Álgebra 1

Notas de Aula 1/2016[1]

José Antônio O. Freitas
Departamento de Matemática
Universidade de Brasília - UnB

SUMÁRIO

LISTA DE FIGURAS

Prefácio

Essas notas de Aula são referentes à matéria Álgebra 1, ministrada na UnB - Universidade de Brasília - durante o 2 Semestre de 2010 pelo professor José Antônio de O. Freitas, Departamento de Matemática. Tais notas foram transcritas e editadas pelo graduando em Ciências Econômicas Luiz Eduardo Sol R. da Silva[2].

[2] luizeduardosol@hotmail.com

Notações e expressões

- $\neg$ Não
- $\forall$ Para todo
- / Tal que
- | Divide
- $\Rightarrow$ Implica
- $\in$ Pertence
- $\emptyset$ Vazio
- $\subseteq$ Contido ou igual a
- $\supseteq$ Contém ou igual a
- $\wedge$ E
- $\vee$ Ou
- = Igual
- $\neq$ Diferente
- $\mathbb{Z}$ Números Inteiros
- $\mathbb{R}$ Números Reais
- $\cap$ Intersecção
- $>$ Maior que
- $\geq$ Maior ou igual a
- $\bigcup_{i=1}^{n}$ União de n conjuntos
- $\bigsqcup_{i=1}^{n}$ União disjunta de n conjuntos
- $\leftrightarrow$ Se, e somente se
- $\veebar$ Ou...,ou..., mas nunca ambos
- $\rightarrow$ Se,... então...
- $\exists$ Existe
- $\Leftrightarrow$ Equivalente a
- $\notin$ Não pertence
- # Fim da demonstração
- $\mathbb{N}$ Números Naturais
- $\mathbb{Q}$ Números Racionais
- $\nsubseteq$ Não contém ou é igual a
- $\cup$ União
- $\sqcup$ União Disjunta
- $<$ Menor que
- $\leq$ Menor ou igual a
- $\bigcap_{i=1}^{n}$ Intersecção de n conjuntos
- Q.E.D. (*Quod Erat Demonstrandum*): Como se queria demonstrar
- P.B.O.: Princípio da boa ordenação
- H.I.: Hipótese de Indução
- *Mutatis Mutandis*: Mudando o que tem que ser mudado

CAPÍTULO 1

CONCEITOS BÁSICOS

Definição 1.1. *Uma **proposição** é todo conjunto de palavras ou símbolos ao qual podemos atribuir um **valor lógico**.*

Definição 1.2. *Diz-se que o **valor lógico** de uma proposição é "verdade" (V) se a proposição é verdadeira e ou "falsidade" (F) se a proposição é falsa.*

1.1 Príncipio da não contradição e do terceiro excluído

1. Uma proposição não pode ser verdadeira e falsa ao mesmo tempo.
2. Toda proposição ou é verdadeira ou é falsa, isto é, verifica-se sempre um destes casos e nunca um terceiro.

Assim esses princípios afirmam que:

"Toda proposição tem um, e um só, dos valores lógicos **verdade** ou **falsidade**."

De modo geral vamos trabalhar com proposições da forma:

1. Se $\mathcal{H}$, então $\mathcal{T}$.

Aqui $\mathcal{H}$ é chamado de hipótese e $\mathcal{T}$ de tese. Neste tipo de proposição iremos admitir que $\mathcal{H}$ é uma verdade e precisaremos provar que $\mathcal{T}$ é verdade. Ou seja precisamos construir um argumento que justifique $\mathcal{T}$ ser verdadeira à partir do fato de $\mathcal{H}$ ser verdadeira.

2. $\mathcal{H}$ se, e somente se, $\mathcal{T}$ ou $\mathcal{H}$ se, e só se, $\mathcal{T}$.

   Esse tipo de proposição será decomposta em duas proposições no formato anterior. Isto é:

   (a) Se $\mathcal{H}$, então $\mathcal{T}$.

   (b) Se $\mathcal{T}$, então $\mathcal{H}$.

   No primeiro caso admitimos $\mathcal{H}$ verdadeira e provamos que $\mathcal{T}$ também é verdadeira e no segundo caso admitimos que $\mathcal{T}$ é verdadeira e provamos que $\mathcal{H}$ é verdadeira.

CAPÍTULO 2

NOÇÕES DE TEORIA DE CONJUNTOS

2.1 Conceitos básicos

Um conjunto é uma "coleção"ou "família"de elementos.

Usaremos letras maiúsculas do alfabeto para denotar os conjuntos e denotaremos elementos por letras minúsculas do alfabeto.

Dado um conjunto A, para indicar o fato de que x é um elemento de A, escrevemos:

$$x \in A.$$

Para dizer que um elemento x não pertence ao conjunto A, escrevemos:

$$x \notin A.$$

Um conjunto sem elementos é chamado de **vazio** ou **conjunto vazio**. Tal conjunto é denotado por $\emptyset$.

Dado um conjunto A e x um elemento, ocorre sempre o uma das seguintes situações:

$$x \in A \text{ ou } x \notin A.$$

Além disso, para dois elementos x, $y \in A$, ocorre exatamente uma das seguinte situações:

$$x = y \text{ ou } x \neq y.$$

2.2 Descrição de um conjunto

Um conjunto A pode ser dado pela simples listagem dos seus elementos, como por exemplo:

$$A = \{1, 2, 3, 4, 5\}$$
$$B = \{verdade, falso\}.$$

Um conjunto também pode ser dado pela descrição das propriedades dos seus elementos, como por exemplo:

$$A = \{n \mid n \text{ é múltiplo de } 2\} = \{2, 4, 6, ...\}.$$

2.3 Alguns conjuntos importantes

1. $\mathbb{N} = \{0, 1, 2, 3, ...\}$ o conjunto do números naturais.

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

3. $\mathbb{N}_0 = \{0, 1, 2, 3, ...\}$ o conjunto dos números inteiros não negativos.

4. $\mathbb{R}$ o conjunto dos números reais.

5. $\mathbb{R}^*$ o conjunto dos números reais não nulos.

6. $\mathbb{Q} = \left\{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\right\}$ o conjunto dos números racionais.

2.4 Propriedades dos conjuntos

Definição 2.1. *Dados dois conjuntos A e B, dizemos que A e B são iguais se, e somente se, eles têm os mesmos elementos. Ou seja, para todo $x \in A$ temos que $x \in B$ e para todo $y \in B$ temos $y \in A$.*

Se A e B são iguais, escrevemos $A = B$

$$\{1, 2, 3, 4\} = \{3, 2, 1, 4\}$$

$$\{1, 2, 3\} \neq \{2, 3\}$$

Definição 2.2. *Se A e B são dois conjuntos, dizemos que A é um **subconjunto** de B ou que A **está contido** em B ou que B **contém** A se todo elemento de A for elemento de B. Ou seja, se para todo elemento $x \in A$, temos $x \in B$. Nesse caso, escrevemos $A \subseteq B$ ou $B \supseteq A$.*

Caso A seja um subconjunto de B mas não é igual a B, escrevemos:

$$A \subsetneq B.$$

Nesse caso, dizemos que A é um subconjunto próprio de B.

Para dizer que A não está contido em B, escrevemos $A \nsubseteq B$

Usando a definição de continência podemos definir igualdade de conjuntos da seguinte forma: dois conjuntos A e B são iguais se, e somente se, $A \subseteq B$ e $B \subseteq A$. Ou seja, se $A = B$ então $A \subseteq B$ e $B \subseteq A$, por outro lado, se $A \subseteq B$ e $B \subseteq A$, então $A = B$.

Quando A e B não são iguais, escrevemos $A \neq B$. Para que $A \neq B$ devemos ter $A \nsubseteq B$ ou $B \nsubseteq A$.

2.4.1 Propriedades da continência

Dados conjuntos A, B e C temos:

1. $A \subseteq A$ (Reflexividade)

2. Se $A \subseteq B$ e $B \subseteq A$, então $A = B$. (Antissimetria)

3. Se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$. (Transitividade)

Considere os seguintes conjuntos:

$$A = \{n \in \mathbb{N} \mid n \text{ é múltiplo de } 2\} = \{2, 4, 6, ...\}$$
$$B = \{n \in \mathbb{N} \mid n \text{ é múltiplo de } 3\} = \{3, 6, 9, ...\}.$$

Neste caso, $2 \in A$ e $2 \notin B$, logo $A \nsubseteq B$. Por outro lado, $3 \in B$ e $3 \notin A$ e com isso $B \nsubseteq A$. Portanto, dados dois conjuntos A e B, nem sempre temos $A \subseteq B$ ou $B \subseteq A$.

Proposição 2.2.1. *Seja A um conjunto. Então $\emptyset \subseteq A$.*

Prova: Suponha que $\emptyset \nsubseteq A$. Logo existe $x \in \emptyset$ tal que $x \notin A$. Mas por definição, o conjunto vazio não contém elementos. Logo a existência de $x \in \emptyset$ é uma contradição. Tal contradição surgiu por termos suposto que $\emptyset \nsubseteq A$. Portanto, $\emptyset \subseteq A$, como queríamos demonstrar. $\diamond$

2.5 Relações entre conjuntos

Definição 2.3 (Intersecção)**.** *Sejam A e B dois conjuntos. Definimos a **intersecção** de A e B como sendo o conjunto $A \cap B$ cujos elementos pertencem ao conjunto A e B simultaneamente. Assim,*

$$A \cap B = \{x \mid x \in A \; e \; x \in B\}.$$

Exemplo: Sejam

$$A = \{1, 2, 3\}$$
$$B = \{2, 3, 4\}$$
$$A \cap B = \{2, 3\}.$$

Proposição 2.3.1. *Sejam A e B dois conjuntos. Então*

1. $(A \cap B) \subseteq A$;

2. $(A \cap B) \subseteq B$;

3. $A \subseteq A \cup B$;

4. $B \subseteq A \cup B$.

Prova: Seja $x \in A \cap B$ um elemento qualquer. Da definição de interseção de conjuntos temos $x \in A$ e $x \in B$. De $x \in A$ segue que $A \cap B \subseteq A$ e de $x \in B$ segue que $A \cap B \subseteq B$, como queríamos demonstrar. ◊

Definição 2.4 (União)**.** *Sejam A e B dois conjuntos. Definimos a **união** de A com B como sendo o conjunto $A \cup B$, cujos elementos pertencem ao conjunto A ou ao conjunto B. Assim,*

$$A \cup B = \{x \mid x \in A \text{ ou } x \in B\}.$$

Exemplo: Sejam

$$\begin{aligned} A &= \{1, 2, 3\} \\ B &= \{2, 3, 4\} \\ A \cup B &= \{1, 2, 3, 4\} \end{aligned}$$

O conceito de união ($\cup$) e intersecção ($\cap$) pode ser estendido para mais de dois conjuntos.

Definição 2.5 (União e Intersecção finita de conjuntos)**.** *Sejam $A_1, \ldots, A_n$ conjuntos. Então*

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{k=1}^{n} A_k$$

é o conjunto dos elementos x tais que x pertence a pelo menos um dos conjuntos $A_1, \ldots, A_n$. Agora,

$$A_1 \cap \cdots \cap A_n = \bigcap_{k=1}^{n} A_k$$

é o conjunto dos elementos x que pertencem a todos os conjuntos $A_1, \ldots, A_n$ simultaneamente.

Quando a intersecção de dois ou mais conjuntos é vazia, dizemos que eles são **conjuntos disjuntos**.

Sejam A e B conjuntos tais que $C = A \cup B$ e $A \cap B = \emptyset$. Neste caso dizemos que C é uma **união disjunta** de A e B. Denotamos tal fato por

$$C = A \sqcup B.$$

Proposição 2.5.1. *Sejam A, B e C três conjuntos, então:*

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Prova:

1. Precisamos mostrar que

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$$
$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C).$$

Seja $x \in A \cap (B \cup C)$. Logo $x \in A$ e $x \in B \cup C$. Agora, de $x \in B \cup C$, segue que $x \in B$ ou $x \in C$. Suponha que $x \in B$. Como $x \in A$, então $x \in A \cap B$. Assim, $x \in (A \cap B) \cup (A \cap C)$, ou seja, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Por outro lado, se $x \in C$, como $x \in A$, então $x \in A \cap C$ e daí $x \in (A \cap B) \cup (A \cap C)$, logo $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Portanto,
$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C).$$

Agora, seja $x \in (A \cap B) \cup (A \cap C)$. Daí, $x \in A \cap B$ ou $x \in A \cap C$. Suponha que $x \in A \cap B$. Assim, $x \in A$ e $x \in B$. Como $x \in B$, segue que $x \in B \cup C$ e então $x \in A \cap (B \cup C)$, ou seja, $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Agora, suponnha que $x \in A \cap C$. Com isso $x \in A$ e $x \in C$. Desse modo, $x \in B \cup C$ e então $x \in A \cap (B \cup C)$ e daí

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C).$$

Portanto
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

como queríamos.

2. Análoga ao caso anterior.

◊

Definição 2.6 (Diferença de Conjuntos)**.** *Dados dois conjuntos A e B, definimos a* ***diferença*** *dos conjuntos A e B, denotado $A - B$ (ou $A \backslash B$) como sendo*

$$A - B = \{x \mid x \in A \text{ e } x \notin B\}.$$

Exemplos:

1. $A = \{1, 2, 3, 5, 4\}$, $B = \{2, 3, 6, 8\}$, $A - B = \{1, 4, 5\}$, $B - A = \{6, 8\}$
2. $A = \{2, 4, 6, 8, 10, ...\}$, $B = \{3, 6, 9, 12, 15, ...\}$, $A - B = \{2, 4, 8, 10, 14, 16, ...\}$, $B - A = \{3, 9, 15, 21, ...\}$

Proposição 2.6.1. *Sejam A, B e C conjuntos não vazios. Então*

$$(A \cup B) - C = (A - C) \cup (B - C).$$

Prova: Segue da definição de diferença de conjuntos. $\diamond$

Definição 2.7 (Complementar)**.** *Dados dois conjuntos A e E tais que $A \subseteq E$, definimos o* ***complementar*** *de A em E, denotado A^C ou $C_E(A)$, como*

$$C_E(A) = \{x \in E \mid x \notin A\}.$$

Observações:

1. Se $A = E$, então $C_A(A) = \{x \in A \mid x \notin A\} = \emptyset$.
2. $(A^C)^C = \{x \in E \mid x \notin A^C\} = \{x \in E \mid x \in A\} = A$

Exemplo:

$$\begin{aligned} A &= \{1, 2, 3, 4\} \\ E &= \{1, 2, 3, 5, 4, 0, 8, 9\} \\ A^C &= \{0, 5, 8, 9\} \end{aligned}$$

Proposição 2.7.1. *Sejam A, B e E conjuntos. Se $A \subseteq B \subseteq E$, então $C_E(B) \subseteq C_E(A)$.*

Prova: Seja $x \in B^C$. Assim $x \notin B$ e como $A \subseteq B$, então $x \notin A$. Daí por definição $x \in A^C$, ou seja, $B^C \subseteq A^C$. $\diamond$

Proposição 2.7.2. *Sejam A, B e E três conjunto tais que $A \subseteq E$ e $B \subseteq E$. Então:*

1. $(A \cup B)^C = A^C \cap B^C$
2. $(A \cap B)^C = A^C \cup B^C$

Prova:

1. Seja $x \in (A \cup B)^C$. Logo $x \notin A \cup B$, assim $x \notin A$ e $x \notin B$. Daí, $x \in A^C$ e $x \in B^C$, isto é, $x \in A^C \cap B^C$. Desse modo,
$$(A \cup B)^C \subseteq A^C \cap B^C. \tag{2.1}$$
Por outro lado, se $x \in A^C \cap B^C$, então $x \in A^C$ e $x \in B^C$. Daí, $x \notin A$ e $x \notin B$, ou seja, $x \notin A \cup B$, logo $x \in (A \cup B)^C$. Desse modo
$$A^C \cap B^C \subseteq (A \cup B)^C. \tag{2.2}$$
Portanto, de (2.1) e (2.2) temos
$$(A \cup B)^C = A^C \cap B^C.$$

2. Seja $x \in (A \cap B)^C$. Logo $x \notin A \cap B$, assim $x \notin A$ ou $x \notin B$. Então $x \in A^C$ ou $x \in B^C$, isto é, $x \in A^C \cup B^C$. Desse modo,
$$(A \cap B)^C \subseteq A^C \cup B^C. \tag{2.3}$$
Por outro lado, se $x \in A^C \cup B^C$, então $x \in A^C$ ou $x \in B^C$. Daí, $x \notin A$ ou $x \notin B$, ou seja, $x \notin A \cap B$, logo $x \in (A \cap B)^C$. Desse modo
$$A^C \cup B^C \subseteq (A \cap B)^C. \tag{2.4}$$
Portanto, de (2.3) e (2.4) temos
$$(A \cap B)^C = A^C \cup B^C.$$

$\diamond$

Definição 2.8 (Produto Cartesiano). *Dados dois conjuntos A e B, definimos o* ***produto cartesiano*** *de A por B como sendo o conjunto*

$$A \times B = \{(x, y) \mid x \in A, y \in B\}.$$

Dados $(x, y), (z, t) \in A \times B$, temos $(x, y) = (z, t)$ se, e somente se, $x = z$ e $y = t$.

Em geral, $A \times B \neq B \times A$.

Exemplo:

$$\begin{aligned} A &= \{1, 2\} \\ B &= \{3\} \\ A \times B &= \{(1, 3), (2, 3)\} \\ B \times A &= \{(3, 1), (3, 2)\} \end{aligned}$$

Definição 2.9 (Conjunto Partes). *Para qualquer conjunto A, indicamos por $\mathcal{P}(A)$ o conjunto*

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

que é chamado de ***conjunto das partes*** *de A.*

Os elementos desse conjunto são todos os subconjuntos de A. Dizer que $Y \in \mathcal{P}(A)$ significa que $Y \subseteq A$. Particularmente, temos $\emptyset \in \mathcal{P}(A)$ e $A \in \mathcal{P}(A)$.

Exemplos:

1. $A = \emptyset, \mathcal{P}(A) = \{\emptyset\}$;

2. $B = \{x\}, \mathcal{P}(B) = \{\emptyset, B\}$;

3. $C = \{a, b, c\}, \mathcal{P}(\mathrm{C}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \mathrm{C}\}$;

4. $D = \mathbb{R}, \mathcal{P}(D) = \{X \mid X \subseteq \mathbb{R}\}$, por exemplo $\mathbb{Q} \in \mathcal{P}(D)$.

CAPÍTULO 3

NÚMEROS INTEIROS

3.1 Conceitos básicos

Indicaremos por $\mathbb{Z}$ o conjunto dos números inteiros. Portanto $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, ...\}$.

3.1.0.1 Propriedades básicas da adição e da multiplicação

Admitiremos as propriedades básicas da adição e da multiplicação em $\mathbb{Z}$. Assim, dados $a, b, c \in \mathbb{Z}$, temos:

Adição

1. $a + b = b + a$
2. $a(b + c) = (a + b) + c$
3. $a + 0 = a$
4. $a + (-a) = 0$

Multiplicação

1. $ab = ba$
2. $a(bc) = (ab)c$
3. $a1 = a$
4. $ab = 0 \to a = 0 \vee b = 0$
5. $ab = 1 \to a = \pm 1 \wedge b = \pm 1$
6. $a(b + c) = ab + ac$

3.1.0.2 Propriedades básicas das desigualdades

Admitiremos também a relação "menor ou igual", em $\mathbb{Z}$, denotada por "$\leq$". Dados a, b, $c \in \mathbb{Z}$, valem as seguintes propriedades:

1. $a \leq a$
2. $a \leq b \wedge b \leq a \to a = b$
3. $a \leq b \wedge b \leq c \to a \leq c$
4. $a \leq b \veebar b \leq a$
5. $a \leq b \to a + c \leq b + c$
6. $0 \leq a \wedge 0 \leq b \to 0 \leq ab$

Para a relação "menor", cujo símbolo é "$<$", vale:

1. Se $a > 0$ e $b > 0$, então $ab > 0$.
2. Se $a > 0$ e $b < 0$, então $ab < 0$.

3.2 Princípio da boa ordenação

Definição 3.1 (Limite Inferior). *Seja A um subconjunto não vazio de $\mathbb{Z}$. Dizemos que A é **limitado inferiormente** se existe $l \in \mathbb{Z}$ tal que $l \leq x$, para todo $x \in A$.*

Por exemplo:
$A = \{-2, 0, 1, 2, 3, ...\}$, $B = \{..., -6, -4, -2, 0\}$, $C = \{8, 16, 24, 32\}$

A e C são limitados inferiormente pois $-3 \leq a$, $7 \leq c$, para todo $a \in A$ e para todo $c \in C$.

Definição 3.2 (Princípio da boa ordenação). *Se A é um subconjunto não vazio de $\mathbb{Z}$ e A é limitado inferiormente, então existe $a_0 \in A$ tal que $a_0 \leq x$ para todo $x \in A$.*

Seja $A \neq \emptyset$, $A \subseteq \mathbb{Z}$ e A limitado inferiormente. Pelo P.B.O., existe $a_0 \in A$ tal que $a_0 \leq x$, para todo $x \in A$. Suponha que existe $a_1 \in A$ tal que $a_1 \leq x$, $x \in A$. Logo devemos ter $a_0 \leq a_1$ e além disso $a_1 \leq a_0$, daí $a_1 = a_0$. Ou seja, o elemento $a_0 \in A$ do P.B.O. é único. Chamamos a_0 de elemento **mínimo** ou **elemento minimal**.

3.3 Princípio da Indução Finita

Teorema 3.1 (Indução finita (1^a versão)). *Dado $a \in \mathbb{Z}$, suponhamos que a cada inteiro $n \geq a$ esteja associada uma proposição $P(n)$ que depende de n. Então $P(n)$ será verdadeira para todo $n \geq a$ desde que seja possível provar o seguinte:*

1. *$P(a)$ é verdadeira.*

2. *Dado $r > a$, se $P(k)$ é verdadeira para todo k tal que $a \leq k \leq r$, então $P(r)$ é verdadeira.*

Teorema 3.2 (Indução finita (2^a versão)). *Dado $a \in \mathbb{Z}$, suponhamos que para cada $n \geq a$ esteja associada uma proposição $P(n)$. Então $P(n)$ é verdadeira para todo $n \geq a$ desde que seja possível provar o seguinte:*

1. *$P(a)$ é verdadeira.*

2. *Se $P(r)$ é verdadeira para $r \geq a$, então $P(r + 1)$ é verdadeira.*

Exemplos 3.2.1. 1. *Mostre que para todo $n \in \mathbb{N}$ vale*

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

Solução: *Para $n = 1$, temos*

$$1 = \frac{1(1+1)}{2}.$$

Agora, suponha que para $r \geq 1$, temos

$$\underbrace{1 + 2 + ... + r = \frac{r(r+1)}{2}}_{H.I}.$$

Assim, para $r + 1$ usando a Hipótese de Indução, obtemos

$$\begin{aligned} 1 + 2 + ... + r + (r+1) &= \frac{r(r+1)}{2} + (r+1) = \frac{r(r+1) + 2(r+1)}{2} \\ &= \frac{(r+2)(r+1)}{2}. \end{aligned}$$

Portanto, pelo princípio da indução finita a afirmação está provada.

2. *Prove que $(1 + p)^n \geq 1 + np$ para todo $n \in \mathbb{N}$ e $p \geq 0$.*

Solução: *Para $n = 1$ temos*

$$(1 + p)^1 \geq 1 + p.$$

Suponha então que para $n = k$ temos

$$(1 + p)^k \geq 1 + kp.$$

Para $n = k + 1$ temos

$$\begin{aligned} (1 + p)^{k+1} &= (1 + p)^r(1 + p) \geq (1 + rp)(1 + p) \\ &= 1 + p + rp + rp^2 \\ &\geq 1 + (r + 1)p. \end{aligned}$$

Logo pelo Princípio da Indução finita a afirmação é verdadeira.

Teorema 3.3. *Dado $a \in \mathbb{Z}$, suponhamos que cada inteiro $n \geq a$ esteja associado uma proposição $P(n)$. Então $P(n)$ será verdadeira $\forall n \geq a$ desde que seja possível provar que:*

1. *$P(a)$ é verdadeira.*
2. *Dado que $r > a$, se $P(k)$ é verdadeira para todo k tal que $a \leq k \leq r$, então $P(r)$ é verdadeira*

Demonstração: Seja $F = \{l \in \mathbb{Z} \mid a \leq l \text{ e } P(l) \text{ é falsa}\}$. Suponha $F \neq \emptyset$. Como F é limitado inferiormente, pelo princípio da boa ordenação, existe $l_0 \in F$ tal que $l_0 \leq x$, para todo $x \in F$. Como $l_0 \in F$, $P(l_0)$ é falsa. Mas $P(a)$ é verdadeira, assim, $l_0 > a$. Agora, como l_0 é o mínimo de F, então $P(x)$ é verdadeira para $a \leq x < l_0$.

Agora pelo item (2) segue que $P(l_0)$ é verdadeira, o que é uma contradição, pois verificamos anteriormente que $P(l_0)$ é falso.

Portanto $F = \emptyset$ e o teorema está demonstrado.#

3.4 Divisibilidade

Definição 3.3 (Divisão)**.** *Sejam a, b números inteiros, $b \neq \emptyset$. Dizemos que b divide a quando existe um inteiro c tal que $a = bc$.*

Exemplos:

1. Os inteiros 1 e -1 dividem todos os números inteiros a, pois

$$a = 1a, a = (-1)(-a)$$

2. O número 0 não divide nenhum inteiro b, pois não existe a tal que $b = 0a$
3. Para todo $b \neq 0$,b divide $\pm b$
4. Para todo inteiro $b \neq 0$, b divide 0, pois $0 = b0$
5. 3 não divide 8, mas 17 divide 51

Notação 3.3.1 (Divisão)**.** *Quando b divide a, escrevemos $b|a$. Quando b não divide a, escrevemos $b \not| a$*

Propriedades

1. $a|a, \forall a \in \mathbb{Z}$

2. Se $a|b$ e $b|a,\ a, b \geq 0 \rightarrow a = b$

   De fato existe $c, d \in \mathbb{Z}/b = ca \wedge a = bd$. Se $a = 0 \vee b = 0$ então $b = 0 \veebar a = 0$. Podemos supor $a \neq 0$ e $b \neq 0$.

   Assim
   $b = c(bd)$
   $b(1 - cd) = 0$. Daí, $1 - cd = 0$, isto é, $cd = 1$.

   Assim, $c = \pm 1 \wedge d = \pm 1$. Como $a > 0$ e $b > 0$, devemos ter $c = d = 1$. Portanto $a = b$

3. Se $a|b$ e $b|c$, então $a|c$

   De fato, $b = pa \wedge c = bq \Rightarrow c = (pq)a$, ou seja, $a|c$

4. Se $a|b$ e $a|c$, então $a|(bx + cy)$, para todos $x, y \in \mathbb{Z}$

   Temos $b = ap$ e $c = aq$, $p, q \in \mathbb{Z}$

   $$bx + cy = apx + aqy = a\underbrace{(px + qy)}_{\in \mathbb{Z}}$$

   Logo $a|(bx + cy)$

3.5 Algoritmo de divisão de Euclides

Teorema 3.4 (Algoritmo de divisão de Euclides)**.** *Para quaisquer $a, b \in \mathbb{Z}$, com $b > 0$, existem únicos q e r inteiros tais que $a = bq + r$, com $0 \leq r < b$.*

Demonstração: Vamos mostrar primeiro a existência de q e r.

Seja $M = \{m \in \mathbb{Z} \mid m = a - bt, t \in \mathbb{Z}\}$. Temos $M \neq \emptyset$ pois $a \in M$. Seja $M^+ = \{x \in M \mid x \geq 0\}$. Por definição M^+ é limitado inferiormente. Além disso, como $t \in \mathbb{Z}$ e $M^+ \subseteq M$ então $M^+ \neq \emptyset$. Logo, pelo princípio da boa ordenação, existe $r \in M^+$ tal que $r \leq x$, para todo

$x \in M^+$. Como $r \in M^+ \subseteq M$, existe $q \in \mathbb{Z}$ tal que $r = a + bq$. Portanto, $a = bq + r$, $q \in \mathbb{Z}$, com $r \geq 0$.

Precisamos provar que $r < b$. Para isso, suponha então que $r \geq b$. Logo $r = a - bq \geq b$, ou seja, $a - bq - b \geq 0$. Isto é, $a - b(q+1) \geq 0$ e desse modo, $a - b(q+1) \in M^+$.

Agora, como $b > 0$ então $bq + b > bq$. Daí $b(q+1) > bq$. Logo $-b(q+1) < -bq$. Finalmente, $a - b(q+1) < a - bq = r$, o que é uma contradição, pois r é o mínimo de M^+. Logo, $r < b$, ou seja, $a = bq + r$, $q, r \in \mathbb{Z}$ com $0 \leq r < b$.

Falta provar a unicidade de q e r. Assim, suponha que existam $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, com $0 \leq r_1 < b$, $0 \leq r_2 < b$, tais que:

$$a = bq_1 + r_1 = bq_2 + r_2.$$

Suponha que $r_1 \neq r_2$. Suponha também que $r_1 > r_2$. Assim,

$$0 \leq r_1 - r_2 = b(q_2 - q_1).$$

E daí, $q_2 - q_1 \geq 0$. Desse modo

$$r_1 = b(q_2 - q_1) + r_2.$$

Mas $r_1 \geq 0$, $q_2 - q_1 \geq 1$, daí $r_1 > b$, o que é uma contradição. Logo $r_1 = r_2$ e então $q_1 = q_2$, o que prova a unicidade.#

3.6 Máximo Divisor Comum

Definição 3.4 (Máximo Divisor Comum). *Dado $a, b \in \mathbb{Z}$, dizemos que $d \in \mathbb{Z}$ é o máximo divisor comum entre a e b se*

1. $d \geq 0$
2. $d|a$ *e* $d|b$
3. *Se d' é um inteiro tal que $d'|a$ e $d'|b$, então $d'|d$*

Observações:

1. Se d e d_1 são máximos divisores comuns entre a e b, então $d = d_1$.

   De fato, dados d e d_1 máximos divisores comuns de a e b, então temos que $d|a, d|b, d_1|a, d_1|b$. Mas pelo item 3 da definição temos $d|d_1$ e $d_1|d$. Agora, como $d_1 \geq 0$ e $d \geq 0$, segue que $d = d_1$

2. Se $a = b = 0$, segue que $d = d_1$

3. Se $a = 0$ e $b \neq 0$, então $d = |b|$

4. Se d é o máximo divisor comum entre a e b, então d também é o máximo divisor comum entre a e $-b$, $-a$ e b e entre $-a$ e $-b$.

Notação 3.4.1 (Máximo Divisor Comum)**.** *Indicaremos por $mdc(a, b)$ o máximo divisor comum ente a e b, que já sabemos que é único quando existe.*

Proposição 3.4.1. *Quaisquer que sejam $a, b \in \mathbb{Z}$, existe $d \in \mathbb{Z}$ que é o máximo divisor comum entre a e b.*

Demonstração: Das observações anteriores podemos considerar somente o caso em que $a > 0$ e $b > 0$.

Seja $L = \{ax + by/x, y \in \mathbb{Z}\}$. Temos que $L \neq \emptyset$ pois tomando $x = 1$ e $y = 0$, temos que $m = a1 + b0$, pelo princípio da boa ordenação, existe $d \in L^+$ tal que $d \leq x$, para todo $x \in L^+$.

Mostremos que $d = mdc(a, b)$

1. $d \geq 0$ pois $d \in L^+$

2. Como $d \in L^+$, existem $x_0, y_0 \in \mathbb{Z}$ tais que $d = ax_0 + by_0$.

   Agora usando o algoritmo da divisão de Euclides para a e d temos que existem $k, r \in \mathbb{Z}, 0 \leq r < d$ tais que $a = kd + r$.

   Assim:

$$a = k(ax_0 + by_0) + r$$

$$r = a(1 - kx_0) + b(-y_0)k$$

Daí, $r \in L$, mas $r \geq 0$, então $r \in L^+$. Como d é o mínimo de L^+ devemos ter $r = 0$ e assim $a = kd$, ou seja, $d|a$.

Analogamente, *Mutatis Mutandis*, mostra-se que $d|b$.

3. Seja $d \in \mathbb{Z}$ tal que $d'|a$ e $d'|b$. Temos que $d'|(ax + by)$, para $x, y \in \mathbb{Z}$, em particular, $d'|(ax_0 + by_0) = d$, ou seja, $d'|d$.

Portanto, $d = mdc(a, b)$.#

Observação:

1. Se $d = mdc(a, b)$, então $d = ax_0 + by_0$, onde $x_0, y_0 \in \mathbb{Z}$. Os elementos x_0 e y_0 satisfazem que tal igualdade não são únicos.

2. Uma igualdade do tipo $d = ax_0 + by_0$ é chamada de **Identidade de Bezout**.

   Exemplos:

   (a) $mdc(2, 3) = 1$
   $1 = 2(-1) + 3.1 = 2.2 + 3(-1)$

   (b) $mdc(4, 8) = 4$

Considere os seguintes subconjuntos de $\mathbb{Z}$:

$$I = \{2k \mid k \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \pm 6, ...\}$$

$$J = \{2r + 1 \mid r \in \mathbb{Z}\} = \{\pm 1, \pm 3, \pm 5, ...\}.$$

Dados quaisquer $a, b \in I$, temos $a + b \in I$. Além disso, dado $n \in \mathbb{Z}$, $na \in I$. Por outro lado, $1, 3 \in J$ mas $1 + 3 = 4 \notin J$.

3.7 Ideais

3.7.0.1 Definição

Definição 3.5. *Um subconjunto não vazio $S \subseteq \mathbb{Z}$ é chamado de um **ideal** de $\mathbb{Z}$ se satisfaz as seguintes condições:*

1. *$r_1 + r_2 \in S$, para todos $r_1, r_2 \in S$,*

2. *$nr \in S$, para todo $n \in \mathbb{Z}$ e para todo $r \in S$.*

3.7.0.2 Propriedades

Seja S um ideal de $\mathbb{Z}$. Então:

1. $r_1 - r_2 \in S$, para todos $r_1, r_2 \in S$, pois $r_1 - r_2 = r_1 + (-r_2)$.

2. $0 \in S$, pois $0 = r - r$, para qualquer $r \in S$.

Exemplos:

1. $S = \{2k \mid k \in \mathbb{Z}\}$ é um ideal de $\mathbb{Z}$.

2. $S = \{0\}$ e $S = \mathbb{Z}$ são ideais de $\mathbb{Z}$, chamados de **ideais triviais**.

3. Dado $a, b, c \in \mathbb{Z}$, o subconjunto $S = \{ax + by/x, y \in \mathbb{Z}\}$ é um ideal de $\mathbb{Z}$.

   $S \neq \emptyset$ pois $0 = a0 + b0 \in S$

   Sejam $ax_1 + by_1, ax_2 + by_2 \in S$. Temos $(ax_1 + by_1) + (ax_2 + by_2) = a(x_1 + x_2) + b(y_1 + y_2) \in S$

   Agora, sejam $ax_1 + by1 \in S$ e $n \in \mathbb{Z}$ temos

$$n(ax_1 + by_1) = a(nx_1) + b(ny_1) \in S$$

De modo geral, dados $a_1, a_2, ..., a_n$ números inteiros, o subconjunto

$$S = \{a_1x_1 + a_2x_2 + ... + a_nx_n/x_1, ..., x_n \in \mathbb{Z}\}$$

é um ideal de $\mathbb{Z}$.

Se S é ideal de $\mathbb{Z}$, então $S = \{nk/n \in \mathbb{Z}\}$.

3.7.0.3 Conjunto dos múltiplos de g

Notação 3.5.1 (Conjunto dos múltiplos de g)**.** *Se $g \in \mathbb{Z}$, denotamos por $g\mathbb{Z}$, ou $\mathbb{Z}g$, o subconjunto dos inteiros que são múltiplos de g (os inteiros que são divisíveis por g). Em outras palavras*

$$g\mathbb{Z} = \{gn/n \in \mathbb{Z}\} = \{0, \pm g, \pm 2g, \pm 3g, ...\}$$

Teorema 3.5. *Seja S um ideal de $\mathbb{Z}$. Então, existe um número $g \in \mathbb{Z}$ tal que $S = g\mathbb{Z}$.*

Demonstração: Se $S = \{0\}$, então tomamos $g = 0$ e daí $S = 0\mathbb{Z}$. Se $S = \mathbb{Z}$, então $g = 1$ e $S = 1\mathbb{Z}$.

Assim podemos supor $S \neq \{0\}$ e $S \neq \mathbb{Z}$. Seja $S^+ = \{x \in S/x > 0\}$. Do ítem 2 da definição de ideal, segue que $S^+ \neq \emptyset$. Assim, pelo princípio da boa ordenação, existe $g \in S^+$ tal que $g \leq x, \forall x \in S^+$.

Como $g \in S^+ \subseteq S$ e S é um ideal de $\mathbb{Z}$, então $gn \in S \forall n \in \mathbb{Z}$, ou seja, $g\mathbb{Z} \subseteq S$.

Agora precisamos mostrar que $a = gq$, onde $q \in \mathbb{Z}$. Assim, dado $a \in S$, o algoritmo da divisão de Euclides garante que existem $q, r \in \mathbb{Z}$ tais que $a = gq + r$, onde $0 \leq r < g$. Como $a, q, g \in S$ e S é um ideal, então $r = a - gq \in S$. Se $r > 0$, então como $r < g$ e g é o mínimo de S^+ obtemos uma contradição. Logo, $r = 0$ e $a = gp$. Daí $S \subseteq g\mathbb{Z}$. Portanto $s = g\mathbb{Z}$.#

Exemplo: O conjunto $S = \{2x - 5y/x, y \in \mathbb{Z}\}$ é ideal de $\mathbb{Z}$. Neste caso,
$S^+ = \{1, 2, 3, ...\}$. Assim, $g = 1$ e $S = 1\mathbb{Z} = \mathbb{Z}$.

CAPÍTULO 4

RELAÇÕES E FUNÇÕES

4.1 Relações

4.1.0.1 Definição

Sejam A e B dois conjuntos não vazios. Os subconjuntos de AxB são chamados relações, ou seja, uma relação em AxB é um subconjunto desse produto cartesiano.

Quando R é uma relação em $A \times B$, também dizemos que R é uma relação de A em B.

Exemplos:

1. Se A={0,1} e B={-1,0,1}, então AxB={(0,-1),(0,0),(0,1),(1,-1),(1,0),(1,1,)}
   São exemplos de relações:
   $R_1 = \{(0,1)\}$
   $R_2 = \emptyset$
   $R_3 = \{(1,-1),(1,1)\}$
   $R_4 = A\text{x}B$

2. Se $A = B = \mathbb{R}$, então AxB é o conjunto formado por todos pares ordenados de números reais. Um exemplo de relação em $\mathbb{R}$x$\mathbb{R}$ é o conjunto:
   $R = \{(x,y) \in \mathbb{R}\text{x}\mathbb{R}/y \geq 0\}$

4.2 Relações de equivalência

4.2.0.1 Definição

Definição 4.1 (Relação de equivalência)**.** *Seja X um conjunto não vazio e $R \subseteq X \times X$ uma relação. Dizemos que R é uma relação de equivalência se:*

Reflexidade *Para todo $a \in X$, $(a,a) \in R$.*

Simetria *Se $(a,b) \in R$, ento $(b,a) \in R$.*

Transitividade *Se $(a,b) \in R$ e $(b,c) \in R$, ento $(a,c) \in R$.*

Quando $R \subseteq XxX$ é uma relação de equivalência, dizemos que R é uma relação de equivalência em X. Quando 2 elementos $a, b \in X$ são tais que $(a,b) \in R$, dizemos que a e b são relacionados.

4.2.1 Equivalência módulo R

Notação 4.1.1 (Equivalência módulo R)**.** *Seja R uma relação de equivalência em X. Para dizermos que $(a,b) \in R$ usaremos a notação $a \equiv b(R)$, que se lê "a equivalente a b módulo R", ou ainda a notação aRb, com o mesmo significado anterior.*

Exemplos:

1. Seja X={1,2,3}. Temos $X \times X = \{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3)\}$. São exemplos de relações de equivalência:
   $R_1 = X \times X$
   $R_2 = \{(1,1),(2,2),(3,3)\}$
   $R_3 = \{(1,1),(2,2),(3,3),(1,2),(2,1)\}$

2. Seja $X = \mathbb{Z}$ e $R \subseteq \mathbb{Z} \times \mathbb{Z}$ definida por $R = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x = y\}$ R é uma relação de equivalência pois:

   - $\forall a \in \mathbb{Z}, (a,a) \in R$ pois a=a

- $(a, b) \in R \rightarrow a = b \wedge b = a \Leftrightarrow (b, a) \in R$
- $(a, b), (b, c) \in R \rightarrow a = b = c \Rightarrow (a, c) \in R$

3. Tome $R = \{(x, y) \in \mathbb{Z}x\mathbb{Z}/2|(x - y)\} = \{(x, y) \in \mathbb{Z}x\mathbb{Z}/x - y = 2k, k \in \mathbb{Z}\}$
   R é uma relação de equivalência pois:
   - $\forall x \in \mathbb{Z}, xRx$ pois $x - x = 2.0$
   - $xRy \rightarrow x - y = 2k \Rightarrow y - x = -(x - y) = 2.(-k) \Rightarrow yRx$
   - $xRy \wedge yRz \rightarrow x - y = 2k \wedge y - z = 2q \Rightarrow x + z = x - y + y - z = 2k + 2q = 2(k + q) \rightarrow xRz$

4.2.2 Classe de equivalência e conjunto quociente

Definição 4.2 (Classe de Equivalência)**.** *Seja R uma relação de equivalência sobre um conjunto X. Dado $a \in X$, chamamos classe de equivalência determinada por a módulo R, denotada por $\bar{a}$ ou C(a), o subconjunto constituído pelos elementos $b \in X$ tais que bRa, ou seja, $\bar{a} = C(a) = \{a \in X/bRa\}$*

Definição 4.3 (Conjunto quociente)**.** *O conjunto das classes de equivalência módulo R será denotado por X/R e é chamado conjunto quociente de X por R.*

Observação: Dado um conjunto $X \neq \emptyset$ e R uma relação de equivalência em X, dado $a \in X$ como R é uma relação de equivalência, aRa, daí $\bar{a} \neq \emptyset$, pois $a \in \bar{a}$

Exemplos:

1. Seja X={a,b,c} e R={(a,a),(b,b),(c,c),(a,c),(c,a)}. Temos:
   $\bar{a} = \{x \in X/xRa\} = \{a, c\}$
   $\bar{b} = \{x \in X/xRb\} = \{b\}$
   $\bar{c} = \{x \in X/xRc\} = \{a, c\}$

2. Seja X={1,2,3,4} e a relação de equivalência R={(1,1),(2,2),(3,3),(4,4)}
   $\bar{1} = \{x \in X/xR1\} = \{1\}$
   $\bar{2} = \{x \in X/xR2\} = \{2\}$

$\bar{3} = \{x \in X/xR3\} = \{3\}$
$\bar{4} = \{x \in X/xR4\} = \{4\}$

Proposição 4.3.1. *Seja R uma relação de equivalência em um conjunto não vazio X, sejam a,b∈X. Se $\bar{a} \cap \bar{b} \neq \emptyset$, então aRb.*

Demonstração: Como $\bar{a} \cap \bar{b} \neq \emptyset$, existe um $y \in \bar{a} \cap \bar{b}$, logo $y \in \bar{a} \wedge y \in \bar{b}$. Da definição de classe de equivalência temos que yRa e yRb. Como R é relação de equivalência temos que aRy e bRy. Por transitividade, aRb, como queríamos demonstrar.#

Proposição 4.3.2. *Se $\bar{a} \cap \bar{b} \neq \emptyset$, então $\bar{a} = \bar{b}$*

Demonstração: Seja $y \in \bar{a}$. Daí yRa. Como $\bar{a} \cap \bar{b} \neq \emptyset$, pela proposição anterior, aRb. Logo, como yRa e aRb, segue que yRb, ou seja, $y \in \bar{b}$. Daí $\bar{a} \subseteq \bar{b}$. Como no caso anterior, mostra-se que $\bar{b} \subseteq \bar{a}$. Portanto $\bar{a} = \bar{b}$.#

Corolário 4.0.1. *As classes de equivalência são conjuntos disjuntos ou iguais.*

Seja R uma relação de equivalência em $X \neq \emptyset$, dado $a \in R$. Se bRa, então $\bar{b} = \bar{a}$, mais ainda, se dRa então $\bar{d} = \bar{a} = \bar{b}$. Como por exemplo:
X={a,b,c,d,e,f,g}
$\bar{a} = \{a, b, c\}$
$\bar{e} = \{e\}$
$\bar{f} = \{f, g\}$

Definição 4.4 (Representante da Classe de Equivalência)**.** *Seja C uma classe de equivalência de uma relação de equivalência R. Qualquer elemento $y \in C$ é chamado representante de C.*

Proposição 4.4.1. *Seja X um conjunto não vazio e R uma relação de equivalência em X. Então X é a união disjunta das classes $\bar{a}, a \in X$, ou seja,*

$$X = \bigsqcup_{a \in X} \bar{a}$$

.

Demonstração: Para todo $a \in X, \bar{a} \subseteq X$, logo $\bigsqcup_{a \in X} \bar{a} \subseteq X$. Seja $b \in X$. Logo $b \in \bar{b}$, daí $b \in \bigsqcup_{a \in X} \bar{a}$, logo $X \subseteq \bigsqcup_{a \in X} \bar{a}$. Portanto, $X = \bigsqcup_{a \in X} \bar{a}$.#

Exemplo:

Em $\mathbb{Z}$x$\mathbb{Z}$ considere a seguinte relação: $R = \{(a, b) \in \mathbb{Z}x\mathbb{Z}/2|(a - b)\}$. Mostre que é uma relação de equivalência e mostre suas classes de equivalência.

1. Dado $a \in \mathbb{Z}$, aRa pois $2|(a - a) = 0$.

2. Se aRb, então $2|(a - b)$, ou seja, a-b=2k, -(a-b)=b-a=2(-k). Logo bRa.

3. Se aRb e bRc, então a-b=2k e b-c=2q. Logo a-b+b-c=2k+2q=2(k+q). Logo, aRc.

Portanto R é uma relação de equivalência.

Dado $a \in \mathbb{Z}$, temos:

$\bar{a} = \{b \in \mathbb{Z}/bRa\} = \{b \in \mathbb{Z}/2|(a - b)\}$ como $2|(a - b)$, temos que:

$a - b = 2k \Leftrightarrow b = a + 2r, r = -k$

Assim, se a é ímpar, b também o é. Logo:

$\bar{a} = \{..., -3, -1, 1, 3, ...\}$

Agora, se a é par, b também é. Logo:

$\bar{a} = \{..., -2, 0, 2, 4, ...\}$

4.3 Funções

4.3.0.1 Definição

Definição 4.5 (Função). *Uma função f de um conjunto A em um conjunto B é uma relação $f \subseteq A \times B$ satisfazendo:*

1. $\forall x \in A, \exists y \in B/(x, y) \in f$

2. $(x_1, y_1), (x_1, y_2) \in f \to y_1 = y_2$

Geralmente, para dizer que f é uma função de A em B escrevemos $f : A \to B$.

4.3.0.2 Domínio e contra-domínio

O conjunto A é chamado de Domínio de f e o conjunto B é chamado de contra-domínio.

Se $f : A \rightarrow B$ é uma função, escrevemos $f(a) = b$ para dizer que $(a, b) \in f$

Exemplos:

1. Sejam A={0,1,2,3} e B={4,5,6,7,8}. Quais das seguintes relações são funções?
    - $R_1 = \{(0,5), (1,6), (2,7)\}$ - Não é função pois o número 3 não têm valor associado à ele.
    - $R_2 = \{(0,4), (1,5), (1,6), (2,7), (3,8)\}$ - Não é função pois o valor 1 tem mais de um valor diferente associado à ele.
    - $R_3 = \{(0,4), (1,5), (2,7), (3,8)\}$ - É função
    - $R_4 = \{(0,5), (1,5), (2,6), (3,7)\}$ - É função
2. $R_5 = \{(x, y) \in \mathbb{R}x\mathbb{R}/y^2 = x^2\}$ - Não é função, pois $x = \pm\sqrt{y}$
3. $R_6 = \{(x, y) \in \mathbb{R}x\mathbb{R}/x^2 + y^2 = 1\}$ - Não é função pois quando $x = 0, y = 1 \wedge y = -1$
4. $R_7 = \{(x, y) \in \mathbb{R}x\mathbb{R}/y = x^2\}$ - É função

4.3.1 Tipos de funções

Definição 4.6 (Função sobrejetora). *Uma função $f : A \rightarrow B$ é sobrejetora se, e somente se, para todo $y \in B$ exista um $x \in A$ tal que $f(x) = y$*

Definição 4.7 (Função injetora). *Uma função $f : A \rightarrow B$ é injetora se, e somente se, para $a_1 \neq a_2$, temos $f(a_1) \neq f(a_2), \forall a_1, a_2 \in A$*

Definição 4.8 (Função bijetora). *Uma função $f : A \rightarrow B$ que é simultaneamente injetora e sobrejetora é chamada de bijetora ou bijetiva.*

Exemplos:

1. A função $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = 3x + 1$ é injetora e sobrejetora.

   Dados $x_1, x_2 \in \mathbb{R}$ tais que $f(x_1) = f(x_2)$, temos:

   $$3x_1 + 1 = 3x_2 + 1$$

   $$x_1 = x_2$$

   Logo f é injetora

   Para verificar se f é sobrejetora precisamos verificar se dado $y \in \mathbb{R}$
   $\exists x \in \mathbb{R} / f(x) = y$.
   Tome $x = \dfrac{y-1}{3} \in \mathbb{R}$. Daí, $f(x) = y$. Logo f é sobrejetora.

2. A função $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2$ é injetora? E sobrejetora?

   Não é injetora pois $f(-1) = f(1) \wedge 1 \neq -1$

   Não é sobrejetora pois $\nexists x \in \mathbb{R} / x^2 = -1$

Dado $f : A \to B$ uma função, considere a relação $f^{-1} \subseteq B \text{x} A$ tal que $(b, a) \in f^{-1}$ se $(a, b) \in f$, ou seja, $f^{-1}(b) = a$ se $f(a) = b$.

Pode ocorrer que f^{-1} não seja função, mesmo f sendo uma função. Por exemplo:

$f : \{0, 1, 2, 3\} \to \{4, 5, 6, 7, 8\}$ dada por:

$f(0) = 5$

$f(1) = 5$

$f(2) = 6$

$f(3) = 7$

Neste caso, f^{-1} é dado por:

$f^{-1}(5) = 0$

$f^{-1}(5) = 1$

$f^{-1}(6) = 2$

$f^{-1}(7) = 3$

Teorema 4.1. *Dada $f : A \to B$ função tome $f^{-1} : B \to A$. Definida com o $f^{-1}(b) = a$ se $f(a) = b$. Então f^{-1} é uma função se, e somente se, f é bijetora.*

Demonstração: Suponha f^{-1} é função. Precisamos provar que f é injetora e sobrejetora.

Dados $a_1, a_2 \in A$ tais que $f(a_1) = b = f(a_2)$. Como $f(a_1) = b$ temos $f^{-1}(b) = a_1$, além disso, $f^{-1}(b) = a_2$. Mas f^{-1} é função, daí $a_1 = a_2$, ou seja, f é injetora.

Dado $b \in B$, como f^{-1} é uma função, $\forall b \in B, f^{-1}(b) = a \in A$, logo $f(a) = b$ e assim f é sobrejetora.

Portanto f é bijetora.

Agora suponha que f é bijetora.

Primeiramente, dado $b \in B$, como f é sobrejetora, existe $a \in A$ tal que $f(a) = b$, ou seja, $f^{-1}(b) = a \in A$.

Suponha que $f^{-1}(b) = a_1$ e $f^{-1}(b) = a_2$. Daí, $f(a_1) = b \wedge f(a_2) = b$. Mas f é injetora, assim $a_1 = a_2$ e então $f^{-1}(b) = a_1 = a_2$.

Portanto f^{-1} é função. #

4.3.2 Composição de funções

4.3.2.1 Definição

Definição 4.9 (Função Composta). *Sejam $f : A \to B$ e $g : B \to C$ funções. Chama-se composta de g e f a função de A em C, denotada $g \circ f$, definida por $g \circ f : A \to C$.*

Temos então que $(g \circ f)(x) = g(f(x)), \forall x \in A$.

Observação: Se $f : A \to B$ e $g : B \to A$ então existem $f \circ g$ e $g \circ f$. Porém, em geral, $f \circ g \neq g \circ f$.

4.3.2.2 Propriedades

Proposição 4.9.1. *Se $f : A \to B$ e $g : B \to C$ são funções injetoras, então $g \circ f$ é injetora.*

Demonstração: Dados $x_1, x_2 \in A$ tais que $(g \circ f)(x_1) = (g \circ f)(x_2)$ temos que $g(f(x_1)) = g(f(x_2))$. Como g é injetora, $f(x_1) = f(x_2)$. Mas f é injetora, daí $x_1 = x_2$. Logo $g \circ f$ é injetora.#

Proposição 4.9.2. *Se $f : A \to B$ e $g : B \to C$ são sobrejetoras, então $g \circ f$ é sobrejetora.*

Demonstração: Temos que $g \circ f : A \to C$. Dado $z \in C$. Como g é sobrejetora, $\exists y \in B / g(y) = z$. Como f é sobrejetora, $\exists x \in A / f(x) = y$. Assim, $z = g(y) = g(f(x)) = (g \circ f)(x)$. Logo $g \circ f$ é sobrejetora.#

4.3.3 Função Identidade

4.3.3.1 Definição

Definição 4.10 (Função Identidade)**.** *Dado um conjunto $A \neq \emptyset$, a função $i_A : A \to A$ dada por $i_A(x) = (x)$ é chamada de função identidade.*

Proposição 4.10.1. *Se $f : A \to B$ é bijetora, então $f \circ f^{-1} = i_B \wedge f^{-1} \circ f = i_A$.*

Demonstração: Temos $i_F : F \to F$ e $i_E : E \to E$. Além disso, $f \circ f^{-1} : F \to F$ e $f^{-1} \circ f : E \to E$, daí $D(f \circ f^{-1}) = D(i_F)$[1] e $D(f^{-1} \circ f) = D(i_E)$. Dado $x \in F$, $(f \circ f^{-1})(x) = f(f^{-1}(x)) = x = i_F(x)$. Dado $x \in E$, $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x = i_E(x)$.#

4.3.3.2 Propriedades

Proposição 4.10.2. *Se $f : A \to B$ e $g : B \to A$ são funções, então:*

1. $f \circ i_A = f, i_B \circ f = f, g \circ i_B = g, i_E \circ g = g$

2. *Se $g \circ f = i_A$, e $f \circ g = i_B$, então f e g são bijetoras e $g = f^{-1}$*

Demonstração:

1. Provemos que $f \circ i_A = f$.
   Primeiro temos $f : A \to B$ e $i_A : A \to A$. Daí, $f \circ i_A : A \to B$, ou seja, $D(f \circ i_A) = D(f)$. Dado $x \in A$, temos $(f \circ i_A)(x) = f(i_A(x)) = f(x)$. Portanto, $f \circ i_A = f$.

2. Provemos que f é bijetora.
   Dados x_1, $x_2 \in B$ tais que $f(x_1) = f(x_2)$. Como $f : A \to B$ e $g : B \to A$, então $g(f(x_1)) = g(f(x_2))$, ou seja, $(g \circ f)(x_1) = (g \circ f)(x_2)$. Daí, $i_A(x_1) = i_A(x_2)$. Logo, $x_1 = x_2$, isto é, f é injetora.

[1] $D(f(x))$ é o domínio da função f

Agora, dado $y \in B$, segue que $y = i_B(y)$. Mas $i_B = f \circ g$. Daí, $y = i_B(y) = (f \circ g)(y) = f(g(y))$. Assim, $x = g(y) \in A$ e $f(x) = y$.

Logo f é sobrejetora. Portanto f é bijetora. Analogamente, prova-se que g é bijetora. Provemos que $g = f^{-1}$. Temos $f^{-1} : B \to A$, daí, $D(g) = B = D(f^{-1})$. Agora, $f \circ g = i_B = f \circ f^{-1}$. Assim, para todo $x \in F$, $(f \circ g)(x) = (f \circ f^{-1})(x)$. Isto é, $f(g(x)) = f(f^{-1}(x))$. Portanto, $g(x) = f^{-1}(x) \forall x \in B$. Logo, $g = f^{-1}$. #

Definição 4.11. *Seja $f : A \to B$ uma função.*

1. *Dado $P \subseteq A$, chama-se* imagem direta *de P, segundo f e indica-se por $f(P)$ o subconjunto de F dado por*
$$f(P) = \{f(x) \mid x \in P\},$$
isto é, $f(P)$ é o conjunto das imagens por f dos elementos de P.

2. *Dado $Q \subseteq B$, chama-se* imagem inversa *de Q, segundo f e indica-se por $f^{-1}(Q)$ o subconjunto de A dado por*
$$f^{-1}(Q) = \{x \in E \mid f(x) \in Q\},$$
isto é, $f^{-1}(Q)$ é o conjunto dos elementos de A que tem imagem em Q através de f.

Exemplos:

1. Seja $A = \{1, 3, 5, 7, 9\}$ e $B = \{0, 1, 2, 3, \ldots, 10\}$ e $f : A \to B$ dada por $f(x) = x + 1$. Temos que

   - $f(\{3, 5, 7\}) = \{f(3), f(5), f(7)\} = \{4, 6, 8\}$
   - $f(A) = \{f(1), f(3), f(5), f(7), f(9)\} = \{2, 4, 6, 8, 10\}$
   - $f(\emptyset) = \emptyset$
   - $f^{-1}(\{2, 4, 10\}) = \{x \in A \mid f(x) \in \{2, 4, 10\}\} = \{1, 3, 9\}$
   - $f^{-1}(\{0, 1, 3, 5, 7, 9\}) = \{x \in A \mid f(x) \in \{0, 1, 3, 5, 7, 9\}\} = \emptyset$

2. Sejam $A = B = \mathbb{R}$ e $f : \mathbb{R} \to \mathbb{R}$ dada por $f(x) = x^2$. Temos

   - $f(\{1, 2, 3\}) = \{1, 4, 9\}$

- $f([0,2]) = \{f(x) \in \mathbb{R} \mid 0 \leq x \leq 2\} = \{x^2 \mid 0 \leq x \leq 2\} = [0,4]$
- $f^{-1}([1,9]) = \{x \in \mathbb{R} \mid 1 \leq f(x) \leq 9\} = \{x \in \mathbb{R} \mid 1 \leq x^2 \leq 9\} = [-1,-3] \cup [1,3]$

Proposição 4.11.1. *Seja $f : A \to B$ uma aplicação (ou função) e sejam $P, Q \subseteq E$, $X, Y \subseteq B$.*

1. *Se $P \subseteq Q$, então $f(P) \subseteq f(Q)$.*
2. $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$.

Demonstração:

1. Se $y \in f(P)$, então existe $x \in P$ tal que $f(x) = y$. Mas como $P \subseteq Q$, então $x \in Q$ e daí $y \in f(Q)$. Logo $f(P) \subseteq f(Q)$.
2. Seja $z \in f^{-1}(X \cup Y)$. Então $f(z) \in X \cup Y$. Se $f(z) \in X$, entao $z \in f^{-1}(X)$ e daí $z \in f^{-1}(X) \cup f^{-1}(Y)$. Se $f(z) \in Y$, então $z \in f^{-1}(Y)$ e assim $z \in f^{-1}(X) \cup f^{-1}(Y)$. Logo, $f^{-1}(X \cup Y) \subseteq f^{-1}(X) \cup f^{-1}(Y)$.

   Agora, seja $z \in f^{-1}(X) \cup f^{-1}(Y)$. Se $z \in f^{-1}(X)$, então $f(z) \in X$, daí $f(z) \in X \cup Y$, isto é, $z \in f^{-1}(X \cup Y)$. Se $z \in f^{-1}(Y)$, então $f(z) \in Y$ e assim $f(z) \in X \cup Y$, isto é, $z \in f^{-1}(X \cup Y)$. Logo $f^{-1}(X) \cup f^{-1}(Y) \subseteq f^{-1}(X \cup Y)$.

   Portanto, $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$. #

CAPÍTULO 5

OPERAÇÕES EM $\frac{\mathbb{Z}}{M\mathbb{Z}}$

Durante esse tópico, m denotará um número inteiro positivo.

5.1 Relações de congruência

5.1.1 Definição

Definição 5.1 (Congruência)**.** *Sejam $a, b \in \mathbb{Z}$, dizemos que a é congruente com b módulo m se $m|(a-b)$. Neste caso, escrevemos $a \equiv_m b$ ou $a \equiv b(mod\ m)$.*

Exemplos:

1. $5 \equiv 2(mod\ 3)$, pois $3|(5-2)$
2. $3 \equiv 1(mod\ 2)$, pois $2|(3-1)$
3. $3 \equiv 9(mod\ 3)$, pois $2|(3-9)$

5.1.2 Propriedades

Proposição 5.1.1. *A congruência módulo m é uma relação de equivalência em $\mathbb{Z}$.*

Demonstração:

1. $\forall a \in \mathbb{Z}, a \equiv a(mod\ m)$ pois $m|(a-a)$ (Reflexidade)

2. Se $a \equiv b(mod\ m)$, então $m|(a-b)$. Daí, $m|(-(a-b))$, ou seja, $m|(b-a)$. Daí $b \equiv a(mod\ a)$ (Simetria)

3. Se $a \equiv b(mod\ m)$ e $b \equiv c(mod\ m)$, então $m|(a-b)$ e $m|(b-c)$. Assim, $m|[(a-b)+(b-c)]$. Logo, $m|(a-c)$, isto é, $a \equiv c(mod\ m)$ (Transitividade)

   Portanto é relação de equivalência. #

Teorema 5.1. *A relação de congruência módulo m satisfaz as seguintes propriedades:*

1. $a_1 \equiv b_1(mod\ m) \Leftrightarrow a_1 - b_1 \equiv 0(mod\ m)$

2. *Se* $a_1 \equiv b_1(mod\ m)$ *e* $a_2 \equiv b_2(mod\ m)$, *então* $a_1 + a_2 \equiv b_1 + b_2(mod\ m)$

3. *Se* $a_1 \equiv b_2(mod\ m)$ *e* $a_2 \equiv b_2(mod\ m)$, *então* $a_1a_2 \equiv b_1b_2(mod\ m)$

4. *Se* $a \equiv b(mod\ m)$, *então* $ax \equiv bx(mod\ m), \forall x \in \mathbb{Z}$

5. *Vale a lei do cancelamento: se* $d \in \mathbb{Z}$ *e* $mdc(d,m) = 1$ *então* $ad \equiv bd(mod\ m)$ *implica* $a \equiv b(mod\ m)$

Demonstração: Provemos o ítem 3
Dizer que $a \equiv b(mod\ m)$ significa dizer que existe $t \in \mathbb{Z}$ tal que $a = b + tm$.
Assim, existem $m, l \in \mathbb{Z}$ tais que $a_1 = b_1 + km, a_2 = b_2 + lm$. Daí

$$a_1a_2 = b_1b_2 + lb_1m + klm^2$$

$$a_1a_2 = b_1b_2 + \underbrace{(lb_1 + kb_2 + klm)}_{\in\mathbb{Z}}m$$

Ou seja, $a_1a_2 = b_1b_2 + pm$, onde $p = lb_1 + kb_2 + klm \in \mathbb{Z}$. Portanto, $a_1a_2 \equiv b_1b_2(mod\ m)$.

Para o ítem 5, se $ad \equiv bd(mod\ m)$, então $m|d(a-b)$. Mas, $mdc(d,m) = 1$, logo $m|(a-b)$, isto é, $a \equiv b(mod\ m)$.#

Como a congruência módulo m é uma relação de equivalência, podemos determinar suas classes de equivalência. Assim, dado $n \in \mathbb{Z}$, temos

$$C(n) = \{x \in \mathbb{Z}/x \equiv n(mod\ m)\}$$

Denotaremos $C(n)$ por $R_m(n)$ ou $\bar{n}$, quando não houver possibilidade de confusão.

Por exemplo, fixando m

$R_m(0) = \{x \in \mathbb{Z}/x \equiv 0(mod\ m)\} = \{x \in \mathbb{Z}/x = mk, k \in \mathbb{Z}\} = m\mathbb{Z}$

$R_m(1) = \{x \in \mathbb{Z}/x \equiv 1(mod\ m)\} = \{x \in \mathbb{Z}/x = 1 + km, k \in \mathbb{Z}\}$

$R_m(n) = \{x \in \mathbb{Z}/x = n + km, k \in \mathbb{Z}\}$

5.1.3 Classes de equivalência módulo m

Proposição 5.1.2. *As classes de equivalência definidas pela congruência módulo m são determinadas pelos restos da divisão euclidiana por m. Em outras palavras, $R_m(n)$ é o conjunto dos números inteiros cujo resto na divisão euclidiana por m é n.*

Demonstração: Dado $x \in \mathbb{Z}$, pela divisão de Euclides, podemos escrever $x = km + r$ onde $0 \leq r < m$. Daí, $x - r = km$, isto é, $m|(x-r)$. Logo $x \in R_m(r)$. Portanto, se $r = n$, então $x \in R_m(n)$ e neste caso, $x = km + n = n + km$, ou seja, o resto da divisão euclidiana de x por m é n.#

Corolário 5.1.1. *$R_m(k) = R_m(l)$ se, e somente se, $k \equiv l(mod\ m)$.*

Exemplos:

1. Se $m = 2$, então os possíveis restos na divisão euclidiana por 2 são 0 e 1. Logo, existem duas classes de equivalência, a saber $R_2(0)$ e $R_2(1)$

2. Se $m = 3$, então os possíveis restos da divisão euclidiana são 0,1 e 2. Daí
   $R_3(0) = 3\mathbb{Z}$
   $R_3(1) = \{x \in \mathbb{Z}/x = 3q + 1, q \in \mathbb{Z}\}$
   $R_3(2) = \{x \in \mathbb{Z}/x = 3q + 2, q \in \mathbb{Z}\}$

Proposição 5.1.3. *Na relação de equivalência módulo m existem m classes de equivalência.*

Demonstração: Os possíveis restos na divisão euclidiana por m são $0, 1, ..., (m-1)$. Como cada possível resto define uma classe de equivalência diferente, existem exatamente m classes de equivalência.#

5.2 Conjunto quociente $\left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)$

Notação 5.1.1 (Conjunto quociente)**.** *Fixado m inteiro positivo, denotaremos*

$R_m(0) = \bar{0}$

$R_m(1) = \bar{1}$

$\vdots$

$R_m(m-1) = \overline{m-1}$

O conjunto quociente desta relação será denotado por $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ *e* $\dfrac{\mathbb{Z}}{m\mathbb{Z}} = \{\bar{0}, \bar{1}, ..., \overline{m-1}\}$

Queremos definir um meio de somar e multiplicar os elementos de $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$. Por exemplo, em $\dfrac{\mathbb{Z}}{2\mathbb{Z}} = \{\bar{0}, \bar{1}\}$ temos que a soma de pares é par, soma de par com ímpar é ímpar e a soma de ímpares é par.

Podemos escrever

$\bar{0} \oplus \bar{0} = \overline{0+0} = \bar{0}$

$\bar{0} \oplus \bar{1} = \overline{0+1} = \bar{1}$

$\bar{1} \oplus \bar{1} = \overline{1+1} = \bar{0}$

Para multiplicação, temos

$\bar{0} \odot \bar{0} = \overline{0.0} = \bar{0}$

$\bar{0} \odot \bar{1} = \overline{0.1} = \bar{0}$

$\bar{1} \odot \bar{1} = \overline{1.1} = \bar{1}$

Em $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ definimos

$$\bar{a} \oplus \bar{b} = \overline{a+b} \tag{5.1}$$

$$\bar{a} \odot \bar{b} = \overline{a.b} \tag{5.2}$$

Para $\bar{a}, \bar{b} \in \dfrac{\mathbb{Z}}{m\mathbb{Z}}$

Proposição 5.1.4. *As operações de soma e produto definidas em (5.1) e (5.2) são independentes dos representantes das classes.*

Demonstração: Dadas duas classes com representantes diferentes, $\bar{a}_1 = \bar{a}_2,\ \bar{b}_1 = \bar{b}_2, a_1 \neq a_2, b_1 \neq b_2$, temos:

$$\overline{a_1 + b_1} = \bar{a}_1 \oplus \bar{b}_1 = \bar{a}_2 \oplus \bar{b}_2 = \overline{a_2 + b_2}$$

$$\overline{a_1 b_1} = \bar{a}_1 \odot \bar{b}_1 = \bar{a}_2 \odot \bar{b}_2 = \overline{a_2 b_2}$$

C.Q.D.#

Exemplo: Determine a some e multiplicação em:
$\dfrac{\mathbb{Z}}{4\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

Tabela 5.1: *Soma*

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Tabela 5.2: *Multiplicação*

$\odot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

5.2.1 Elementos Inversíveis de $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$

5.2.1.1 Inversibilidade

Definição 5.2 (Inversibilidade)**.** *Um elemento* $\bar{a} \in \dfrac{\mathbb{Z}}{m\mathbb{Z}}$ *é inversível se, e somente se, existem* $\bar{b} \in \dfrac{\mathbb{Z}}{m\mathbb{Z}}$ *tal que* $\bar{a} \odot \bar{b} = \bar{1}$.

Neste caso, $\bar{b}$ é chamado inverso de $\bar{a}$ e denotaremos $\bar{b} = (\bar{a})^{-1}$.

Quando $\bar{b}$ existe, ele é único. De fato, dado $\bar{a} \in \dfrac{\mathbb{Z}}{m\mathbb{Z}}$, se existem $\bar{b}, \bar{d} \in \dfrac{\mathbb{Z}}{m\mathbb{Z}}$ tais que $\bar{a} \odot \bar{b} = \bar{1} = \bar{a} \odot \bar{d}$, então $\bar{b} = \bar{b} \odot \bar{1} = \bar{b} \odot (\bar{a} \odot \bar{d}) = (\bar{b} \odot \bar{a}) \odot \bar{d} = \bar{1} \odot \bar{d} = \bar{d}$.

Proposição 5.2.1. *Um elemento* $\bar{a} \in \dfrac{\mathbb{Z}}{m\mathbb{Z}}$ *é inversível se, e somente se,*

$$mdc(a, m) = 1$$

Demonstração: Suponha que existe $\bar{b} \in \dfrac{\mathbb{Z}}{m\mathbb{Z}}$ tal que $\bar{a} \odot \bar{b} = \bar{1}$. Assim, $\overline{ab} = \bar{1}$, ou seja, $ab \equiv 1(mod\ m)$. Daí, $ab - 1 = km, k \in \mathbb{Z}$, logo $ab + m(-k) = 1$, e então $mdc(a, m) = 1$.

Agora suponha que $mdc(a, m) = 1$. Logo, existem $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + my_0 = 1$, isto é, $ax_0 - 1 = m(-y_0)$. Logo $ax_0 \equiv 1(mod\ m)$, ou seja, $\overline{ax_0} = \bar{1}$. Portanto, $\bar{a} \odot \bar{x_0} = \bar{1}$.#

Exemplos:

1. Em $\dfrac{\mathbb{Z}}{4\mathbb{Z}}$ existem dois elementos inversíveis que são $\bar{1}$, cujo inverso é $\bar{1}$, e o $\bar{3}$, cujo inverso é $\bar{3}$.

2. Em $\dfrac{\mathbb{Z}}{11\mathbb{Z}}$, todos elementos, exceto $\bar{0}$, possuem inverso:

Tabela 5.3: *Inversos em* $\dfrac{\mathbb{Z}}{11\mathbb{Z}}$

Elemento	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\bar{10}$
Inverso	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{3}$	$\bar{9}$	$\bar{2}$	$\bar{8}$	$\bar{7}$	$\bar{5}$	$\bar{10}$

O número de elementos inversíveis de $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ é igual a quantidade de números coprimos com m. Esse número é denotado por $\varphi(m)$ e é chamado função φ de Euler. Pode-se demonstrar que

$$\varphi(m) = m \prod_{p/m} \left(1 - \frac{1}{p}\right)$$

Onde o produto varia sobre todos os divisores primos de m, sem repetição.

Por exemplo, para $\dfrac{\mathbb{Z}}{100\mathbb{Z}}$ temos:
$100 = 2^2 5^2$

Daí,
$\varphi(100) = 100\left(1 - \dfrac{1}{2}\right)(1 - 15) = 40$

Logo, em $\dfrac{\mathbb{Z}}{100\mathbb{Z}}$ existem 40 elementos inversíveis.

Notação 5.2.1 (Conjunto dos elementos inversíveis)**.** *Denotaremos o conjunto de todos os elementos inversíveis de* $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ *por* $\left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$*, ou ainda* $U\left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)$.

Proposição 5.2.2. *Sejam* $\bar{a}, \bar{b} \in \left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$. *Então* $\bar{a} \odot \bar{b} \in \left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$.

Demonstração: Por uma proposição anterior, basta verificar que
$mdc(ab, m) = 1$. Para que $\bar{a} \odot \bar{b} \in \left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$.

Como $\bar{a}, \bar{b} \in \left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$, então $mdc(a, m) = 1$ e $mdc(b, m) = 1$.

Assim, existem $x_0, y_0, x_1, y_1 \in \mathbb{Z}$ tais que
$ax_0 + my_0 = 1$
$bx_1 + my_1 = 1$

Daí,

$$abx_0x_1 + max_0y_1 + mbx_1y_0 + m^2y_0y_1 = 1$$

$$\underbrace{abx_0x_1}_{\in\mathbb{Z}} + m\underbrace{(ax_0y_1 + bx_1y_0 + my_0y_1)}_{\in\mathbb{Z}} = 1$$

Logo, $mdc(ab, m) = 1$, ou seja, $\bar{a} \odot \bar{b} \in \left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$.#

CAPÍTULO 6

ANÉIS

6.1 Definições

Definição 6.1. *Um conjunto não vazio A munido de duas operações "+"e "·", chamados soma e produto, é chamado de* ***anel*** *quando as seguintes condições são verdadeiras:*

1. ***Elemento Neutro****: Existe em A um elemento denotado por 0 (zero) ou 0_A tal que para todo elemento $a \in A$ vale*
$$a + 0 = 0 + a = a.$$

2. ***Elemento Oposto****: Para cada elemento $a \in A$, existe $b \in A$ tal que*
$$a + b = b + a = 0_A.$$

3. ***Associatividade****: para todos $a, b, c \in A$ vale que*
$$(a + b) + c = a + (b + c).$$
Essa propriedade é chamada ***propriedade associativa*** *da soma.*

4. ***Comutatividade****: Para todos $a, b \in A$ vale*
$$a + b = b + a.$$

5. ***Distributividade**: Para todos a, b, c $\in$ A vale*

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

*Essa propriedade é chamada **distributiva em relação ao produto**.*

6. ***Distributividade**: Para todos a, b, c $\in$ A vale*

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

*Essa é a propriedade **distributiva do produto em relação à soma**.*

Além disso, se A satisfizer

7. ***Comutatividade**: Para todos a, b $\in$ A vale*

$$a \cdot b = b \cdot a.$$

*Dizemos que A é um **anel comutativo**.*

8. ***Elemento um**: Se existe em A um elemento denotado por 1 ou 1_A tal que*

$$a \cdot 1 = 1 \cdot a = a.$$

*Para todo a $\in$ A, então chamamos de anel com unidade ou anel unitário. O elemento 1 é chamado de **unidade** de A e A é chamado de **anel com unidade** ou **anel unitário**.*

9. ***Associatividade**: Se para todos a, b, c $\in$ A, vale que*

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

*Dizemos que A é um **anel associativo**.*

Quando A, munido de duas operações "+" e "$\cdot$" é um anel, ele será denotado $(A, +, \cdot)$, para indicar claramente as operações binárias em A.

Exemplo 6.1.1. *Em*

$$M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$$

defina a soma como a soma usual de matrizes e defina o produto do seguinte modo: dados A e $B \in M_2(\mathbb{R})$

$$[A, B] = AB - BA,$$

onde AB denota o produto usual de matrizes. Verifique que $M_2(\mathbb{R})$ com a soma usual de matrizes e produto $[,]$ é um anel, mas não é associativo.

Solução: *De fato,*

1. $A \in M_2(\mathbb{R})$, *existe* $0_2 \in M_2(\mathbb{R})$ *tal que* $A + 0_2 = 0_2 + A$. *A saber:*

$$0_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

2. *Para todo* $A \in M_2(\mathbb{R})$ *existe* $B \in M_2(\mathbb{R})$ *tal que* $A + B = B + A = 0_2$. *A saber:*

$$B = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$$

3. $(A + B) + C = A + (B + C)$ *pois em* $\mathbb{R}$ *vale a associatividade*

4. $A + B = B + A$, *pois em* $\mathbb{R}$ *a soma é comutativa*

5. $[(A + B), C] = (A + B)C - C(A + B)$
   $= AC + BC - CA - CB = AC - CA + BC - CB = [A, C] + [B, C]$

6. $[A, B] = AB - BA, [B, A] = BA - AB \Rightarrow [A, B] = -[B, A]$

$$[[A, B], C] \neq [A, [B, C]]$$

Exemplos:

1. $(\mathbb{Z}, +, .), (\mathbb{Q}, +, .), (\mathbb{R}, +, .), (\mathbb{C}, +, .), \left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)$
   São anéis associativos, comutativos e com unidade em $\left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)$, o elemento neutro é a classe $\bar{0}$ e a unidade é a classe $\bar{1}$.

2. Seja $A = \mathbb{Z} = \{f : \mathbb{Z} \to \mathbb{Z}/f$ é função$\}$. Dadas duas funções quaisquer $f, g \in \mathbb{Z}x\mathbb{Z}$, definimos $f \oplus g : \mathbb{Z} \to \mathbb{Z}$ e $f \odot g : \mathbb{Z} \to \mathbb{Z}$ como:

   $(f \oplus g) = f(x) + g(x)$
   $(f \odot g) = f(x)g(x)$

   (a) Dado $x \in \mathbb{Z}$
   $(f \oplus g)(x) = f(x) + g(x) = g(x) + f(x) = (g \oplus f)(x)$, portanto $f \oplus g = g \oplus f$

   (b) Dado $x \in \mathbb{Z}$
   $(f \odot g)(x) = f(x)g(x) = g(x)f(x) = (g \odot f)(x)$, portanto $f \odot g = g \odot f$

   (c) Definida $0\mathbb{Z} \to \mathbb{Z}$ como $0(x) = 0, \forall x \in \mathbb{Z}$, temos
   $(f(x) \oplus 0)(x) = f(x) \oplus 0(x) = 0(x) \oplus f(x) = f(x)$

6.2 Propriedades de um Anel

1. O elemento neutro é único.
   Suponha que exista $0_1, 0_2 \in A$ tais que
   $a + 0_1 = 0_1 + a = a;\ b + 0_2 = 0_2 + b = b$, daí $0_1 = 0_1 + 0_2 = 0_2$

2. Para cada $a \in A$ existe um único oposto.
   De fato, suponha que existam $b_1, b_2 \in A$ tais que
   $a + b_1 = 0;\ a + b_2 = 0$. Daí $b_1 = b_2 + 0 = b_1 + (a + b_2) = (b_1 + a) + b_2 = 0 + b_2 = b_1 = b_2$

3. Para todo $a \in A, -(-a) = a$
   Dado $a \in A, -a$ é oposto de a, isto é, $a + (-a) = 0$. Logo o oposto de $(-a)$ é a, daí $-(-a) = a$.

4. Dados $a_1, a_2, ..., a_n \in A, n \leq 2$, então
   $-(a_1 + a_2 + ... + a_n) = (-a_1) + (-a_2) + ... + (-a_n)$

5. Para todo $a, x, y \in A$, se $a + x = a + y$, então $x = y$

6. Para todo $a \in A,\ a0 = 0a = 0$

   Temos $0 + 0.0 = a0 = a(0 + 0) = a0 + a0$, daí

   $\underbrace{0.0}_{a0} + 0 = \underbrace{0.0}_{a0} + a0$. Pela propriedade 5 $a0 = 0$

7. Para todo $a, b \in A$, temos $a(-b) = -ab$

   Provemos que $a(-b) = -ab$

   $a(-b) + ab = a((-b) + b) = a0 = 0$, portanto $-ab = a(-b)$

8. Para todo $a, b \in A,\ ab = (-a)(-b)$

6.3 Anel de Integridade

6.3.0.1 Definição

Definição 6.2 (Anel de Integridade)**.** *Um anel comutativo A é um anel de integridade quando para todos $a, b \in A$, se $ab = 0$,então $a = 0 \vee b = 0$. Um anel de integridade também é chamado de domínio de integridade ou simplesmente de domínio.*

Se a e b são elementos não nulos de um anel A tais que $ab = 0$, então a e b são chamados de divisores próprios de zero.

Exemplos:

1. Os anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ são anéis de integridade.

2. Em geral, $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ não é anel de integridade, por exemplo, em $\dfrac{\mathbb{Z}}{4\mathbb{Z}}$, $\bar{2} \neq \bar{0}$, no entanto $\bar{2} \odot \bar{2} = \bar{4} = \bar{0}$

3. $M_n(\mathbb{R})$ não é um anel de integridade, por exemplo, em $M_2(\mathbb{R})$

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},\ B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Suponha que $m = nk,\ m > n > 1$ e $m > k >$. Logo, em $\dfrac{\mathbb{Z}}{m\mathbb{Z}}, \bar{n} \neq \bar{0}$ e $\bar{k} \neq \bar{0}$. Logo, se m não é primo, então $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ não é um anel de integridade.

Agora, suponha que $m = p$ primo. Sejam $\bar{a}, \bar{b} \in \dfrac{\mathbb{Z}}{m\mathbb{Z}}$ tais que $\bar{a} \odot \bar{b} = \bar{0}$, ou seja, $ab \equiv 0(mod\ p)$. Daí $p|ab$. Logo $p|a \vee p|b$. Portanto, $\bar{a} = \bar{0} \vee \bar{b} = \bar{0}$. Assim, $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ é anel de integridade se, e somente se, m é primo.

Definição 6.3. *Seja $(A, +, \cdot)$ um anel. Dizemos que um subconjunto não vazio $B \subseteq A$ é um* ***subanel*** *quando $(B, +, \cdot)$ é um anel.*

Exemplos:

1. Todo anel A sempre tem dois subanéis: $\{0_A\}$ e A, que são chamados de **subanéis triviais**.

2. Em $(\mathbb{Z}_4, \oplus, \odot)$ o conjunto $B = \{\overline{0}, \overline{2}\}$ é um subanel.

3. No anel $\mathbb{Z}$, o conjunto $m\mathbb{Z}$, $m > 1$ é um subanel de $\mathbb{Z}$.

Proposição 6.3.1. *Seja $(A, +, \cdot)$ um anel. Um subconjunto não vazio $B \subseteq A$ é um subanel de A se, e somente se, $x - y \in B$, e $x \cdot y \in B$ para todos $x, y \in B$.*

$(A, +, .), (B, \oplus, \odot)$ Anéis

$f : A \to B$

$a \to f(a)$

$g : \mathbb{Z} \to \dfrac{\mathbb{Z}}{m\mathbb{Z}}$

$x \to \bar{x}$

$g(x + y) = \overline{x + y} = \bar{x} \oplus \bar{y} = g(x) \oplus g(y)$

$g(x + y) = g(x) \oplus g(y)$

$g(xy) = \overline{xy} = \bar{x} \odot \bar{y} = g(x) \odot g(y)$

$g(1) = \bar{1}$

6.4 Homomorfismo

6.4.0.1 Definição

Definição 6.4 (Homomorfismo). *Um homomorfismo do anel (A,+,.) no anel* $(B, \oplus, \odot)$ *é uma função* $f : A \to B$ *que satisfaz:*

1. $f(x + y) = f(x) + f(y), \forall x, y \in A$
2. $f(xy) = f(x)f(y), \forall x, y \in A$

Se (A,+,.) é um anel, então $f : A \to A$ dada por $f(a) = a$ é um homomorfismo de A em A pois:

1. $f(x + y) = x + y = f(x) + f(y)$
2. $f(xy) = xy = f(x)f(y)$
3. $f(1_A) = 1_A$

6.4.0.2 Propriedades

Proposição 6.4.1. *Seja* $f : A \to B$ *homomorfismo do anel A no anel B. Então:*

1. $f(0_A) = 0_B$
2. $f(-a) = -f(a), \forall a \in A$

Demonstração:

1. Da condição 1 da definição de homomorfismo, fazendo $x = y0_A$, temos
   $f(0_A + 0_A) = f(0_A) \oplus f(0_A)$
   mas $0_A + 0_A = 0_A$. Daí
   $f(0_A) = f(0_A) + f(0_A)$
   Somando $-f(0_A)$ em ambos os lados
   $f(0_A) \oplus (-f(0_A)) = (f(0_A) + f(0_A)) + (-f(0_A))$
   $0_B = f(0_A) + 0_B$
   $f(0_A) = 0_B$

2. Temos $0_B = f(0_A) = f(a + (-a)) = f(a) \oplus f(-a)$
   Somando $-f(a)$ em ambos os lados
   $0_B \oplus (-f(a)) = [f(a) \oplus f(-a)] + (-f(a)) - f(a) = f(-a) \oplus (f(a) \oplus (-f(a)))$
   $f(-a) = -f(a)$.#

Seja $f : \mathbb{Z} \to \mathbb{Z}$ um homomorfismo. Dado $n \in \mathbb{Z}, n \geq 0$. Temos daí,

$$f(n) = f(\underbrace{1 + ... + 1}_{n\ vezes}) = \underbrace{f(1) + ... + f(1)}_{n\ vezes} = nf(1) = n1$$

$f(n) = n$, para todo $n \in \mathbb{Z}$.

Proposição 6.4.2. *Seja $f : A \to B$ um homomorfismo sobrejetor de anéis.*

1. *Se A tem unidade, então B tem unidade e $f(1_A) = 1_B$.*

2. *Se A tem unidade e $x \in A$ possui inverso multiplicativo, então $f(x)$ tem inverso e $f(x^{-1} = (f(x))^{-1}$.*

6.4.1 Epimorfismo, monomorfismo e isomorfismo

Definição 6.5 (Epimorfismo, monomorfismo e isomorfismo)**.** *Seja $f : A \to B$ um homomorfismo, onde A e B são anéis. Dizemos que*

1. *f é um epimorfismo se f for sobrejetora*

2. *f é um monomorfismo se f for injetora*

3. *f é um isomorfismo se f for bijetora*

4. *Quando $A = B$ e f é um isomorfismo, então f é um automorfismo*

6.5 Ideal de um anel

6.5.0.1 Definição

Definição 6.6 (Ideal em um anel)**.** *Seja $(A, +, .)$ um anel comutativo. Um ideal em A é um conjunto não vazio I tal que:*

1. *Para todo $a, b \in I$, devemos ter $a - b \in I$.*

2. *Para todo $b \in A$ e todo $x \in I$, $bx \in I$.*

Quando $I = A$ ou $I = \{0_A\}$, I é chamado de ideal trivial.

6.5.0.2 Propriedades

Proposição 6.6.1. *Seja A um anel comutativo e I um ideal de A. Então:*

1. *$0_A \in I$.*

2. *$-a \in I$ para todo $a \in I$.*

3. *Se $1_A \in I$, então $I = A$.*

Demonstração: Temos que da definição de ideal, $ab \in I$, para todo $a, b \in I$.
Assim, dado $a \in I$, $a0_A = 0_A \in I$.#

Demonstração: Como I é ideal, $1_A x \in I$, para todo $x \in A$, ou seja, $x = 1_A x \in I$ para qualquer $x \in A$, logo, $A \subseteq I$. Como $I \subseteq A$, então $I = A$.#

Exemplos:

1. Em $\mathbb{Z}$ todos os ideais não triviais são da forma $m\mathbb{Z}, m > 1$

2. No anel $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, onde p é um número primo, os únicos ideais são os triviais $\{\bar{0}\}$ e $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

   Demonstração: Seja $I \subseteq \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ um ideal, $I \neq \{\bar{0}\}$. Provemos que $I = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$. Para isso, vamos provar que $\bar{1} \in I$. Seja $\bar{a} \in I, \bar{a} \neq \bar{0}$, pois $I \neq \{\bar{0}\}$. Mas como p é primo, $mdc(a, p) = 1$, daí existe $\bar{b} \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}, \bar{b} \neq \bar{0}$, tal que $\bar{1} = \bar{a}\bar{b}$. Mas I é ideal e $\bar{a} \in I$, logo $\bar{1} = \bar{a}\bar{b} \in I$.

   Portanto $I = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$.#

3. Os únicos ideais não triviais de $\dfrac{\mathbb{Z}}{8\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$ são:
   $I_1 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$ e $I_2 = \{\bar{0}, \bar{4}\}$

Observação: Num anel $(A, +, .)$, a diferença $a - b$ é definida como

$$a - b = a + (-b),\ a, b \in A$$

6.5.1 Congruência módulo I

6.5.1.1 Definição

Definição 6.7 (Congruência módulo I). *Seja I um ideal de um anel $(A, +, .)$. Dizemos que x é congruente a y módulo I quando $x - y \in I$. Neste caso, escrevemos $x \equiv y(mod\ I)$.*

6.5.1.2 Propriedades

Proposição 6.7.1. *A congruência Módulo I é uma relação de equivalência em A timesA(A anel unitário).*

Demonstração: Como $0 = 0_A \in I$ e para todo $x \in I$, $x - x = 0 \in I$, então $x \equiv x(mod\ I)$.

Suponha que $x \equiv y(mod\ I)$. Então $x - y \in I$. Como $-1 \in A$,$y - x = -(x - y) = -[(x - y)1] = (x - y)(-1) \in I$, ou seja, $y \equiv x(mod\ I)$.

Agora,s e $x \equiv y(mod\ I)$ e $y \equiv z(mod\ I)$, então $x - y \in I$ e $y - z \in I$. Daí, $x - z = (x - z) + (y - z) \in I$, ou seja, $x \equiv z(mod\ I)$.

Logo, é uma relação de equivalência.#

Seja $y \in A$. A classe de equivalência módulo I é

$$C(y) = \{x \in A/x \equiv y(mod\ I)\} = \{x \in A/x - y \in I\}$$

Agora, $x - y \in I$ significa que existe $t \in I$, tal que $x - y = t$. Logo, $x = y + t$, onde $t \in I$.

Assim,

$$C(y) = \{y + t, t \in I\} = y + I$$

Notação 6.7.1 (Congruência Módulo I). *Denotamos por $y + I$ (ou $I + y$) a classe de equivalência módulo I. Denotamos por $\dfrac{A}{I}$ o conjunto de todas as classes de equivalência, tal conjunto é chamado quociente do anel A pelo ideal I.*

Exemplos:

1. A anel e $I_1 = \{0\}$ e $I_2 = A$ ideais.

   (a) $\dfrac{A}{I_1}; a \in A$
   $C(a) = a + I_1 = \{a + 0\} = \{a\}$

$\dfrac{A}{I_1} = \{a + I, a \in A\}$
Tantas classes de equivalência quantos elementos em A

(b) $\dfrac{A}{I_2}; a \in A, I_2 = A$
$C(a) = a + I = \{a + t/t \in I_2\}$

$C(0_A) = 0_A + I]\{0_A + t/t \in I_2\}$

$0_A + I = \{t/t \in I_2 = A\}$
$\dfrac{A}{I_2} = \{0_A + I\}$
Apenas uma classe de equivalência

2. Seja $A = \mathbb{Z}$. Sabemos que os ideais de $\mathbb{Z}$ são da forma $m\mathbb{Z}, m > 1$. Seja $I = m\mathbb{Z}$ um ideal de $\mathbb{Z}$. Então

$$x \equiv y(mod\ I) \Leftrightarrow x - y \in I \Leftrightarrow x - y = mk, k \in \mathbb{Z} \Leftrightarrow m|(x - y) \Leftrightarrow x \equiv y(mod\ m)$$

Portanto, $\dfrac{\mathbb{Z}}{I} = \dfrac{\mathbb{Z}}{m\mathbb{Z}}$.

Agora seja I ideal e A anel.

$$\frac{A}{I}\{y + I/y \in A\}$$

$$y + I = \{y + t/t \in I\}$$

Vamos definir uma soma $\oplus$ e um produto $\odot$ em $\dfrac{A}{I}$ por

$$(x + I) \oplus (y + I) = (x + y) + I$$

$$(x + I) \odot (y + I) = (xy) + I$$

Verifiquemos que a soma e o produto em $\dfrac{A}{I}$ não dependem do representante da classe de equivalência. Dados $x + I, x_1 + I, y + I, y_1 + I \in \dfrac{A}{I}$ tais que

$$x + I = x_1 + I$$

$$y + I = y_1 + I$$

Então

$$(x + I) \oplus (y + I) = (x + y) + I$$

$$(x_1 + I) \oplus (y_1 + I) = (x_1 + y_1) + I$$

Como $x + I = x_1 + I$, então $x - x_1 \in I$ e como $y + I = y_1 + I$, então $y = y_1 \in I$. Mas I é ideal, logo $(x - x_1) + (y - y_1) = (x + y) - (x_1 + y_1) \in I$, ou seja

$$(x + I) \oplus (y + I) = (x_1 + I) \oplus (y_1 + I)$$

Agora,

$$(x + I) \odot (y + I) = (xy) + I$$

$$(x_1 + I) \odot (y_1 + I) = (x_1 y_1) + I$$

Como $(x - x_1)y \in I$ e $(y - y_1)x_1 \in I$. Logo,

$$(x - x_1)y + (y - y_1)x_1 \in I$$

$$xy - \underbrace{x_1 y + y x_1}_{=0} - y_1 x_1 \in I$$

$$xy - x_1 y_1 \in I$$

, ou seja, $xy + I + x_1 y_1 + I$. Portanto,

$$(x + I) \odot (y - I) = (x_1 + I) \odot (y_1 + I)$$

Teorema 6.1. *Seja $(A, +, .)$ um anel associativo, comutativo e com unidade. Então, se I é um ideal de A, o quociente $\dfrac{A}{I}$ com as operações $\oplus$ e $\odot$ é um anel associativo, comutativo e com unidade. O elemento zero desse anel é a classe $0_A + I$ e o elemento um de $\dfrac{A}{I}$ é $1_A + I$.*

CAPÍTULO 7

GRUPOS

7.1 Definição

Definição 7.1. *Seja A um conjunto não vazio. Toda função $f : A \times A \to A$ é chamada de uma* ***operação binária*** *sobre A.*

Nas considerações que faremos a seguir uma opereção binária f sobre A associa a cada par ordenado $(x, y) \in A \times A$ um elemento $f(x, y) \in A$ será denotada simplesmente por $*$. Assim escreveremos $f(x, y) = x * y$. Por exemplo a operação $* : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $x * y = x^y$ está bem definida pois $x^y \in \mathbb{N}$ sempre que $x, y \in \mathbb{N}$. Observe que esta operação não pode ser definida em $\mathbb{Z}$ pois por exemplo $2^{-1} \notin \mathbb{Z}$. Também não pode ser definida em $\mathbb{Q}$ pois $2^{1/2} \notin \mathbb{Q}$.

Definição 7.2 (Grupo)**.** *Um grupo G é um conjunto não vazio munido de uma operação binária $*$ tal que:*

1. *Para todo $x, y, z \in G$ temos $(x * y) * z = x * (y * z)$. (Associatividade)*

2. *Existe $e \in G$ tal que $x * e = e * x = x$ para todo $x \in G$. Tal elemento e é chamado de* ***elemento neutro*** *ou* ***unidade****.*

3. *Para cada $x \in G$, existe $x^{-1} \in G$ tal que $x * x^{-1} = x^{-1} * x = e$. O elemento x^{-1} é chamado de* ***inverso*** *ou* ***oposto***[1] *de x.*

Denotamos um grupo G, cuja operação binária é $*$, por $(G, *)$. Quando $*$ é a soma, dizemos que $(G, *)$ é um grupo aditivo. Se $*$ é a multiplicação, dizemos que $(G, *)$ é um grupo multiplicativo.

7.2 Grupo comutativo ou abeliano

Definição 7.3 (Grupo comutativo ou abeliano). *Um grupo $(G, *)$ é chamado de* ***grupo comutativo*** *ou* ***abeliano*** *quando $*$ é comutativa, ou seja,*

$$x * y = y * x$$

para todo $x, y \in G$.

Exemplos:

1. $(\mathbb{Z}, +)$ é um grupo abeliano.
2. $(\mathbb{Q}, +)$ é um grupo abeliano.
3. $(\mathbb{Q}^*, \cdot)$ é um grupo abeliano.
4. $(\mathbb{R}, +)$ é um grupo abeliano.
5. $(\mathbb{R}^*, \cdot)$ é um grupo abeliano.
6. Considere o conjunto dos números reais $\mathbb{R}$ com a operação $*$ definida por

$$x * y = x + y - 3$$

, $x, y \in \mathbb{R}$. Então $(\mathbb{R}, *)$ é um grupo abeliano.

[1] $x^{-1} \neq \dfrac{1}{x}$

Solução: *De fato,*

$$
\begin{aligned}
(x * y) * z &= (x + y - 3) * z = (x + y - 3) + z - 3 \\
&= x + (y - 3 + z) - 3 = x + (y + z - 3) - 3 = x * (y + z - 3) \\
&= x * (y * z)
\end{aligned}
$$

para todo $x, y, z \in \mathbb{R}$.

Agora,

$$x * y = x + y - 3 = y + x - 3 = y * x$$

para todo $x, y \in \mathbb{R}$. *Logo,* $*$ *é comutativa.*

Para todo $x \in \mathbb{R}$, *temos* $x * 3 = x + 3 - 3 = x$. *Logo, 3 é o elemento neutro de* $*$.

Dado $x \in \mathbb{R}$, *tome* $x^{-1} = 6 - x$. *Assim*

$$x * x^{-1} = x + (6 - x) - 3 = 3$$

Logo, para $x \in \mathbb{R}$ *o inverso de* x *por* $*$ *é* $6 - x$.

Portanto $(\mathbb{R}, *)$ *é um grupo comutativo.*

7. $\left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}, \oplus\right)$ é grupo.

8. $\left(\dfrac{\mathbb{Z}}{m\mathbb{Z}} - \{\bar{0}\}, \odot\right)$ é grupo?
   $\dfrac{\mathbb{Z}}{4\mathbb{Z}} - \{\bar{0}\} = \{\bar{1}, \bar{2}, \bar{3}\} = G$
   $\bar{2} \in G,\ \bar{2} \odot \bar{2} = \bar{0} \notin G$

9. $\left(U\left(\dfrac{\mathbb{Z}}{m\mathbb{Z}}\right), \odot\right)$ é um grupo.

10. ver **https://en.wikipedia.org/wiki/XOR_swap_algorithm**

7.3 Propriedades Imediatas de um grupo

Seja $(G, *)$ um grupo. É fácil ver que

1. O elemento neutro é único

2. Existe um único inverso para cada $x \in G$

3. Para todos $x, y \in G, (x * y)^{-1} = y^{-1} * x^{-1}$. Por indução, $x_1, x_2, ..., x_{n-1}, x_n \in G$,

$$(x_1 * x_2 * ... * x_{n-1} * x_n)^{-1}$$

$$= x_n^{-1} * x_{n-1}^{-1} * ... * x_2^{-1} * x_1^{-1}$$

4. Para todo $x \in G, (x^{-1})^{-1} = x$

7.4 Ordem de um Grupo

Definição 7.4 (Ordem de um grupo)**.** *Quando um grupo $(G, *)$, G é um conjunto com um número finito de elementos, dizemos que G é um grupo finito. Denotamos por $|G|$ o número de elementos de G que será chamado de ordem de G ou cardinalidade de G. Quando G não é finito, dizemos que G é um grupo infinito.*

Exemplos:

1. $(\mathbb{Z}_m, +)$ é um grupo finito para todo $m > 1$.

2. $(\mathbb{Z}, +)$ é um grupo infinito.

7.5 Subgrupo

7.5.0.1 Definição

Definição 7.5 (Subgrupo)**.** *Seja $(G, *)$ um grupo. Um subconjunto não vazio $H \subseteq G$ é um subgrupo se, e somente se, $(H, *)$ é um grupo.*

7.5.0.2 Propriedades

Proposição 7.5.1. *Um subconjunto não vazio $H \subseteq G$ é um subgrupo de G se, e somente se*

1. $x^{-1} \in H, \forall x \in H$

2. $x * y \in H, \forall x, y \in H$

Demonstração: Se H é subgrupo, então H é um grupo. Logo 1 e 2 são satisfeitos.
Agora provemos que se H satisfaz 1 e 2, então H é grupo.
Como G é grupo, então $*$ é associativo, logo $*$ é associativo em H.
De 1, $\forall x \in H, x^{-1} \in H$. Mas de 2, $\forall x, y \in H$, $x*y \in H$. Logo, se $x \in H$, então $e = x*x^{-1} \in H$
Novamente por 1, todo elemento de H possui inverso em H.
Logo, $(H, *)$ é um grupo.#
Exemplos:

1. Dado $(G, *)$ grupo, $H = \{e\}$ e $H = G$ são subgrupos de G, chamados de subgrupos triviais

2. $(\mathbb{Z}, +)$, $H = m\mathbb{Z}$, $m > 1$

   Então H é subgrupo de $\mathbb{Z}$

3. $G = U\left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

   $(G, \odot)$ é um grupo

   $|G|$=4

   $H_1 = \{\bar{1}, \bar{3}\}$ é subgrupo de G
   $H_2 = \{\bar{1}, \bar{5}\}$ é subgrupo de G
   $H_3 = \{\bar{1}, \bar{7}\}$ é subgrupo de G

7.6 Ordem de um subgrupo

Teorema 7.1 (Lagrange)**.** *Seja G um grupo finito. Se $H \subseteq G$ é um subgrupo, então $|H|$ divide $|G|$.*

Exemplo: Quais são as possíveis ordens dos subgrupos de um grupo de ordem 48?

Seja G um grupo tal que $|G| = 48$. Se H é um subgrupo de G, então $|H|$ divide $|G|$

$48 = 2^4 3$

$|H| = 2, 3, 2^2, 2^3, 2^4, 2.3, 2^2 3, 2^2 3$

Observação: O teorema não diz que haverá um subgrupo de ordem n para todo n tal que $n||G|$. Diz apenas que se H é subgrupo de G, então $|H|$ divide $|G|$.

Corolário 7.1.1. *Os únicos subgrupos de um grupo de ordem prima são os triviais*

Demonstração: Quando $|G| = p$ primo, temos que os únicos divisores de p positivos são 1 e p.

Então, se H é subgrupo de G, então $|H| = 1$ ou $|H| = p$.

Portanto, $H = \{e\}$ ou $H = G$.#

7.7 Homomorfimos de Grupos

Sejam $(G, *)$ e $(H, \triangle)$ grupos quaisquer. Considere uma função $f : G \to H$. Entre todas as possíveis funções entre G e H vamos considerar somente aquelas que satisfação a condição

$$f(x * y) = f(x) \triangle f(y)$$

para todos $x, y \in G$, ou seja, podemos determinar a imagem de $f(x * y)$ a partir da imagem de x e de y,

Definição 7.6. *Dados doi grupos $(G, *)$ e $(H, \triangle)$ dizemos que uma função $f : G \to H$ é um **homomorfismo de grupos** se*

$$f(x * y) = f(x) \triangle f(y)$$

para todos $x, y \in G$.

Observação 7.6.1. *Sejam $(G, *)$ e $(H, \triangle)$ grupos e $f : G \to H$ um homomorfismo.*

1. *Se $G = H$, neste caso $f : G \to G$ é chamado de um **endomorfimos** de grupos.*

2. *Se $f : G \to H$ é uma função injetora, então dizemos que f é um **monomorfismo** de grupos.*

3. *Se $f : G \to H$ é uma função sobrejetora, então dizemos que f é um* ***epimorfismo*** *de grupos.*

4. *Se $f : G \to H$ é uma função bijetora, então dizemos que f é um* ***isomorfismo*** *de grupos.*

5. *Se $f : G \to G$ é uma função bijetora, então dizemos que f é um* ***automorfismo*** *de grupos.*

Exemplos 7.6.1. 1. *A função $f : \mathbb{Z} \to \mathbb{C}$ dada por $f(x) = i^x$ é um homomorfismo de $(\mathbb{Z}, +)$ em $(\mathbb{C}, \cdot)$. De fato,*

$$f(x + y) = i^{x+y} = i^x \cdot i^y = f(x) \cdot f(y)$$

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

2. *A função $f : \mathbb{R}_+^* \to \mathbb{R}$ dada por $f(x) = \ln(x)$ é um homomorfismo de $(\mathbb{R}_+^*, \cdot)$ em $(\mathbb{R}, +)$. De fato,*

$$f(xy) = \ln(xy) = \ln(x) + \ln(y) = f(x) + f(y)$$

para todos $x, y \in \mathbb{R}_+^*$. Além disso, como $\ln(x)$ é uma função bijetora, então f é um isomorfismo de grupos.

3. *Sejam m um inteiro positivo fixo. A função $f : \mathbb{Z} \to \mathbb{Z}_m$ definida por $f(x) = \overline{x}$ é um homomorfimos de $(\mathbb{Z}, +)$ em $(\mathbb{Z}_m, \oplus)$. De fato,*

$$f(x + y) = \overline{x + y} = \overline{x} + \overline{y} = f(x) + f(y).$$

Além disso, esse homomorfismo é sobrejetor.

Proposição 7.6.1. *Sejam $(G, *)$ e $(H, \triangle)$ grupos e $f : G \to H$ um homomorfismo. Denote por 1_G e 1_H os elementos neutros de G e H, respectivamente.*

1. $f(1_G) = 1_H$

2. $f(x^{-1}) = (f(x))^{-1}$ *para todo $x \in G$.*

Proposição 7.6.2. *Sejam I é um subgrupo de G e $f : G \to H$ um homomorfismo de grupos. Então $f(I)$ é um subgrupo de H.*

Prova: Como I é um subgrupo de G, então $1_G \in G$. Agora f é um homomorfismo, logo $f(1_G) = 1_H \in f(I)$ e assim $f(I) \neq \emptyset$.

Agora, dado $y \in f(I)$ precisamos mostrar que $y^{-1} \in f(I)$. Mas se $y \in f(I)$, então $y = f(x)$ com $x \in I$. Daí

$$y^{-1} = [f(x)]^{-1} = f(x^{-1})$$

e como I é um subgrupo de G, $x^{-1} \in I$ e como isso $y^{-1} \in f(I)$.

Finalmente, dados $y, z \in f(I)$ existem $x_1, x_2 \in I$ tais que $y = f(x_1)$ e $z = f(x_2)$. Mas f é homomorfismo, daí

$$y \triangle z = f(x_1) \triangle f(x_2) = f(x_1 * x_2)$$

e como I é subgrupo, $x_1 * x_2 \in I$. Logo $y \triangle z \in f(I)$.

Portanto $f(I)$ é um subgrupo de H. $\diamond$

Definição 7.7. *Sejam $(G, *)$ e $(H, \triangle)$ grupos e $f : G \to H$ um homomorfismo de grupos. Chama-se de **núcleo** ou **kernel** de f e denota-se por $N(f)$ ou $\ker(f)$ o seguinte subconjunto de G:*

$$\ker(f) = \{x \in G \mid f(x) = 1_H\}.$$

Exemplos 7.7.1. 1. *Considere o homomorfismo $f : \mathbb{Z} \to \mathbb{C}^*$ dado por $f(x) = i^x$. Temos*

$$\ker(f) = \{x \in \mathbb{Z} \mid f(x) = 1\} = \{x \in \mathbb{Z} \mid i^x = 1\} = \{0, \pm 4, \pm 8, \cdots\} = 4\mathbb{Z}.$$

2. *O núcleo do homomorfismo $f : \mathbb{R}_+^* \to \mathbb{R}$ dado por $f(x) = \ln(x)$. Temos*

$$\ker(f) = \{x \in \mathbb{R}_+^* \mid f(x) = 0\} = \{x \in \mathbb{R}_+^* \mid \ln(x) = 0\} = \{1\}.$$

3. *O núcleo do homomorfismo $f : \mathbb{Z} \to \mathbb{Z}_m$ dado por $f(x) = \overline{x}$, $m > 0$ fixo. Temos*

$$\ker(f) = \{x \in \mathbb{Z} \mid f(x) = \overline{0}\} = \{x \in \mathbb{Z} \mid \overline{x} = \overline{0}\} = \{0, \pm m, \pm 2m, \cdots\}.$$

Proposição 7.7.1. *Sejam $f : G \to H$ um homomorfismo de grupos. Então:*

1. *$\ker(f)$ é um subgrupo de G.*

2. *f é um monomorfismo se, e somente se, $\ker(f) = \{1_G\}$.*

Prova:

1. Como $f(1_G) = 1_H$, então $1_G \in \ker(f)$ e com isso $\ker(f) \neq \emptyset$. Se $x \in \ker(f)$, então $f(x^{-1}) = [f(x)]^{-1} = 1_H^{-1} = 1_H$ e daí $x^{-1} \in \ker(f)$. Finalmente se $x, y \in \ker(f)$, então $f(x * y) = f(x) \triangle f(y) = 1_H \triangle 1_H = 1_H$, ou seja, $x * y \in \ker(f)$.

   Portanto $\ker(f)$ é um subgrupo de G.

2. Suponha que f é um monomorfismo de grupos. Tome $x \in \ker(f)$. Temos $f(x) = 1_H = f(1_G)$ e como f é injetora $x = 1_G$. Logo $\ker(f) = \{1_G\}$.

   Agora suponha que $\ker(f) = \{1_G\}$. Sejam $x, y \in G$ tais que

$$\begin{aligned} f(x) &= f(y) \\ f(x) \triangle f(y)^{-1} &= 1_H \\ f(x) \triangle f(y^{-1}) &= 1_H \\ f(x * y^{-1}) &= 1_H \end{aligned}$$

   e daí $x * y^{-1} \in \ker(f) = \{1_G\}$. Logo $x * y^{-1} = 1_G$, isto é, $x = y$. Portanto f é injetora.

◇

7.8 Grupos de Permutação

Fazer a parte de S_n.

7.9 Grupos Cíclicos

Fazer a parte de grupos cíclicos.

BIBLIOGRAFIA

[1] H.H. Domingues, G.Iezzi: *Álgebra Moderna*, 2ł Ed., Atual, 1982

[2] S. Shokranian: *Álgebra 1*, Ciência Moderna, 2010

[3] Adilson Gonçalves: *Introdução à Álgebra*, 5ł Ed., IMPA, 2003

[4] G. Birkhoff, S. MacLane: *Álgebra Moderna Básica*, 4ł Ed., Guanabara Dois, 1980

[5] E. A. Filho: *Iniciação à Lógica Matemática*, Nobel, 2002

ÍNDICE REMISSIVO