\ \hline -x^4 - x^3 - x^2 & x^2 + 3x + 5 \\ \hline x + 1 & \end{array}$$

Assim, na divisão temos um resto de $x + 1 \neq 0$, ou seja $x^2 + x + 1$ não é um fator de $f(x)$. Portanto $\bar{g}(x)$ é irredutível.

Portanto pelo Teorema 2.5.19 , $g(x)$ é irredutível em $\mathbb{Q}[x]$.

Teorema 2.5.20. (Critério de Eisenstein-1850). *Seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. Se existe um primo p tal que*

- $p \nmid a_n$
- $p|a_i$ *para* $i = 0, 1 \cdots, (n-1)$
- $p^2 \nmid a_0$

Então f não se escreve como produto de polinômios de grau ≥ 1 em $\mathbb{Z}[x]$. Em particular, f é irredutível sobre $\mathbb{Q}[x]$.

Exemplo 2.5.18. *Mostre que $f(x) = x^8 + 6x^5 - 12x^3 + 18x^2 - 24x - 60$ é irredutível em $\mathbb{Q}[x]$.*

Solução. *Para mostrar que $f(x) = x^8 + 6x^5 - 12x^3 + 18x^2 - 24x - 60$ é irredutível em $\mathbb{Q}[x]$, usamos o Critério de Eisenstein com $p = 3$.*
De fato

$$3 \nmid 1,\ 3|6,\ 3|(-12),\ 3|18,\ 3|(-24),\ e\ 3|60,\ mas\ 3^2 \nmid 60$$

Portanto, pelo Critério de Eisenstein, $f(x)$ é irredutível em $\mathbb{Q}[x]$.

2.5.5 Anéis Quociente de polinômios sobre um corpo

Neste seção, vamos explorar a estrutura do anel quociente $K[x]/I$, onde K é um corpo e I é um ideal de $K[x]$.

Teorema 2.5.21. *Seja K um corpo e seja I um ideal não nulo de $K[x]$. Então existe um único polinômio mônico $f(x) \in K[x]$ tal que I é gerado por $h(x)$, isto é,*

$$I = \langle f(x) \rangle = f(x)K[x] = \{f(x)g(x) \mid g(x) \in K[x]\}.$$

Demonstração. Seja I um ideal não nulo de $K[x]$. Então I contem polinômios não nulos e portanto ele contem polinômios mônicos (pois como I um ideal, podemos multiplicar qualquer polinômio pelo inverso do coeficiente dominante para obter um polinômio mônico em I). Entre todos estes polinômios mônicos em I, escolhemos aquele de grau minimal. Portanto $\langle f(x) \rangle \subset I$.

Agora suponha que $f(x) \in I$. Pelo Algoritmo da Divisão, podemos escrever

$$g(x) = q(x)f(x) + r(x) \text{ onde } q(x), r(x) \in K[x] \text{ com } r(x) = 0 \text{ ou grau } r(x) < \text{grau } f(x).$$

Suponha que $r(x) \neq 0$ e seja a o coeficiente dominante de $r(x)$. Então $a^{-1}r(x)$ é um polinômio mônico e

$$a^{-1}r(x) = a^{-1}\Big(f(x) - q(x)g(x)\Big) \in I.$$

Mas grau$\Big(a^{-1}r(x)\Big)$ = grau $r(x)$ < grau $f(x)$, que contradiz o escolhe de $h(x)$. Portanto $r(x) = 0$ e $I = \langle f(x) \rangle$. ■

Assim, do Teorema 2.5.21, vamos explorar a estrutura de anéis $\dfrac{K[x]}{< f(x) >}$, *K um corpo e $f(x) \in K[x]$ um polinômio mônico.*

Teorema 2.5.22. *Sejam K um corpo, $f(x) = a_0 + a_1x + a_nx^n \in K[x]$ e $I = \langle f(x) \rangle$ com $n = grau\ f(x)$. Então todo elemento de $R = {}^{K[x]}\!/_{I}$ tem uma representação única de grau$\leq n-1$. Portanto o anel quociente $R = {}^{K[x]}\!/_{I}$ é dado por*

$$R \cong \{b_0 + b_1t + b_2t^2 + \cdots + b_{n-1}t^{n-1} \mid b_0, \cdots, b_{n-1} \in K\}.$$

Além disto $f(t) = 0$.

Demonstração. Seja $g(x) + I \in {}^{K[x]}\!/_{I}$. Pelo Algoritmo da Divisão de Euclides, Teorema 2.5.3, existem $q(x)$, $r(x) \in K[x]$ tais que

$$g(x) = q(x)f(x) + r(x)$$

com $r(x) = 0$ ou $0 \leq$ grau $r(x) < n$. Assim,

$$r(x) = b_0 + a_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1}$$

é um polinômio de grau $\leq (n-1)$ e

$$\begin{aligned} g(x)+I &= b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1} + q(x)f(x) + I \\ &= b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1} + I \qquad \text{pois } q(x)f(x) \in I = \left\langle f(x) \right\rangle \\ &= b_0 + b_1(x+I) + b_2(x+I)^2 + \cdots + b_{n-1}(x+I)^{n-1} \\ &= b_0 + b_1t + b_2t^2 + \cdots + b_{n-1}t^{n-1} \qquad \text{pela mudança } t = x+I \end{aligned}$$

Portanto

$$\frac{K[x]}{< f(x) >} = \left\{ b_0 + b_1t + b_2t^2 + \cdots + b_{n-1}t^{n-1} \;\mid\; b_0, b_1, \cdots, b_{n-1} \in K \right\}.$$

Além disto

$$\begin{aligned} f(t) &= f(x+I) \\ &= a_0 + a_1(x+I) + a_2(x+I)^2 + \cdots + a_n(x+I)^n \\ &= a_0 + a_1x + a_2x^2 + a_nx^n + I \\ &= I + I = 0 \end{aligned}$$

■

Exemplo 2.5.19. *Descrever o anel quociente* $\dfrac{\mathbb{Q}[x]}{< x^3 - 2 >}$.

Solução. *Pelo Teorema 2.5.22, temos que*

$$\frac{\mathbb{Q}[x]}{< x^3 - 2 >} \cong \left\{ at^2 + bt + c \mid a, b, c \in \mathbb{Q} \right\}, \; com \;\; t^3 - 2 = 0.$$

Exemplo 2.5.20. *Descrever o anel quociente* $\dfrac{\mathbb{R}[x]}{< x^2 + 1 >}$.

Solução. *Pelo Teorema 2.5.22, temos que*

$$\frac{\mathbb{R}[x]}{< x^2 + 1 >} \cong \{ at + b \mid a, b \in \mathbb{R} \}, \; com \;\; t^2 + 1 = 0.$$

Vamos mostrar que

$$\frac{\mathbb{R}[x]}{< x^2 + 1 >} \cong \mathbb{C}.$$

Definimos uma aplicação

$$\varphi : R \to \mathbb{C}, \;\; \varphi([at+b]) = ai + b$$

Como $t^2 + 1 = 0$ *temos que* $t^2 = -1$ *e portanto,*

$$\begin{aligned}
\varphi\Big([at+b][ct+d]\Big) &= \varphi\Big([act^2 + (ad+bc)t + bd]\Big) \\
&= \varphi\Big([ac(-1) + (ad+bc)t + bd]\Big) \\
&= \varphi\Big([(ad+bc)t + (bd-ac)]\Big) \\
&= (ad+bc)i + (bd-ac) \\
&= (ai+b)(ci+d) \\
&= \varphi\Big([at+b]\Big)\varphi\Big([ct+d]\Big)
\end{aligned}$$

Além disto,

$$\begin{aligned}
\varphi\Big([at+b] + [ct+d]\Big) &= \varphi\Big([(a+c)t + (b+d)]\Big) \\
&= (a+c)i + (b+d) \\
&= (ai+b) + (ci+d) \\
&= \varphi\Big([at+b]\Big) + \varphi\Big([ct+d]\Big)
\end{aligned}$$

Portanto φ *é um isomorfismo de anéis. Logo*

$$\frac{\mathbb{R}[x]}{< x^2+1 >} \cong \mathbb{C}.$$

Exemplo 2.5.21. *Construa as tabelas da soma e produto do anel quociente* $\dfrac{\mathbb{Z}_2[x]}{< x^2 >}$. *Conclua que* $\dfrac{\mathbb{Z}_2[x]}{< x^2 >}$ *não é um corpo.*

Solução. *Pelo Teorema 2.5.22, temos que*

$$\frac{\mathbb{Z}_2[x]}{< x^2 >} \cong \{at+b \mid a,b \in \mathbb{Z}_2\} = \{\overline{0},\ \overline{1},\ t,\ \overline{1}+t\},\ com\ \ t^2 = 0.$$

Usando o fato que $t^2 = 0$ *construirmos as tabelas de soma e multiplicação:*

$+$	$\overline{0}$	$\overline{1}$	t	$\overline{1}+t$
$\overline{0}$	$\overline{0}$	$\overline{1}$	t	$\overline{1}+t$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{1}+t$	t
t	t	$\overline{1}+t$	$\overline{0}$	$\overline{1}$
$\overline{1}+t$	$\overline{1}+t$	t	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	t	$\overline{1}+t$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	t	$\overline{1}+t$
t	$\overline{0}$	t	$\overline{0}$	t
$\overline{1}+t$	$\overline{0}$	$\overline{1}+t$	t	$\overline{1}$

Observe que o anel $\dfrac{\mathbb{Z}_2[x]}{< x^2 >}$ *não é um corpo pois, por exemplo, o elemento não nulo t não é inversível.*

Exemplo 2.5.22. *Construa as tabelas da soma e produto do anel quociente* $\dfrac{\mathbb{Z}_2[x]}{< x^2+x+\overline{1} >}$. *Conclua que* $\dfrac{\mathbb{Z}_2[x]}{< x^2+x+\overline{1} >}$ *é um corpo.*

Solução. *Pelo Teorema 2.5.22, temos que*

$$\frac{\mathbb{Z}_2[x]}{< x^2+x+\overline{1} >} \cong \{at+b \mid a,b \in \mathbb{Z}_2\} = \{\overline{0},\ \overline{1},\ t,\ \overline{1}+t\},\ com\ \ t^2+t+1=0.$$

Usando o fato que $t^2+t+1=0$, *temos que* $t^2 = -t-\overline{1} = t+\overline{1}$. *As tabelas de soma e multiplicação:*

$+$	$\overline{0}$	$\overline{1}$	t	$\overline{1}+t$
$\overline{0}$	$\overline{0}$	$\overline{1}$	t	$\overline{1}+t$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{1}+t$	t
t	t	$\overline{1}+t$	$\overline{0}$	$\overline{1}$
$\overline{1}+t$	$\overline{1}+t$	t	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	t	$\overline{1}+t$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	t	$\overline{1}+t$
t	$\overline{0}$	t	$\overline{1}+t$	$\overline{1}$
$\overline{1}+t$	$\overline{0}$	$\overline{1}+t$	$\overline{1}$	t

Observe que o anel $\dfrac{\mathbb{Z}_2[x]}{< x^2+x+\overline{1} >}$ *é um corpo com 4 elementos.*

(Como $\mathbb{Z}_4$ *não é um corpo, este anel quociente não é isomorfo a* $\mathbb{Z}_4$*).*

Teorema 2.5.23. *Sejam K um corpo e $f(x) \in K[x]$ com grau $f(x) \geq 1$. Então o anel quociente $\frac{K[x]}{\langle f(x) \rangle}$ é um corpo se $f(x)$ é irredutível.*

Demonstração. Vamos provar que em $\frac{K[x]}{< f(x) >}$, toda classe não nula $g(x) + < f(x) >$ é invertível. De fato, se $g(x) + < f(x) > \neq 0 + < f(x) >$ então $g(x) \notin < f(x) >$. Logo existe $q(x) \in K[x]$ satisfazendo $g(x) \neq f(x)q(x)$.
Assim $f(x)$ não é fator de $g(x)$ e consequentemente, como $f(x)$ é irredutível,

$$\text{MDC}(f(x), g(x) = 1$$

Logo pelo Teorema 2.5.6, existem polinômios $a(x),\ b(x) \in K[x]$ satisfazendo

$$a(x)f(x) + b(x)g(x) = 1$$

Daí,

$$[a(x)f(x) + b(x)g(x)] + < f(x) >= 1 + < f(x) >$$

■

Exemplo 2.5.23. *Determine todos os valores de $a \in \mathbb{Z}_3$ tal que o anel quociente $\frac{\mathbb{Z}_3[x]}{< x^3 + x^2 + ax + 1 >}$ é um corpo.*

Solução. *Seja $f(x) = x^3 + x^2 + ax + 1$. Basta determinar o valores de $a \in \mathbb{Z}_3$ para que $f(x)$ seja irredutível. Como $f(x)$ é grau 3, basta verifique que $f(x)$ não tem raiz em $\mathbb{Z}_3$.*

x	$\overline{0}$	$\overline{1}$	$\overline{2}$
$f(x)$	1	a	$2a + 2$

Portanto $f(x)$ não possui raiz em $\mathbb{Z}_3$ se $a = 1$.

2.5.6 Exercícios Resolvidos

Exercício 2.5.1. *Dados $f(x)$ e $g(x) \in A[x]$, determine*

$$h(x) = f(x) + g(x) \ \ e \ \ p(x) = f(x)g(x) \ \ para$$

(a) $f(x) = -x^3 + x^2 - x + 4, \quad g(x) = 3x^2 - 4x - 2 \ \in \mathbb{R}[x]$

(b) $f(x) = \overline{2}x^3 + x^2 - x + \overline{4}, \quad g(x) = \overline{3}x^2 + \overline{2} \ \in \mathbb{Z}_6[x]$

(c) $f(x) = \overline{3}x^4 + x^2 - x + \overline{4}, \quad g(x) = \overline{2}x^2 + x + \overline{3} \ \in \mathbb{Z}_5[x]$

(d) $f(x) = \overline{2}x^2 - \overline{4}x + \overline{3}, \quad g(x) = \overline{4}x - \overline{5} \ \in \mathbb{Z}_8[x]$

Solução. *(a)*

$h(x) = f(x) + g(x)$:

$$\begin{array}{r} -x^3 \ +x^2 \ -x \ +4 \\ +\quad 3x^2 \ -4x \ -2 \\ \hline -x^3 \ +4x^2 \ -5x \ +2 \end{array} \quad \Rightarrow h(x) = -x^3 + 4x^2 - 5x + 2$$

$p(x) = f(x)g(x)$:

$$\begin{array}{r} -x^3 \ +x^2 \ -x \ +4 \\ \times \quad 3x^2 \ -4x \ -2 \\ \hline -3x^5 \ +3x^4 \ -3x^3 \ +12x^2 \\ +4x^4 \ -4x^3 \ +4x^2 \ -16x \\ +2x^3 \ -2x^2 \ +2x \ -8 \\ \hline -3x^5 \ +7x^4 \ -5x^3 \ +14x^2 \ -14x \ -8 \end{array} \quad \Rightarrow p(x) = -3x^5 + 7x^4 - 5x^3 + 14x^2 - 14x - 8$$

(b)

$h(x) = f(x) + g(x)$:

$$\begin{array}{r} 2x^3 \ +x^2 \ -x \ +4 \\ +\quad 3x^2 \ \ +2 \\ \hline 2x^3 \ +4x^2 \ -x \ +6 \end{array} \quad \Rightarrow h(x) = \overline{2}x^3 + \overline{4}x^2 - x$$

$p(x) = f(x)g(x)$:

$$\begin{array}{r} 2x^3 \ +x^2 \ -x \ +4 \\ \times \quad 3x^2 \ \ +2 \\ \hline 6x^5 \ +3x^4 \ -3x^3 \ +12x^2 \\ +4x^3 \ +2x^2 \ -2x \ +8 \\ \hline 6x^5 \ +3x^4 \ +x^3 \ +14x^2 \ -2x \ +8 \end{array} \quad \Rightarrow p(x) = \overline{3}x^4 + x^3 + \overline{2}x^2 - \overline{2}x + \overline{2}$$

(c)
$$\begin{cases} h(x) = f(x) + g(x): \\ \quad 3x^4 + x^2 - x + 4 \\ + \quad 2x^2 + x + 3 \\ \hline \quad 3x^4 + 3x^2 + 7 \end{cases} \Rightarrow h(x) = \overline{3}x^4 + \overline{3}x^2 + 2$$

$$\begin{cases} p(x) = f(x)g(x): \\ \quad 3x^4 + x^2 - x + 4 \\ \times \quad 2x^2 + x + 3 \\ \hline \quad 6x^6 + 0x^5 - 2x^4 - 2x^3 + 8x^2 \\ \qquad +3x^5 + 0x^4 + x^3 - x^2 + 4x \\ \qquad\quad +9x^4 + 3x^2 - 3x + 12 \\ \hline \quad 6x^6 + 3x^5 + 11x^4 - x^3 + 10x^2 + x + 12 \end{cases} \Rightarrow p(x) = x^6 + \overline{3}x^5 + x^4 - x^3 + x + \overline{2}$$

(d)
$$\begin{cases} h(x) = f(x) + g(x): \\ \quad 2x^2 - 4x + 3 \\ + \quad 4x - 5 \\ \hline \quad 2x^2 - 2 \end{cases} \Rightarrow h(x) = \overline{2}x^2 - \overline{2}$$

$$\begin{cases} p(x) = f(x)g(x): \\ \quad 2x^2 - 4x + 3 \\ \times \quad 4x - 5 \\ \hline \quad 8x^3 - 16x^2 + 12x \\ \qquad -10x^2 + 20x - 15 \\ \hline \quad 8x^3 - 26x^2 + 32x - 15 \end{cases} \Rightarrow p(x) = -\overline{2}x^2 - \overline{7}$$

Exercício 2.5.2. *Dados $f(x)$ e $g(x) \in A[x]$, determine $p(x) \in A[x]$ tal que $f(x) = g(x)p(x)$ para*

(a) $f(x) = x^6 + x^4 + x^3 + x^2 - x - \overline{1}, \quad g(x) = x^4 + \overline{2}x^3 + \overline{2}x^2 - x + \overline{1} \in \mathbb{Z}_4[x]$

(b) $f(x) = x^4 - x^3 + \overline{4}x + \overline{5}, \quad g(x) = \overline{3}x^2 + \overline{2} \in \mathbb{Z}_7[x]$

Solução. *(a) Como f é um polinômio mônico de grau 6 e g também é um polinômio mônico de grau 4, temos que p é um polinômio mônico de grau 2, ou seja $p(x) = x^2 + bx + c$.*

$f(x) = g(x)p(x)$:

$$\begin{array}{lllll} x^4 & +2x^3 & +2x^2 & -x & +1 \\ \times & & x^2 & +bx & +c \\ \hline x^6 & +2x^5 & +2x^4 & -x^3 & +x^2 \\ & +bx^5 & +2bx^4 & +2bx^3 & -bx^2 \quad +bx \\ & & +cx^4 & +2cx^3 & +2cx^2 \quad -cx \quad +c \\ \hline x^6 & +(2+b)x^5 & +(2+2b+c)x^4 & +(-1+2b+2c)x^3 & +(1-b+2c)x^2 \quad +(b-c)x \quad +c \end{array}$$

Agora comparamos com $f(x) = x^6 + x^4 + x^3 + x^2 - x - \overline{1}$:

- *Igualando os coeficientes dos termos* x^5*, temos*

$$\overline{2} + b = \overline{0} \Rightarrow b = -\overline{2} \Rightarrow b = \overline{2} \text{ em } \mathbb{Z}_4$$

- *Igualando os coeficientes dos termos constantes, temos*

$$c = -\overline{1} \Rightarrow c = \overline{3} \text{ em } \mathbb{Z}_4$$

Portanto $p(x) = x^2 + \overline{2}x + \overline{3}$.

(b) Como f *é um polinômio grau* 4 *e* g *também é um polinômio de grau* 2*, temos que* p *é um polinômio de grau* 2*, ou seja* $p(x) = ax^2 + bx + c$.

$f(x) = g(x)p(x)$:

$$\begin{array}{llll} 3x^2 & & +2 & \\ \times\ ax^2 & +bx & +c & \\ \hline 3ax^4 & & +2ax^2 & \\ & +3bx^3 & & +2bx \\ & & +3cx^2 & +2c \\ \hline 3ax^4 & +3bx^3 & +(2a+3c)x^2 & +2bx \quad +2c \end{array}$$

Agora comparamos com $f(x) = x^4 - x^3 + \overline{4}x + \overline{5}$:

- *Igualando os coeficientes dos termos* x^4*, temos*

$$\overline{3}a = \overline{1} \Rightarrow a = \overline{5} \text{ em } \mathbb{Z}_7$$

- *Igualando os coeficientes dos termos x^3, temos*

$$\overline{3}b = -\overline{1} \Rightarrow b = \overline{2} \text{ em } \mathbb{Z}_7$$

- *Igualando os coeficientes dos termos constantes, temos*

$$\overline{2}c = \overline{5} \Rightarrow c = \overline{6} \text{ em } \mathbb{Z}_7$$

Portanto $p(x) = \overline{5}x^2 + \overline{2}x + \overline{6}$.

Exercício 2.5.3. *Determine todos os polinômios de grau 2 em* (*a*) $\mathbb{Z}_2[x]$ (*b*) $\mathbb{Z}_3[x]$.

Solução. *(a) Os polinômios de grau 2 em* $\mathbb{Z}_2[x]$ *são da forma*

$$\overline{a}x^2 + \overline{b}x + \overline{c}, \text{ com } \overline{a} \in \{1\}, \ \overline{b} \in \{0,1\} \text{ e } \overline{c} \in \{0,1\}.$$

Há 1 escolha para a e 2 escolhas para b e c. Aplicando o Principio Multiplicativo da Analise Combinatória, concluímos que há $(1 \times 2 \times 2) = 4$ *polinômios de grau 2 em* $\mathbb{Z}_2[x]$.
Logo os polinômios de grau 2 em $\mathbb{Z}_2[x]$ *são* x^2, $(x^2 + \overline{1})$, $(x^2 + x)$, $(x^2 + x + \overline{1})$.

(b) Os polinômios de grau 2 em $\mathbb{Z}_3[x]$ *são da forma*

$$\overline{a}x^2 + \overline{b}x + \overline{c}, \text{ com } \overline{a} \in \{1,2\}, \ \overline{b} \in \{0,1,2\} \text{ e } \overline{c} \in \{0,1,2\}.$$

Há 2 escolha para a e 3 escolhas para b e c. Aplicando o Principio Multiplicativo da Analise Combinatória, concluímos que há $(2 \times 3 \times 3) = 18$ *polinômios de grau 2 em* $\mathbb{Z}_3[x]$.
Logo os polinômios de grau 2 em $\mathbb{Z}_3[x]$ *são* x^2, $(x^2 + \overline{1})$, $(x^2 + \overline{2})$, $(x^2 + x)$,
$(x^2 + x + \overline{1})$, $(x^2 + x + \overline{2})$, $(x^2 + \overline{2}x)$, $(x^2 + \overline{2}x + \overline{1})$, $(x^2 + \overline{2}x + \overline{2})$, $\overline{2}x^2$, $(\overline{2}x^2 + \overline{1})$,
$(\overline{2}x^2 + \overline{2})$, $(\overline{2}x^2 + x)$, $(\overline{2}x^2 + x + \overline{1})$, $(\overline{2}x^2 + x + \overline{2})$, $(\overline{2}x^2 + \overline{2}x)$, $(\overline{2}x^2 + \overline{2}x + \overline{1})$, $(\overline{2}x^2 + \overline{2}x + \overline{2})$.

Exercício 2.5.4. *Seja* $A = \{p(x) \in \mathbb{Z}_4[x] - \{0\}; gr(p(x)) \leq 3\}$. *Determine quantos elementos o conjunto A possui.*

Solução. *Sejam* $q(x) \in \mathbb{Z}_4[x]$ *o polinômio identicamente nulo e* $B = \{q(x)\} \cup A$
Se $t(x) \in B$, *podemos escrever* $t(x) = \overline{a}x^3 + \overline{b}x^2 + \overline{c}x + \overline{d}$, *onde* $\{a,b,c,d\} \in \{0,1,2,3\}$. *Aplicando o Princípio Multiplicativo da Análise Combinatória, obtemos que há*
$(4 \times 4 \times 4 \times 4) = 256$, *polinômios em B. Portanto há* $256 - 1 = 255$ *polinômios* $p(x) \in A$.

Exercício 2.5.5. *Determine as raízes em A dos seguintes polinômios $p(x) \in A[x]$:*

(a) $p(x) = x^4 + \overline{2}x^3 + \overline{2}x^2 - x + \overline{2} \in \mathbb{Z}_4[x]$

(b) $p(x) = -\overline{2}x^{600} + \overline{3}x^{219} + \overline{3}x^{74} + \overline{3}x^{57} + \overline{3}x^{44} + \overline{2} \in \mathbb{Z}_7[x]$.

(c) $p(x) = x^6 + x^2 + 1 \in \mathbb{R}[x]$

Solução. *(a)* $p(x) = x^4 + \overline{2}x^3 + \overline{2}x^2 - x + \overline{2}$

$$p(\overline{0}) = \overline{0}^4 + \overline{2} \cdot \overline{0}^3 + \overline{2} \cdot \overline{0}^2 - \overline{0} + \overline{2} = \overline{2}$$
$$p(\overline{1}) = \overline{1}^4 + \overline{2} \cdot \overline{1}^3 + \overline{2} \cdot \overline{1}^2 - \overline{1} + \overline{2} = \overline{2}$$
$$p(\overline{2}) = \overline{2}^4 + \overline{2} \cdot \overline{2}^3 + \overline{2} \cdot \overline{2}^2 - \overline{2} + \overline{2} = \overline{0}$$
$$p(\overline{3}) = \overline{3}^4 + \overline{2} \cdot \overline{3}^3 + \overline{2} \cdot \overline{3}^2 - \overline{3} + \overline{2} = \overline{0}$$

Portanto, as únicas raízes em $\mathbb{Z}_4$ são $\overline{2}$ e $\overline{3}$.

(b) $p(x) = -\overline{2}x^{600} + \overline{3}x^{219} + \overline{3}x^{74} + \overline{3}x^{57} + \overline{3}x^{44} + \overline{2}$

Como $p(\overline{0}) = \overline{2}$, temos que $\overline{0}$ não é raiz de $p(x)$.

Se $\overline{k} \neq \overline{0}$, isto é, se 7 não divide k, podemos aplicar o Teorema de Fermat, ou seja

$$k^6 \equiv 1 \ (mod\ 7)$$

Logo,

$$\begin{cases} k^{600} \equiv (k^6)^{100} \equiv 1 \ (mod\ 7) \\ k^{219} \equiv (k^6)^{54} \cdot k^3 \equiv k^3 \ (mod\ 7) \\ k^{74} \equiv (k^6)^{12} \cdot k^2 \equiv k^2 \ (mod\ 7) \\ k^{57} \equiv (k^6)^9 \cdot k^3 \equiv k^3 \ (mod\ 7) \\ k^{44} \equiv (k^6)^7 \cdot k^2 \equiv k^2 \ (mod\ 7) \end{cases}$$

Portanto, se $\overline{k} \neq \overline{0}$,, temos

$$\begin{aligned} p(\overline{k}) &= -\overline{2} \cdot \overline{k}^{600} + \overline{3} \cdot \overline{k}^{219} + \overline{3} \cdot \overline{k}^{74} + \overline{3} \cdot \overline{k}^{57} + \overline{3} \cdot \overline{k}^{44} + \overline{2} = \\ &= -\overline{2} + \overline{3} \cdot \overline{k}^3 + \overline{3} \cdot \overline{k}^2 + \overline{3} \cdot k^3 + \overline{3} \cdot k^2 + \overline{2} = \\ &= \overline{6} \cdot \overline{k}^3 + \overline{6} \cdot \overline{k}^2 = \overline{6} \cdot \overline{k}^2 (\overline{k} + \overline{1}) \end{aligned}$$

Como 7 não divide k, temos que

$$p(\overline{k}) = \overline{0} \Leftrightarrow (\overline{k} + \overline{1}) = \overline{0} \Leftrightarrow \overline{k} = -\overline{1} = \overline{6}$$

Portanto, a única raíz em $\mathbb{Z}_7$ *é* $\overline{6}$.

(c) $p(x) = x^6 + x^2 + 1$

Para qualquer $\alpha \in \mathbb{R}$, *temos que* $\alpha^2 \geq 0$ *e* $\alpha^6 = (\alpha^2)^3 \geq 0$.

Logo $f(\alpha) = \alpha^6 + \alpha^2 + 1 \geq 1 > 0$ *para todo* $\alpha \in \mathbb{R}$.

Portanto, $f(x)$ *não possui raízes em* $\mathbb{R}$.

Exercício 2.5.6. *Seja* F *um corpo*

(a) Prove que $\langle x \rangle = \{xp(x) \mid p(x) \in F[x]\}$ *é um ideal de* $F[x]$.

(b) Seja $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. *Prove que a função*
$\Phi_0 : F[x] \longrightarrow F$ *definida por* $\Phi_0\big(p(x)\big) = a_0$ *é um homomorfismo.*

(c) Determine o núcleo de Φ_0.

(d) Usando o Teorema Fundamental do Homomorfismo, conclua que $F[x]\Big/\langle x \rangle \approx F$

Solução. *(a)* $\langle x \rangle = \{xp(x) \mid p(x) \in F[x]\}$

(i) $0 = x \cdot 0 \in \langle x \rangle \neq \emptyset$.

(ii) Sejam $f(x) = xp(x)$ *e* $g(x) = xq(x) \in \langle x \rangle$. *Temos*

$$f(x) + g(x) = xp(x) + xq(x) = x\big(p(x) + q(x)\big) \in \langle x \rangle.$$

(iii) Sejam $f(x) = xp(x) \in \langle x \rangle$ *e* $g(x) \in F[x]$. *Temos*

$$f(x)g(x) = xp(x) \cdot g(x) = x\big(p(x)g(x)\big) \in \langle x \rangle.$$

Resulta de (i), (ii) e (iii) que $\langle x \rangle$ *é ideal de* $F[x]$.

(b) Sejam $p(x) = \sum_{i=1}^{n} a_i x_i$ *e* $q(x) = \sum_{i=1}^{m} b_i x_i \in F[x]$.

Se $p(x) + q(x) = \sum_{i=1}^{k} c_i x_i$ *e* $p(x)q(x) = \sum_{i=1}^{m+n} d_i x_i$, *temos* $c_0 = a_0 + b_0$ *e* $d_0 = a_0 \cdot b_0$, *portanto:*

(i) $\Phi_0\big(p(x) + q(x)\big) = c_0 = a_0 + b_0 = \Phi_0(p(x)) + \Phi_0(q(x))$.

(ii) $\Phi_0\big(p(x)q(x)\big) = d_0 = a_0 \cdot b_0 = \Phi_0(p(x)) \cdot \Phi_0(q(x))$.

Resulta de (i) e (ii) que Φ_0 *é homomorfismo.*

(c) Seja $N(\Phi_0)$ o núcleo de Φ_0.

(i) Se $f(x) = \sum_{i=1}^{n} a_i x_i \in N(\Phi_0)$, *então*

$$0 = a_0 = \Phi_0(p(x)) \Rightarrow p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x =$$

$$= x(a_n x^{n-1} + a_{n-1}x^{n-2} + \cdots a_1) \in \left\langle x \right\rangle$$

Logo $N(\Phi_0) \subset \left\langle x \right\rangle$.

(ii) Se $f(x) = xp(x) \in \left\langle x \right\rangle$, *como* $f(x)$ *tem termo independente nulo, temos*

$$\Phi_0(f(x)) = 0 \Rightarrow f(x) \in N(\Phi_0) \Rightarrow \left\langle x \right\rangle \subset N(\Phi_0).$$

Resulta de (i) e (ii) que $\Phi_0 = \left\langle x \right\rangle$.

(d) Vamos mostrar que $Im(\Phi_0) = F$, *ou seja, que* Φ_0 *é sobrejetora.*

De fato, dado $a \in F$ *considere o polinômio constante* $p_a(x) = a$. *Temos que* $\Phi_0(p_a(x)) = a$, *o que mostra que* Φ_0 *é sobrejetora.*

Portanto, resulta do Teorema Fundamental do Homomorfismo que

$$F[x]\Big/\left\langle x \right\rangle = F[x]\Big/_{N(\Phi_0)} \approx Im(\Phi_0) = F$$

Exercício 2.5.7. *Determine polinômios $q(x)$ e $r(x)$ tais que $f(x) = g(x)q(x) + r(x)$, e $r(x) = 0$ ou grau $r(x) <$ grau $g(x)$:*

(a) $f(x) = x^4 - 7x + 1, \quad g(x) = 2x^2 + 1 \ \in \mathbb{Q}[x]$

(b) $f(x) = \overline{4}x^4 + \overline{2}x^3 + \overline{6}x^2 + \overline{4}x + \overline{5}, \quad g(x) = \overline{3}x^2 + \overline{2} \ \in \mathbb{Z}_7[x]$

(c) $f(x) = \overline{3}x^6 + \overline{2}x^5 + \overline{2}x^4 + \overline{4}x^3 + x^2 - x + \overline{4}, \quad g(x) = \overline{2}x^3 + \overline{4}x^2 - x + \overline{3} \ \in \mathbb{Z}_5[x]$

(d) $f(x) = \overline{2}x^2 - \overline{4}x + \overline{3}, \quad g(x) = \overline{7}x - \overline{5} \ \in \mathbb{Z}_8[x]$

Solução. *(a)*

$$\begin{array}{rr|l} x^4 & -7x+1 & 2x^2+1 \\ \cline{3-3} -x^4-\frac{1}{2}x^2 & & \frac{1}{2}x^2-\frac{1}{4} \\ \cline{1-1} -\frac{1}{2}x^2-7x+1 & & \\ \frac{1}{2}x^2+\frac{1}{4} & & \\ \cline{1-1} -7x+\frac{5}{4} & & \end{array}$$

Portanto, $q(x) = \frac{1}{2}x^2 - \frac{1}{4}$ *e* $r(x) = -7x + \frac{5}{4}$

(b)

$$\begin{array}{rr|l} 4x^4+2x^3+6x^2+4x+5 & & 3x^2+2 \\ \cline{3-3} -4x^4 \quad -5x^2 & & 6x^2+3x+5 \\ \cline{1-1} 2x^3+x^2+4x & & \\ -2x^3 \quad -6x & & \\ \cline{1-1} x^2-2x+5 & & \\ -x^2 \quad -3 & & \\ \cline{1-1} -2x+2 & & \end{array}$$

Portanto, $q(x) = \overline{6}x^2 + \overline{3}x + \overline{5}$ *e* $r(x) = \overline{5}x + \overline{2}$

(c)

$$\begin{array}{rr|l} 3x^6+2x^5+2x^4+4x^3+x^2-x+4 & & 2x^3+4x^2-x+3 \\ \cline{3-3} -3x^6-x^5+4x^4-2x^3 & & 4x^3+3x^2+2x+1 \\ \cline{1-1} x^5+x^4+2x^3+x^2 & & \\ -x^5-2x^4+3x^3-4x^2 & & \\ \cline{1-1} 4x^4 \quad -3x^2-x & & \\ -4x^4-3x^3+2x^2-x & & \\ \cline{1-1} 2x^3-x^2-2x+4 & & \\ -2x^3-4x^2+x-3 & & \\ \cline{1-1} -x+1 & & \end{array}$$

Portanto, $q(x) = \overline{4}x^3 + \overline{3}x^2 + \overline{2}x + \overline{1}$ *e* $r(x) = \overline{4}x + \overline{1}$

(d)

$$\begin{array}{r|l} 2x^2 - 4x + 3 & 7x - 5 \\ \cline{2-2} -2x^2 - 2x & 6x + 6 \\ \cline{1-1} \quad 2x + 3 & \\ -2x - 2 & \\ \cline{1-1} \quad 1 & \end{array}$$

Portanto, $q(x) = 6x + 6$ *e* $r(x) = 1$

Exercício 2.5.8. *Seja* $\mathcal{R}$ *o anel* $F[x]/(x^4 + x^2 + 1)$. *Suponha que*

$$x^7 = a_3x^3 + a_2x^2 + a_1x + a_0 \quad \text{em } \mathcal{R}$$

Calcule os números a_0, a_1, a_2, a_3.

Solução. *Dividimos* x^7 *por* $x^4 + x^2 + 1$:

$$\begin{array}{r|l} x^7 & x^4 + x^2 + 1 \\ \cline{2-2} -x^7 - x^5 - x^3 & x^3 - x \\ \cline{1-1} \quad -x^5 - x^3 & \\ x^5 + x^3 + x & \\ \cline{1-1} \quad x & \end{array}$$

Portanto

$$x^7 = (x^4 + x^2 + 1)(x^3 - x) + x \qquad (*)$$

Reduzindo $(*)$ *modulo* $(x^4 + x^2 + 1)$ *podemos ver que* $x^7 = x$ *em* $\mathcal{R}$

Portanto, $a_0 = a_2 = a_3 = 0$ *e* $a_1 = 1$.

Exercício 2.5.9. *(a) Ache todos os zeros e suas multiplicidades de* $x^5 + 4x^4 + 4x^3 - x^2 - 4x + 1 \in \mathbb{Z}_5[x]$

(b) Determine se o anel $\mathbb{Z}[x]/(x^4 - 16)$ *é um domínio de integridade.*

Solução. *(a) Seja* $f(x) = x^5 + 4x^4 + 4x^3 - x^2 - 4x + 1$. *Podemos verificar que*

$$\begin{cases} f(1) = (1)^5 + 4(1)^4 + 4(1)^3 - (1)^2 - 4(1) + 1 = 5 = 0 \text{ em } \mathbb{Z}_5 \\ f(3) = (3)^5 + 4(3)^4 + 4(3)^3 - (3)^2 - 4(3) + 1 = 555 = 0 \text{ em } \mathbb{Z}_5 \end{cases}$$

Portanto 1 *e* 3 *são raízes de* $f(x)$*, podemos aplicar Briot-Ruffini*

1	4	4	−1	−4	1	1
1	0	4	3	−1	0	3
1	3	3	2	0		

Isto nos dá a fatoração

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

Seja $g(x) = x^3 + 3x^2 + 3x + 2$*. Podemos verificar que*

$$g(3) = (3)^3 + 3(3)^2 + 3(3) + 2 = 65 = 0 \text{ em } \mathbb{Z}_5$$

Portanto 3 *é uma raíz de* $g(x)$ *e podemos aplicar o Briot-Ruffini*

1	3	3	2	3
1	1	1	0	

Isto nos dá a fatoração

$$\begin{aligned} g(x) &= x^3 + 3x^2 + 3x + 2 \\ &= (x-3)(x^2 + x + 1) \end{aligned}$$

Seja $h(x) = x^2 + x + 1$*. Podemos verificar que*

$$\begin{cases} h(1) = (1)^2 + 1 + 1 = 3 \neq 0 \text{ em } \mathbb{Z}_5 \\ h(2) = (2)^2 + 2 + 7 = 2 \neq 0 \text{ em } \mathbb{Z}_5 \\ h(3) = (3)^2 + 3 + 1 = 3 \neq 0 \text{ em } \mathbb{Z}_5 \\ h(4) = (4)^2 + 4 + 1 = 1 \neq 0 \text{ em } \mathbb{Z}_5 \end{cases}$$

Portanto $h(x)$ *não possui raízes em* $\mathbb{Z}_5$*. Assim, a decomposição de* $f(x)$ *em* $\mathbb{Z}_5[x]$ *é*

$$f(x) = (x-1)(x-3)^2(x^2 + x + 1)$$

Logo os zeros de $f(x)$ *são* $x = 1$ *com multiplicidade 1 e* $x = 3$ *com multiplicidade 2.*

(b) $\mathbb{Z}[x]/(x^4 - 16)$ **NÃO** *é um domínio de integridade, pois* $\left(x^2 - 4 + (x^4 - 16)\right)$ *e* $\left(x^2 + 4 + (x^4 - 16)\right)$ *são 2 elementos não nulo em* $\mathbb{Z}[x]/(x^4 - 16)$. *Mas*

$$\left(x^2 - 4 + (x^4 - 16)\right)\left(x^2 + 4 + (x^4 - 16)\right) = 0 \text{ em } \mathbb{Z}[x]/(x^4 - 16).$$

Exercício 2.5.10. *(a) Mostre que* $x^2 + 2$ *é irredutível em* $\mathbb{Z}_5[x]$.

(b) Factorize $x^4 - 4$ *como um produto de fatores irredutíveis em* $\mathbb{Z}_5[x]$.

(c) Para que valores de k, $(x + 1)$ *é um fator de* $(x^4 + 2x^3 - 3x^2 + kx + 1)$ *em* $\mathbb{Z}_5[x]$?

(d) Para que valores de k, $(x - 2)$ *é um fator de* $(x^4 - 5x^3 + 5x^2 + 3x + k)$ *em* $\mathbb{Q}[x]$?

Solução. *(a) Suponha que por contradição que* $x^2 + 2$ *é redutível. Então* $x^2 + 2 = (x + a)(x + b)$ *para algum* $a, b \in \mathbb{Z}_5$. *Portanto,*

$$x^2 + 2 = (x + a)(x + b) = x^2 + (a + b)x + ab.$$

Implica que $a + b = 0$ *e* $ab = 2$, *ou seja,* $b = -a$ *e* $a^2 = -ab = -2 = 3$. *Mas para* $a \in \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, *podemos verificar que* $a^2 = 0, 1$ *ou* 4. *Este contradiz o fato que* $a^2 = 3$. *Portanto* $x^2 + 2$ *é irredutível em* $\mathbb{Z}_5$.

Outra Solução:

Seja $f(x) = x^2 + 2$. *Queremos os raízes de* $f(x)$ *em* $\mathbb{Z}_5[x]$.

Verificando os valores de $f(x)$ *para cada elemento de* $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, *temos*

$$\begin{cases} f(\overline{0}) = (\overline{0})^2 + 2 = \overline{2} \\ f(\overline{1}) = (\overline{1})^2 + 2 = \overline{3} \\ f(\overline{2}) = (\overline{2})^2 + 2 = \overline{6} = \overline{1} \\ f(\overline{3}) = (\overline{3})^2 + 2 = \overline{11} = \overline{1} \\ f(\overline{4}) = (\overline{4})^2 + 2 = \overline{18} = \overline{3} \end{cases}$$

Portanto $f(x) = x^2 + 2$ *não possui raízes em* $\mathbb{Z}_5[x]$ *e portanto ela é irredutível em* $\mathbb{Z}_5[x]$.

(b) De parte (a) sabemos que $x^2 + 2$ *é irredutível em* $\mathbb{Z}_5[x]$ *e um argumento similar mostra que* $x^2 + 3$ *é*

também irredutível em $\mathbb{Z}_5[x]$ *Portanto*

$$x^4 - 4 = (x^2)^2 - 2^2 = (x^2 - 2)(x^2 + 2) = (x^2 + 3)(x^2 + 2)$$

o produto em irredutíveis.

(c) Seja $f(x) = x^4 + 2x^3 - 3x^2 + kx + 1$. *Aplicamos o Teorema do Fator que diz que* $(x + 1)$ *é um fator de* $f(x)$ *em* $\mathbb{Z}_5[x]$ *se e somente se* -1 *é uma raiz de* $f(x)$, *ou seja ,*

$$0 = f(-1) = (-1)^4 + 2(-1)^3 - 3(-1)^2 + k(-1) + 1 = -k - 3.$$

Portanto $(x + 1)$ *é um fator de* $x^4 + 2x^3 - 3x^2 + kx + 1$ *em* $\mathbb{Z}_5$ *se* $k = -3$ *ou* $k = 2$.

(d) Seja $f(x) = x^4 - 5x^3 + 5x^2 + 3x + k$. *Aplicamos o Teorema do Fator que diz que* $x - 2$ *é um fator de* $f(x)$ *em* $\mathbb{Q}[x]$ *se e somente se* 2 *é uma raiz de* $f(x)$, *ou seja,*

$$0 = f(2) = 2^4 - 5 \cdot 2^3 + 5 \cdot 2^2 + 3 \cdot 2 + k = k + 2.$$

Portanto $(x - 2)$ *é um fator de* $x^4 - 5x^3 + 5x^2 + 3x + k$ *em* $\mathbb{Q}[x]$ *se* $k = -2$.

Exercício 2.5.11. *Determine quais dos seguintes polinômios no anel* $\mathcal{R}$ *são irredutíveis. Para aqueles que são redutíveis, escreva eles como produto de polinômios irredutíveis.*

(a) $\mathcal{R} = \dfrac{\mathbb{Z}}{2\mathbb{Z}}[x]$, $\quad f(x) = x^3 + x^2 + x + 1$

(b) $\mathcal{R} = \dfrac{\mathbb{Z}}{3\mathbb{Z}}[x]$, $\quad f(x) = x^3 + x + 1$

(c) $\mathcal{R} = \mathbb{R}[x]$, $\quad f(x) = x^4 + x - 1$

(d) $\mathcal{R} = \mathbb{Z}[x]$, $\quad f(x) = x^7 - x^6 + 2x^2 - 2$

(e) $\mathcal{R} = \mathbb{Q}[x]$, $\quad f(x) = 2x^5 + 5x^4 + 4x^3 + 7x^2 + 7x + 2$

(f) $\mathcal{R} = \mathbb{Z}_{11}[x]$, $\quad f(x) = x^{11} + 1$

Solução. *(a) Primeiramente observamos que* $f(1) = 1 + 1 + 1 + 1 = 4 = 0$ *portanto* $x - 1$ *é um fator de* $f(x)$. *Aplicando o Briot-Ruffini*

1	1	1	1	|	1
1	0	1	|	0	

Isto nos dá a fatoração

$$\begin{aligned} f(x) &= x^3 + x^2 + x + 1 \\ &= (x-1)(x^2+1) \end{aligned}$$

Mas $x^2 + 1 = (x-1)(x-1)$ *em* $\frac{\mathbb{Z}}{2\mathbb{Z}}$.
Portanto a decomposição de $f(x)$ *em* $\frac{\mathbb{Z}}{2\mathbb{Z}}$ *é*

$$f(x) = (x-1)(x-1)(x-1) = (x-1)^3$$

(b) Primeiramente observamos que $f(1) = 1+1+1 = 3 = 0$ *portanto* $x-1$ *é um fator de* $f(x)$. *Aplicando o Briot-Ruffini*

	1	0	1	1	1
	1	1	2	0	

Isto nos dá a fatoração

$$\begin{aligned} f(x) &= x^3 + x + 1 \\ &= (x-1)(x^2+x+2) \end{aligned}$$

Como $x^2 + x + 2$ *não tem raízes em* $\frac{\mathbb{Z}}{3\mathbb{Z}}$ *ela é irredutível.*
Portanto a decomposição de $f(x)$ *em* $\frac{\mathbb{Z}}{3\mathbb{Z}}$ *é*

$$f(x) = (x-1)(x^2+x+2)$$

(c) Se $f(x) = x^4 + x - 1$ *então* $f(0) = -1$ *e* $f(1) = 1$. *Portanto pelo Teorema do Valor Intermediário existe uma raiz real entre 0 e 1. Portanto* $f(x)$ *não é irredutível em* $\mathbb{R}[x]$.

(d) Se $f(x) = x^7 - x^6 + 2x^2 - 2$ *então* $f(1) = 0$. *Portanto pelo Teorema do Fator,* $(x-1)$ *é uma raiz de* $f(x)$. *Aplicando o Briot-Ruffini*

	1	−1	0	0	0	2	0	−2	1
	1	0	0	0	0	2	2	0	

Isto nos dá a fatoração

$$\begin{aligned} f(x) &= x^7 - x^6 + 2x^2 - 2 \\ &= (x-1)(x^6 + 2x + 2) \end{aligned}$$

Seja $g(x) = x^6+2x+2$. *Então* $g(x)$ *é irredutível em* $\mathbb{Z}[x]$ *usamos o Teorema 6(Critério de Eisenstein) com* $p = 2$.

De fato

$$2 \nmid 1, \;\; 2|2, \;\; e \;\; 2|2, \;\; mas \;\; 2^2 \nmid 2$$

Portanto, pelo Critério de Eisenstein, $g(x)$ *é irredutível em* $\mathbb{Z}[x]$..

Portanto a decomposição de $f(x)$ *em* $\mathbb{Z}[x]$ *é*

$$f(x) = (x+1)(x^6 + 2x + 2).$$

(e) $f(x) = 2x^5 + 5x^4 + 4x^3 + 7x^2 + 7x + 2 \in \mathbb{Q}[x]$.

- *Primeiramente procuramos raízes. Como* $a_0 = 2$ *e* $a_5 = 2$, *pelo Teorema 2 (Critério da Raiz Racional), temos como candidato* $x = -2$. *Verificando esta possibilidade temos*

$$f(-2) = -64 + 80 - 32 + 28 - 14 + 2 = 0$$

Portanto $x = -2$ *é uma raíz, ou seja* $(x + 2)$ *divide* $f(x)$.

- *Aplicando o Briot-Ruffini*

2	5	4	7	7	2	-2
2	1	2	3	1	0	

Isto nos dá a fatoração

$$\begin{aligned} f(x) &= 2x^5 + 5x^4 + 4x^3 + 7x^2 + 2 \\ &= (x+2)(2x^4 + x^3 + 2x^2 + 3x + 1) \end{aligned}$$

- *Agora consideramos* $g(x) = 2x^4 + x^3 + 2x^2 + 3x + 1$. *Como* $a_0 = 1$ *e* $a_4 = 2$, *pelo Teorema 2 (Critério da Raiz Racional), temos como candidato* $x = -\frac{1}{2}$. *Verificando esta possibilidade*

temos

$$f\left(-\frac{1}{2}\right) = \frac{1}{8} - \frac{1}{8} + \frac{1}{2} - \frac{3}{2} + 1 = 0$$

Portanto $x = -\frac{1}{2}$ *é uma raíz, ou seja* $\left(x + \frac{1}{2}\right)$ *divide* $f(x)$.

- *Aplicando o Briot-Ruffini*

2	1	2	3	1	$-\frac{1}{2}$
2	0	2	2	0	

Isto nos dá a fatoração

$$\begin{aligned} g(x) &= 2x^4 + x^3 + 2x^2 + 3x + 1 \\ &= \left(x + \frac{1}{2}\right)(2x^3 + 2x + 2) \\ &= (2x + 1)(x^3 + x + 1) \end{aligned}$$

- *Agora* $h(x) = x^3 + x + 1$ *não tem raízes em* $\mathbb{Q}$, *porque pelo Critério da Raiz Racional as únicas possibilidades são* ± 1 *(pois* $a_0 = a_3 = 1$*), mas*

$$h(1) = 1 + 1 + 1 = 3 \neq 0 \quad e \quad h(-1) = -1 - 1 + 1 = 1 \neq 0$$

Porque, $h(x) = x^3 + x + 1$ *é irredutível, pois pelo Teorema 3:(Teste de redutibilidade para graus 2 e 3), um polinômio de grau 3 sem raízes é irredutível.*

Portanto, a decomposição de $f(x)$ *em* $\mathbb{Q}[x]$ *é*

$$2x^5 + 5x^4 + 4x^3 + 7x^2 + 7x + 2 = (x + 2)(2x + 1)(x^3 + x + 1)$$

(f) $f(x) = x^{11} + 1 \in \mathbb{Z}_{11}[x]$.

Consideramos $g(x) = (x + 1)^{11}$. *Usando a expansão Binômio temos que*

$$\begin{aligned} g(x) &= x^{11} + \binom{11}{1}x^{10} + \binom{11}{2}x^9 + \binom{11}{3}x^8 + \cdots + \binom{11}{10}x + 1 \\ &= f(x) + \binom{11}{1}x^{10} + \binom{11}{2}x^9 + \binom{11}{3}x^8 + \cdots + \binom{11}{10}x \end{aligned}$$

Usando o fato que $11 \Big| \begin{pmatrix} 11 \\ k \end{pmatrix}$ *para* $1 \leq k \leq 10$, *temos que em* $\mathbb{Z}_{11}$

$$x^{11} + 1 = (x+1)^{11}.$$

Exercício 2.5.12. *Prove os seguintes polinômios são irredutíveis.*

(a) $x^4 + x^3 + x^2 + x + 1$ *é irredutível em* $\mathbb{Z}_2[x]$

(b) $x^4 - 7x^3 + 5x^2 - 3x - 9$ *é irredutível em* $\mathbb{Q}[x]$

(c) $x^8 + 6x^5 - 12x^3 + 18x^2 - 24x - 60$ *é irredutível em* $\mathbb{Q}[x]$

Solução. *(a) Para mostrar que* $f(x) = x^4 + x^3 + x^2 + x + 1$ *é irredutível em* $\mathbb{Z}_2[x]$,

- *Observamos primeiro que* $f(x)$ *não tem raízes em* $\mathbb{Z}_2$ *pois* $f(0) = 1$ *e* $f(1) = 1$. *Portanto pelo Teorema do Fator* $f(x)$ *não tem fatores lineares. Além disto,* $f(x)$ *não tem polinômios de grau 3.*
- *Portanto precisa verificar fatores irredutíveis de grau 2. De exemplo 2 (pagina 143 do livro), sabemos que* $x^2 + x + 1$ *é o único polinômio irredutível de grau 2 em* $\mathbb{Z}_2[x]$, *portanto vamos divide* $f(x)$ *por* $x^2 + x + 1$:

$$\begin{array}{r|l} x^4 + x^3 + x^2 + x + 1 & x^2 + x + 1 \\ \hline -x^4 - x^3 - x^2 & x^2 + 3x + 5 \\ \hline x + 1 & \end{array}$$

Assim, na divisão temos um resto de $x + 1 \neq 0$, *ou seja* $x^2 + x + 1$ *não é um fator de* $f(x)$. *Portanto* $f(x)$ *é irredutível.*

(b) Para mostrar que $g(x) = x^4 - 7x^3 + 5x^2 - 3x - 9$ *é irredutível em* $\mathbb{Q}[x]$, *usamos o Teorema 5(Teste de Irredutibilidade mod p) acima:*
Seja $\bar{g}$ *é o polinômio obtido de g reduzindo todos os coeficientes mod* 2. *Então* $\bar{g}(x) = x^4 + x^3 + x^2 + x + 1$ *que sabemos que é irredutível em* $\mathbb{Z}_2[x]$ *em parte (a). Portanto pelo Teorema 4,* $g(x)$ *é irredutível em* $\mathbb{Q}[x]$.

(c) Para mostrar que $h(x) = x^8 + 6x^5 - 12x^3 + 18x^2 - 24x - 60$ *é irredutível em* $\mathbb{Q}[x]$, *usamos o Teorema 6(Critério de Eisenstein) com* $p = 3$.
De fato

$$3 \nmid 1, \quad 3|6, \quad 3|(-12), \quad 3|18, \quad 3|(-24), \quad e \quad 3|60, \quad mas \quad 3^2 \nmid 60$$

Portanto, pelo Critério de Eisenstein, $h(x)$ é irredutível em $\mathbb{Q}[x]$.

Exercício 2.5.13. *Quais dos ideais I são maximal no anel R?*

(b) $I =< x >, \quad R = \mathbb{Z}[x]$;

(c) $I =< x >, \quad R = \mathbb{Q}[x]$;

(c) $I =< x^2 + x + 1 >, \quad R = \mathbb{Z}_2[x]$;

Solução.

(a) Como $\mathbb{Z}[x]/_{< x >} \cong \mathbb{Z}$, *que não é um corpo, temos que* $< x > \subset \mathbb{Z}[x]$ *não é um ideal maximal.*

(b) Como $\mathbb{Q}[x]/_{< x >} \cong \mathbb{Q}$, *que é um corpo, temos que* $< x > \subset \mathbb{Q}[x]$ *é um ideal maximal.*

(c) Como $x^2 + x + 1$ *é irredutível em* $\mathbb{Z}_2[x]$ *temos que* $\mathbb{Z}_2/_{< x^2 + x + 1 >}$ *é um corpo.*
Portanto $< x^2 + x + 1 > \subset \mathbb{Z}_2[x]$ *é um ideal maximal.*

2.5.7 Atividade

1. *Determine todas raízes e suas multiplicidades do polinômio* $p(x) = x^5 + \overline{4}x^4 + \overline{4}x^3 - x^2 - \overline{4}x + \overline{1} \in \mathbb{Z}_5[x]$

2. *Calcule o produto* $(2x^2 + x + 1)(2x^2 + 3x + 2)$ *em* $\mathbb{Z}_m[x]$ *para* $m = 2, 3, 6$.

3. *Seja* $f(x) = x^4 + x^3 + \overline{1} \in \mathbb{Z}_2[x]$. *Determine se existem polinômios* $q(x), p(x) \in \mathbb{Z}_2[x]$, *ambos de grau 2, tais que* $f(x) = q(x) \cdot p(x)$.

4. *Resolva a equação* $x^2 = -\overline{1}$ *em* $\mathbb{Z}_5$.

5. *Seja* $A = \{p(x) \in \mathbb{Z}_9[x]; gr(p(x)) = 9\}$. *Determine quantos elementos o conjunto A possui.*

6. *Determine as raízes em* $\mathbb{Z}_5$ *do polinômio*

$$p(x) = x^{504} + \overline{4}x^{415} + \overline{2}x^{212} + \overline{2}x^{31} + \overline{1} \in \mathbb{Z}_5[x].$$

(Sugestão: aplique o Teorema de Fermat: Seja p um numero primo, então $a^{p-1} \equiv 1$ *(mod p)* $\forall\, a \in \mathbb{Z}$, *tal que p não divide a.)*

7. *Em* $\mathbb{Z}_9[x]$ *considere os polinômios* $p_1(x) = 3x + 5$ *e* $p_2(x) = 6x + 3$

   (a) Determine, caso exista, um polinômio $q \in \mathbb{Z}_9[x]$, *tal que grau q=1 e* $p_1 q = 1$.

(b) Determine, caso exista, um polinômio $q \in \mathbb{Z}_9[x]$, *tal que grau* $q=1$ *e* $p_2 q = 0$.

8. *Determine se os anéis abaixo são domínios de integridade. Justifique suas respostas.* (*a*) $\mathbb{Z}_6[x]$ (*b*) $\mathbb{Z}_5[x]$

9. *Se* F *é um corpo e* $f(x), g(x) \in F[x]$, *prove que*

$$J = \left\{ h(x) = p(x)f(x) + q(x)g(x) \mid p(x), q(x) \in F[x] \right\}$$

é um ideal de $F[x]$.

10. *Determine polinômios* $q(x)$ *e* $r(x)$ *tais que* $f(x) = g(x)q(x) + r(x)$, *e* $r(x) = 0$ *ou grau* $r(x) <$ *grau* $g(x)$:

(a) $f(x) = x^4 + x^3 + \overline{2}x^2 + x + \overline{1}, \quad g(x) = x^3 + \overline{3}x^2 + x + \overline{3} \in \mathbb{Z}_5[x]$

(b) $f(x) = x^7 + x^6 + \overline{2}x^5 + x^3 + \overline{2}x^2 + \overline{2}x, \quad g(x) = \overline{2}x^5 + +x^3 + \overline{2}x^2 + 1 \in \mathbb{Z}_3[x]$

11. *Suponha que o polinômio* $f(x) = x^5 + ax^4 + bx^3 + cx^2 + 4 \in \mathbb{R}[x]$ *tem resto 4 quando dividido pelo polinômio* $(x - 1)$, *tem resto 6 quando dividido pelo polinômio* $(x + 1)$ *e que é divisível pelo polinômio* $(x - 2)$. *Determine o valor do produto* abc.

12. *O polinômio* $p(x) = x + \overline{2}$ *divide* $f(x) = x^4 + x^3 + x + \overline{1}$ *em* $\mathbb{Z}_2[x]$? *em* $\mathbb{Z}_3[x]$? *em* $\mathbb{Z}_5[x]$? *em* $\mathbb{Z}_7[x]$? *em* $\mathbb{Z}_{23}[x]$?

13. *Determine para que números primos* p *o polinômio* $(x^4 + x^3 + x^2 + x) \in \mathbb{Z}_p[x]$, *admite a raiz* 2.

14. *Em cada um dos seguintes casos escreve o polinômio* $f(x)$ *em produtos de polinômio irredutíveis no anel* $\mathcal{R}$:

(a) $\mathcal{R} = \dfrac{\mathbb{Z}}{5\mathbb{Z}}[x], \quad f(x) = x^3 + 4x + 4$

(b) $\mathcal{R} = \dfrac{\mathbb{Z}}{3\mathbb{Z}}[x], \quad f(x) = x^3 - 2x^2 - x + 1$

(c) $\mathcal{R} = \mathbb{Z}[x], \quad f(x) = x^4 + 3x^3 + 6x + 15$

(d) $\mathcal{R} = \mathbb{Z}_3[x], \quad f(x) = x^4 + 2x^3 + 2x + 2$

(e) $\mathcal{R} = \mathbb{Q}[x], \quad f(x) = x^3 - 6x - 1$

(f) $\mathcal{R} = \mathbb{Q}[x], \quad f(x) = 7x^5 + 14x^3 + 8x^2 - 4x + 2$

(g) $\mathcal{R} = \mathbb{Q}[x], \quad f(x) = x^4 - 6x^2 + 1$

15. *Determine todos os polinômios mônicos irredutíveis de grau 2 em* $\mathbb{Z}_3[x]$. *Justifique porque cada um destes polinômios são irredutíveis e porque destes são os únicos irredutíveis.*

16. *Determine todos os valores de* $a \in \mathbb{Z}_5$ *tal que o anel quociente* $\dfrac{\mathbb{Z}_5[x]}{< x^3 + 2x^2 + ax + 3 >}$ *é um corpo.*

Bibliografia

[1] *Domingues, H. H.; Iezzi, G.* ***Álgebra Moderna.*** *4ª edição. Atual Editora 2003.*

[2] *Fraleigh, John B.* ***A First Course in Abstract Algebra.*** *6th Edition, New York, Addison Wiley, (2000).*

[3] *Gallian, Joseph A.* ***Contemporary Abstract Algebra.*** *7th Edition. Brooks/Cole. Cengage Learning.*

[4] *Garcia, A.; Lequain, Y.* ***Elementos de Álgebra****, Rio de Janeiro, Projeto Euclides/IMPA. (2002).*

[5] *Gonçalves, Adilson.* ***Introdução à Álgebra.*** *5ª edição. Rio de Janeiro. Projeto Euclides/IMPA, 1999.*

[6] *Herstein, I. N.* ***Tópicos de Álgebra.*** *2ª edição. John Wiley & Sons, Inc.(1975).*

[7] *Lang, Serge.* ***Esrutura Algébricas.*** *Rio de Janeiro: Livros Técnicos e Científicos.(1972) .*

[8] *Monteiro, L. H.* ***Elementos de Álgebra****, Rio de Janeiro, Projeto Euclides/IMPA. (1971).*

Universidade Federal da Bahia

PROGRAD
PRÓ-REITORIA DE GRADUAÇÃO

Instituto de Matemática
UNIVERSIDADE FEDERAL DA BAHIA

SEAD
Superintendência de Educação a Distância | UFBA

UAB UNIVERSIDADE ABERTA DO BRASIL

NELT NÚCLEO DE ESTUDOS DE Linguagens & Tecnologias