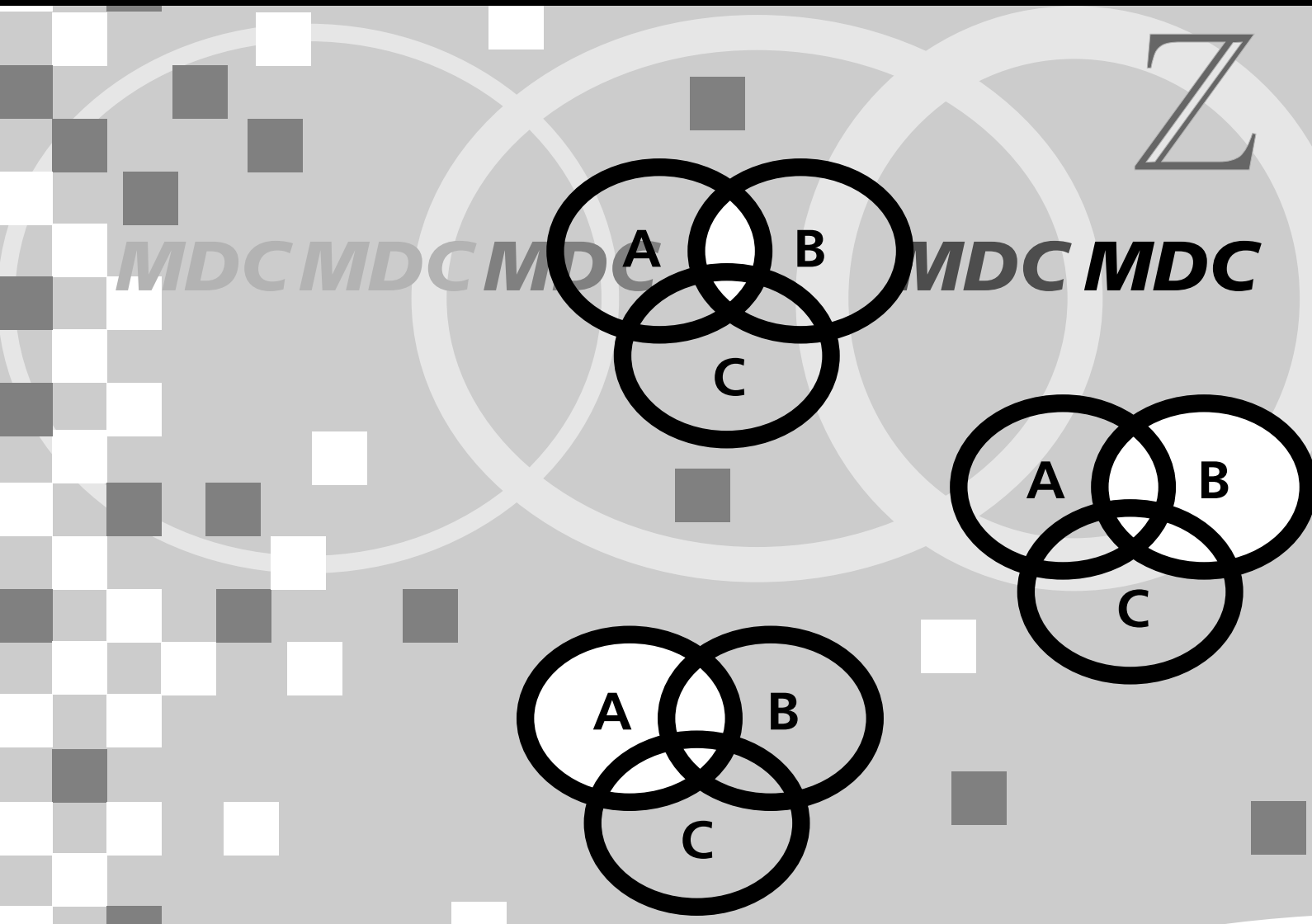
**Módulo 1** **Volume** | 1

Adilson Gonçalves
Luiz Manoel Figueiredo

# Álgebra I




Fundação CECIERJ
Consórcio cederj

Fundação CECIERJ

Consórcio cederj

Centro de Educação Superior a Distância do Estado do Rio de Janeiro

# Álgebra I

**Volume 1 - Módulo 1**

Adilson Gonçalves

Luiz Manoel Figueiredo

GOVERNO DO Rio de Janeiro

SECRETARIA DE CIÊNCIA E TECNOLOGIA

UAB UNIVERSIDADE ABERTA DO BRASIL

Ministério da Educação

BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL

**Apoio:**

FAPERJ Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro

# Fundação Cecierj / Consórcio Cederj

Rua Visconde de Niterói, 1364 – Mangueira – Rio de Janeiro, RJ – CEP 20943-001
Tel.: (21) 2334-1569 Fax: (21) 2568-0725

**Presidente**
Masako Oya Masuda

**Vice-presidente**
Mirian Crapez

**Coordenação do Curso de Matemática**
UFF - Regina Moreth
UNIRIO - Luiz Pedro San Gil Jutuca

## Material Didático

**ELABORAÇÃO DE CONTEÚDO**
Adilson Gonçalves
Luiz Manoel Figueiredo

**COORDENAÇÃO DE DESENVOLVIMENTO INSTRUCIONAL**
Cristine Costa Barreto

**COORDENAÇÃO DE LINGUAGEM**
Maria Angélica Alves

## Departamento de Produção

**EDITORA**
Tereza Queiroz

**COORDENAÇÃO EDITORIAL**
Jane Castellani

**COORDENAÇÃO DE PRODUÇÃO**
Jorge Moura

**CAPA**
Eduardo Bordoni

**PRODUÇÃO GRÁFICA**
Patricia Seabra





G635a
Gonçalves, Adilson.
Álgebra I. v.1 / Adilson Gonçalves. – Rio de Janeiro: Fundação CECIERJ, 2010.
76p.; 21 x 29,7 cm.

ISBN: 85-7648-130-8

1. Álgebra. 2. Conjuntos. 3. Relações de equivalência. 4. Teorema da divisão de Euclides. 5. Números inteiros. I. Figueiredo, Luiz Manoel. II. Título.

CDD: 512

**2010/1**

Referências Bibliográficas e catalogação na fonte, de acordo com as normas da ABNT.

# Governo do Estado do Rio de Janeiro

**Governador**
Sérgio Cabral Filho

**Secretário de Estado de Ciência e Tecnologia**
Alexandre Cardoso

## Universidades Consorciadas

**UENF - UNIVERSIDADE ESTADUAL DO NORTE FLUMINENSE DARCY RIBEIRO**
Reitor: Almy Junior Cordeiro de Carvalho

**UERJ - UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO**
Reitor: Ricardo Vieiralves

**UFF - UNIVERSIDADE FEDERAL FLUMINENSE**
Reitor: Roberto de Souza Salles

**UFRJ - UNIVERSIDADE FEDERAL DO RIO DE JANEIRO**
Reitor: Aloísio Teixeira

**UFRRJ - UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO**
Reitor: Ricardo Motta Miranda

**UNIRIO - UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO**
Reitora: Malvina Tania Tuttman

## SUMÁRIO

# Aula 1 – Conjuntos

## Meta

Introduzir as noções básicas de conjunto e produto cartesiano de conjuntos.

## Objetivos

Ao final desta aula, você deve ser capaz de:

- Definir as noções básicas de conjunto e subconjunto; união, interseção e diferença entre dois conjuntos.
- Identificar os conjuntos numéricos: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.
- Desenvolver os conceitos de par ordenado e produto cartesiano de conjuntos.

## Introdução

O estudo mais rigoroso da teoria dos conjuntos despontou no séc. XIX, com os trabalhos do matemático **Georg Cantor**. Em um de seus trabalhos, ele abalou a comunidade matemática da época, provando que a *a cardinalidade infinita do conjunto* $\mathbb{R}$*, dos números reais, é maior que a cardinalidade infinita do conjunto* $\mathbb{N}$ *dos números naturais.*

As idéias fundamentais da teoria dos conjuntos foram desenvolvidas pelo matemático Georg Cantor (1845 –1918).
Muitas de suas idéias geniais não foram aceitas inicialmente por outros matemáticos. No entanto, tiveram uma influência profunda na Matemática do século XX.

A cardinalidade de um conjunto finito é o número de elementos deste conjunto. Cantor mostrou que há vários tipos de conjuntos infinitos e que existem infinitos "maiores" que outros infinitos. O conjunto dos números racionais $\mathbb{Q}$ tem a mesma cardinalidade infinita que $\mathbb{N}$, mas $\mathbb{R}$ tem cardinalidade maior.

A noção de conjunto desempenha papel fundamental na organização e no desenvolvimento da Matemática e de suas aplicações.

Observe que $\mathbb{Q}$ tem mais elementos que $\mathbb{N}$ no sentido de que todo número natural é racional, mas há muitos racionais (na verdade, infinitos racionais) que não são inteiros. No entanto, $\mathbb{N}$ e $\mathbb{Q}$ têm a mesma cardinalidade infinita.

Nesta primeira aula, abordaremos, de maneira resumida e intuitiva, os fundamentos básicos da teoria dos conjuntos. Uma outra apresentação elementar para este tópico são as Aulas 1 a 4 da disciplina Matemática Discreta, pela qual você, aluno, provavelmente já passou.

Então, segure-se firme. Vamos iniciar uma viagem por uma das áreas mais bonitas da Matemática: a Álgebra.

## Conjuntos: uma breve apresentação

Em Matemática, conjuntos e elementos são noções primitivas, assim como ponto, reta e plano. Entendemos *conjunto* como uma coleção de objetos. Os objetos que formam um conjunto são chamados *elementos* do conjunto.

É conveniente admitir a existência do *conjunto vazio*, representado pelo símbolo $\emptyset$. Assim, o conjunto vazio é um conjunto sem elementos.

Quando todos os elementos de um conjunto $A$ são também elementos de um conjunto $B$, dizemos que *o conjunto $A$ está contido no conjunto $B$*, ou que *$A$ é subconjunto de $B$*.

Assim, um conjunto $A$ não é subconjunto de um conjunto $B$ quando existe algum elemento de $A$ que não é elemento de $B$. **O conjunto $\emptyset$ é considerado subconjunto de qualquer conjunto.**

Por que o conjunto vazio é considerado subconjunto de qualquer conjunto? Raciocine por absurdo: se $\emptyset$ não fosse subconjunto de algum conjunto $A$, deveria haver um elemento de $\emptyset$ não pertencente a $A$. Porem, $\emptyset$ não tem elemento algum!

Dois conjuntos $A$ e $B$ são iguais quando possuem os mesmos elementos, isto é, todo elemento de $A$ é elemento de $B$ ($A \subset B$) e todo elemento de $B$ é elemento de $A$ ($B \subset A$). Assim,

$$A = B \quad \text{se, e somente se, } A \subset B \text{ e } B \subset A\ .$$

Assim, todo conjunto é subconjunto de si mesmo. Quando $A$ é um subconjunto de $B$, mas não é igual a $B$, então dizemos que $A$ é subconjunto próprio de $B$.

Usaremos as seguintes notações:

- $x \in A$, $x$ é um elemento do conjunto $A$ ou $x$ pertence a $A$.
- $x \notin A$, $x$ não é elemento do conjunto $A$, ou $x$ não pertence a $A$.
- $A \subset B$, o conjunto $A$ é um subconjunto do conjunto $B$ ou $A$ está contido em $B$.

  Se $A \subset B$, dizemos também que o conjunto $B$ contém o conjunto $A$ e denotamos $B \supset A$.
- $A \not\subset B$. O conjunto $A$ não está contido no conjunto $B$.
- $A \subsetneq B$, o conjunto $A$ é subconjunto próprio de $B$. Assim,

$$A \subsetneq B \quad \text{se, e somente se,} A \subset B \text{ e } A \neq B\ .$$

## Conjuntos numéricos

Os conjuntos numéricos são os seguintes:

- O conjunto dos números naturais, representado por $\mathbb{N}$, é o conjunto

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\} .$$

- O conjunto dos números inteiros, representado por $\mathbb{Z}$, é o conjunto

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} .$$

- O conjunto dos números racionais, representado por $\mathbb{Q}$, é o conjunto

$$\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z} \text{ e } n \neq 0\} ,$$

  isto é, os números racionais são as frações.

- O conjunto dos números reais representado por $\mathbb{R}$ é o conjunto formado pelos números racionais e irracionais. Números irracionais representam quantidades que não podem ser expressas na forma de fração, por exemplo, $\sqrt{2}$, $\pi$ etc.

- O conjunto dos números complexos, denotado por $\mathbb{C}$, é o conjunto

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R} \text{ e } i = \sqrt{-1}\} .$$

  Observe que

$$\mathbb{N} \subsetneqq \mathbb{Z} \subsetneqq \mathbb{Q} \subsetneqq \mathbb{R} \subsetneqq \mathbb{C} .$$

Para uma construção detalhada dos conjuntos numéricos, dos números naturais até os reais, consulte o Módulo 1 da disciplina Pré-cálculo. Os números complexos foram apresentados no Módulo 3 de Pré-cálculo.

## União e interseção entre conjuntos

O conjunto formado pelos elementos que pertencem tanto ao conjunto $A$ quanto ao conjunto $B$ é chamado *interseção* de $A$ e $B$, denotado por $A \cap B$. Assim,

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

Um elemento de $A \cap B$ pertence *simultaneamente* aos conjuntos $A$ e $B$.

O conjunto formado pelos elementos que estão em $A$ **ou** estão em $B$ é chamado de *união* de $A$ e $B$, denotado por $A \cup B$. Assim,

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

O "ou" da matemática é *não exclusivo*, quer dizer, se $x \in A$ ou $x \in B$, então $x$ pode estar em $A$, pode estar em $B$ ou pode estar em ambos.
Repare que "ou" na linguagem cotidiana é, em geral, exclusivo. Quando dizemos "hoje à noite vou ao cinema ou ao teatro", queremos dizer que iremos a um ou ao outro, mas não a ambos.

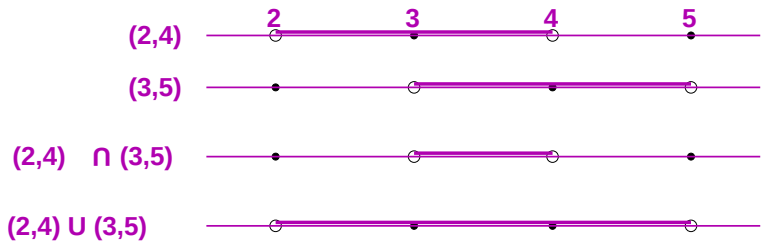
Quando usamos o conectivo *ou* ao escrevermos $x \in A$ ou $x \in B$, o elemento $x$ pode estar no conjunto $A$, ou pode pertencer ao conjunto $B$. Basta pertencer a um deles para pertencer à união.

Para quaisquer conjuntos $A$ e $B$ valem as seguintes propriedades:

- $A \cap \emptyset = \emptyset$;
- $A \cup \emptyset = A$;
- $A \cap B \subset A \quad$ e $\quad A \cap B \subset B$;
- $A \cup B \supset A \quad$ e $\quad A \cup B \supset B$.

Exemplo 1

1. $\mathbb{Z} \cap \mathbb{Q} = \mathbb{Z}$ e $\mathbb{Z} \cup \mathbb{Q} = \mathbb{Q}$.
2. $\mathbb{Q} \cup \{\text{números irracionais}\} = \mathbb{R}$.
3. $(2,4) \cap (3,5) = (3,4)$ e $(2,4) \cup (3,5) = (2,5)$. Observe o diagrama a seguir:




4. $[1,2] \cap [2,5) = \{2\}$.
5. $(0,1) \cap (0,\frac{1}{2}) \cap (0,\frac{1}{3}) \cap (0,\frac{1}{4}) \cap (0,\frac{1}{5}) \cap \ldots \cap (0,\frac{1}{n}) \cap \ldots = \emptyset$.

Intervalos:
você se lembra dos intervalos abertos e fechados? A notação é:
$(a,b) = \{x \in \mathbb{R} \mid a < x < b\}$
$[a,b) = \{x \in \mathbb{R} \mid a \leq x < b\}$
$(a,b] = \{x \in \mathbb{R} \mid a < x \leq b\}$
$[a,b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$.

## Diagramas

Muitas vezes é conveniente representar conjuntos por meio de diagramas geométricos, em que conjuntos são representados por regiões do plano. Estes diagramas são chamados *Diagramas de Venn*.

Por exemplo, dados dois conjuntos $A$ e $B$ tais que $A \not\subset B$ e $B \not\subset A$, podemos representá-los pelo diagrama a seguir, no qual a área mais escura representa o conjunto interseção $A \cap B$.

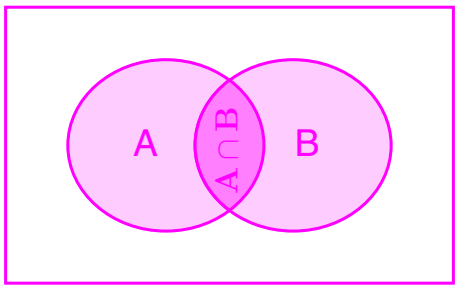



Fig. 1.1: A interseção $A \cap B$ é a área mais escura do gráfico

Se $A \subset B$, podemos representá-los pela figura

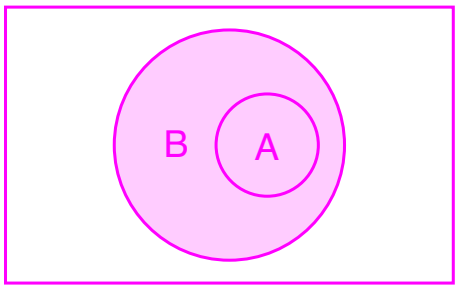



Fig. 1.2: $A \cap B = A$

O conjunto *diferença* de $A$ e $B$, denotado por $A - B$, é o conjunto dos elementos de $A$ que não pertencem ao conjunto $B$. Assim,

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

O diagrama a seguir representa a diferença $A - B$.

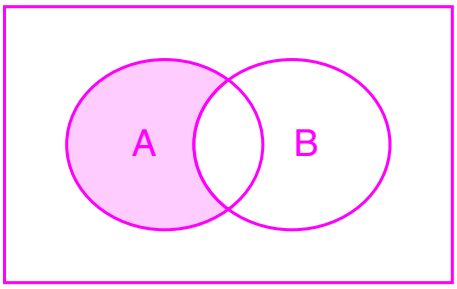



Fig. 1.3: Diferença entre $A$ e $B$

**Exemplo 1**

Prove a seguinte igualdade:

$$(A - B) \cup (B - A) = (A \cup B) - (A \cap B) \, .$$

*Solução:*

Devemos mostrar que todo elemento de $(A - B) \cup (B - A)$ é também elemento de $(A \cup B) - (A \cap B)$, e vice-versa.

Seja $x$ um elemento de $(A - B) \cup (B - A)$. Temos $x \in (A - B)$ ou $x \in (B - A)$. Vamos analisar cada um destes dois casos separadamente.

Se $x \in (A - B)$, então $x \in A$ e $x \notin B$. Se $x \in A$, então $x \in A \cup B$. Se $x \notin B$, então $x \notin A \cap B$ (se $x$ não está em $B$, não pode estar na interseção de $B$ com conjunto algum!). Como $x \in A \cup B$ e $x \notin A \cap B$, então $x \in (A \cup B) - (A \cap B)$. Mostramos que

$$x \in (A - B) \cup (B - A) \Rightarrow x \in (A \cup B) - (A \cap B) \, .$$

Vamos, agora, demonstrar a recíproca. Seja $x \in (A \cup B) - (A \cap B)$. Assim, $x \in (A \cup B)$ e $x \notin (A \cap B)$. Como $x \in (A \cup B)$, então $x \in A$ ou $x \in B$. Vamos analisar os dois casos separadamente.

Se $x \in A$, como $x \notin (A \cap B)$, então $x \notin B$ e, portanto, $x \in (A - B)$.

Se $x \in B$, como $x \notin (A \cap B)$, então $x \notin A$ e, portanto, $x \in (B - A)$.

Assim, concluímos que $x \in (A - B)$ ou $x \in (B - A)$, isto é, $x \in (A - B) \cup (B - A)$, o que completa a demonstração.

A figura a seguir mostra, em um diagrama, o conjunto $(A-B)\cup(B-A)$.

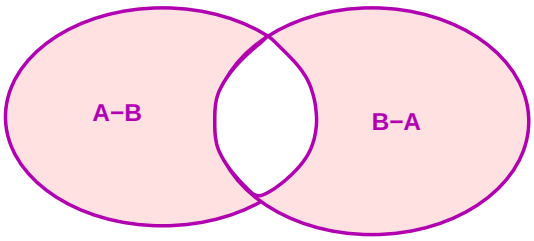



Fig. 1.4: Diagrama de $(A - B) \cup (B - A)$.

Você achou este exemplo um pouco complicado? Repasse o exemplo até ter certeza de que entendeu todos os passos. Tente fazê-lo sem olhar a aula. No fundo, é mais fácil do que parece!

Vamos apresentar um outro exemplo, do mesmo tipo, mas agora com três conjuntos.

**Exemplo 2**

Mostre que, quaisquer que sejam os conjuntos $A$, $B$ e $C$, vale o seguinte:

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

*Solução:* Vamos começar mostrando que todo elemento do conjunto à esquerda é também elemento do conjunto à direita da igualdade.

Seja $x \in A \cap (B \cup C)$. Então, pela definição de interseção, temos que $x \in A$ e $x \in (B \cup C)$, simultaneamente.

Como $x \in (B \cup C)$, então $x \in B$ ou $x \in C$. Como $x \in A$ temos $x \in A$ e ($x \in B$ ou $x \in C$), ou seja, ($x \in A$ e $x \in B$) ou ($x \in A$ e $x \in C$), ou ainda, $x \in A \cap B$ ou $x \in A \cap C$, o que resulta em $x \in (A \cap B) \cup (A \cap C)$. Concluímos que

$$A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C) \, .$$

Vamos agora provar a recíproca. Suponha que $x \in (A \cap B) \cup (A \cap C)$. Portanto, $x \in (A \cap C)$ ou $x \in (A \cap B)$. Vamos analisar os dois casos.

Se $x \in (A \cap C)$, então $x \in A$ e $x \in C$. Logo, $x \in A$ e $x \in (B \cup C)$, já que $c \subset (B \cup C)$. Nesse caso, concluímos que $x \in A \cap (B \cup C)$.

Se $x \in (A \cap B)$, raciocinamos de maneira análoga:

$$x \in (A \cap B) \Rightarrow x \in A \text{ e } x \in B \Rightarrow x \in A \text{ e } x \in (B \cup C) \Rightarrow x \in A \cap (B \cup C) \, .$$

Concluímos que

$$(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C) \, ,$$

o que completa a demonstração.

A figura a seguir mostra, em um diagrama, o conjunto $A \cap (B \cup C)$.

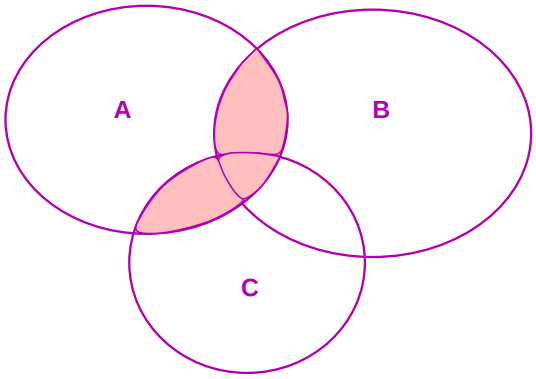



Fig. 1.5: O conjunto $A \cap (B \cup C)$.

### Produto cartesiano de conjuntos

Um *par ordenado* é uma seqüência ordenada de dois elementos. Escreve-se o par entre parêntesis, como em $(a, b)$. Repare que a ordem dos elementos no par é significativa. Por exemplo, os pares ordenados de inteiros $(1, 2)$ e $(2, 1)$ são diferentes. Dois pares ordenados são iguais se têm os mesmos elementos na mesma ordem, isto é,

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

Você notou a coincidência de notação? Se $a, b$ são números reais, o mesmo símbolo $(a, b)$ é usado para denotar o intervalo aberto $a < x < b$ e o par ordenado $(a, b)$ que, evidentemente, são duas coisas inteiramente diferentes. Isto, em geral, não causa problemas visto que pelo contexto normalmente sabemos a quais dos dois objetos estamos nos referindo

Analogamente, uma *tripla ordenada* de elementos é uma seqüência de 3 elementos em que a ordem é significativa, isto é,

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

De maneira geral, chamamos de uma *n-upla ordenada* de elementos uma lista ordenada $(a_1, a_2, \ldots, a_n)$, na qual a ordem é significativa. Duas $n$-uplas são iguais quando possuem os elementos nas mesmas posições:

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \quad \text{se, e somente se,} \quad a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n \ .$$

Sejam os conjuntos $A$ e $B$. O *produto cartesiano* de $A$ e $B$, denotado por $A \times B$, é o conjunto de todos os pares ordenados $(a, b)$, com $a \in A$ e $b \in B$. Assim,

$$A \times B = \{(a, b) \mid a \in A \text{ e } b \in B\} \ .$$

Podemos generalizar esta definição para vários conjuntos. Dados os conjuntos $A_1, A_2, A_3, \ldots, A_n$, o produto cartesiano $A_1 \times A_2 \times A_3 \times \cdots \times A_n$ é definido por

$$A_1 \times A_2 \times A_3 \times \cdots \times A_n = \{(a_1, a_2, a_3, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\} \ .$$

### Exemplo 3

Seja $A = \{1, 2\}$ e $B = \{3, 4, 5\}$, então

$$\begin{aligned} A \times B &= \{(1,3), (1,4), (1,5), (2,3), (2,4), (2,5)\} \quad \text{e} \\ B \times A &= \{(3,1), (3,2), (4,1), (4,2), (5,1), (5,2)\}. \end{aligned}$$

Note que, neste exemplo, para estes conjuntos, $A \times B \neq B \times A$. O produto cartesiano de conjuntos não é uma operação comutativa.

Note, ainda em relação ao exemplo anterior, que o produto cartesiano de um conjunto $A$ de 2 elementos por um conjunto $B$ de 3 elementos é um conjunto $A \times B$ de $2 \times 3 = 6$ elementos. Vamos deixar como exercício a prova da proposição que enunciamos a seguir.

Proposição 1
Se $A$ e $B$ são conjuntos finitos, então

$$|A \times B| = |A| \times |B| \, ,$$

onde $|A|$ indica o número de elementos de um conjunto $A$.

## Resumo

O conceito de conjunto pertence aos fundamentos. está presente em todas as formas em que a Matemática se manifesta, sendo especialmente importante neste curso de Álgebra. Assim, faça uma revisão criteriosa nos conceitos de união, interseção e produto cartesiano apresentados nesta primeira aula.

Os exemplos apresentados são considerados atividades com roteiro de solução. Você deve reescrevê-los com suas próprias palavras.

Para você, aluno, que se inscreveu em Álgebra 1, essas noções básicas de conjunto provavelmente são já bem conhecidas. Assim, procuramos apresentá-las dentro de um princípio de revisão dinâmica, onde à revisão dos conceitos básicos acrescentamos alguns aspectos específicos e procuramos fixar a notação que será utilizada ao longo desta disciplina.

Nos Exemplos 1 e 2 apresentamos demonstrações de duas proposições básicas envolvendo conjuntos, que você deveria tentar reescrever com suas palavras.

## Atividades propostas

1. Para os conjuntos $A = \{1, 2, 3, 4\}$ e $B = \{3, 4, 5, 6\}$, calcule:
   (a) $A \cup B$.
   (b) $A \cap B$.
   (c) $A - B$.
   (d) $B - A$.
   (e) $A \times B$.

2. Seja $A$ um conjunto. Prove que $A - \emptyset = A$ e $\emptyset - A = \emptyset$.

3. Prove que $A \subset B$ se, e somente se, $A - B = \emptyset$.

4. Sejam $A$ e $B$ conjuntos não-vazios. Prove que $A \times B = B \times A$ se, e somente se, $A = B$. Por que razão é necessária a condição de $A$ e $B$ serem não-vazios?

5. Demonstre a igualdade $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

6. Mostre que se $A$ e $B$ são conjuntos finitos, então $|A \times B| = |A| \times |B|$ .

7. Sejam $A$ e $B$ conjuntos quaisquer. Mostre que

$$|A \cup B| = |A| + |B| - |A \cap B| .$$

8. Escreva os seguintes subconjuntos $A \subset \mathbb{R}$, dos números reais, como união de intervalos:

   (a) $A = \{x \in \mathbb{R} \mid x^2 > 1 \text{ e } x^2 < 4\}$.

   (b) $A = \{x \in \mathbb{R} \mid x^2 \geq 4 \text{ e } x^2 < 9\}$.

   (c) $A = \{x \in \mathbb{R} \mid x^2 \geq 2 \text{ e } x^2 \geq 1\}$.

   (d) Escreva $A \cap \mathbb{Z}$ para cada um dos três conjuntos acima descritos.

**Auto-avaliação**

Você deveria ter sido capaz de resolver todos os exercícios propostos. As respostas, propositadamente, não estão descritas aqui para que você tente, sozinho, achar o caminho da solução a partir do que é apresentado no próprio texto.

Se você tiver alguma dificuldade, volte ao texto da aula e tente novamente. Procure também o tutor para esclarecer dúvidas que ainda persistam e discutir soluções dos exercícios propostos.

Os exemplos inclusos na aula são consideradas atividades com roteiro de solução. Você deve conseguir reproduzí-los com suas próprias palavras.

Não avance para a próxima aula antes de conseguir fazer todas as atividades propostas.

# Aula 2 – Relações e relações de equivalência

### Meta

Abordar relações e relações de equivalências.

### Objetivos

Ao final desta aula, você deve ser capaz de:

- Definir os conceitos de relação em um conjunto e entre dois conjuntos.
- Enunciar as propriedades das relações.
- Reconhecer uma relação de equivalência e dar alguns exemplos.

### Introdução

Um dos conceitos mais importantes na Matemática é o de *relação*. Ele está ligado à idéia de comparação entre objetos, de acordo com algum critério ou alguma regra.

Podemos citar como exemplo a relação "é mais novo que" no conjunto dos alunos de uma escola. Outro exemplo é a relação "menor que" ($<$) no conjunto dos números inteiros. Ainda no conjunto dos inteiros, temos várias relações: maior que, ser igual a, ser divisível por, ser múltiplo de etc.

Mas como definimos uma relação? Veja que há duas coisas importantes em uma relação: um conjunto e uma regra de comparação entre os elementos deste conjunto. **Uma relação sempre envolve pares de elementos do conjunto**.

Relações que comparam pares de elementos de um conjunto são chamadas relações binárias. Nesta disciplina, trataremos apenas de relações binárias.

Se temos uma relação $R$ em um conjunto $A$, é comum escrever $xRy$ quando o elemento $x$ está relacionado ao elemento $y$, sendo $x, y \in A$. Usamos o símbolo $x \not R\, y$ quando $x$ não está relacionado ao elemento $y$.

Por exemplo, na relação "$<$" ("é menor que") no conjunto $\mathbb{Z}$, temos $2 < 3,\ 4 < 10,\ 1 < 100$ etc. Familar, não?

Há uma outra maneira, talvez menos intuitiva, de escrever uma relação: por pares ordenados. Podemos convencionar que o par $(x, y)$ diz que $x$ está relacionado a $y$. Assim, dada uma relação em um conjunto $A$, os "relacionamentos" são pares ordenados $(x, y)$, com $x$ e $y$ pertencentes ao conjunto $A$, isto é, uma relação é definida através de um dado subconjunto do produto cartesiano $A \times A$.

### Relação em um conjunto

A seguir, veremos como podemos definir uma relação.

Definição 1 (Relação em um conjunto)
Uma relação $R$ em um conjunto $A$ é um subconjunto do produto cartesiano de $A$ por si mesmo:

$$R \subset A \times A \, .$$

Exemplo **2**

1. Se $A = \{1, 2, 3\}$, a relação $<$ é dada por

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

   enquanto a relação $\leq$ é dada por

   $$S = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\} \, .$$

   Podemos, também, descrever $R$ como

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

2. No conjunto $B = \{1, 2, 3, 4, 5, 6\}$, a relação "$x$ divide $y$", é dada por

   $$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (6, 6)\} \, .$$

   Podemos, também, descrever o conjunto $R$ como

   $$R = \{(x, y) \in B \times B \mid x \text{ divide } y\} \, .$$

Em resumo, uma relação em um conjunto $A$ é um conjunto de pares ordenados $(x, y)$, onde $x, y \in A$. Dizemos que $x$ e $y$ satisfazem a relação, ou que $x$ está relacionado a $y$, se o par $(x, y)$ está na relação. Assim, uma relação é um subconjunto de $A \times A$. Qualquer subconjunto de $A \times A$ constitui uma relação. Se $R$ é uma relação, escrevemos $xRy$ quando $(x, y) \in R$, isto é,

$$xRy \iff (x, y) \in R \, .$$

É conveniente ampliar a definição que demos de relação, para incluir relações entre dois conjuntos diferentes.

Definição 2 (Relação entre conjuntos)
Sejam $A$ e $B$ conjuntos. Uma relação entre $A$ e $B$ é um subconjunto de $A \times B$.

Observe a distinção: um subconjunto de $A \times A$ é uma relação **em** $A$, enquanto um subconjunto de $A \times B$ é uma relação **entre** $A$ e $B$.

## Propriedades das relações

Vamos usar termos especiais para descrever certas propriedades que uma relação pode ter. Vamos considerar uma relação $R$ em um conjunto $A$.

- Propriedade Reflexiva.

  Dizemos que uma relação $R$ é reflexiva quando, para qualquer $x \in A$, temos $xRx$. Isto é, *todo* elemento do conjunto está relacionado a si mesmo.

- Propriedade Anti-reflexiva.

  Dizemos que uma relação $R$ é anti-reflexiva quando, para qualquer $x \in A$, temos $x \not R x$. Isto é, *nenhum* elemento do conjunto está relacionado a si mesmo.

- Propriedade Simétrica.

  Dizemos que uma relação $R$ é simétrica quando, para quaisquer $x, y \in A$, se $xRy$, então $yRx$. Isto é, se $x$ estiver relacionado a $y$, então $y$ está relacionado a $x$.

- Propriedade Anti-simétrica.

  Dizemos que uma relação $R$ é anti-simétrica quando, para quaisquer $x, y \in A$, se $xRy$ e $yRx$, então $x = y$. Assim, se $x$ e $y$ são elementos distintos de $A$, não pode acontecer de $x$ estar relacionado a $y$ e $y$ estar relacionado a $x$.

- Propriedade Transitiva.

  Dizemos que uma relação $R$ é transitiva quando, para quaisquer $x, y, z \in A$, se $xRy$ e $yRz$, então $xRz$. Isto é, se $x$ estiver relacionado a $y$ e $y$ estiver relacionado a $z$, então $x$ está relacionado a $z$.

Vamos a alguns exemplos para tornar estes conceitos mais claros e para mostrar que muitas relações comuns apresentam várias destas propriedades.

### Exemplo 1

A relação $=$ (igualdade) sobre os inteiros. Ela é reflexiva (todo inteiro é igual a si mesmo), simétrica ($x = y \Rightarrow y = x$) e transitiva ($x = y$ e $y = z \Rightarrow x = z$).

**Exemplo 2**

A relação $\leq$ (menor ou igual a) sobre os inteiros. Ela é reflexiva (todo inteiro é menor ou igual a si mesmo), anti-simétrica ($x \leq y$ e $y \leq x \Rightarrow x = y$) e transitiva ($x \leq y$ e $y \leq z \Rightarrow x \leq z$).

**Exemplo 3**

A relação $<$ (estritamente menor que) sobre os inteiros. Ela é anti-reflexiva (nenhum inteiro é menor que si mesmo), não é simétrica (porque $x < y$ não implica $y < x$). Na verdade, ela é anti-simétrica. Isto pode causar estranheza, mas, veja bem: a condição de anti-simetria é

$$(x < y \text{ e } y < x) \Rightarrow x = y \ .$$

Esta condição é correta por vacuidade: não há inteiros tais que $x < y$ e $y < x$, portanto, a implicação é sempre verdadeira.

A relação $<$ é também transitiva:

$$(x < y \text{ e } y < z) \Rightarrow x < z \ .$$

**Exemplo 4**

Seja $A$ o conjunto das retas no plano e $R$ a relação de perpendicularismo entre retas. Esta relação é anti-reflexiva (nenhuma reta é perpendicular a si mesma), simétrica e não é transitiva.

**Exemplo 5**

Seja $A$ o conjunto das retas no plano e $R$ a relação de paralelismo ou igualdade entre retas, isto é, $xRy$ quando as retas $x$ e $y$ são iguais ou paralelas. Esta relação é, claramente, reflexiva, simétrica e transitiva.

Dois triângulos $\triangle ABC$ e $\triangle DEF$ são ditos congruentes quando existe uma correspondência entre seus vértices, tal que a correspondência entre os lados e ângulos, determinada por esta correspondência entre os vértices, leva lados e ângulos em lados e ângulos congruentes.

**Exemplo 6**

Seja $A$ o conjunto dos **triângulos**. A relação $R$ de congruência de triângulos é reflexiva, simétrica e transitiva.

**Exemplo 7**

Considere a relação $\mid$ (divide) no conjunto dos números inteiros positivos. Esta relação é anti-simétrica, pois, para $x$ e $y$ números positivos, se $x \mid y$ e $y \mid x$ então $x = y$.

Por outro lado, a relação $\mid$ (divide) sobre o conjunto dos números inteiros não é anti-simétrica, pois , por exemplo, $2 \mid -2$ e $-2 \mid 2$, mas $2 \neq -2$. Também não é simétrica, por exemplo, $2 \mid 6$, mas $6 \nmid 2$.

Este exemplo mostra que uma relação pode não ser nem simétrica nem anti-simétrica.

**Exemplo 8**

Seja $R$ a relação de bijeção definida sobre o conjunto de todos os subconjuntos finitos. Se $S_1$ e $S_2$ são dois conjuntos finitos, então $S_1RS_2$ quando há uma relação bijetiva entre $S_1$ e $S_2$, o que é o mesmo que dizer que $S_1$ e $S_2$ têm o mesmo número de elementos.

A relação $S$ é claramente reflexiva, simétrica e transitiva.

O que é o número de elementos de um conjunto finito $S$? Uma maneira de conhecer este número é através de bijeções. Podemos dizer que um conjunto $S$ é finito e tem $n$ elementos quando existe uma bijeção de $S$ com o conjunto $\{1, 2, \ldots, n\}$.

## Relações de equivalência

Em várias áreas da Matemática, encontramos relações que trazem uma certa noção de "quase igualdade" entre objetos distintos. Por exemplo, em Geometria, a congruência de triângulos. Triângulos congruentes não são iguais, mas têm lados e ângulos correspondentes de mesma medida. Assim, "funcionam" como se fossem iguais.

Entre conjuntos finitos, a relação de **bijeção** não é uma igualdade, mas, para muitas aplicações, conjuntos bijetivos "funcionam" como se fossem iguais.

Estas relações, assim como a relação de igualdade em um conjunto numérico, têm a característica de serem reflexivas, simétricas e transitivas. Damos a uma relação com estas propriedades o nome de relação de equivalência.

Definição 3 (Relação de equivalência)
Seja $R$ uma relação em um conjunto $A$. Dizemos que $R$ é uma *relação de equivalência* em A quando ela é reflexiva, simétrica e transitiva.

Os exemplos 1 (relação de igualdade nos inteiros), 6 (congruência de triângulos), 5 (retas iguais ou paralelas) e 8 (relação de ter o mesmo número de elementos sobre o conjunto de todos os subconjuntos finitos) são exemplos de relações de equivalência.

Vamos ver mais um exemplo de relação de equivalência.

**Exemplo 9**

Sejam $A$ e $B$ dois conjuntos não-vazios, e seja $f\colon A \longrightarrow B$ uma dada função. Vamos definir, usando a função $f$, uma relação de equivalência $\sim_f$, no conjunto $A$, que é o domínio de $f$.

Definição:

$$\text{Para } x_1, x_2 \in A,\ x_1 \sim_f x_2 \text{ quando } f(x_1) = f(x_2)\ .$$

Esta relação é de equivalência, pois vale:

1. Reflexividade: $x \sim_f x$, pois $f(x) = f(x)$.
2. Simetria:

$$x_1 \sim_f x_2 \Rightarrow f(x_1) = f(x_2) \Rightarrow f(x_2) = f(x_1) \Rightarrow x_2 \sim_f x_1\ .$$

3. Transitividade:

$$\begin{aligned} x_1 \sim_f x_2 \text{ e } x_2 \sim_f x_3 &\Rightarrow f(x_1) = f(x_2) \text{ e } f(x_2) = f(x_3) \\ &\Rightarrow f(x_1) = f(x_3) \Rightarrow x_1 \sim_f x_3\ . \end{aligned}$$

### Classes de equivalência

Seja $A$ um conjunto não-vazio e seja $\sim$ uma relação de equivalência no conjunto $A$.

Definição 4 (Classe de equivalência)
Se $a \in A$, chamamos de classe de equivalência do elemento $a$, denotado por $\overline{a}$, o subconjunto de todos os elementos de $A$ que são equivalentes ao elemento $a$, isto é

$$\overline{a} = \{x \in A \ / \ x \sim a\}\ .$$

Note que, como $a \sim a$, por reflexividade, então $a \in \overline{a}$. Assim, uma classe de equivalência nunca é vazia.

Por exemplo, na relação de congruência de triângulos, a classe de equivalência de um triangulo $T$ é o conjunto de todos os triângulos que são congruentes a $T$.

Seja $R$ a relação *tem o mesmo número de elementos que*, no conjunto de todos os subconjuntos finitos de $\mathbb{Z}$, por exemplo. Já vimos que $R$ é uma relação de equivalência (veja o exemplo 8). O que são, neste caso, as classes de equivalência?

A classe do conjunto vazio é a classe dos conjuntos que não têm nenhum elemento, portanto, somente ele mesmo.

$$\overline{\emptyset} = \{\emptyset\}$$

Em seguida, temos a classe dos conjuntos que têm 1 elemento. Todos eles estão na mesma classe, e somente eles (os conjuntos de 1 elemento) estão nesta classe.

$$\overline{\{1\}} = \{\ldots, \{-2\}, \{-1\}, \{0\}, \{1\}, \{2\}, \ldots\} .$$

Passamos, então, à classe dos subconjuntos de $\mathbb{Z}$ que têm dois elementos, três elementos etc. Observe que todos os subconjuntos finitos de $\mathbb{Z}$ estão em alguma classe (se um subconjunto tem $n$ elementos, então pertence à classe dos subconjuntos que têm $n$ elementos!). Note, também, que estas classes são disjuntas duas a duas.

A próxima proposição irá mostrar o que dissemos anteriormente para qualquer relação de equivalência $R$ em um conjunto $A$. Mostraremos que as classes de equivalência de $R$ são subconjuntos de $A$, não vazios, disjuntos dois a dois, cuja união é o conjunto $A$.

Proposição 1

Seja $\sim$ uma relação de equivalência em um conjunto não vazio $A$ e sejam $x, y \in A$. Então, as seguintes afirmações são verdadeiras.

1. Dois elementos são equivalentes se, e somente se, estão na mesma classe de equivalência:
$$x \sim y \Longleftrightarrow \overline{x} = \overline{y} .$$

2. Duas classes distintas são disjuntas:
$$\overline{x} \neq \overline{y} \Longleftrightarrow \overline{x} \cap \overline{y} = \emptyset .$$

3. O conjunto $A$ é a união das classes de equivalência da relação:
$$A = \bigcup_{x \in A} \overline{x}$$

*Demonstração.*

Sejam $x, y \in A$.

**1.** Assumimos $x \sim y$. Vamos mostrar que $\overline{x} = \overline{y}$.

Se $a \in \overline{x}$, temos $a \sim x$. Da hipótese $x \sim y$, segue por transitividade que $a \sim y$. Isso nos diz que $a \in \overline{y}$.

Assim, $\overline{x} \subset \overline{y}$. De modo análogo, pode-se mostrar que $\overline{y} \subset \overline{x}$. Dessas duas inclusões, mostramos que $\overline{x} = \overline{y}$.

Assumimos $\overline{x} = \overline{y}$. Vamos mostrar que $x \sim y$.

Pela reflexividade, $x \sim x$, portanto, $x \in \overline{x}$. Como $\overline{x} = \overline{y}$, então $x \in \overline{y}$, e isso nos diz que $x \sim y$.

**2**. Suponha que $\overline{x} \neq \overline{y}$ e suponhamos, por absurdo, que $\overline{x} \cap \overline{y} \neq \emptyset$. Seja $z \in \overline{x} \cap \overline{y}$. Assim, $z \in \overline{x}$ implica $z \sim x$ e $z \in \overline{y}$ implica $z \sim y$. Pela simetria, $z \sim x$ implica $x \sim z$.

Assim, $x \sim z$ e $z \sim y$. Pela transitividade, temos $x \sim y$, e de (1) segue que $\overline{x} = \overline{y}$, contradizendo nossa hipótese.

Daí, segue que $\overline{x} \cap \overline{y} = \emptyset$, quando $\overline{x} \neq \overline{y}$.

**3.** De $\overline{x} \subset A$ para todo $x \in A$, segue que $\bigcup_{x \in A} \overline{x} \subset A$ e do fato de $x \in \overline{x}$ para todo $x \in A$, segue que $A \subset \bigcup_{x \in A} \overline{x}$.

Logo, dessas duas informações concluímos que $A = \bigcup_{x \in A} \overline{x}$. □

## Conjuntos quocientes e partição em um conjunto

Seja $\sim$ uma relação de equivalência em um conjunto não vazio $A$ e, para todo $a \in A$, seja $\overline{a} = \{x \in A \mid x \sim a\}$ a classe de equivalência do elemento $a$.

O conjunto das classes $\{\overline{a} \mid a \in A\}$ denotado por $\mathcal{P} = A/\sim = \overline{A}$ é chamado conjunto quociente de $A$ pela relação de equivalência $\sim$ .

Pela proposição anterior, o conjunto quociente é um conjunto de subconjuntos de $A$, não vazios, dois a dois disjuntos, e cuja união é o próprio conjunto $A$. Esta é exatamente a noção de *partição de um conjunto*.

Você deve ter estudado partições de um conjunto na disciplina Matemática Discreta, no primeiro período do curso (lá, quando você ainda era um calouro!).

Vamos relembrar a definição de **partição de um conjunto**.

Definição 5 (partição de um conjunto $A$)
Seja $A$ um conjunto não vazio e seja $\mathcal{P}$ uma coleção cujos elementos são subconjuntos de $A$.

Dizemos que $\mathcal{P}$ é uma *partição do conjunto* $A$ se as seguintes propriedades são satisfeitas:

1. Os elementos de $\mathcal{P}$ são não vazios.

2. Quaisquer dois elementos distintos $P_1, P_2$ de $\mathcal{P}$ são disjuntos, isto é, $P_1 \neq P_2$ em $\mathcal{P}$ implica $P_1 \cap P_2 = \emptyset$

3. $A = \bigcup\limits_{P\in\mathcal{P}}^{\cdot} P$ ($A$ é união disjunta dos elementos $P \in \mathcal{P}$).

Repare na notação $A = \bigcup\limits_{P\in\mathcal{P}}^{\cdot} P$, usada para indicar união disjunta

Se $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$ for uma partição finita, podemos representar a partição na figura a seguir

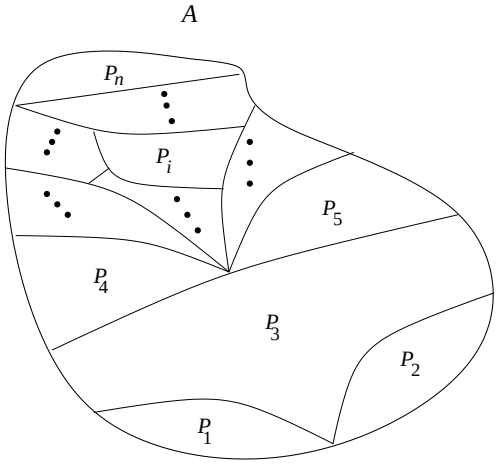



Fig. 2.1: Partição de um conjunto

Pela proposição anterior, se $\sim$ é uma relação de equivalência em um conjunto não vazio $A$, então $\mathcal{P} = \mathcal{A}/\sim = \overline{\mathcal{A}}$ define uma partição no conjunto $A$ ns qual os elementos dessa partição são as classes de equivalência $\overline{a}$, onde $a \in A$.

Um fato muito interessante é que a recíproca também é verdadeira, isto é, dada uma partição $\mathcal{P}$ de um conjunto $A$, fica naturalmente definida uma relação de equivalência $\sim$ em $A$ de modo que $\mathcal{P} = A/\sim = \overline{A}$.

Proposição 2

Seja $A$ um conjunto não vazio e seja $\mathcal{P}$ uma partição do conjunto $A$. Defina a relação $\sim$ sobre $A$ por

$$x \sim y, \quad \text{se existe} \quad P \in \mathcal{P} \quad \text{tal que} \quad x, y \in P$$

1. $\sim$ é relação de equivalência.

2. $A/\sim \; = \mathcal{P}$.

Em outras palavras, a relação de equivalência é definida por: *dois elementos se relacionam quando estão no mesmo conjunto da partição.*

*Demonstração.*

**1.** Vamos mostrar que as propriedades que definem relação de equivalência são satisfeitas.

- Reflexividade.

  $x \sim x$ pois, $x \in A = \bigcup\limits_{P \in \mathcal{P}} P$ então existe $P \in \mathcal{P}$ tal que $x \in P$.

- Simetria.

  Assumimos $x \sim y$. Isso nos diz que existe $P \in \mathcal{P}$ tal que $\{x, y\} \subset P$ e, como $\{y, x\} = \{x, y\}$, segue que $y \sim x$.

- Transitividade.

  Assumimos $x \sim y$ e $y \sim z$ com $x, y, z \in A$.

  Se $x \sim y$, então existe $P_1 \in \mathcal{P}$ tal que $\{x, y\} \subset P_1$.

  Se $y \sim z$, então existe $P_2 \in \mathcal{P}$ tal que $\{y, z\} \subset P_2$.

  Assim, $y \in P_1 \cap P_2 \neq \emptyset$ e como $\mathcal{P}$ é uma partição, isso nos diz que, de fato, $P_1 = P_2$.

  Assim, $\{x, y\}$ e $\{y, z\}$ estão contidas em $P_1 = P_2$.

  Então,

  $$\{x, y, z\} \subset P_1 \Longrightarrow \{x, z\} \subset P_1 \Longrightarrow x \sim z\,.$$

  Isso demonstra que a relação $\sim$ define uma relação de equivalência em $A$.

**2.** Vamos provar que $\overline{A} = A/\sim \; = \mathcal{P}$.

Seja $P \in \mathcal{P}$ e seja $a \in P \subset A$. Vamos mostrar que

$$P = \overline{a} = \{x \in A \mid x \sim a\}\,.$$

Se $x \sim a$, então existe $P' \in \mathcal{P}$ tal que $\{x, a\} \subset P'$.

Como $a \in P \cap P' \neq \emptyset$, temos:

$$P = P' \Longrightarrow \{x, a\} \subset P = P' \Longrightarrow x \in P \Longrightarrow \overline{a} \subseteq P\,.$$

De $a \in P$ segue, pela definição de $\sim$, que $y \sim a$ para todo $y \in P$ e isso nos diz que $P \subseteq \overline{a}$.

De $\overline{a} \subseteq P$ e $P \subseteq \overline{a}$ segue que $P = \overline{a}$.

Tendo em vista que cada $a \in A$ pertence, sempre, a algum $P \in \mathcal{P}$ (pois $\mathcal{P}$ é uma partição de $A$), temos, de fato, que

$$\overline{A} = A/\sim \; = \mathcal{P}\,.$$

□

**Resumo**

As noções de Relação e Relação de Equivalência são noções destacadas na Matemática e, em especial, na Álgebra. É particularmente importante que você, aluno, domine esses conceitos e tenha um entendimento claro das propriedades reflexiva, simétrica e transitiva.

Uma relação de equivalência permite partir um conjunto em uma coleção especial de subconjuntos chamada Partição do Conjunto. O conjuntos das classes de equivalência determina uma partição e, vice-versa, uma partição determina uma relação de equivalência em um conjunto, onde os elementos da partição são, exatamente, as classes de equivalência da relação.

Esse é o recado da Aula 2.

## Atividades Propostas

1. Seja $\mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$ o conjunto dos pontos no plano, representados por pares ordenados de números reais. Seja $\Omega$ o subconjunto de $\mathbb{R}^2$ definido por

$$\Omega = \{(x, y) \in \mathbb{R}^2 \mid xy \geq 0\} .$$

   É fácil ver que $\Omega$ é a união do $1^o$ e $3^o$ quadrantes com os eixos cartesianos (que são as retas $x = 0$ e $y = 0$).

   Definimos uma relação $R$ no conjunto $\mathbb{R}$ dos números reais por

$$\text{para } x, y \in \mathbb{R}, \quad xRy \text{ quando } (x, y) \in \Omega .$$

   Mostre que a relação assim definida é uma relação de equivalência.

2. Discuta a validade das propriedades reflexiva, simétrica e transitiva para as relações em $\mathbb{R}$, definidas de maneira análoga, através dos conjuntos

   (a) $\Omega = \{(x, y) \in \mathbb{R}^2 \mid x \leq 0 \text{ e } y \geq 0\}$

   (b) $\Omega = \{(x, y) \in \mathbb{R}^2 \mid xy \leq 0\}$

   (c) $\Omega = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$

## Auto-avaliação

Você deveria ter sido capaz de resolver todos os exercícios propostos. Se você tiver alguma dificuldade, volte ao texto da aula ou procure o tutor antes de avançar para a próxima aula.

# Aula 3 – Relação de ordem em um conjunto: O princípio da boa ordenação dos inteiros

### Meta

Estudar relação de ordem em um conjunto, as noções de conjunto limitado superiormente e inferiormente e o princípio da boa ordenação.

### Objetivos

Ao final desta aula, você deve ser capaz de:

- Listar as propriedades que definem uma relação de ordem.
- Definir a noção de conjunto ordenado e destacar aspectos específicos nos conjuntos numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$.
- Definir conjunto limitado superiormente e inferiormente.
- Apresentar o princípio da boa ordenação, mostrar sua validade em $\mathbb{Z}$ e mostrar sua não validade em $\mathbb{Q}$ e $\mathbb{R}$.

### Introdução

Na Aula passada, você viu a definição de relação em um conjunto e também viu uma classe de relações especialmente importantes, que são as relações reflexivas, simétricas e transitivas, as chamadas relações de equivalência.

Nesta aula, veremos outra classe de relações muito importantes, que são as relações de ordem. Elas traduzem a noção intuitiva de ordem. Por exempo, o conjunto dos números inteiros é "ordenado", de maneira natural, pela relação "menor ou igual a". Defiremos relação de ordem em um conjunto, listando as propriedades que uma relação deve ter para ser de ordem, e analisaremos essas relações nos conjuntos numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$.

Apresentaremos o Princípio da boa ordenação que tem validade em $\mathbb{Z}$ mas não possui validade em $\mathbb{Q}$ ou $\mathbb{R}$ e, apresentaremos o exemplo da relação de ordem lexicográfica em $\mathbb{C}$.

Através do princípio da boa ordenação em $\mathbb{Z}$, provaremos, na próxima aula, o chamado princípio da Indução, que servirá de base para demonstração de fórmulas envolvendo números inteiros.

Bom, é um bocado de assunto novo nesta aula! Vamos começar pela definição de relação de ordem.

## Relação de ordem em um conjunto: uma breve apresentação

Seja $A$ um conjunto não vazio e seja $\mathcal{R}$ uma relação (binária) entre pares ordenados de elementos de $A$. Se $a, b \in A$ estão relacionados, nessa ordem, escrevemos $a\mathcal{R}b$. Caso contrário, escrevemos $a \not\mathcal{R}b$.

Começaremos definindo uma *ordem parcial*. Esta é uma relação reflexiva, anti-simétrica e transitiva.

Definição 1 (Ordem parcial de um conjunto $A$)
Dizemos que $\mathcal{R}$ é uma relação de ordem parcial em $A$ se, para todo $a, b, c \in A$, são válidas as seguintes propriedades:

(1) $a\mathcal{R}a$ (Reflexiva)

(2) $a\mathcal{R}b$, $b\mathcal{R}a \Longrightarrow a = b$ (Anti-simétrica)

(3) $a\mathcal{R}b$, $b\mathcal{R}c \Longrightarrow a\mathcal{R}c$ (Transitiva)

Exemplo **3**
A relação $\leq$ no conjunto $\mathbb{Z}$ é uma relação de ordem parcial, pois é claramente reflexiva ($x \leq x$), anti-simétrica ($x \leq y$ e $y \leq x$ implica $x = y$) e transitiva ( $x \leq y$ e $y \leq z$ implica $x \leq z$).
Na verdade, a relação $\leq$ nos inteiros é um exemplo que vem sempre à mente quando falamos de ordem. É comum, também, usar-se a notação $\leq$ para qualquer relação de ordem parcial em qualquer conjunto.

Assim, dizemos que $\leq$ é uma ordem parcial em $A$ se, para todo $a, b, c \in A$, vale que:

1. $a \leq a$;
2. $a \leq b, b \leq a \Longrightarrow a = b$;
3. $a \leq b, b \leq c \Longrightarrow a \leq c$.

Agora, devemos distinguir um tipo especial de relação de ordem. Note que, se $\leq$ é uma relação de ordem em um conjunto $A$, pode acontecer de dois

elementos em $A$ não estarem relacionados, isto é, pode acontecer de existirem elementos $a, b \in A$ tais que não vale $a \leq b$ nem $b \leq a$.

Se dois elementos em $A$ estão sempre relacionados, então dizemos que a relação é *total* (ou *linear*).

**Definição 2 (Relação total ou linear)**
Se uma relação de ordem $\leq$ em um conjunto $A$ satisfizer a propriedade

4. Para todo $a, b \in A$ tem-se $a \leq b$ ou $b \leq a$

então dizemos que a ordem $\leq$ em $A$ é *total* ou *linear*.

Vamos agora dar um exemplo de ordem parcial que não é total.

**Exemplo 4**
Seja $X$ um conjunto e seja $A = \mathcal{P}(X)$ o conjunto das partes de $X$. Isto é,

$$A = \mathcal{P}(X) = \{Y \mid Y \subset X\} .$$

Para relembrar, vamos ver alguns exemplos de conjunto das partes de um conjunto:

- Se $X = \emptyset$, tem-se $\mathcal{P}(X) = \{\emptyset\}$ $(\neq \emptyset)$ possui um elemento (que é o conjunto vazio).
- Se $X = \{1\}, \mathcal{P}(X) = \{\emptyset, \{1\}\}$ possui exatamente dois elementos.
- Se $X = \{1, 2\}, \mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ possui exatamente quatro elementos.
- Se $X = \{1, 2, \cdots, n\}$ mostraremos mais tarde que $\mathcal{P}(X)$ possui exatamente $2^n$ elementos.

Claramente, a relação de inclusão em $\mathcal{P}(X)$ é uma relação de ordem, pois é:

1. Reflexiva: todo subconjunto de $X$ está contido em si mesmo.
2. Anti-simétrica: se $X_1$ e $X_2$ são subconjuntos de $X$ e vale que $X_1 \subset X_2$ e $X_2 \subset X_1$, então $X_1 = X_2$.
3. Transitiva: se $X_1 \subset X_2$ e $X_2 \subset X_3$ então $X_1 \subset X_3$, para $X_1, X_2$ e $X_3$ subconjuntos de $X$.

Esta relação de ordem parcial não é, em geral, uma relação de ordem total. Por exemplo, se $X = \{1, 2\}$ então

$$A = P(X) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} .$$

Os conjuntos $X_1 = \{1\}$ e $X_2 = \{2\} \in A$ não estão relacionados por inclusão: $X_1 \not\subset X_2$ e $X_2 \not\subset X_1$.

Se $A$ é um conjunto e $R$ é uma relação de ordem parcial em $A$, dizemos que o conjunto $A$ é *ordenado* pela relação $R$. No exemplo anterior, dizemos que o conjunto das partes de um conjunto $X$ é ordenado por inclusão.

Se a relação em $R$ em $A$ é total, então dizemos que $A$ é linearmente ordenado por $R$.

**Relação de ordem no conjunto dos números reais**

Nesta seção, definiremos a relação de ordem natural nos conjuntos numéricos $\mathbb{Z}, \mathbb{Q}$ e $\mathbb{R}$. Mostraremos que, com esta relacão, estes conjuntos são linearmente ordenados.

Na construção dos números reais, definimos uma ordem total (linear) $\leq$ em $\mathbb{R}$. Para isto, admitimos a existência de um conjunto especial $P \subset \mathbb{R}$ satisfazendo as seguintes propriedades:

1. $P$ é um subconjunto próprio, não vazio, e $0 \notin P$.
2. Para todo $x, y \in P$, tem-se $x + y \in P$ e $xy \in P$
3. Para todo $x \in \mathbb{R}$ ou $x = 0$, ou $x \in P$, ou $-x \in P$ (lei da tricotomia)

$P$ é conhecido como o subconjunto dos números reais positivos.

Definimos a relação $\leq$ de ordem em $\mathbb{R}$ por:

$$x, y \in P, x \leq y \Longleftrightarrow x = y \text{ ou } (y - x) \in P\,.$$

Em outra palavras, $x \leq y$ quando $x = y$ ou $y - x$ é positivo.

Tendo em vista propriedades algébricas básicas de reais, por exemplo:

$$(-x)^2 = (-x)(-x) = x^2,\ \forall x \in \mathbb{R}$$

e

$$1^2 = 1\,.$$

Podemos provar várias propriedades da ordem em $\mathbb{R}$.

Vamos provar que $x^2 > 0,\ \forall x \in \mathbb{R},\ x \neq 0\,.$

De fato, se $x \in \mathbb{R}$ e $x \neq 0$, temos, pela propriedade (2), que, se $x \in P$, então $x^2 = x \cdot x \in P$.

Se $x \notin P$, pela propriedade (3), temos $(-x) \in P$, logo, pela proposição 2, $(-x)(-x) = x^2 \in P\,.$

Assim, se $x \in \mathbb{R}, x \neq 0, x^2 \in P$, isto é,

$$x^2 > 0,\ \forall x \in \mathbb{R},\ x \neq 0\,.$$

Em particular,

$$1 = (1)^2 > 0\,.$$

Partindo de $1 > 0$, usando a propriedade (2), podemos provar que todo natural é positvo:

$$\begin{aligned} 1 &> 0 \\ 1+1 &= 2 \in P, \quad 2 > 0 \\ 3 &= 2+1 > 0 \\ &\vdots \\ n &= (n-1)+1 > 0 \\ &\vdots \end{aligned}$$

e isto nos mostra que

$$\{1, 2, 3, \cdots, n, \cdots\} \subset P\,.$$

Se denotarmos $\mathbb{R}^+ = \mathbb{P} = \{x \in \mathbb{R} \mid x > 0\}$, o conjunto dos números reais positivos, e $\mathbb{Z}^+ = \{x \in \mathbb{Z} \mid x > 0\}$, o conjunto dos números inteiros positivos, então vale que

$$\mathbb{Z}^+ = \mathbb{Z} \cap \mathbb{P} = \{1, 2, 3, \cdots, n, \cdots\}\,.$$

**A ordem lexicográfica em $\mathbb{C}$**

Sabemos que

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}\,,$$

onde

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\} \quad \text{e} \quad i = \sqrt{-1}\,.$$

No item anterior definimos uma relação de ordem $\leq$ em $\mathbb{R}$ através de um subconjunto $\mathbb{P} \subset \mathbb{R}$, dos números reais positivos, satisfazendo as propriedades (1), (2) e (3).

Vimos também que, a partir da ordenação do números reais $\mathbb{R}, \leq$, temos que os conjuntos

$$\mathbb{Z}^+ = \mathbb{Z} \cap \mathbb{P} \qquad \mathbb{Q}^+ = \mathbb{Q} \cap \mathbb{P}$$

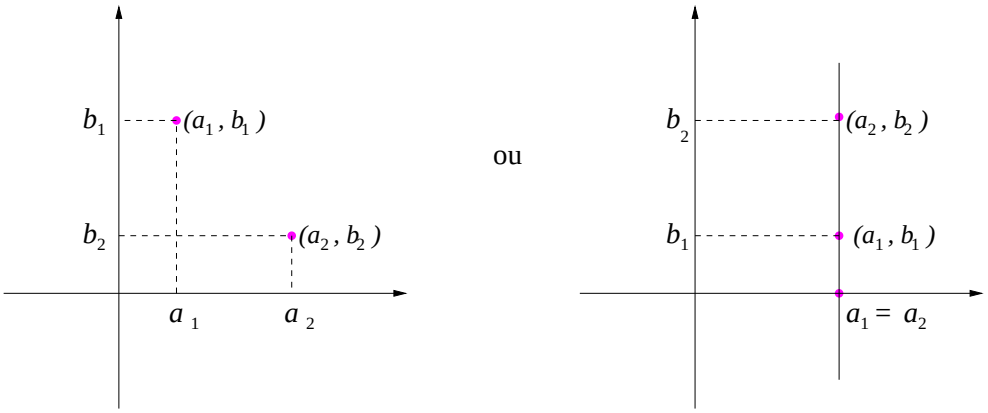
que são, respectivamente, os subconjuntos dos inteiros e racionais positivos, também são ordenados pela ordem $\leq$ (restrição da ordem $\leq$ nos complexos).

Apresentaremos agora uma forma de definir uma ordenação em $\mathbb{C}$, através da ordem lexicográfica.

Definição 3 (Ordem lexicográfica $\leq_L$ em $\mathbb{C}$ )
Seja $\leq$ a ordem definida em $\mathbb{R}$ e sejam $z_1, z_2 \in \mathbb{C}$. Definimos $\leq_L$ do seguinte modo:

$$z_1 = a_1 + b_1 i \leq_L z_2 = a_2 + b_2 i \iff a_1 \leq a_2 \text{ ou } (a_1 = a_2 \text{ e } b_1 \leq b_2)\,.$$

No plano complexo temos:




$$(a, b) \leftrightarrow a + bi$$

Observe que, se $a_1, a_2 \in \mathbb{R}$, então

$$a_1 = a_1 + 0i \leq_L a_2 = a_2 + 0i \Leftrightarrow a_1 \leq a_2 \quad \text{em } \mathbb{R}\,,$$

Portanto, a ordem $\leq_L$, quando restrita aos reais, coincide com a ordem $\leq$ dos reais. Por isso, dizemos que a ordem $\leq_L$ nos complexos *estende* a ordem $\leq$ nos reais.

**Atividades**

1. Verifique que
   - $1 + i \leq_L 2$
   - $i \leq_L 1 + i$
   - $1 + i \leq_L 2 + i$
   - $1 + i \leq_L 1 + 2i$
   - $2 \leq_L 3$
   - $i \leq_L 1$
2. Mostre que $\leq_L$ define uma relação de ordem linear linear em $\mathbb{C}$.
3. Temos que $i = 0 + 1 \cdot i > 0$ na relação $\leq_L$ lexicográfica de $\mathbb{C}$. Mas,

$$i^2 = i \cdot i = -1 = -1 + 0i < 0 + 0i = 0\,.$$

### Estensão da ordem nos reais para os complexos

Vamos desenvolver um pouco mais esta idéia da estensão da ordem nos reais para os complexos.

Vimos que a ordem $\leq_L$ nos complexos estende a ordem $\leq$ nos reais. Isto é muito bom. Veremos, porem, que não é possível definir uma ordem em $\mathbb{C}$ através de um subconjunto $\bar{\mathbb{P}} \subset \mathbb{C}$, satisfazendo as condições (1), (2) e (3), do item anterior, tal que $\mathbb{R}^+ = \bar{\mathbb{P}} \cap \mathbb{R}$, como fizemos para $\mathbb{R}$.

Em outras palavras, não é possível estender a ordem $\leq$ dos reais para os complexos definindo esta ordem estendida através de um conjunto $\bar{\mathbb{P}} \subset \mathbb{C}$ dos "complexos positivos", como fizemos nos reais.

Isto pode parecer um pouco complicado, mas não é. Para ver que não podemos definir uma ordem em $\mathbb{C}$, através de um subconjunto $\bar{\mathbb{P}} \subset \mathbb{C}$, satisfazendo as condições (1), (2) e (3), como fizemos para $\mathbb{R}$, tal que $\mathbb{R}^+ = \bar{\mathbb{P}} \cap \mathbb{R}$, basta observar teríamos:

$$x \neq 0 \Rightarrow x^2 \in \bar{\mathbb{P}} \, .$$

Agora, tomando $x = i = \sqrt{-1}$, vemos que $x \neq 0$ e $x^2 = -1 \in \bar{\mathbb{P}}$.

Assim, $-1 = x^2 \in \bar{\mathbb{P}} \cap \mathbb{R} = \mathbb{R}^2$, o que é um absurdo, já que $-1$ não é um real positivo.

### Subconjuntos limitados inferiormente e superiormente

Seja $A, \leq$ um conjunto parcialmente ordenado e seja $S \subset A$ um subconjunto não vazio de $A$.

Dizemos que $S$ é um conjunto *limitado inferiormente* em $A$ se existe $a \in A$ tal que $a \leq x$ para todo $x \in S$

Analogamente, dizemos que $S$ é um conjunto *limitado superiormente* em $A$ se existe $b \in A$ tal que $x \leq b$ para todo $x \in S$

Dizemos que $S$ possui um *máximo* se existe $s \in S$ tal que $s \geq x$ para todo $x \in S$. Analogamente, $S$ possui um *mínimo* se existe $s \in S$ tal que $s \leq x$ para todo $x \in S$.

Se um conjunto tem um máximo, então ele é limitado superiormente e se possui um mínimo, é limitado inferiormente. No entanto, um conjunto pode ser limitado superiormente e não ter um máximo, como pode ser limitado inferiormente e não ter um mínimo. Nesta situação, os limites inferiores e superiores do conjunto $S$ não pertencem à $S$.

Vejamos alguns exemplos.

Exemplo 5

1. O intervalo $(2,3) \subset \mathbb{R}$ é limitado inferiormente e superiormente, mas não possui máximo ou mínimo. Observe que 2 e 3 não são elementos do conjunto $(2,3)$, por isso não são mínimo e máximo, respectivamente.

2. O intervalo $[2,3)$ é limitado inferiormente e superiormente e possui mínimo 2, mas não possui máximo.

3. O conjunto $\{x \in \mathbb{R} \mid x > 0\}$ é limitado inferiormente, não é limitado superiormente e não possui máximo nem mínimo.

4. O conjunto $\mathcal{P}(X)$, das partes de um conjunto não vazio $X$, ordenado por inclusão, possui mínimo $\varnothing \in \mathcal{P}(X)$ e máximo $X \in \mathcal{P}(X)$.

A próxima proposição mostra que um conjunto não pode ter mais de um máximo.

Proposição 1
O máximo de um subconjunto não vazio $S \subset A$, se existir, é único.

*Demonstração.*

Se $S$ não possui um máximo, nada há para demonstrar. Se $S$ possui dois máximos $s_1$ e $s_2$, então $s_1$ e $s_2$ pertencem ao conjunto $S$ e

$$s_1 \leq x, \ \ \forall x \in S \Longrightarrow s_1 \leq s_2 \tag{1}$$
$$s_2 \leq x, \ \ \forall x \in S \Longrightarrow s_2 \leq s_1 \tag{2}$$

De (1) e (2) temos $s_1 = s_2$.

■

Analogamente, podemos provar que um conjunto não pode possuir mais de um mínimo.

## Princípio da Boa Ordenação

Seja $A, \leq$ um conjunto totalmente ordenado. Dizemos que $A, \leq$ satisfaz ao *princípio da boa ordenação* se todo subconjunto não vazio $S \subset A$ de $A$ limitado inferiormente possui um mínimo.

Por exemplo, o conjunto do números reais, com a ordenação usual, não satisfaz o princípio da boa ordenação. Por exemplo, o subconjunto $\mathbb{R}^+$ é limitado inferiormente mas não possui mínimo.

O princípio da boa ordenação também não vale para os racionais. Por exemplo, o conjunto

$$\{x \in \mathbb{Q} \mid x^2 \geq 2 \text{ e } x > 0\}$$

é limitado inferiormente, mas não tem um mínimo. O mínimo seria o número $\sqrt{2} \notin \mathbb{Q}$.

O princípio da boa ordenação não vale para os reais nem para os racionais, mas vale para os inteiros, é o que veremos na próxima seção.

Seja $\mathbb{Z} = \{\cdots, -m, \cdots, -1, 0, 1, 2, \cdots, n, \cdots\}$ o conjunto dos inteiros com sua ordem (natural) linear $\leq$ dada por

$$\underbrace{\cdots < -m-1 < -m < -m+1 < \cdots < -2 < -1}_{\mathbb{Z}_- \text{ (inteiros negativos)}} < 0 < \underbrace{1 < 2 < \cdots < n < \cdots}_{\mathbb{Z}_+ \text{ (inteiros positivos)}}$$

então

$$\mathbb{Z} = \mathbb{Z}_- \cup \{0\} \cup \mathbb{Z}_+ .$$

Vamos assumir em $\mathbb{Z}, \leq$ que o seguinte princípio é verdadeiro.

**Princípio da boa ordenação**

Em $\mathbb{Z}, \leq$ todo subconjunto não vazio limitado inferiormente possui um mínimo, também chamado de $1^0$ elemento desse conjunto.

O que significa dizer que adotaremos a propriedade da boa ordenação de $\mathbb{Z}$ como um Princípio?

Na verdade, a boa ordenação é fundamental para a demonstração de várias propriedades muito importantes dos números inteiros. A propriedade dos inteiros que permite demonstrações por indução, por exemplo, se fundamenta no Princípio da boa ordenação. Esta, por sua vez, é utilizada na demonstração do Teorema da Divisão de Euclides e várias propriedades e fórmulas envolvendo inteiros.

Estamos chamando de princípio a propriedade da boa ordenação porque ela será adotada sem demonstração. Na verdade, ela pode ser enunciada como proposição e demonstrada a partir de uma construção dos números inteiros, o que está fora do escopo deste texto.

### Ínfimo e Supremo

De fato, sendo $\mathbb{Z} = \{\cdots, -m, -2, -1, 0, 1, 2, \cdots, n, \cdots\}$ observamos que não existe número inteiro entre dois inteiros consecutivos, isto é,

$$(r, r+1) \cap \mathbb{Z} = \emptyset, \forall r \in \mathbb{Z}\ .$$

A ausência dessa característica dos inteiros ($\mathbb{Z}$ é um conjunto discreto) é que permite a existência em $\mathbb{Q}$ e $\mathbb{R}$ de situações onde não é válido o Princípio da Boa Ordenação.

Em $\mathbb{Q}$, o conjunto

$$S = \{x \in \mathbb{Q}\ /\ x > 0 \text{ e } x^2 > 2\} = (\sqrt{2}, \infty) \cap \mathbb{Q}$$

é limitado inferiormente em $\mathbb{Q}$, mas não possui mínimo em $\mathbb{Q}$.

Em $\mathbb{R}$, o conjunto

$$T = \{x \in \mathbb{R} \mid x^2 < 4 \text{ e } x > 0\} = (-2, 2)$$

é limitado inferiormente em $\mathbb{R}$, mas não possui mínimo em $\mathbb{R}$.

Observe que o intervalo real $(-2, 2)$ não possui mínimo porque $-2 \notin (-2, 2)$, mas $-2$ é o maior dos limites inferiores de $(-2, 2)$. Isto serve como motivação para definirmos ínfimo e supremo de um conjunto.

Definição 4 (Ínfimo e Supremo)
Seja $A, \leq$ um conjunto totalmente ordenado e $S \subset A$ um subconjunto não vazio de $A$, limitado inferiormente em $A$.

Se existir em $A$ um elemento que é o maior dos limites inferiores de $S$, chamamos este elemento de *ínfimo* do conjunto $S$ em $A$.

Analogamente, se $S$ é limitado superiormente em $A$ e existe em $A$ um menor limite superior, então este elemento é chamado *supremo* de $S$ em $A$.

Exemplo **6**

1. O conjunto

$$T = \{x \in \mathbb{R} \mid x^2 < 4 \text{ e } x > 0\} = (-2, 2)$$

tem ínfimo $-2$ e supremo 2.

2. O conjunto

$$S = \{x \in \mathbb{R} \ / \ x > 0 \text{ e } x^2 > 2\} = (\sqrt{2}, \infty)$$

tem ínfimo $\sqrt{2}$ e não é limitado superiormente,

O conjunto dos números reais $\mathbb{R}$ satisfaz uma propriedade muito importante, que enunciamos a seguir:

Todo subconjunto $T \subset \mathbb{R}$, não vazio, limitado inferiormente, possui um ínfimo em $\mathbb{R}$ e todo subconjunto não vazio $T$, limitado superiormente, possui um supremo em $\mathbb{R}$.

Esta propriedade é chamada propriedade da completude dos números reais. O conjunto $\mathbb{Q}$, dos números racionais, não possui esta mesma propriedade. Veja o exemplo a seguir.

Exemplo **7**

O conjunto

$$S = \{x \in \mathbb{Q} \mid x > 0 \text{ e } x^2 > 2\} = (\sqrt{2}, \infty) \cap \mathbb{Q}$$

é limitado inferiormente, mas $S$ não possui ínfimo em $\mathbb{Q}$. O ínfimo do intervalo real $(\sqrt{2}, \infty)$ é $\sqrt{2}$, mas $\sqrt{2} \notin \mathbb{Q}$.

## Resumo

Nesta aula estudamos uma classe especial de relações chamadas relações de ordem, que têm como exemplo fundamental a relação $\leq$ no conjunto dos números inteiros. Tanto é assim, que usamos a notação $\leq$ para relações de ordem em geral.

Neste ponto, observamos algumas diferenças importantes entre os conjunto dos inteiros e o dos reais, em relação a sua ordenação total por $\leq$.

O conjunto do números inteiros possui uma propriedade fundamental chamada princípio da boa ordenação, pela qual todo conjunto limitado inferiormente possui um mínimo.

Para o conjunto dos números racionais e reais não vale o princípio da boa ordenação, mas, para o conjunto $\mathbb{R}$, do número reais, vale um princípio muito importante de completude, pelo qual todo conjunto limitado inferiormente possui um ínfimo. Por isto, dizemos que o conjunto dos números reais $\mathbb{R}$ é um conjunto linearmente ordenado completo.

# Aula 4 – A demonstração por Indução e o Teorema da Divisão de Euclides

**Metas**

- Demonstrar, a partir da boa ordenação dos inteiros, o Princípio da Indução em suas duas formas.
- Dar exemplos da aplicação da Indução na demonstração de fórmulas envolvendo inteiros.
- Apresentar o Teorema da Divisão de Euclides como uma importante aplicação da Indução nos inteiros.

**Objetivos**

Ao final desta aula, você deve ser capaz de:

- Listar as nove propriedades básicas satisfeitas pelas operações de soma e produto no conjunto $\mathbb{Z}$ dos números inteiros.
- Utilizar uma das duas formas apresentadas do princípio da indução na demonstração de afirmações envolvendo números inteiros.

## Introdução

Nesta aula iniciamos uma caminhada que nos levará a uma visão algébrica dos números inteiros a partir das suas operações de soma e produto, com suas nove propriedades básicas essenciais.

O Teorema da Divisão de Euclides permite calcular o quociente e o resto de uma divisão de um número inteiro por um número inteiro não nulo ( o divisor). Este Teorema desempenha um papel fundamental para o entendimento algébrico dos inteiros e sua demonstração é feita usando o argumento de indução que envolve a relação de ordem (linear) natural de $\mathbb{Z}$.

Vimos, na aula passada, que $\mathbb{Z}$ possui a propriedade da boa ordenação.

Admitiremos que o aluno já esteja familiarizado com o conjunto dos números inteiros $\mathbb{Z}$, suas operações de soma e produto e com a relação de ordem linear $\leq$ em $\mathbb{Z}$. De fato, denotaremos por $\mathbb{Z}$ ao sistema $\mathbb{Z}, +, \cdot, \leq$, dos inteiros com as operações $+$ e $\cdot$ e a relação $\leq$.

## As nove propriedades básicas de soma e produto em $\mathbb{Z}$

### Soma

(1) A soma é uma operação associativa, isto é, para todo $a, b, c \in \mathbb{Z}$ tem-se

$$(a + b) + c = a + (b + c)\,;$$

(2) Existe um elemento neutro para a soma, denotado por 0. Isto é, para todo $a \in \mathbb{Z}$ tem-se

$$a + 0 = 0 + a = a\,;$$

(3) Todo número inteiro $a \in \mathbb{Z}$, possui um inverso aditivo, isto é, existe $x \in \mathbb{Z}$ tal que

$$x + a = a + x = 0\,;$$

O inverso aditivo de $a \in \mathbb{Z}$ é denotado por $-a$.

(4) A soma é uma operação comutativa, isto é, para todo $a, b \in \mathbb{Z}$ tem-se

$$a + b = b + a\,.$$

### Produto

(5) O produto é uma operação associativa, isto é, para todo $a, b, c \in \mathbb{Z}$ tem-se

$$(ab)c = a(bc)\,;$$

(6) Existe um elemento neutro para o produto denotado por 1. Isto é, para todo $a \in \mathbb{Z}$ tem-se

$$a \cdot 1 = 1 \cdot a = a\,;$$

(7) O produto é uma operação comutativa, isto é, para todo $a, b \in \mathbb{Z}$ tem-se

$$ab = ba\,;$$

(8) Os números inteiros não possuem divisores de zero, isto é, para todo $a, b \in \mathbb{Z}$ tem-se

$$ab = 0 \Longrightarrow a = 0 \quad \text{ou} \quad b = 0\,.$$

**Relação entre as operações**

(9) Vale a propriedade distributiva do produto em relação a soma, isto é, para todo $a, b, c \in \mathbb{Z}$ tem-se

$$a(b+c) = ab + ac\,.$$

Observe que, usando a propriedade comutativa (7) acima, vale também que, para todo $a, b, c \in \mathbb{Z}$ tem-se

$$(b+c)a = ba + ca\,.$$

Devido a propriedade (9), dizemos que valem as leis distributivas em $\mathbb{Z}, +, \cdot$ .

Assim, denotamos por $\mathbb{Z}$ o sistema $(\mathbb{Z}, +, \cdot, \leq)$, de tal modo que:

- $(\mathbb{Z}, +, \cdot)$ satifaz as nove propriedades acima enunciadas;
- $(\mathbb{Z}, \leq)$ satisfaz o princípio da boa ordenação.

Mais tarde vamos apresentar outros sistemas $(S, +, \cdot)$, satisfazendo as mesmas nove propriedades básicas satisfeitas pelo sistema $(\mathbb{Z}, +, \cdot)$ dos inteiros. Esses sistemas serão chamados de *Domínios de Integridade*. Em outras palavras, um Domínio de Integridade $(S, +, \cdot)$ é um conjunto $S$, munido de duas operações $+, \cdot$, tal que valem as propriedades (1) a (9) enunciadas acima para os inteiros.

Estes sistemas formados por um conjunto e uma ou mais operações neste conjunto que satizfazem certas propriedades são chamados *Estruturas Algébricas*. Uma boa parte das disciplinas de Álgebra 1 e Álgebra 2 é dedicada ao estudo das estruturas algébricas de anel, domínio de integridades, corpos e grupos.

Mas cada coisa a seu tempo! Vamos voltar aos inteiros resolvendo alguns exercícios.

**Atividades 1**

1. Mostre que os elementos neutros 0 e 1 são únicos.
2. Prove que o inverso aditivo de cada elemento $a \in \mathbb{Z}$ é único. Denotaremos esse inverso por $-a$.

## Duas formas de indução nos inteiros

Antes de começarmos, recordaremos o princípio da boa ordenação nos inteiros:

> *"Todo subconjunto não vazio $S$ de $\mathbb{Z}$ limitado inferiormente possui um mínimo"*

Em particular, todo subconjunto não vazio S de $\mathbb{Z}$ formado por elementos não-negativos (isto é, todo elemento é $\geq 0$), possui um mínimo, uma vez que este conjunto é limitado inferiormente pelo 0.

Usando a boa ordenação de $\mathbb{Z}$ vamos provar a chamada propriedade da indução em $\mathbb{Z}$ em duas formas.

### Indução: primeira forma

Teorema 1 (Indução - $1^a$ forma)
Vamos supor que para cada inteiro $n \geq 1$, seja dada uma afirmação $A(n)$, que depende de $n$. Suponha que valha:

(1) A afirmação $A(1)$ é verdadeira.

(2) Para todo $n \in \mathbb{Z}$ com $n \geq 1$, se $A(n)$ é verdadeira então $A(n+1)$ também é verdadeira.

Então, $A(n)$ é verdadeira para todo $n \in \mathbb{Z}$ com $n \geq 1$.

*Demonstração:*

Seja $S$ o subconjunto de todos os inteiros $n > 0$ tais que a afirmação $A(n)$ seja falsa. Assim,

$$S = \{n \in \mathbb{Z} \mid n > 0 \text{ e } A(n) \text{ é falsa}\}.$$

Observe que $A(n)$ é verdadeira para todo $n \in \mathbb{Z}$ com $n \geq 1$ se, e somente se, $S = \emptyset$.

Assim, provar o Teorema 1 é equivalente a provarmos que $S = \emptyset$. Argumentaremos por redução ao absurdo.

Vamos supor que o Teorema 1 seja falso. Então, existe um inteiro positivo $n > 0$ tal que $A(n)$ é falsa, e assim, $n \in S$ e $S \neq \emptyset$.

Mas os elementos $s \in S$ são todos maiores que zero ($> 0$) e portanto, $S$ é um subconjunto não vazio de $\mathbb{Z}$ limitado inferiormente. Pelo princípio da boa ordenação de $\mathbb{Z}$, temos que $S$ possui um primeiro elemento $n_0 \in S$.

Assim, $n_0 \leq s$, para todo $s \in S$ e $n_0 \in S$, isto é, $A(n_0)$ é falsa.

Mas pela hipótese (1) do nosso Teorema, $A(1)$ é verdadeira. Logo $1 \notin S$ e segue-se que $n_0 \geq 2$. Seja $k = n_0 - 1$. Temos $k \geq 1$ de $k \notin S$, já que $k < n_0$ e $n_0$ é mínimo de $S$.

Portanto $k \geq 1$ e $A(k)$ verdadeira. Mas, pela hipótese (2) do Teorema, segue-se que $A(k+1)$ é verdadeira. Como $k+1 = (n_0 - 1) + 1 = n + 0$, então $A(n_0)$ é verdadeira, isto é $n_0 \notin S$.

Mas $n_0 \in S$ (lembre-se que $n_0$ é o mínimo de $S$). Daí segue que nossa hipótese de admitir $S \neq \emptyset$ nos leva a contradição $n_0 \in S$ e $n_0 \notin S$, o que é um absurdo!

Portanto, $S = \emptyset$ e $A(n)$ é verdadeira para todo $n \in \mathbb{Z}$ com $n \geq 1$ como queríamos demonstrar.

□

**Observação**

Poderíamos começar em $A(0)$ em vez de $A(1)$ verdadeira, no Teorema 1, assumindo $A(0)$ verdadeira.

Exemplo 8

Prove que a seguinte afirmação $A(n)$ é verdadeira para todo $n \in \mathbb{Z}$ com $n \geq 1$:

A(n): A soma dos primeiros $n$ números inteiros positivos é dada pela fórmula

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

*Solução:*

Vamos usar o Teorema 1.

(1) A fórmula é verdadeira para $n = 1$.

De fato,

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

(2) Para atender à condição 2 do Teorema, devemos provar que se $A(n)$ é verdadeiro para algum $n \geq 1$, então $A(n+1)$ tambem é verdadeiro. Vamos provar isto.

Considere a fórmula $A(n)$ verdadeira, isto é,

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

Vamos provar que a fórmula $A(n+1)$ também é verdadeira.

De fato,

$$1+2+\cdots+(n+1)=(1+2+\cdots+n)+(n+1)\,.$$

Como estamos considerando $A(n)$ verdadeira, segue que:

$$\underbrace{(1+2+\cdots+n)}_{=A(n)}+(n+1)=\frac{n(n+1)}{2}+(n+1)=(n+1)\left[\frac{n}{2}+1\right]=\frac{(n+1)(n+2)}{2}$$

o que nos diz que $A(n+1)$ também é verdadeira.

Assim, a fórmula

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

é verdadeira para todo $n\in\mathbb{Z}$ com $n\geq 1$.

Exemplo **9**

Prove que seguinte afirmação é verdadeira para todo $n\in\mathbb{Z}$ com $n\geq 1$:

A(n): a soma dos números ímpares consecutivos de 1 até $2n-1$ é igual ao quadrado do número $n$, isto é,

$$1+3+5+\cdots+(2n-1)=n^2\,.$$

*Solução:*

(1) A fórmula é verdadeira para $n=1$, pois $1=1^2$.

(2) Suponha que $A(n)$ é verdadeira. Provaremos que $A(n+1)$ também é verdadeira.

De fato,

$$\begin{aligned}1+3+5+\cdots+(2(n+1)-1) &= 1+3+5+\cdots+(2n+2-1)=\\ &= 1+3+5+\cdots+2n+1=\\ &= [1+3+5+\cdots+(2n-1)]+(2n+1)\,.\end{aligned}$$

Como $A(n)$ é verdadeira, temos:

$$\underbrace{1+3+5+\cdots+(2n-1)}_{=A(n)}+(2n+1)=n^2+(2n+1)=n^2+2n+1=(n+1)^2$$

como queríamos mostrar.

**Atividades 2**

3. Prove, por indução, que as seguintes fórmulas são verdadeiras para todo $n \in \mathbb{Z}$ com $n \geq 1$:

   (a) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$

   (b) $1^3 + 2^3 + 3^3 + \cdots + n^3 = \left(\dfrac{n(n+1)}{2}\right)^2$

4. Mostre, por indução sobre $n \geq 1$ que:
   (a) Todo número inteiro da forma $n^3 + 2n$ com $n \geq 1$ é divisível por 3.
   (b) Todo número inteiro da forma $n^3 - n$ com $n \geq 1$ é divisível por 24.
   (c) Seja $\Omega = \{1, 2, \cdots, n\}$ com $n \geq 1$ e seja $P(\Omega) = \{B \,/\, B \subset \Omega\}$ o conjunto das partes de $\Omega$ (isto é, o conjunto de todos os subconjuntos de $\Omega$). Mostre, por indução, que o número de elementos $|P(\Omega)|$, do conjunto $P(\Omega)$ é igual a $2^n$.

Exemplo **10**

Vamos mostrar, através deste exemplo, que a hipótese de que $A(1)$ é verdadeiro é realmente necessária no Teorema 1.

Vimos no exemplo 8 que a fórmula $A(n) = 1+2+\cdots+n = \frac{n(n+1)}{2}$ é verdadeira para todo $n \in \mathbb{Z}$ com $n \geq 1$.

Agora considere a fórmula $\beta(n)$:

$$\beta(n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2} + 1\,.$$

Como $A(n)$ é verdadeira para todo $n \geq 1$ temos que $\beta(n)$ é falsa para todo $n \geq 1$.

Embora $\beta(1)$ seja falsa (e portanto não podemos aplicar o Teorema 1), a condição (2) do teorema é válida. É fácil ver (verifique!) que: se $\beta(n)$ fosse verdadeira então $\beta(n+1)$ também seria verdadeira.

Portanto, a afirmação $\beta(n)$, que é falsa, atende a condição (2) do teorema, mas não atende a condição (1).

**Indução: segunda forma**

Aqui apresentaremos uma variação da $1^a$ forma do princípio da indução que será útil na demonstração por indução do Teorema da Divisão de Euclides que demonstraremos em seguida.

Teorema 2 (Indução - $2^a$ forma)
Vamos supor que para cada inteiro $n \geq 0$ esteja dada uma afirmação $A(n)$, dependendo de $n$ e vamos admitir que sejam válidas:

(1) A afirmação $A(0)$ é verdadeira.

(2) Para todo $n \in \mathbb{Z}$ com $n > 0$ se $A(k)$ é verdadeira para todo $k < n$ então $A(n)$ também é verdadeira.

Então $A(n)$ é verdadeira para todo $n \in \mathbb{Z}$ com $n > 0$.

*Demonstração:*

A demonstração segue a mesma linha de argumento usada na demonstração do Teorema 1.

Seja $S$ o subconjunto de todos os inteiros $n \geq 0$ tais que a afirmação $A(n)$ seja falsa. Assim,

$$S = \{n \in \mathbb{Z} \mid n \geq 0 \text{ e } A(n) \text{ é falsa}\}.$$

Observe que $A(n)$ é verdadeira para todo $n \in \mathbb{Z}$ com $n \geq 1$ se, e somente se, $S = \emptyset$.

Assim, provar o Teorema 2 é equivalente provar que $S = \emptyset$.

Vamos argumentar por redução ao absurdo, supondo que o Teorema 2 seja falso. Portanto, existirá um $n \in \mathbb{Z}$ com $n \geq 0$ tal que $A(n)$ é falsa. Nessa situação $n \in S$ e $S \neq \emptyset$.

Mas, $S$ é, evidentemente, limitado inferiormente $(0 \leq s, \forall s \in S)$. Pelo princípio da boa ordenação de $\mathbb{Z}$, temos que $S$ possui um primeiro elemento $n_0 \in S$.

Como $A(0)$ é verdadeira, por hipótese do nosso Teorema, temos que $0 \notin S$ e $n_0 \in S$ com $n_0 \geq 1$.

Assim, para todo $k$ com $0 \leq k < n_0$, temos que $k \notin S$ e também temos que $A(k)$ é verdadeira. Pela nossa hipótese (2), segue que $A(n_0)$ deve ser verdadeira. Uma contradição pois $n_0 \in S$.

Portanto, supor o Teorema 2 falso nos leva a um absurdo! Logo o Teorema 2 é verdadeiro como queríamos demonstrar. □

Vamos utiizar esta segunda forma da indução neste próximo exemplo.

Exemplo **11**

Os números de Fibonacci são a seqüência de inteiros $(F_0, F_1, F_2, \ldots)$, onde

$$\begin{aligned} &F_0 = 1 \\ &F_1 = 1 \quad \text{e} \\ &F_n = F_{n-1} + F_{n-2}, \quad \text{para } n \geq 2. \end{aligned}$$

Os primeiros números da seqüência são $(1, 1, 2, 3, 5, 8, 13, \cdots)$.

Vamos mostrar que, para todo $n \in \mathbb{N}$, vale que $F_n \leq (1{,}7)^n$.

*Solução:* A afirmação vale para $n = 0$, pois $F_0 = 1 \leq (1{,}7)^0 = 1$. A afirmação também vale para $n = 1$, pois $F_0 = 1 \leq (1{,}7)^1 = 1{,}7$.

Aqui tivemos que considerar os dois casos iniciais $n = 0$ e $n = 1$, ao invés de considerar somente o caso $n = 0$, porque $n = 1$ também é definido de uma maneira diferente da definição geral de $F_n$.

Suponha agora que a afimação $F_n \leq (1{,}7)^n$ valha para um certo inteiro $x$, $x \geq 2$, e para todos os valores $k \leq x$. Vamos provar que vale para $x + 1$. Como a afirmação vale para $n = x$ e $n = x - 1$, temos:

$$F_x \leq (1{,}7)^x \quad \text{e} \quad F_{x-1} \leq (1{,}7)^{x-1} \, . \qquad (1)$$

Por definição,

$$F_{x+1} = F_x + F_{x-1} \, .$$

Combinado as desigualdades (1) na equação anterior, obtemos:

$$\begin{aligned} F_{x+1} &= F_x + F_{x-1} \\ &\leq (1{,}7)^x + (1{,}7)^{x-1} \\ &= (1{,}7)^{x-1}(1{,}7 + 1) \\ &= (1{,}7)^{x-1}(2{,}7) \\ &= (1{,}7)^{x-1}(2{,}89) \qquad \text{pois } 2{,}7 < 2{,}89 \\ &= (1{,}7)^{x-1}(1{,}7)^2 \qquad \text{pois } (1{,}7)^2 = 2{,}89 \\ &= (1{,}7)^{x+1} \end{aligned}$$

portanto, a afirmação é verdadeira para $n = x + 1$, o que completa a demonstração. □

Agora é hora de você aplicar a segunda forma de indução para demonstrar um resultado sobre inteiros.

**Atividades 3**

5. Mostre, usando indução, que a soma os ângulos internos de um polígono de $n$ lados é $180^0(n-2)$.

   Sugestão: Trace uma diagonal para separar o polígono em dois com menos número de lados.

## O Teorema da Divisão de Euclides

Aqui vamos enunciar e demonstrar o Teorema da Divisão de Euclides para inteiros não negativos.

Teorema 3 (Teorema da Divisão de Euclides)
Seja $n \geq 0$ e $d > 0$ números inteiros. Então existem inteiros $q \geq 0$ e $r \geq 0$ tal que $0 \leq r < d$ e $n = qd + r$. Mais ainda, os inteiros $q$ e $r$ são univocamente determinados ($n$ é chamado de *dividendo*, $d$ é chamado de *divisor*, $q$ é chamado de *quociente* e $r$ é chamado de *resto*).

*Demonstração:*

Usaremos indução sobre $n \geq 0$. O Teorema 3 é verdadeiro para $n = 0$ pois,

$$0 = 0 \cdot d + 0 \qquad (q = 0 \quad \text{e} \quad r = 0)\,.$$

Vamos assumir $n > 0$. Se $n < d$, podemos escrever

$$n = 0 \cdot d + n \qquad (q = 0 \quad \text{e} \quad r = n < d)\,.$$

Assim, vamos assumir $n > 0$ e $d \leq n$.

Nessa situação teremos:

$$0 \leq n - d < n\,.$$

Pela nossa hipótese de indução, o Teorema é verdadeiro para $k = n - d < n$.

Portanto, existem inteiros $q_1$ e $r$ tal que $0 \leq r < d$ e $n - d = k = q_1 d + r$. Daí, segue que

$$n = (q_1 + 1)d + r\,,$$

provando a primeira parte do Teorema 3 com os inteiros $q = q_1 + 1$ e $r$.

Agora vamos provar a unicidade dos inteiros $q$ e $r$.

Suponhamos que

$$n = qd + r = q'd + r'\,,$$

onde $0 \leq r < d$ e $0 \leq r' < d$.

Se $r \neq r'$, digamos $r > r'$ teríamos

$$0 < (q' - q)d = r - r' < d$$

e

$$r - r' > 0\,.$$

Uma contradição! Logo $r = r'$. Mas de $n = qd + r = q'd + r$, teremos $q = q'$ e isto completa a demonstração do Teorema 3. □

Repare que, dados inteiros $n$ e $d$, podemos escrever $n = qd + r$ de várias maneiras com $q, r$ inteiros. No entanto, $q$ será o quociente e $r$ o resto da divisão, apenas na representação em que $0 \leq r < d$.

Exemplo **12**

1. A divisão de 10 por 3 tem quociente 3 e resto 1, pois $10 = 3.3 = 1$.
2. A divisão de $-10$ por 3 tem quociente $-4$ e resto 2, pois $-10 = 3(-4) + 2$.
3. A divisão de $-10$ por $-3$ tem quociente 4 e resto 2, pois $-10 = (-3).4 + 2$.

Para praticar um pouco, crie, você mesmo, alguns exemplos. Certifique-se que você não tem dúvidas na determinação do quociente e resto com inteiros negativos.

## Resumo

Esta aula apresentou duas formas do princípio da indução, que são ferramentas básicas muito utilizadas nas demosntrações envolvendo inteiros. Apresentamos também a demonstração do Teorema da Divisão de Euclides (Teorema 3). Este estabelece uma propriedade fundamental dos números inteiros e será bastante utilizado no desenvolvimento que faremos nas próximas aulas.

**Atividades**

1. Prove, por indução, as seguintes fórmulas sobre os inteiros:
   (a) $1+2+\ldots+n=\frac{n(n+1)}{2}, \forall n \geq 1$.
   (b) $1+4+\cdots+n^2=n(n+1)\frac{2n+1}{6}, \forall n \geq 1$.
   (c) $1+8+\cdots+n^3=\left[\frac{n(n+1)}{2}\right]^2, \forall n \geq 1$.
   (d) $1+3+\cdots+(2n-1)=n^2, \forall n \geq 1$.

2. Prove, por indução, que $n^3+2n$ é sempre um múltiplo de 3.

3. Para $n, m \in \mathbb{N}$ e $n \geq m$, definimos o número binomial $\binom{n}{m}$ como

$$\binom{n}{m}=\frac{n!}{(n-m)!m!},$$

   onde $n!=n(n-1)(n-2)\ldots 3.2.1$ e $0!=1$. Prove, por indução sobre $n$, a fórmula:

$$\binom{n}{m-1}+\binom{n}{m}=\binom{n+1}{m}$$

   É comum definir-se $\binom{n}{m}=0$ no caso de $n<m$.

4. Em uma fila de supermercado, a primeira pessoa da fila é uma mulher e a última é um homem. Use o princípio da indução para mostrar que em alguma ponto da fila uma mulher estará diretamente na frente de um homem.

5. Se $n$ é um número ímpar, prove que $n^3-n$ é sempre divisível por 24.

6. Seja $F_n$ o $n-$ésimo número de Fibonacci, introduzado no Exemplo 11. Mostre que

$$\binom{n}{0}+\binom{n-1}{1}+\binom{n-2}{2}+\cdots\binom{0}{n}=F_n$$

   Note que vários dos últimos fatores da soma acima serão iguais a zero, pois $\binom{n}{m}=0$ se $n<m$. Por exemplo, para $n=4$,

$$\binom{4}{0}+\binom{3}{1}+\binom{2}{2}+\binom{1}{3}+\binom{0}{4}=1+3+1+0+0=5=F_4\,.$$

# Aula 5 – Divisibilidade nos inteiros: o Máximo Divisor Comum

**Metas**

Apresentar através da divisibilidade nos inteiros, a existência de mdc e o Algoritmo de Euclides.

**Objetivos**

Ao final desta aula o aluno deve ser capaz de:

- Definir a noção de divisibilidade nos inteiros, e usando a estrutura ordenada de $\mathbb{Z}$, mostrar a existência do Máximo Divisor Comum.
- Demonstrar a convergência do algoritmo de Euclides no cálculo do MDC, e demonstrar uma forma equivalente de definir MDC nos inteiros.

subsectionIntrodução

O Teorema da Divisão de Euclides (o Teorema3 da aula passada) foi, historicamente, introduzido e demonstrado, com o objetivo de se calcular o máximo divisor de 2 números inteiros positivos (o MDC), através do chamado Algoritmo de Euclides. Ele aparece em um dos mais famosos livros da Matemática, os "Elementos" de Euclides, em Alexandria, no século III a.C.

As demonstrações aparecem nas proposições 1 e 2 do livro 7 dos "Elementos" que de fato é uma coleção de 13 livros. Três desses livros lidam com a Teoria dos Números, os demais envolvem temas ligados a números reais e a Geometria. No livro 7, o primeiro a tratar da Teoria dos Números, encontramos o conceito de números primos e o método para o cálculo do MDC entre dois números inteiros positivos.

Nessa aula apresentaremos a noção de divisibilidade nos inteiros, mostrando a existência de MDC em $\mathbb{Z}$ e provando o Algoritmo de Euclides para o cálculo do Máximo Divisor Comum. Na próxima aula voltaremos a tratar do tema MDC ligado a uma primeira visão estrutural algébrica de $\mathbb{Z}$.

## Divisibilidade dos inteiros

Inicialmente vamos dar algumas definições envolvendo o conceito de divisibilidade.

Dizemos que um número inteiro $m$ divide outro número inteiro $n$, se existe um inteiro $q$ tal que

$$n = q \cdot m \, .$$

Nesse caso, dizemos ainda que *"$m$ é um divisor de $n$"* ou *"$n$ é um múltiplo de $m$"*. O número $q$ é chamado de *quociente* de $n$ por $m$.

Assim, *"$n$ é múltiplo de $m$"* se o resto da divisão de $n$ por $m$ é $r = 0$, no Teorema da divisão de Euclides,

$$n = q \cdot m + 0 \, .$$

Observe que, como

$$n = q \cdot m \leftrightarrow n = (-q)(-m) \leftrightarrow (-n) = (-q) \cdot m$$

segue-se que quando $m$ é divisor de $n$, então $-m$ tambem é divisor de $n$ e $m$ é divisor de $-n$.

Exemplo **13**
Os divisores de 12 são os inteiros

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12 \, .$$

Por outro lado, estes inteiros são também os divisores de $-12$.

Aqui, é natural estabelecermos uma notação para os conjunto de todos os divisores de um inteiros, e tambem para os divisores positivos e negativos.

Definição 1
Dado um número inteiro $n$, definimos

1. $\mathcal{D}(n) = \{m \in \mathbb{Z} \mid m \text{ é divisor de } n\}$
2. $\mathcal{D}(n)^+ = \{m \in \mathbb{Z} \mid m > 0 \text{ e } m \text{ é divisor de } n\}$
3. $\mathcal{D}(n)^- = \{m \in \mathbb{Z} \mid m < 0 \text{ e } m \text{ é divisor de } n\}$

Assim, pela observação que fizemos acima, vale que:

$$\mathcal{D}(n)^- = -(\mathcal{D}(n)^+) = \{-m \in \mathbb{Z} \mid m \in \mathcal{D}(n)^+\}$$

$$\mathcal{D}(n) = \mathcal{D}(n)^- \bigcup \cdot \; \mathcal{D}(n)^+$$

isto é, o conjunto $\mathcal{D}(n)$ é união disjunta dos subconjuntos $\mathcal{D}(n)^-$ e $\mathcal{D}(n)^+$.

Exemplo **14**

$$\mathcal{D}(12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$$
$$\mathcal{D}(12)^+ = \{1, 2, 3, 4, 6, 12\}$$
$$\mathcal{D}(12)^- = \{-1, -2, -3, -4, -6, -12\}$$

Claramente, vale que

$$\mathcal{D}(12)^+ = -\mathcal{D}(12)^- \quad \text{e} \quad \mathcal{D}(12) = \mathcal{D}(12)^+ \cup \mathcal{D}(12)^-$$

**Exercícios**

1. Encontre $\mathcal{D}(60)$, $\mathcal{D}(60)^+$ e $\mathcal{D}(60)^-$.
2. Quantos divisores tem um número primo?

## Finitude do conjunto dos divisores de um inteiro

A proposição a seguir mostra que um inteiro possui um número finito de divisores.

Proposição 1
Seja $n \neq 0$ um dado número inteiro. Então o conjunto $\mathcal{D}(n)$ dos divisores de $n$ é sempre finito.

*Demonstração:*

É suficiente demonstrarmos que $\mathcal{D}(n)^+$ é finito. Isto porque, se isto for verdade, como $\mathcal{D}(n)^- = \mathcal{D}(n)^+$, então $\mathcal{D}(n)^-$ tem o mesmo número de elementos de $\mathcal{D}(n)^+$ e, portanto, tambem é finito. Como $\mathcal{D}(n) = \mathcal{D}(n)^+ \cup \mathcal{D}(n)^-$ então $\mathcal{D}(n)$ é a união de dois conjuntos finitos, logo, também é finito.

Vamos começar demonstrando um lema.

Lema 1
Seja $n$ um inteiro positivo. Então

(a) $1, n \in \mathcal{D}(n)^+$

(b) Se $m \in \mathcal{D}(n)^+$ então $0 < m \leq n$.

*Demonstração do Lema:*

A demonstração de (a) é óbvia pois $n = n \cdot 1 = 1 \cdot n$. Agora vamos provar (b): Seja $m \in \mathcal{D}(n)^+$. Assim, $m > 0$ e existe $q > 0$, tal que $n = q \cdot m$.

Se $q = 1$, $n = m$ e se $q \geq 2$ e $n = q \cdot m \geq 2 \cdot m = m + m > m$. Isto prova o lema.

Como corolário do Lema, teremos que

$$\mathcal{D}(n)^+ \subseteq \{m \in \mathbb{Z} \mid 1 \leq m \leq n\},$$

e portanto, $\mathcal{D}(n)^+$ é um conjunto finito com número de elementos menor ou igual a $n$, já que o conjunto

$$\{m \in \mathbb{Z} \mid 1 \leq m \leq n\}$$

possui exatamente $n$ elementos.

Como $|\mathcal{D}(n)| = 2 \cdot |\mathcal{D}(n)^+|$, temos $\mathcal{D}(n)$ finito.

**Exercícios**

1. Dê exemplos em que inteiros positivos $n$ tal que

$$|\mathcal{D}(n)| = n$$

Quantos inteiros positivos satisfazem esta condição?

## O Máximo Divisor Comum (mdc) de dois inteiros

Agora estamos em condição de definir o máximo divisor comum de dois números $a$ e $b$.

Definição 2 (mdc)
Dizemos que o número inteiro positivo $d$ é o *máximo divisisor comum* de dois números inteiros não nulos $a$ e $b$, se:

1. $d$ é um divisor comum de $a$ e $b$, isto é, $d$ divide $a$ e $d$ divide $b$.

2. $d$ é o maior divisor comum, isto é, se $d'$ é outro divisor comum de $a$ e $b$ então $d' \leq d$.

Usamos a notação $\text{mdc}(a, b)$ para denotar o máximo divisor comum de $a$ e $b$.

Podemos expressar as condições da definição anterior de outra forma. O conjunto dos dividores positivos comuns de $a$ e $b$ é a interseção do conjunto dos divisores positivos de $a$ e do conjunto dos divisores positivos de $b$, isto é,

$$\text{divisores comuns de } a \text{ e } b \ = \mathcal{D}(a) \cap \mathcal{D}(b) \ .$$

Observe que este conjunto interseção nunca é vazio, pois

$$1 \in \mathcal{D}(a) \cap \mathcal{D}(b) \ .$$

O maior dividor comum de $a$ e $b$ é, simplesmente, o máximo do conjunto dos divisores comuns:

$$\text{mdc}(a, b) = \max \mathcal{D}(a) \cap \mathcal{D}(b) \ .$$

Lembre-se que, pela propriedade da boa ordenação do conjunto dos números inteiros, todo conjunto finito tem um único máxico, o que assegura a existência e unicidade do mdc de dois inteiros positivos.

A definição de máximo divisor comum pode ser generalizada, de modo análogo, para mdc de mais de dois números. Assim, teríamos: se $a_1, a_2, \cdots, a_k$ são números inteiros não nulos, então $d = \text{mdc}\{a_1, a_2, \cdots, a_k\}$ é o maior inteiro divisor comum de $a_1, a_2, \cdots, a_k$.

Exemplo **15**
Verifique que:

1. $\text{mdc}(10, 15) = 5$
2. $\text{mdc}(70, 121) = 1$
3. $\text{mdc}(n, n) = n$ para qualquer inteiro positivo $n$.
4. $\text{mdc}(1, n) = 1$ para qualquer inteiro positivo $n$.
5. $\text{mdc}(p, q) = 1$ para quaisquer $p$ e $q$ primos distintos.

**Atividades**

1. Pense em alguns pares de inteiros e calcule o mdc destes números.

## O algoritmo de Euclides

Sejam $a$ e $b$ dois dados números inteiros positivos. Podemos assumir $a \geq b$ (caso contrário, invertemos a ordem dos números).

Se $a = b$, teremos $D = \text{mdc}(a, b) = a = b$.

Vamos considerar $a > b$. Pelo Teorema da Divisão de Euclides, existem números $q_1$ e $r_1$ tais que:

$$a = q_1 \cdot b + r_1 \ ,$$

onde $0 \leq r_1 < b$.

Se $r_1 = 0$ temos $a = q_1 \cdot b$ e $b$ é um dos divisores positivos de $a$. Nesse caso,

$$b \in \mathcal{D}(a)^+ \Rightarrow \mathcal{D}(b)^+ \subset \mathcal{D}(a)^+ \ .$$

Daí segue que:

$$I = \mathcal{D}(a)^+ \cap \mathcal{D}(b)^+ = \mathcal{D}(b)^+$$

e teremos

$$D = \text{mdc}(a, b) = \max(I) = \max(\mathcal{D}(b)^+) = b \, .$$

Se $r_1 \neq 0$, teremos $0 < r_1 < b$, $a = q \cdot b + r_1$. Agora observe que:

Lema 2
Um inteiro $d > 0$ é divisor comum de a e b se, e somente se, $d > 0$ é divisor comum de b e $r_1$.

Isto é conseqüência das igualdades

$$a = q \cdot b + r_1 \Rightarrow r_1 = a - q \cdot b \ .$$

Assim,

$$d \text{ divide } a \text{ e } b \Rightarrow d \text{ divide } a - q \cdot b \Rightarrow d \text{ divide } r_1 \ .$$

Por outro lado,

$$d \text{ divide } b \text{ e } r_1 \Rightarrow d \text{ divide } q \cdot b + r_1 \Rightarrow d \text{ divide } a$$

Portanto, os divisores comuns de $a$ e $b$ são também divisores comuns de $b$ e $r_1$ e vice-versa, o que resulta em

$$\text{mdc}(a, b) = \text{mdc}(b, r_1) \ .$$

Isto é o que faz o algoritmo de Euclides funcionar! Se $r_1 = 0$ então $\text{mdc}(a, b) = b$. Caso contrário, $r_1 > 0$, e

$$\text{mdc}(a, b) = \text{mdc}(b, r_1)$$

Fazemos um novo passo do algoritmo, agora com os inteiros $b$ e $r_1$. O mdc encontrado será também o mdc dos inteiros $a$ e $b$.

Mas, qual a vantagem do algoritmo se temos que repetir a mesma operação de novo? A vantagem é que, a cada passo, estamos lidando com inteiros positivos menores. Portanto, em algum momento, o algoritmo termina!

Se $r_1 > 0$, o próximo passo é dividir $b$ por $r_1$, achando quociente $q_2$ e resto $r_2$:

$$b = q_2 \cdot r_1 + r_2 \, .$$

Se $r_2 = 0$, temos $b = q_2 \cdot r_1$, e nesse caso, como argumentamos anteriormente,

$$\text{mdc}(b, r_1) = r_1 = \text{mdc}(a, b),$$

e paramos o nosso algoritmo nesse estágio.

Se $r_2 \neq 0$, teremos $b = q_2 \cdot r_1 + r_2$ onde $0 < r_2 < r_1$. Nessa situação dividimos $r_1$ por $r_2$, achando quociente $q_3$ e resto $r_3$:

$$r_1 = q_3 \cdot r_2 + r_3$$

onde $0 \leq r_3 < r_2$.

Analogamente ao que mostramos anteriormente, temos:

$$\text{mdc}(a, b) = \text{mdc}(b, r_1) = \text{mdc}(r_1, r_2).$$

Se $r_3 = 0$, $\text{mdc}(a, b) = \text{mdc}(r_1, r_2) = r_2$, pois $r_1 = q_3 \cdot r_2 + 0 = q_3 \cdot r_2$, e paramos o algoritmo nesse estágio.

Se $r_3 > 0$, prosseguimos sucessivamente com nosso algoritmo, determinando quocientes $q_1, q_2, q_3, \cdots, q_k, \cdots$ e restos $r_1, r_2, r_3, \cdots, r_k, \cdots$ de modo que

$$\begin{array}{rcccc}
a & = & q_1 \cdot b + r_1 & , & 0 \leq r_1 < b \\
b & = & q_2 \cdot r_1 + r_2 & , & 0 \leq r_2 < r_1 \\
r_1 & = & q_3 \cdot r_2 + r_3 & , & 0 \leq r_3 < r_2 \\
\vdots & & \vdots & & \vdots \\
r_k & = & q_k \cdot r_{k-1} + r_k & , & 0 \leq r_k < r_{k-1}
\end{array}$$

Como a seqüência dos restos satisfaz as condições:

$$b > r_1 > r_2 > \cdots > r_k > \cdots \geq 0\,,$$

partindo de um $b$ fixado, temos que existirá um primeiro índice $k$ tal que $r_k = 0$.

Nessa etapa $k$ paramos o algoritmo e teremos que

$$\mathcal{D} = \text{mdc}(a, b) = \text{mdc}(b, r_1) = \cdots = \text{mdc}(r_{k-2}, r_{k-1}) = r_{k-1}$$

Exemplo **16**

Vamos aplicar o algoritmo de Euclides para determinar o mdc de 3600 e 540.

$$\begin{aligned} 3600 &= 6 \times 540 + 360 \\ 540 &= 1 \times 360 + 180 \\ 360 &= 2 \times 180 + 0 \end{aligned}$$

Quando encontramos resto 0, então o divisor da última divisão é o mdc dos inteiros. Portanto, $\text{mdc}(3600, 540) = 180$.

Observe que

$$\text{mdc}(3600, 540) = \text{mdc}(540, 360) = \text{mdc}(360, 180) = 180\,.$$

É comum representar-se estas etapas pelo esquema a seguir:

| | 6 | 1 | 2 |
|---|---|---|---|
| 3600 | 540 | 360 | 180 |
| 360 | 180 | 0 | |

Em geral, temos um esquema:

| | q | $q_1$ | $q_2$ | $q_3$ | $\cdots$ |
|---|---|---|---|---|---|
| a | b | r | $r_1$ | $r_2$ | $\cdots$ |
| r | $r_1$ | $r_2$ | $\cdots$ | | |

Quando obtemos um resto igual a zero, o mdc é o último divisor, isto é, o último número na fila do meio do esquema anterior.

**Atividades**

1. Mostre que $\mathrm{mdc}(585, 527) = 1$.
2. Sejam $a$ e $b$ inteiros positivos, e vamos supor que existe inteiros $s$ e $t$ tais que $a = b \cdot s + t$. Mostre que

$$\mathrm{mdc}(a, b) = \mathrm{mdc}(b, t)\,.$$

**Solução**

1. Temos que:

$$\begin{aligned} 585 &= 1 \times 527 + 58 \\ 527 &= 9 \times 58 + 5 \\ 58 &= 11 \times 5 + 3 \\ 5 &= 1 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

   Portanto:

   $\mathrm{mdc}(585, 527) = \mathrm{mdc}(527, 58) = \mathrm{mdc}(58, 5) = \mathrm{mdc}(5, 3) = \mathrm{mdc}(3, 2) = \mathrm{mdc}(2, 1) = 1$

   Esquematicamente:

| | 1 | 9 | 11 | 1 | 1 | 2 |
|---|---|---|---|---|---|---|
| 585 | 527 | 58 | 5 | 3 | 2 | 1 |
| 58 | 5 | 3 | 2 | 1 | 0 | |

2. A demostração é totalmente análoga ao que fizemos na demonstração do Algoritmo de Euclides para mostrar que $\mathrm{mdc}(a, b) = \mathrm{mdc}(b, r)$.

## Uma formulação equivalente para o mdc

Nesta seção, vamos provar a uma propriedade importante do mdc de dois inteiros.

Proposição 2
Sejam $a$ e $b$ dois dados inteiros positivos e seja $d = \text{mdc}(a, b)$ o máximo divisor comum de $a$ e $b$. Mostre que, se $a' = \frac{a}{d}$ e $b' = \frac{b}{d}$ então $\text{mdc}(a', b') = 1$.

*Demonstração.* Seja $I' = \mathcal{D}(a')^+ \cap \mathcal{D}(b')^+$. Vamos mostrar que $I' = \{1\}$ e, portanto, $\text{mdc}(a', b') = \max I' = 1$.

De fato, seja $d = \max(a, b)$, e seja $k$ um divisor comum positivo de $a'$ e $b'$. Assim,

$$\begin{aligned} a' &= r' \cdot k \\ b' &= s' \cdot k \end{aligned}$$

Daí segue que

$$\frac{a}{d} = k \cdot r' \Longrightarrow a = (k \cdot d)r' \tag{3}$$

$$\frac{b}{d} = k \cdot s' \Longrightarrow b = (k \cdot d)s' \tag{4}$$

De (1) e (2) concluimos que $k \cdot d$ é divisor comum de $a$ e $b$. Mas $d = \text{mdc}(a, b)$. Logo $d \geq k \cdot d$ o que implica $0 < k \leq 1$, isto é, $k = 1$. □

Agora vamos apresentar uma formulação equivalente para o mdc, que nos será útil nas aulas seguintes. Ela nos diz que $\text{mdc}(a, b)$ não só é o maior divisor comum de $a$ e $b$, como também é múltiplo de todos os outros divisores comuns de $a$ e $b$. Alguns autores usam esta formulação como definição de mdc.

Proposição 3
Sejam $a$ e $b$ dois números inteiros positivos dados. Então $D = \text{mdc}(a, b)$ se, e somente se,

1. $D$ é divisor comum de $a$ e $b$
2. Dado um arbitrário divisor comum $d$ de $a$ e $b$, então $d$ é divisor de $D$.

*Demonstração.*

($\Longrightarrow$)

Seja $D = \text{mdc}(a, b)$. Vamos mostrar que $D$ satisfaz as condições (1) e (2) acima.

A condição (1) é imediata da definição de mdc. Vamos provar a condição (2).

Seja $d$ um arbitrário divisor comum de $a$ e $b$. Sem perda de generalidade podemos assumir $d > 0$. Vamos mostrar que $d$ divide $D$.

Pela definição de mdc sabemos que $d \leq D$. Se $d = D$, $d$ é divisor de $D$.

Agora vamos assumir $d < D$, e vamos escrever $a = q \cdot D$ e $b = q' \cdot D$. Pela proposição anterior temos que $D = \text{mdc}(q, q') = 1$ já que $q = \frac{a}{D}$ e $q' = \frac{b}{D}$.

Como $D > d$, pelo Teorema da Divisão de Euclides, existem inteiros $m$ e $r$ tais que $D = m \cdot d + r$ com $0 \leq r < d$.

Assim,

$$(*) \begin{cases} a = q \cdot D = q(md + r) = (qm)d + qr, & 0 \leq r < d \\ b = q' \cdot D = q'(md + r) = (q'm)d + q'r & . \end{cases}$$

Mas $d$ é divisor comum de $a$ e $b$, e daí segue que existe inteiros $s$ e $s'$ tais que

$$a = s \cdot d \text{ e } b = s' \cdot d.$$

Usando as igualdades $(*)$ acima, temos

$$(**) \begin{cases} sd = (qm)d + qr \implies (s - qm)d = qr \\ s'd = (q'm)d + q'r \implies (s' - q'm)d = q'r\,. \end{cases}$$

Seja $t = \text{mdc}(d, r)$, e sejam $\alpha$ e $\beta$ inteiros definidos por: $\alpha = \frac{d}{t}, \beta = \frac{r}{t}$. Pelo exercício anterior temos que $\text{mdc}(\alpha, \beta) = 1$ e $d = \alpha \cdot t$ e $r = \beta \cdot t$. Substituindo em $(**)$ temos:

$$\begin{cases} (s - qm)\alpha t = q\beta t \implies (s - qm)\alpha = q\beta \\ (s' - q'm)\alpha t = q'\beta t \implies (s' - q'm)\alpha = q'\beta\,. \end{cases}$$

Como $\text{mdc}(\alpha, \beta) = 1$, segue que $\alpha$ é divisor de $q$, e $\alpha$ é divisor de $q'$. Mas sabemos que $\text{mdc}(q, q') = 1$, e isto nos diz que $\alpha = 1$.

Assim,

$$\alpha = 1 \implies d = \alpha t = \text{mdc}(d, r) \implies d \text{ é divisor de } r \implies d \leq r$$

o que é um absurdo. Portanto, $r = 0$ e $D = md$, $d$ divisor de $D$.

$(\Longleftarrow)$

Assumimos as propriedades (1) e (2) para $D$. Vamos provar que $D = \text{mdc}(a, b)$.

A propriedade (1) nos diz que $D$ é divisor comum de $a$ e $b$. Seja $d \in I = \mathcal{D}(a)^+ \cap \mathcal{D}(b)^+$, um divisor comum positivo de $a$ e $b$. Pela propriedade (2), $d$ é divisor de $D$, logo $d \leq D$, e $D$ é máximo divisor comum de $a$ e $b$.

Assim, as propriedades (1) e (2) caracterizam o mdc.

□

**Atividades**

1. Determine os conjuntos $\mathcal{D}(156)$ e $\mathcal{D}(130)$. Determine $d = \text{mdc}(156, 136)$ e verifique que $d$ é múltiplo de todos os elementos de $\mathcal{D}(156) \cap \mathcal{D}(130)$, isto é, $d$ é múltiplo de todos os divisores comuns de 156 e 130.

2. Verifique que $\text{mdc}(\frac{156}{d}, \frac{130}{d}) = 1$.

3. Escolha alguns pares de inteiros $a$ e $b$ e verifique que

$$\text{mdc}\left(\frac{a}{\text{mdc}(a,b)}, \frac{b}{\text{mdc}(a,b)}\right) = 1$$

## Divisibilidade como relação de ordem

Usaremos a notação $a|b$ significando "$a$ é divisor de $b$".

A relação "é divisor de ", no conjunto dos números inteiros, satisfaz as seguintes propriedades:

1. $a|a, \ \forall a \in \mathbb{Z}^*$ (reflexiva).

2. $a|b$ e $b|a$ implica em $a = \pm b$.

3. $a|b$ e $b|c$ implica em $a|c$ (transitividade).

A verificação das propriedades acima é bastante simples e será deixada como exercício.

Note que não vale a propriedade antissimétrica da relação linear $\leq$, natural em $\mathbb{Z}$:

$$a \leq b \ \text{ e } \ b \leq a \Longrightarrow a = b\,.$$

No entanto, se $a$ e $b$ são inteiros positivos e $a|b$ e $b|a$, teremos que $a = b$. Portanto, restringindo a relação "a divide b" ao conjunto dos números inteiros positivos, ela será anti-simétrica:

2' Se $a, b \in \mathbb{Z}^+$, $a|b$ e $b|a$ implica em $a = b$ (anti-simetria).

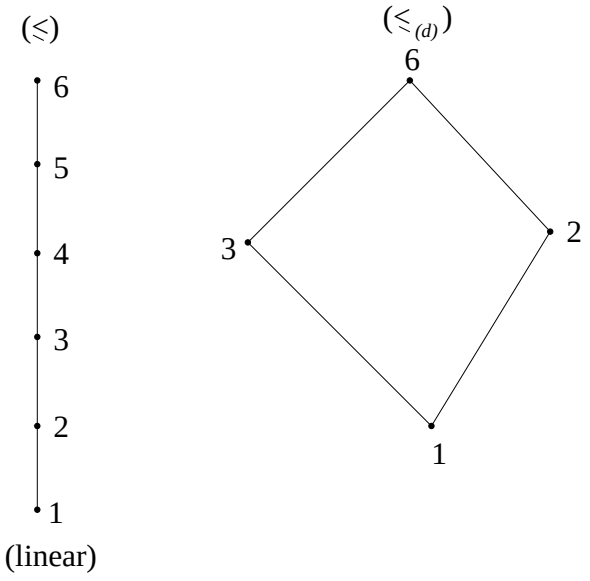
Mas propriedades de reflexividade, transitividade e anti-simetria caracterizam as relações de ordem parcial em um conjunto. Concluímos assim que a relação "a divide b", no conjuntos dos inteiros positivos, é uma relação de ordem parcial.

**Atividades**

1. Verifique que a ordem "a divide b" não é linear (total) em $A = \mathbb{Z}^+$.
2. Entenda a diferença entre as ordens $\leq$ e "a divide b". A primeira $\leq$ é linear e a segunda não é.

**Comentários das atividades**

1. Por exemplo, 2 não divide 3 e 3 não divide 2.
2. É fácil entender a diferença através de um grafo simbólico:




## Convergência do Algoritmo de Euclides

Nesta seção, vamos adotar uma visão um pouco mais computacional sobre o Algoritmo de Euclides.

Para calcular o mdc de dois inteiros positivos $a$ e $b$, poderíamos fazer simplesmente o seguinte: listamos todos os divisores positivos de $a$ e $b$ e determinamos o máximo da interseção.

Um algorítmo deste tipo seria o seguinte:

*Entrada:* Inteiros positivos $a$ e $b$.
*Saída:* $\text{mdc}(a, b)$.

- Para todo inteiro $k$ entre 1 e o mínimo de $a$ e $b$ teste se $k|a$ e $k|b$. Caso afirmativo inclua $k$ em um conjunto $I$.
- Retorne o máximo do conjunto $I$.

Este é um algoritmo que sempre funciona, no sentido que sempre retorna o mdc de dois inteiros $a$ e $b$. No entanto, é extremamente lento. Ainda que possa ser melhorado de diversas maneiras, este algoritmo não é prático para inteiros grandes, uma vez que envolve um número muito grande de divisões.

O Algoritmo de Euclides tem as vantagens de ser rápido e muito fácil de ser implementado computacionalmente.

Podemos descrever o Algoritmo de Euclides da seguinte maneira:

*Entrada:* Inteiros positivos $a$ e $b$.
*Saída:*$\text{mdc}(a, b)$.

- Seja $r$ o resto da divisão de $a$ e $b$.
- Se $r = 0$ então o resultado é $b$ e paramos.
- Se $r \neq 0$ então calculamos $\text{mdc}(b, r)$ e retornamos este valor como resposta.

Este algoritmo é definido por **recorrência**, isto é, o algoritmo invoca ele mesmo várias vezes a fim de obter o resultado.

Mais quão rápido converge o Algoritmo de Euclides? Por exemplo, iniciando com inteiros $a$ e $b$ de 1000 algarismos, quanto passos, no máximo, seriam necessário para chegarmos ao final do algoritmo?

Este é uma pergunta muito importante quando consideramos aplicações computacionais práticas que utilizam o Algoritmo de Euclides.

Para respondermos esta pergunta, precisamos da proposição a seguir.

Proposição 4
Sejam $a$ e $b$ inteiros positivos, com $a \geq b$, e seja $r$ o resto da divisão de $a$ e $b$. Então $r \leq \frac{a}{2}$.

*Demonstração.* Sempre vale que $0 \leq r < b$. Se $b \leq \frac{a}{2}$, então $r < b \Rightarrow r \leq \frac{a}{2}$.

Caso contrário, $b > \frac{a}{2}$ e o quociente da divisão de $a$ por $b$ é 1:

$$a = b \cdot 1 + r \Rightarrow r = a - b\,.$$

Mas $b > \frac{a}{2} \Rightarrow -b < -\frac{a}{2} \Rightarrow a - b < a - \frac{a}{2} = \frac{a}{2}$ . Portanto $r < \frac{a}{2}$.

□ No algoritmo de Euclides, temos

$$\text{mdc}(a, b) = \text{mdc}(b, r) = \text{mdc}(r, r_1) = \cdots$$

onde, a cada dois passos, trocamos o primeiro elementos de um par pelo resto da divisão dos dois elementos do par. Observe:

$$\text{mdc}(a,b) = \text{mdc}(b,r) = \text{mdc}(r,r_1) = \text{mdc}(r_1,r_2) = \text{mdc}(r_2,r_3) = \cdots$$

Assim, $r \leq \frac{a}{2}$, $r_2 \leq \frac{r}{2} \leq \frac{a}{4}$. A cada dois passos o maior número do par fica reduzido a, no máximo, metade do valor. Na pior hipótese, o livro para quando encontramos resto 1. Se o algoritmo leva $n$ passos para encontrar resto $r$, então

$$r \leq \frac{a}{2^{\frac{n}{2}}} .$$

Para $r = 1$ então

$$\frac{a}{2^{\frac{n}{2}}} = 1 \Rightarrow 2^{\frac{n}{2}} = a \Rightarrow \frac{n}{2}\log 2 = \log a \Rightarrow n = \frac{2}{\log 2}\log a .$$

**Exemplo 1**

Se $a$ tem 1000 dígitos então $a \leq 10^{1000}$. Assim,

$$n \leq \frac{2}{\log 2}\log 10^{1000} = \frac{2000}{\log 2} \cong 6643$$

O algoritmo chega ao resultado em, no máximo, 6643 passos.

**Exercícios**

Resolva os seguintes exercícios:

1. Determine, usando o algoritmo de Euclides os seguintes MDC's:
   (i) $MDC\{24, 138\}$ (ii) $MDC\{143, 227\}$
   (iii) $MDC\{306, 657\}$ (iv) $MDC\{12.378, 3054\}$
2. Mostre que: Sejam $a, b, c$ inteiros não nulos. Se $a$ divide $b$ e $a$ divide $c$, então $a$ divide $(b \pm c)$. (vale a recíproca?)
3. Seja $r \neq 0$ com $r \in \mathbb{Z}$ uma raiz inteira do polinômio $x^2 + ax + b$, onde $a, b$ são inteiros. Mostre que $r$ é divisor de $b$.
4. Seja $a$ um inteiro ímpar. Mostre que $a^2 - 1$ é sempre divisível por 8.
5. Sejam $a_1, a_2, \cdots, a_n$ inteiros positivos. Generalize a noção de MDC de dois inteiros definindo (de modo similar) $MDC\{a_1, a_2, \cdots, a_n\}$.

# Aula 6 – As subestruturas ideais de $\mathbb{Z}$: MDC e MMC

### Metas

Nesta aula apresentaremos a noção de ideal de $\mathbb{Z}$. demonstrando o Teorema dos ideais principais e relacionando ideais MDC e MMC.

### Objetivos

- Definir a noção de ideal nos inteiros, dando exemplos;
- Caracterizar, através do Teorema dos ideais principais, os ideais de $\mathbb{Z}$;
- Demonstrar a existência de MDC e MMC em $\mathbb{Z}$, usando o Teorema dos ideais principais.

## Introdução

Na aula anterior, definimos o $\text{mdc}(a, b)$ de dois inteiros $a$ e $b$, mostramos algumas propriedades e apresentamos o Algoritmo de Euclides para a determinação de $\text{mdc}(a, b)$. Nesta aula vamos apresentar uma visão algébrica de $\mathbb{Z}$ através dos chamados ideais de $\mathbb{Z}$. Ideais em um anel são subconjuntos que possuem certas propriedades, como veremos um pouco a frente, nesta aula. Podemos dizer que eles representam subestruturas de um anel.

Usando o Teorema da Divisão de Euclides vamos provar que todo ideal $I$ de $\mathbb{Z}$ é principal, isto é, todo ideal $I$ de $\mathbb{Z}$ é da forma $I = \mathbb{Z} \cdot n$, para algum inteiro $n$. A partir desse fato, de que todo ideal é gerado por um único elemento (Teorema dos ideais principais), vamos inferir conclusões a respeito do mdc e mmc de dois inteiros.

Bom, este foi um panorama geral do que acontecerá nesta aula. Agora, vamos iniciar com a definição de ideal.

## Ideais em $\mathbb{Z}$

Seja $n$ um dado número inteiro. Considere o subconjunto $I$ de $\mathbb{Z}$, formado por todos os múltiplos inteiros de $n$.

Usaremos a seguinte notação para esse subconjunto:

$$I = \mathbb{Z} \cdot n = \{k \cdot n \mid k \in \mathbb{Z}\}\,.$$

Vamos destacar em seguida, três propriedades essenciais que o subconjunto $I = \mathbb{Z} \cdot n$ satisfaz.

Propriedades de $I = \mathbb{Z} \cdot n$

(1) $0 \in I$

(2) Para todo $x, y \in I$, tem-se $(x - y) \in I$

(3) $\mathbb{Z} \cdot I \subseteq I$, isto é, para todo $r \in \mathbb{Z}$ e para todo $x \in I$, tem-se $r \cdot x \in I$

Vamos demonstrar essas propriedades.

(1) $0 = 0 \cdot n \in I = \mathbb{Z} \cdot n$

(2) Se $x = r \cdot n$ e $y = s \cdot n$ então em $I = \mathbb{Z} \cdot n$, temos:

$$x - y = r \cdot n - s \cdot n = (r - s) \cdot n \in I = \mathbb{Z} \cdot n\,.$$

(3) Para todo $r \in \mathbb{Z}$ e $x = k \cdot n \in I = \mathbb{Z} \cdot n$, tem-se

$$r \cdot x = r \cdot (k \cdot n) = (r \cdot k) \cdot n \in I\ .$$

O conjunto $\mathbb{Z} \cdot n$ é um exemplo de ideal de $\mathbb{Z}$. Em geral,

Definição 1 (Ideal de $\mathbb{Z}$)
Um subconjunto $I$ de $\mathbb{Z}$ satisfazendo as três propriedades acima é dito uma substrutura ideal de $\mathbb{Z}$ ou, simplesmente, um ideal de $\mathbb{Z}$ .

Assim, $I \subset \mathbb{Z}$ é uma subestrutura ideal de $\mathbb{Z}$ se:

1. $0 \in I$
2. Para todo $x, y \in I$, tem-se $(x - y) \in I$
3. $\mathbb{Z} \cdot I \subset I$

Lembrando, novamente, que $\mathbb{Z} \cdot I \subset I$ é uma maneira resumida de dizer que para todo $r \in \mathbb{Z}$ e todo $x \in I$ temos $rx \in I$.

Exemplo **17**

Nós mostramos, acima, que $I = \mathbb{Z} \cdot n$ é um ideal de $\mathbb{Z}$. Assim, $\{0\} = \mathbb{Z} \cdot 0$ e $\mathbb{Z} = \mathbb{Z} \cdot 1$ são dois ideais de $\mathbb{Z}$ chamados de ideais triviais de $\mathbb{Z}$.

O ideal $I = \mathbb{Z} \cdot n$ é chamado de ideal principal gerado por $n$.

Exemplo **18**

Sejam $a, b \in \mathbb{Z}$ e seja $J$ o subconjunto

$$J = \mathbb{Z} \cdot a + \mathbb{Z} \cdot b = \{m = k \cdot a + s \cdot b \mid k, s \in \mathbb{Z}\}\,.$$

O conjunto $J$ é chamado conjunto gerado por $a$ e $b$ em $\mathbb{Z}$. Vamos provar que $J$ é um ideal de $\mathbb{Z}$ (chamado de ideal gerado por $a$ e $b$), contendo os ideais principais $\mathbb{Z} \cdot a$ e $\mathbb{Z} \cdot b$.

1. $0 \in J$, pois $0 = 0 \cdot a + 0 \cdot b \in J$.

2. Para todo $x, y \in J$, tem-se $(x - y) \in J$

   Seja $x = r \cdot a + s \cdot b$, e seja $y = r' \cdot a + s' \cdot b$, dois elementos de $J$. Daí segue que

   $$x - y = (r \cdot a + s \cdot b) - (r' \cdot a + s' \cdot b) = (r - r') \cdot a + (s - s') \cdot b \in J\,.$$

3. $\mathbb{Z} \cdot J \subset J$.

   Seja $m \in \mathbb{Z}$ e $x = r \cdot a + s \cdot b \in J$. Daí segue que

   $$m \cdot x = m \cdot (r \cdot a + s \cdot b) = (m \cdot r) \cdot a + (m \cdot s) \cdot b \in J\,.$$

   Alem disso, $\mathbb{Z} \cdot a \subset J$, pois $r \cdot a = r \cdot a + 0 \cdot b \in J$ para todo $r \in \mathbb{Z}$. Analogamente $\mathbb{Z} \cdot b \subset J$.

   Assim, o ideal $J = \mathbb{Z} \cdot a + \mathbb{Z} \cdot b$ contem os ideais principais $\mathbb{Z} \cdot a$ e $\mathbb{Z} \cdot b$.

**Atividades**

1. Verifique qual dos seguintes subconjuntos $I \subset \mathbb{Z}$ é (ou não) ideal de $\mathbb{Z}$.

   (a) $I = \{m \in \mathbb{Z} \mid m \text{ é divisor de } 24\}$

   (b) $I = \{m \in \mathbb{Z} \mid m \text{ é múltiplo de } 24\}$

   (c) $I = \{m \in \mathbb{Z} \mid m \text{ é múltiplo comum de } 18 \text{ e } 24\}$

   (d) $I = \{m \in \mathbb{Z} \mid (21) \cdot m \text{ é múltiplo de } 9\}$

2. Generalize o Exemplo 17 para:

$$J = \mathbb{Z}\cdot a_1+\mathbb{Z}\cdot a_2+\cdots+\mathbb{Z}\cdot a_k = \{m = r_1\cdot a_1+r_2\cdot a_2+\cdots+r_k\cdot a_k \mid r_i \in \mathbb{Z}\}$$

mostrando que $J$ é um ideal de $\mathbb{Z}$.

O conjunto $J = \mathbb{Z}\cdot a_1 + \mathbb{Z}\cdot a_2 + \cdots + \mathbb{Z}\cdot a_k$ é o ideal gerado por $a_1, a_2, \cdots, a_k$.

## Teorema dos Ideais Principais em $\mathbb{Z}$

Quando definimos ideal de $\mathbb{Z}$, observamos que, para todo $n \in \mathbb{Z}$, $\mathbb{Z}\cdot n$ é um ideal de $\mathbb{Z}$. Ideais deste tipo são chamados ideais principais.

Vimos também que, para todo $a, b \in \mathbb{Z}$, o conjunto $\mathbb{Z}\cdot a + \mathbb{Z}\cdot b$ é um ideal de $\mathbb{Z}$, chamado ideal gerado por $a$ e $b$. Analogamente, podemos ideais gerados por um número qualquer de elementos.

Aqui se coloca uma questão: se um ideal é gerado por, por exemplo, 2 elementos, ele pode ser escrito como ideal principal? Por exemplo, $\mathbb{Z}\cdot 30+\mathbb{Z}\cdot 20$ pode ser escrito como $\mathbb{Z}\cdot n$, para algum $n$?

A resposta é sim. É fácil ver que $\mathbb{Z}\cdot 30 + \mathbb{Z}\cdot 20 = \mathbb{Z}\cdot 10$. Veja bem,

$$10 = 30\cdot 1 + 20\cdot(-1) \Rightarrow 10 \in \mathbb{Z}\cdot 30 + \mathbb{Z}\cdot 20\ .$$

Pela propriedade (3) da definição de ideal, se $J$ é ideal e $10 \in J$ então $\mathbb{Z}\cdot 10 \subset J$. Assim, temos que $\mathbb{Z}\cdot 10 \subset \mathbb{Z}\cdot 30 + \mathbb{Z}\cdot 20$.

Por outro lado, se $x \in \mathbb{Z}\cdot 30 + \mathbb{Z}\cdot 20$ então existem $a, b \in \mathbb{Z}$ tais que

$$x = 30a + 20b = 10(3a + 2b) \in \mathbb{Z}\cdot 10 \Rightarrow \mathbb{Z}\cdot 30 + \mathbb{Z}\cdot 20 \subset \mathbb{Z}\cdot 10\ .$$

A conclusão é que o ideal gerado por 20 e 30 é principal: é o ideal principal $\mathbb{Z}\cdot 10$. Observe também que $10 = \text{mdc}(20, 30)$. Isto não é coincidência, como veremos mais tarde.

O teorema a seguir mostra que o mesmo é verdade para qualquer ideal de $\mathbb{Z}$. Esta é uma propriedade algébrica importante do anel dos inteiros. Domínios de integridade que têm esta propriedade são chamados *Domínios principais*. Haverá uma aula dedicada aos domínios principais mais tarde. Mas vamos voltar aos inteiros:

Teorema 1 (Teorema dos Ideais Principais)
Todo ideal de $\mathbb{Z}$ é principal

*Demonstração:*

Seja $J$ um ideal qualquer de $\mathbb{Z}$. Temos que demonstrar que existe $d \in \mathbb{Z}$ tal que $J = \mathbb{Z} \cdot d$.

Se $J = \{0\}$ então $J = \mathbb{Z} \cdot 0$ é principal. Vamos assumir que $J \neq \{0\}$.

Observe que, como $0 \in J$ temos:

$$\begin{array}{rcrcl} 0, x \in J & \Longrightarrow & 0 - x & = & -x \in J \\ 0, -x \in J & \Longrightarrow & 0 - (-x) & = & x \in J\,. \end{array}$$

Assim,

$$x \in J \Longleftrightarrow (-x) \in J\,.$$

Portanto,

$$J = J^- \cup \{0\} \cup J^+$$

onde

$$J^+ = \{x \in J \mid x > 0\} \quad \text{e} \quad J^- = \{x \in J \mid x < 0\}\,.$$

Vale também que $J^- = -(J^+)$.

Assim, $J \neq \{0\}$ implica $J^+$ e $J^-$ são não vazios e podemos escolher, pela boa ordenação de $\mathbb{Z}$, o primeiro (menor) elemento $d \in J^+$.

Portanto $d = \min J^+$ é único inteiro $d$ tal que $0 < d \leq x$, para todo $x \in J^+$.

Vamos provar que $J = \mathbb{Z} \cdot d$.

Primeiramente, $d \in J^+ \subset J$ implica $\mathbb{Z} \cdot d \subset J$, pela propriedade (3) que define ideal. Assim, basta provar que $J \subset \mathbb{Z} \cdot d$.

Como $\mathbb{Z} \cdot d$ é ideal de $\mathbb{Z}$, se provarmos que $J^+ \subset \mathbb{Z} \cdot d$, teremos:

$$J = J^- \cup \{0\} \cup J^+ \subset \mathbb{Z} \cdot d\,.$$

Seja $y \in J^+$. Pela escolha de $d$, temos $0 < d \leq y$. Se $d = y$, temos $y \in \mathbb{Z} \cdot d$. Vamos assumir $d \neq y$. Assim, $0 < d < y$. Pelo teorema da divisão de Euclides, existem $q, r \in \mathbb{Z}$ tais que

$$y = q \cdot d + r, \quad 0 \leq r < d\,.$$

Vamos provar que $r = 0$ e, portanto, $y = q \cdot d \in \mathbb{Z} \cdot d$.

Vamos supor, por absurdo, que $r > 0$. Então,

$$y = q \cdot d + r \Longrightarrow r = y - q \cdot d\,.$$

Mas $y \in J$ e $q \cdot d \in \mathbb{Z} \cdot d \subset J$ implica $r = y - q \cdot d \in J$, pela propriedade (2), da definição de ideal.

Mas

$$0 < r < d, r \in J \Longrightarrow r \in J^+ \text{ e } r < d\,,$$

o que contraria a minimalidade de $d = \min J^+$. Assim, essa contradição nos diz que $r = 0$ e $y = q \cdot d \in J$.

De $\mathbb{Z} \cdot d \subset J$ e $J \subset \mathbb{Z} \cdot d$, temos $J = \mathbb{Z} \cdot d$, como queríamos demonstrar.

□

A demonstração do teorema nos diz que $J = \mathbb{Z} \cdot a + \mathbb{Z} \cdot b = \mathbb{Z} \cdot d$, onde $d = \min J^+$, o menor elemento positivo de $J$.

Da mesma forma, o ideal de $J = \mathbb{Z} \cdot a_1 + \mathbb{Z} \cdot a_2 + \cdots + \mathbb{Z} \cdot a_k$, gerado por $a_1, a_2, \cdots, a_k$, inteiros não nulos, pode ser expresso por

$$J = \mathbb{Z} \cdot a_1 + \mathbb{Z} \cdot a_2 + \cdots + \mathbb{Z} \cdot a_k = \mathbb{Z} \cdot d, \quad d = \min J^+\,.$$

Aqui cabe a pergunta: Qual a relação desse número $d = \min J^+$ com os geradores de $J$?

Se $\mathbb{Z} \cdot d = \mathbb{Z} \cdot a + \mathbb{Z} \cdot b$, mostraremos que $d = \text{mdc}(a, b)$. Mais geralmente, se $\mathbb{Z} \cdot d = \mathbb{Z} \cdot a_1 + \mathbb{Z} \cdot a_2 + \cdots + \mathbb{Z} \cdot a_k$, mostraremos que $d = \text{mdc}(a_1, a_2, \cdots, a_k)$.

Como o inteiro $d = \text{mdc}(a, b)$, satisfaz a igualdade estrutural de ideais $\mathbb{Z} \cdot a + \mathbb{Z} \cdot b = \mathbb{Z} \cdot d$, então, $d \in Z \cdot a + \mathbb{Z} \cdot b$ e, portanto, $d = r \cdot a + s \cdot b$, para alguns inteiros $r$ e $s$. Este fato nos será bastante útil no futuro.

Exemplo **19**

$\text{mdc}(18, 24) = d = 6$. Nesse caso, podemos escrever

$$d = 6 = (-1) \cdot 18 + (1) \cdot 24 \quad (r = -1,\ s = 1)$$

ou ainda

$$d = 6 = (-5) \cdot 18 + (24) \cdot 4 \quad (r = -5,\ s = 4)$$

Portanto, os números $r$ e $s$ não são únicos e o número $d = \text{mdc}(a, b)$ pode ser expresso de mais de uma maneira na forma $d = ra + sb$ com $r, s \in \mathbb{Z}$.

**Atividades**

1. Encontre $d$ tal que $\mathbb{Z} \cdot d = \mathbb{Z} \cdot a + \mathbb{Z} \cdot b$, onde $a = 84$ e $b = 30$. Encontre $r, s \in \mathbb{Z}$ tal que $d = ra + sb$.

## O $\mathrm{mdc}(a,b)$ é o gerador de $\mathbb{Z}\cdot a+\mathbb{Z}\cdot b$

Agora vamos provar o seguinte teorema

Teorema 2

Sejam $a$ e $b$ inteiros não nulos dados e seja $d>0$ um número inteiro. Então

$$\mathbb{Z}\cdot a+\mathbb{Z}\cdot b=\mathbb{Z}\cdot d \Longleftrightarrow d=\mathrm{mdc}(a,b)\,.$$

*Demonstração:*

($\Longrightarrow$) Vamos supor $\mathbb{Z}\cdot a+\mathbb{Z}\cdot b=\mathbb{Z}\cdot d$ e mostrar que $d=\mathrm{mdc}(a,b)$.

Lembre-se que na Aula 5 mostramos que o conceito de $mdc\{a,b\}=d$ de dois números não nulos $a$ e $b$ é equivalente ao seguinte:

(i) $d$ é um divisor comum de $a$ e $b$

(ii) Se $d'$ é um divisor comum de $a$ e $b$ então $d'$ também é divisor de $d$.

Vamos usar aqui essa caracterização de mdc.

Primeiro observe que $\mathbb{Z}\cdot a+\mathbb{Z}\cdot b=\mathbb{Z}\cdot d$ implica $\mathbb{Z}\cdot a\subset\mathbb{Z}\cdot d$ e $\mathbb{Z}\cdot b\subset\mathbb{Z}\cdot d$.

De $\mathbb{Z}\cdot a\subset\mathbb{Z}\cdot d$ implica $a\in\mathbb{Z}\cdot d$ o que implica que $d$ é divisor de $a$. De $\mathbb{Z}\cdot b\subset\mathbb{Z}\cdot d$ implica $b\in\mathbb{Z}\cdot d$ o que implica $d$ é divisor de $b$.

Assim, concluimos que $d$ é divisor comum de $a$ e $b$.

Agora, a segunda parte: seja $d'$ um divisor comum qualquer de $a$ e $b$. Vamos provar que $d'$ também é divisor de $d$.

$$\begin{array}{rcl} d' \text{ divisor de } a & \Longrightarrow & \exists\ q_1'\in\mathbb{Z} \text{ tal que } a=q_1'\cdot d' \\ d' \text{ divisor de } b & \Longrightarrow & \exists\ q_2'\in\mathbb{Z} \text{ tal que } b=q_2'\cdot d' \end{array}$$

Assim, $\mathbb{Z}\cdot a\subseteq\mathbb{Z}\cdot d'$ e $\mathbb{Z}\cdot b\subseteq\mathbb{Z}\cdot d'$ e isso nos diz que

$\mathbb{Z}\cdot d=\mathbb{Z}\cdot a+\mathbb{Z}\cdot b\subseteq\mathbb{Z}\cdot d'\Longrightarrow d\in\mathbb{Z}\cdot d\subseteq\mathbb{Z}\cdot d'\Longrightarrow d\in\mathbb{Z}\cdot d'\Longrightarrow\exists\, r\in\mathbb{Z}$ tal que $d=r\cdot d'\Longrightarrow d'$ também é divisor de $d$.

Logo $d>0$ é de fato o $\mathrm{mdc}(a,b)$.

($\Longleftarrow$) Assumiremos $\mathrm{mdc}(a,b)=d$. Devemos provar que $\mathbb{Z}\cdot a+\mathbb{Z}\cdot b=\mathbb{Z}\cdot d$. Usaremos a unicidade do MDC.

Pelo teorema do ideal principal, existe $d'$ tal que $\mathbb{Z}\cdot a+\mathbb{Z}\cdot b=\mathbb{Z}\cdot d'$. Pela parte 1 dessa demonstração, temos $d'=\mathrm{mdc}(a,b)$ e pela unicidade do $\mathrm{mdc}(a,b)$ temos que $d=d'$ e $\mathbb{Z}\cdot a+\mathbb{Z}\cdot b=\mathbb{Z}\cdot d$.

□

Como observamos antes, uma conseqüência direta que nos será muito útil é o seguinte:

Corolário 1
Sejam $a$ e $b$ dois inteiros não nulos e seja $d = \text{mdc}(a, b)$. Então existe $r, s \in \mathbb{Z}$ tais que $d = ra + sb$.

O Teorema 2 acima vale para mais de dois números, isto é, dados inteiros não nulos $a_1, a_2, \cdots, a_k$ e $d = \text{mdc}(a_1, a_2, \cdots, a_k)$ temos $\mathbb{Z} \cdot a_1 + \mathbb{Z} \cdot a_2 + \cdots + \mathbb{Z} \cdot a_k = \mathbb{Z} \cdot d$ e existem $r_1, r_2, \cdots, r_k \in \mathbb{Z}$ tais que $d = r_1 \cdot a_1 + r_2 \cdot a_2 + \cdots r_k \cdot a_k$. A demonstração é análoga à demonstração do Teorema 2.

**Atividades**

1. Descreva os seguintes subconjuntos $J$ de $\mathbb{Z}$.
   (a) $J = \mathbb{Z} \cdot 36 + \mathbb{Z} \cdot 25$.
   (b) $J = \mathbb{Z} \cdot 18 + \mathbb{Z} \cdot 24 + \mathbb{Z} \cdot 21$.
   (c) $J = \mathbb{Z} \cdot 105 + \mathbb{Z} \cdot 52$.

## O mmc de dois inteiros

Agora vamor relacionar o mmc de dois inteiros $a$ e $b$ aos ideais gerados por $a$ e $b$. Como a interseção de ideais é sempre um ideal, então $\mathbb{Z} \cdot a \cap \mathbb{Z} \cdot b$ é um ideal de $\mathbb{Z}$. Pelo Teorema 1, este ideal é principal. O próximo teorema nos diz que $\mathbb{Z} \cdot a \cap \mathbb{Z} \cdot b$ é o ideal principal gerado por $\text{mmc}(a, b)$.

Teorema 3
Sejam $a$ e $b$ dois dados inteiros não nulos e seja $M > 0$ tal que $\mathbb{Z} \cdot a \cap \mathbb{Z} \cdot b = \mathbb{Z} \cdot M$ (existe tal $M > 0$, pelo teorema dos ideais principais). Então $M$ é o menor múltiplo comum positivo de $a$ e $b$.

*Demonstração:*

Sejam $a$ e $b$ dois inteiros não nulos e $I = \mathbb{Z} \cdot a$ e $J = \mathbb{Z} \cdot b$ os ideais principais gerados, respectivamente, por $a$ e $b$.

Temos que $I \cap J = \mathbb{Z} \cdot a \cap \mathbb{Z} \cdot b$ é também um ideal de $\mathbb{Z}$ (ver Exercício 1).

Pelo teorema dos ideais principais, existe $M > 0$ tal que $I \cap J = \mathbb{Z} \cdot a \cap \mathbb{Z} \cdot b = \mathbb{Z} \cdot M$.

Vamos provar que $M$ é o menor múltiplo comum positivo de $a$ e $b$.

$$\mathbb{Z} \cdot a \cap \mathbb{Z} \cdot b = \mathbb{Z} \cdot M \Longrightarrow \mathbb{Z} \cdot M \subset \mathbb{Z} \cdot a \quad \text{e} \quad \mathbb{Z} \cdot M \subset \mathbb{Z} \cdot b\,.$$

Como $M \in \mathbb{Z} \cdot M$, então $M \in \mathbb{Z} \cdot a$ e $M \in \mathbb{Z} \cdot b$, o que implica que existem $r, s \in \mathbb{Z}$ tais que $M = ra$ e $M = sb$, isto é, $M$ é um múltiplo comum de $a$ e $b$.

Seja $M' > 0$ um qualquer múltiplo comum de $a$ e $b$. Vamos provar que $M'$ é múltiplo de $M$ (e portanto $M' \geq M$).

De fato, $M'$ múltiplo comum de $a$ e $b$ implica que existem $r', s' \in \mathbb{Z}$ tais que $M' = r' \cdot a$ e $M' = s' \cdot b$. Portanto,

$$M' \in \mathbb{Z} \cdot a \text{ e } M' \in \mathbb{Z} \cdot b \Rightarrow M' \in \mathbb{Z} \cdot a \cap \mathbb{Z} \cdot b = \mathbb{Z} \cdot M \Rightarrow M' \in \mathbb{Z} \cdot M \ ,$$

o que implica $M' = t \cdot M$, para algum inteiro $t > 0$, ou seja, $M'$ é múltiplo de $M$, o que completa a demonstração.

□

Embora já estejamos nos referindo ao mínimo múltiplo comum de dois inteiros, vamos fazer uma definição formal.

Definição 2 (Mínimo múltiplo comum)
Sejam $a$ e $b$ dois dados inteiros não nulos. Dizemos que $M$ é o *mínimo múltiplo comum* de $a$ e $b$, denotado $M = \text{mmc}(a, b)$, se $M > 0$ e $M$ é o menor múltiplo comum positivo de $a$ e $b$.

O Teorema 3 mostra a existência do $\text{mmc}(a, b)$ (através do teorema dos ideais principais) como o inteiro positivo $M > 0$ gerador do ideal $\mathbb{Z} \cdot a \cap \mathbb{Z} \cdot b$, isto é, $\mathbb{Z} \cdot a \cap \mathbb{Z} \cdot b = \mathbb{Z} \cdot M$. Alem disso, vimos na demonstração do teorema que o $\text{mmc}(a, b)$ não só é o menor múltiplo comum de $a$ e $b$ como também é divisor de qualquer outro múltiplo comum de $a$ e $b$. Podemos, assim, caracterizar o $\text{mmc}(a, c)$ pelas seguintes propriedades:

1. $M$ é múltiplo de $a$ e $b$.
2. Se $M'$ é um múltiplo comum de $a$ e $b$, então $M'$ é múltiplo de $M$.

Alguns autores usam a caracterização acima como definição de $\text{mmc}(a, b)$.

Exemplo **20**
Sejam $a = 6$ e $b = 9$. Temos:

$$\begin{aligned}
&\mathbb{Z} \cdot 6 = \{\cdots, -6, 0, 6, 12, 18, 24, 30, 36, 42, \cdots\} \\
&\mathbb{Z} \cdot 9^{+} = \{\cdots, -9, 0, 9, 18, 27, 36, 45, 54, \cdots\} \\
&\mathbb{Z} \cdot 6 \cap \mathbb{Z} \cdot 9 = \{\cdots, -18, 0, 18, 36, 54, \cdots\} = \mathbb{Z} \cdot 18 \ .
\end{aligned}$$

Assim, $\text{mmc}(6, 9) = 18$.

### Atividades

1. Escreva os conjuntos $\mathbb{Z} \cdot 12$ e $\mathbb{Z} \cdot 15$. Determine que $\mathbb{Z} \cdot 12 \cap \mathbb{Z} \cdot 15$ e verifique $\text{mmc}(12, 15) = 60$.

2. Mostre que $a$ divide $b$ implica em $\text{mmc}(a, b) = b$.

### Relação entre o mdc e o mmc de dois inteiros

Podemos sempre determinar o mmc de dois inteiros como no exemplo acima: escrevendo vários elementos dos conjuntos $\mathbb{Z} \cdot a$ e $\mathbb{Z} \cdot b$ e determinando o primeiro elemento da interseção. No entanto, este método é computacionalmente impraticável para inteiros grandes.

Felizmente, há maneiras muito mais rápidas de determinarmos o mmc de dois inteiros. Há uma relação simples entre o mmc e o mdc de dois inteiros, que demonstraremos a seguir.

Teorema 4
Sejam $a$ e $b$ inteiros positivos. Então vale que

$$\text{mmc}(a, b).\, \text{mdc}(a, b) = ab$$

Assim, uma vez calculado o $\text{mdc}(a, b)$, que pode ser feito pelo Algoritmo de Euclides, a fórmula acima fornece facilmente o $\text{mmc}(a, b)$.

Retornando ao exemplo anterior, é fácil ver que $\text{mdc}(6, 9) = 3$. Então:

$$\text{mmc}(6, 9) = \frac{6 \cdot 9}{\text{mdc}(6, 9)} = \frac{54}{3} = 18$$

*Demonstração do Teorema.*

Sejam $a$ e $b$ inteiros positivos, $m = \text{mmc}(a, b)$ e $d = \text{mdc}(a, b)$.

Lembre-se que o $\text{mmc}(a, b)$ é divisor de qualquer múltiplo comum de $a$ e $b$.

Como $ab$ é múltiplo comum de $a$ e $b$, então $m$ divide $ab$. Logo $\frac{ab}{m}$ é um número inteiro. Seja $g = \frac{ab}{m}$. Vamos provar que $g = d$, isto é, $\frac{ab}{m} = d$, o que implica em $ab = md$.

Vamos mostrar que $g = \text{mdc}(a, b)$ mostrando que:

1. $g$ é divisor comum de $a$ e $b$.

2. Se $f$ é divisor comum de $a$ e $b$ então $f \mid g$.

Como vimos, estas duas propriedades demosntram que $g = \text{mdc}(a, b)$. Vamos, então, prová-las.

1. De $\frac{ab}{m} = g$ segue que
$$\frac{a}{g} = \frac{m}{b} \quad \text{e} \quad \frac{b}{g} = \frac{m}{a} ,$$
o que mostra que $\frac{a}{g}$ e $\frac{b}{g}$ são inteiros, isto é, $g$ é divisor comum de $a$ e $b$.

2. Seja $f$ um inteiro tal que $f \mid a$ e $f \mid b$. Vamos mostrar que $f \mid g$. Como $\frac{a}{f}$ e $\frac{b}{f}$ são inteiros, então
$$a \mid a\left(\frac{b}{f}\right) \text{ e } b \mid b\left(\frac{a}{f}\right)$$
implica em que $\frac{ab}{f}$ é múltiplo comum de $a$ e $b$.
Como $m = \text{mmc}(a, b)$, então
$$m \mid \frac{ab}{f} .$$
Mas $g = \frac{ab}{m}$, logo $m = \frac{ab}{g}$ e temos que
$$\frac{ab}{g} \mid \frac{ab}{f}$$
isto é
$$\frac{ab}{f} \div \frac{ab}{g} = \frac{g}{f} \quad \text{é um inteiro} .$$
Portanto $f \mid g$, o que completa a demosntração.

□

Note que se $a$ e $b$ não forem inteiros positivos então a igualdade $ab = \text{mdc}(a, b)\,\text{mmc}(a, b0$ não é mais válida, uma vez que $\text{mdc}(a, b) \geq 0$ e $\text{mmc}(a, b) \geq 0$, por definição. No entanto, a igualdade continua válida para $|a|$ e $|b|$.

Um caso particular interessante do Teorema 4 é quando $\text{mdc}(a, b) = 1$. Neste caso, vale que
$$\text{mmc}(a, b) = ab .$$

Definição 3 (Inteiros primos entre si)
Dizemos que dois inteiros $a$ e $b$ são primos entre si, ou que $a$ e $b$ são relativamente primos, quando $\text{mdc}(a, b) = 1$.

## Atividades

1. Escolha alguns pares de inteiros positivos $a$ e $b$, calcule $\text{mdc}(a, b)$ e $\text{mmc}(a, b)$. Verifique que $\text{mdc}(a, b)\,\text{mmc}(a, b) = ab$.

2. Mostre que $a$ divide $b$ implica em $\text{mmc}(a, b) = b$.

3. Mostre que se $a$ e $b$ são primos entre si, então $\text{mmc}(a, b) = ab$.

## Mais três teoremas sobre o mdc

Você ainda tem fôlego para mais alguns teoremas? Nesta seção, para terminar a aula, provaremos mais três teoremas muito interessantes sobre o mdc.

Teorema 5
Se $d = \text{mdc}(a, b)$ então $\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

*Demonstração.* Quero provar que $\frac{a}{d}$ e $\frac{b}{d}$ não têm divisor comum. Se $f > 1$ fosse um divisor comum destes inteiros, então

$$f \mid \frac{a}{d} \quad \text{e} \quad f \mid \frac{b}{d}$$

o que implica em

$$df \mid a \quad \text{e} \quad df \mid b\,.$$

Portanto, teríamos que $df$ é divisor comum de $a$ e $b$. Como $f > 1$ então $df > d$, o que contraria o fato de que $d$ é o maior dividor comum. Assim, provamos que não há $f > 1$ divisor comum de $\frac{a}{d}$ e $\frac{b}{d}$.

□

O próximo teorema é uma espécie de recíproca deste último.

Teorema 6
Se $c > 0$, $c \mid a$, $c \mid b$ e $\text{mdc}\left(\frac{a}{c}, \frac{b}{c}\right) = 1$ então $c = \text{mdc}(a, b)$.

*Demonstração.* Sejam $a$ $b$ inteiros positivos e seja $d = \text{mdc}(a, b)$.

Como $c \mid a$ e $c \mid b$, então $c$ é um dividor comum de $a$ e $b$,o que implica em $c \mid d$, isto é, $\frac{d}{c}$ é um inteiro.

De

$$\frac{d}{c}\frac{a}{d} = \frac{a}{c} \quad \text{e} \quad \frac{d}{c}\frac{b}{d} = \frac{b}{d}$$

resulta que $\frac{d}{c}$ é um divisor comum de $\frac{a}{d}$ e $\frac{b}{d}$. Mas $\frac{a}{d}$ e $\frac{b}{d}$ são relativamente primos por hipótese, seus únicos divisores comuns são $\pm 1$, assim

$$\frac{d}{c} = 1 \Rightarrow c = d$$

□

O próximo teorema nos diz que se um número divide o produto de dois números e é relativamente primo com um deles então divide o outro.

Teorema 7

Sejam $a$,$b$ e $c$ inteiros positivos. Se $a \mid bc$ e $\text{mdc}(a,b) = 1$ então $a \mid c$.

*Demonstração.* Como $\text{mdc}(a,b) = 1$ então $m = \text{mmc}(a,b) = ab$.

Como $a \mid bc$ (por hipótese) e $b \mid bc$ então $bc$ é múltiplo comum de $a$ e $b$. Assim $bc$ é múltiplo de $\text{mmc}(a,b) = ab$, isto é

$$ab \mid bc\ ,$$

o que resulta em $a \mid c$.

□

## Resumo

Nesta aula definimos ideal em $\mathbb{Z}$ e mostramos que o mdc e mmc de dois inteiros $a$ e $b$ são geradores de certos ideais em $\mathbb{Z}$. O $\text{mdc}(a,b)$ gera o ideal $\mathbb{Z} \cdot a + \mathbb{Z} \cdot b$, enquanto que o $\text{mmc}(a,b)$ gera o ideal $\mathbb{Z} \cdot a \cap \mathbb{Z} \cdot b$.

Mostramos que em $\mathbb{Z}$ todo ideal é principal, o que é uma propriedade algébrica muito importante dos inteiros.

demonstramos a relação entre o $\text{mdc}(a,b)$ e o $\text{mmc}(a,b)$ para dois inteiros $a$ e $b$:

$$\text{mmc}(a,b).\,\text{mdc}(a,b) = ab$$

Em particular, para $a$ e $b$ primos entre si, vale que

$$\text{mmc}(a,b) = ab\ .$$

## Exercícios

1. Sejam $I$ e $J$ dois dados ideais de $\mathbb{Z}$. Mostre que $I \cap J$ é um ideal de $\mathbb{Z}$.

2. Generalize o exercício anterior mostrando que

$$I_1, I_2, \cdots, I_k$$

ideais de $\mathbb{Z}$ implica

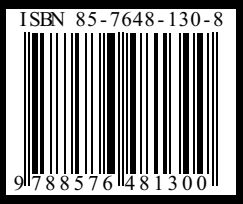
$$I_1 \cap I_2 \cap \cdots \cap I_k = I$$

também é ideal de $\mathbb{Z}$.

3. Generalize o exercício 2 acima mostrando que: se $\{I_k\}_{k\in\mathbb{N}}$ é uma coleção de ideais de $\mathbb{Z}$ então $I = \bigcap_{k=0}^{\infty} I_k$ também é ideal de $\mathbb{Z}$.

4. Demonstre a generalização do Teorema 2. Isto é, prove que dados inteiros não nulos $a_1, a_2, \cdots, a_k$ e $d = \text{mdc}(a_1, a_2, \cdots, a_k)$ temos $\mathbb{Z} \cdot a_1 + \mathbb{Z} \cdot a_2 + \cdots + \mathbb{Z} \cdot a_k = \mathbb{Z} \cdot d$ e existem $r_1, r_2, \cdots, r_k \in \mathbb{Z}$ tais que $d = r_1 \cdot a_1 + r_2 \cdot a_2 + \cdots r_k \cdot a_k$.

ISBN 85-7648-130-8




UENF
Universidade Estadual
do Norte Fluminense

UERJ

Universidade Federal Fluminense

Universidade Federal Rural
do Rio de Janeiro

UNIRIO

FAPERJ
Fundação Carlos Chagas Filho de Amparo
à Pesquisa do Estado do Rio de Janeiro

GOVERNO DO
Rio de Janeiro
SECRETARIA DE
CIÊNCIA E TECNOLOGIA

UAB
UNIVERSIDADE
ABERTA DO BRASIL

Ministério
da Educação

BRASIL
UM PAÍS DE TODOS
GOVERNO FEDERAL