Álgebra 1

Notas de Aula 2/2017

José Antônio O. Freitas

1 de setembro de 2017

Sumário

Prefácio

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

Revisão e ampliação das notas feita por José Antônio O. de Freitas.

[1] luizeduardosol@hotmail.com

1. Conceitos Básicos

Definição 1.0.1 Uma **proposição** é todo conjunto de palavras ou símbolos ao qual podemos atribuir um **valor lógico**.

Definição 1.0.2 Diz-se que o **valor lógico** de uma proposição é "verdade" (V) se a proposição é verdadeira ou "falsidade" (F) se a proposição é falsa.

■ **Exemplos 1.1** Julgue se as seguintes sentenças são ou não proposições:

1. Todo número primo é ímpar. Essa setença é uma proposição de valor lógico "Falsidade."
2. $x^2 + y^2 \geq 0$ para todos $x, y \in \mathbb{R}$. Esse setença é uma proposição de valor lógico "Verdade".
3. Amanhã irá chover. Essa sentença não é uma proposição. Não é possível atribuir um valor lógico a ela.

1.1 Princípio da não contradição e do terceiro excluído

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

Assim esses princípios afirmam que:

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

De modo geral vamos trabalhar com proposições da forma:

1. Se $\mathscr{H}$, então $\mathscr{T}$.
   Aqui $\mathscr{H}$ é chamado de hipótese e $\mathscr{T}$ de tese. Neste tipo de proposição iremos admitir que $\mathscr{H}$ é uma verdade e precisaremos provar que $\mathscr{T}$ é verdade. Ou seja precisamos construir um argumento que justifique $\mathscr{T}$ ser verdadeira à partir do fato de $\mathscr{H}$ ser verdadeira.
2. $\mathscr{H}$ se, e somente se, $\mathscr{T}$ ou $\mathscr{H}$ se, e só se, $\mathscr{T}$.
   Esse tipo de proposição será decomposta em duas proposições no formato anterior. Isto é:
   (a) Se $\mathscr{H}$, então $\mathscr{T}$.
   (b) Se $\mathscr{T}$, então $\mathscr{H}$.

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

2. Noções de Teoria de Conjuntos

2.1 Conceitos básicos

Um conjunto é uma "coleçã o" ou "família" de elementos.

Usaremos letras maiúsculas do alfabeto para denotar os conjuntos e denotaremos elementos de um dado conjunto por letras minúsculas do alfabeto.

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

$$x \in A.$$

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

$$x \notin A.$$

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

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

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

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

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

2.2 Descrição de um conjunto

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

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

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

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

2.3 Alguns conjuntos importantes

1. $\mathbb{N} = \{0,1,2,3,...\}$ o conjunto do números naturais.
2. $\mathbb{Z} = \{...,-2,-1,0,1,2,...\}$ o conjunto dos números inteiros.
3. $\mathbb{N}_0 = \{0,1,2,3,...\}$ o conjunto dos números inteiros não negativos.
4. $\mathbb{R}$ o conjunto dos números reais.
5. $\mathbb{R}^*$ o conjunto dos números reais não nulos.
6. $\mathbb{Q} = \left\{ \frac{p}{q} \mid p,q \in \mathbb{Z}, q \neq 0 \right\}$ o conjunto dos números racionais.

2.4 Propriedades dos conjuntos

Definição 2.4.1 Dados dois conjuntos A e B, dizemos que A e B são **iguais** se, e somente se, eles têm os mesmos elementos. Ou seja, para todo $x \in A$ temos que $x \in B$ e para todo $y \in B$ temos $y \in A$.

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

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

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

Definição 2.4.2 Se A e B são dois conjuntos, dizemos que A é um **subconjunto** de B ou que A **está contido** em B ou que B **contém** A se todo elemento de A for elemento de B. Ou seja, se para todo elemento $x \in A$, temos $x \in B$. Nesse caso, escrevemos $A \subseteq B$ ou $B \supseteq A$.

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

$A \subsetneq B$.

Nesse caso, dizemos que A é um **subconjunto próprio** de B.
Para dizer que A não está contido em B, escrevemos $A \nsubseteq B$
Usando a definição de continência de conjuntos podemos definir igualdade de conjuntos da seguinte forma:

dois conjuntos A e B são iguais se, e somente se, $A \subseteq B$ **e** $B \subseteq A$.

Ou seja,

se $A = B$ **então** $A \subseteq B$ **e** $B \subseteq A$.

Além disso,

se $A \subseteq B$ **e** $B \subseteq A$**, então** $A = B$.

Quando A e B não são iguais, escrevemos $A \neq B$. Para que $A \neq B$ devemos ter $A \nsubseteq B$ ou $B \nsubseteq A$. Isto é, precisamos encontrar algum elemento $x \in A$ tal que $x \notin B$ ou então encontrar $y \in B$ tal que $y \notin A$.

Proposição 2.4.1 Dados três conjuntos A, B e C temos:
1. $A \subseteq A$ (Reflexividade)
2. Se $A \subseteq B$ e $B \subseteq A$, então $A = B$. (Antissimetria)
3. Se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$. (Transitividade)

Considere os seguintes conjuntos:

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

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

Proposição 2.4.2 Seja A um conjunto. Então $\emptyset \subseteq A$.

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

2.5 Relações entre conjuntos

Definição 2.5.1 — Intersecção. Sejam A e B dois conjuntos. Definimos a **intersecção** de A e B como sendo o conjunto $A \cap B$ cujos elementos pertencem ao conjunto A e B simultaneamente. Assim,

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

■ **Exemplo 2.1** Sejam $A = \{1,2,3\}$, $B = \{2,3,4\}$ e $C = \{r,s,t\}$. Então

$$A \cap B = \{2,3\}$$
$$A \cap C = \emptyset.$$

Definição 2.5.2 — União. Sejam A e B dois conjuntos. Definimos a **união** de A com B como sendo o conjunto $A \cup B$, cujos elementos pertencem ao conjunto A ou ao conjunto B. Assim,

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

■ **Exemplo 2.2** Sejam $A = \{1,2,3\}$, $B = \{2,3,4\}$ e $C = \{r,s,t\}$. Então

$$A \cup B = \{1,2,3,4\}$$
$$A \cup C = \{1,2,3,r,s,t\}.$$

Proposição 2.5.1 Sejam A e B dois conjuntos. Então:

1. $(A \cap B) \subseteq A$;
2. $(A \cap B) \subseteq B$;
3. $A \subseteq A \cup B$;
4. $B \subseteq A \cup B$.

Prova: Para provar a primeira afirmação seja $x \in A \cap B$ um elemento qualquer. Da definição de interseção de conjuntos, Definição 2.5.1, temos $x \in A$ e $x \in B$. Assim podemos afirmar com certeza que $x \in A$. Logo todo elemente de $A \cap B$ também está em A, ou seja, $A \cap B \subseteq A$. De modo análogo prova-se a segunda afirmação sobre interseção.

Para a terceira afirmação, seja $x \in A$. Da definição de união de conjuntos, Definição 2.5.2, segue que $x \in A \cup B$. Logo todo elemento de A também está em $A \cup B$, ou seja, $A \subseteq (A \cup B)$. De modo análogo prova-se a quarta afirmação. ■

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

Definição 2.5.3 — União e Intersecção finita de conjuntos. Sejam $A_1, \ldots, A_n$ conjuntos. Então

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

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

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

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

Definição 2.5.4 Sejam A e B conjuntos. Se $A \cap B = \emptyset$, dizemos que A e B são **conjuntos disjuntos**.

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

$$C = A \sqcup B.$$

Proposição 2.5.2 Sejam A, B e C três conjuntos, então:

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

Prova:

1. Precisamos mostrar que
   i) $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$;
   ii) $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.
   Para provar i) seja $x \in A \cap (B \cup C)$. Logo $x \in A$ e $x \in B \cup C$. Agora, de $x \in B \cup C$, segue que $x \in B$ ou $x \in C$. Suponha que $x \in B$. Como $x \in A$ e $x \in B$, então $x \in A \cap B$. Assim, $x \in (A \cap B) \cup (A \cap C)$, ou seja, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Por outro lado, se $x \in C$, como $x \in A$, então $x \in A \cap C$ e daí $x \in (A \cap B) \cup (A \cap C)$, logo $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Portanto,

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

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

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

   Portanto

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

   como queríamos.
2. Análoga ao caso anterior.

■

Definição 2.5.5 — Diferença de Conjuntos. Dados dois conjuntos A e B, definimos a **diferença** dos conjuntos A e B, denotada por $A-B$ ou $A\backslash B$ como sendo o conjunto

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

■ **Exemplos 2.1** 1) Se $A=\{1,2,3,5,4\}$, $B=\{2,3,6,8\}$, então

$$A-B=\{1,4,5\}$$
$$B-A=\{6,8\}.$$

2) Se $A=\{2,4,6,8,10,...\}$, $B=\{3,6,9,12,15,...\}$, então

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

Proposição 2.5.3 Sejam A, B e C conjuntos não vazios. Então

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

Prova: Segue da definição de diferença de conjuntos. ■

Definição 2.5.6 — Complementar. Dados dois conjuntos A e E tais que $A\subseteq E$, definimos o **complementar** de A em E, denotado A^C ou $C_E(A)$, como

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

■ **Observações 2.1** 1. Se $A=E$, então $C_A(A)=\{x\in A \mid x\notin A\}=\emptyset$.
2. $(A^C)^C=\{x\in E \mid x\notin A^C\}=\{x\in E \mid x\in A\}=A$

■ **Exemplo 2.3** Sejam $A=\{1,2,3,4\}$ e $E=\{1,2,3,5,4,0,8,9\}$. Primeiro note que $A\subseteq E$, daí

$$A^C=C_E(A)=\{0,5,8,9\}.$$

Proposição 2.5.4 Sejam A, B e E conjuntos. Se $A\subseteq B\subseteq E$, então $C_E(B)\subseteq C_E(A)$.

Prova: Seja $x\in C_E(B)$. Assim $x\notin B$ e como $A\subseteq B$, então $x\notin A$. Daí por definição $x\in C_E(A)$, ou seja, $C_E(B)\subseteq C_E(A)$. ■

Proposição 2.5.5 Sejam A, B e E três conjunto tais que $A\subseteq E$ e $B\subseteq E$. Então:
1. $(A\cup B)^C=A^C\cap B^C$
2. $(A\cap B)^C=A^C\cup B^C$

Prova:
1. Seja $x\in(A\cup B)^C$. Logo $x\notin A\cup B$, assim $x\notin A$ e $x\notin B$. Daí, $x\in A^C$ e $x\in B^C$, isto é, $x\in A^C\cap B^C$. Desse modo,

$$(A\cup B)^C\subseteq A^C\cap B^C. \tag{2.1}$$

Por outro lado, se $x\in A^C\cap B^C$, então $x\in A^C$ e $x\in B^C$. Com isso, $x\notin A$ e $x\notin B$, ou seja, $x\notin A\cup B$, logo $x\in(A\cup B)^C$. Desse modo

$$A^C\cap B^C\subseteq(A\cup B)^C. \tag{2.2}$$

Portanto, de (2.1) e (2.2) temos

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

2. Seja $x \in (A \cap B)^C$. Logo $x \notin A \cap B$, assim $x \notin A$ ou $x \notin B$. Então $x \in A^C$ ou $x \in B^C$, isto é, $x \in A^C \cup B^C$. Desse modo,

$$(A \cap B)^C \subseteq A^C \cup B^C. \tag{2.3}$$

Por outro lado, se $x \in A^C \cup B^C$, então $x \in A^C$ ou $x \in B^C$. Daí, $x \notin A$ ou $x \notin B$, ou seja, $x \notin A \cap B$, logo $x \in (A \cap B)^C$. Desse modo

$$A^C \cup B^C \subseteq (A \cap B)^C. \tag{2.4}$$

Portanto, de (2.3) e (2.4) temos

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

■

Definição 2.5.7 — Produto Cartesiano. Dados dois conjuntos A e B, definimos o **produto cartesiano** de A por B como sendo o conjunto

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

Dados $(x,y), (z,t) \in A \times B$, temos

$$(x,y) = (z,t) \textbf{ se, e somente se, } x = z \textbf{ e } y = t.$$

■ **Exemplo 2.4** Sejam $A = \{1,2\}$ e $B = \{3,4\}$. Então

$$A \times B = \{(1,3),(1,4),(2,3),(2,4)\}$$
$$B \times A = \{(3,1),(3,2),(4,1),(4,2)\}$$

■ **Observaçao 2.1** Do Exemplo (2.4) vemos que em geral $A \times B \neq B \times A$.

Definição 2.5.8 — Conjunto Partes. Para qualquer conjunto A, indicamos por $\mathscr{P}(A)$ o conjunto

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

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

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

■ **Exemplos 2.2**
1. $A = \emptyset$, $\mathscr{P}(A) = \{\emptyset\}$;
2. $B = \{x\}$, $\mathscr{P}(B) = \{\emptyset, \{x\}\}$;
3. $C = \{a,b,c\}$, $\mathscr{P}(C) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, C\}$;
4. $D = \mathbb{R}$, $\mathscr{P}(D) = \{X \mid X \subseteq \mathbb{R}\}$, por exemplo $\mathbb{Q} \in \mathscr{P}(D)$.

3. Relações

3.1 Relações de equivalência

Definição 3.1.1 Seja A um conjunto não vazio e $R \subseteq A \times A$. Dizemos que R é uma **relação de equivalência** se:

i) Para todo $x \in A$, $(x,x) \in R$. *(Propriedade Reflexiva)*
ii) Se $(x,y) \in R$, então $(y,x) \in R$. *(Propriedade Simétrica)*
iii) Se $(x,y) \in R$ e $(y,z) \in R$, então $(x,z) \in R$. *(Propriedade Transitiva)*

Quando $R \subseteq A \times A$ é uma relação de equivalência, dizemos que R é uma relação de equivalência em A. Quando dois elementos $x, y \in A$ são tais que $(x,y) \in R$, dizemos que x e y **são relacionados** ou que x e y **estão relacionados**.

■ **Exemplos 3.1** 1) Seja A={1,2,3,4}. Temos

$$A \times A = \{(1,1);(1,2);(1,3);(1,4);(2,1);(2,2);(2,3);(2,4);$$
$$(3,1);(3,2);(3,3);(3,4);(4,1);(4,2);(4,3);(4,4)\}.$$

Quais dos seguintes conjuntos são exemplos de relações de equivalência?

- $R_1 = A \times A$
- $R_2 = \{(1,1);(2,2);(3,3)\}$
- $R_3 = \{(1,1);(2,2);(3,3);(4,4);(1,2);(2,1)\}$
- $R_4 = \{(1,1);(2,2);(3,3);(4,4)\}$
- $R_5 = \{(1,1);(2,2);(3,3);(4,4);(1,2);(2,1);(2,4);(4;2)\}$

■ **Solução:** *R_2 não é relação de equivalência pois $(4,4) \notin R_2$.*
R_5 não é relação de equivalência pois, por exemplo, $(1,4) \notin R_5$.
Os demais são exemplos de relações de equivalência.

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

■ **Solução:** *De fato,*

- *Para todo $x \in \mathbb{Z}$ temos $x = x$ daí $(x,x) \in R$.*
- *Se $(x,y) \in R$, então pela definição de R temos $x = y$. Logo $y = x$ e então $(y,x) \in R$.*
- *Se $(x,y) \in R$ e $(y,z) \in R$, então $x = y$ e $y = z$. Logo $x = z$ e assim $(x,z) \in R$ como queríamos.*

Portanto R é uma relação de equivalência sobre $\mathbb{Z}$.

3) Seja $A = \mathbb{Z}$ e tome $R = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x - y = 2k, \text{ para algum } k \in \mathbb{Z}\}$. Mostre que R é uma relação de equivalência sobre $\mathbb{Z}$.

■ **Solução:** *De fato,*

- *Para todo $x \in \mathbb{Z}$ temos $x - x = 2 \cdot 0$ e com isso $(x,x) \in R$.*
- *Se $(x,y) \in R$ então existe $k \in \mathbb{Z}$ tal que $x - y = 2k$. Agora $y - x = -(x-y) = -2k = 2(-k)$ e como $-k \in \mathbb{Z}$ segue que $(y,x) \in R$.*
- *Se $(x,y) \in R$ e $(y,z) \in R$, então existem k, $l \in \mathbb{Z}$ tais que $x - y = 2k$ e $y - z = 2l$. Somando essas duas equações obtemos*

$$\begin{aligned}(x-y)+(y-z) &= 2k+2l \\ x-z &= 2(k+l)\end{aligned}$$

e como $k+l \in \mathbb{Z}$ segue que $(x,z) \in \mathbb{Z}$.

Assim R é uma relação de equivalência.

■ **Observaçao 3.1** Seja R uma relação de equivalência em A. Para dizermos que $(x,y) \in R$ usaremos a notação $x \equiv y \ (R)$, que se lê "x é equivalente a y módulo R", ou ainda a notação xRy, com o mesmo significado anterior.

Em virtude da observação anterior a definição de relação de equivalência pode ser reescrita como:

Definição 3.1.2 Seja A um conjunto não vazio e $R \subseteq A \times A$. Dizemos que R é uma **relação de equivalência** se:

i) Para todo $x \in A$, xRx. *(Propriedade Reflexiva)*
ii) Se xRy, então yRx. *(Propriedade Simétrica)*
iii) Se xRy e yRz, então xRz. *(Propriedade Transitiva)*

Definição 3.1.3 Seja R uma relação de equivalência sobre um conjunto A. Dado $b \in A$, chamamos de **classe de equivalência determinada por b módulo R**, denotada por $\overline{b}$ ou $C(b)$, o subconjunto de A dado por

$$\overline{b} = C(b) = \{x \in A \mid (x,b) \in R\} = \{x \in A \mid xRb\}.$$

■ **Observaçao 3.2** Seja $A \neq \emptyset$ e R uma relação de equivalência sobre A. Segue da definição de relação de equivalência que para todo $b \in A$, $\overline{b} \neq \emptyset$ pois $(b,b) \in R$ logo $b \in \overline{b}$.

■ **Exemplos 3.2** Do Exemplo 3.1 temos

1) As classes de equivalência de R_1 são:

$$\begin{aligned}\overline{1} &= \{x \in A \mid (x,1) \in R_1\} = \{1,2,3,4\} \\ \overline{2} &= \{x \in A \mid (x,2) \in R_1\} = \{1,2,3,4\} \\ \overline{3} &= \{x \in A \mid (x,3) \in R_1\} = \{1,2,3,4\} \\ \overline{4} &= \{x \in A \mid (x,4) \in R_1\} = \{1,2,3,4\}\end{aligned}$$

Nesse caso temos somente uma classe de equivalência.

2) As classes de equivalência de R_3 são:

$$\overline{1} = \{x \in A \mid (x,1) \in R_3\} = \{1,2\}$$
$$\overline{2} = \{x \in A \mid (x,2) \in R_3\} = \{1,2\}$$
$$\overline{3} = \{x \in A \mid (x,3) \in R_3\} = \{3\}$$
$$\overline{4} = \{x \in A \mid (x,4) \in R_3\} = \{4\}$$

Aqui temos três classes de equivalência diferentes.

3) As classes de equivalência de R_4 são:

$$\overline{1} = \{x \in A \mid (x,1) \in R_4\} = \{1\}$$
$$\overline{2} = \{x \in A \mid (x,2) \in R_4\} = \{2\}$$
$$\overline{3} = \{x \in A \mid (x,3) \in R_4\} = \{3\}$$
$$\overline{4} = \{x \in A \mid (x,4) \in R_4\} = \{4\}$$

Aqui temos quatro classes de equivalência diferentes.

4) Para a relação de equivalência $R = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x - y = 2k, \text{ para algum } k \in \mathbb{Z}\}$ temos:

$$\overline{0} = \{x \in \mathbb{Z} \mid xR0\} = \{x \in \mathbb{Z} \mid x - 0 = 2k,\ k \in \mathbb{Z}\}$$
$$\overline{0} = \{x \in \mathbb{Z} \mid x = 2k,\ k \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \pm 6, \dots\}$$
$$\overline{1} = \{x \in \mathbb{Z} \mid xR1\} = \{x \in \mathbb{Z} \mid x - 1 = 2k,\ k \in \mathbb{Z}\}$$
$$\overline{1} = \{x \in \mathbb{Z} \mid x = 2k + 1,\ k \in \mathbb{Z}\} = \{\pm 1, \pm 3, \pm 4, \pm 7, \dots\}$$

Neste caso existem somente duas classes de equivalência. (*Por quê?*)

Proposição 3.1.1 Seja R uma relação de equivalência em um conjunto não vazio A. Dados a, $b \in A$ temos:

i) se $\overline{a} \cap \overline{b} \neq \emptyset$, então aRb.
ii) se $\overline{a} \cap \overline{b} \neq \emptyset$, então $\overline{a} = \overline{b}$.

Prova:

i) Como $\overline{a} \cap \overline{b} \neq \emptyset$, existe um $y \in \overline{a} \cap \overline{b}$, logo $y \in \overline{a}$ e $y \in \overline{b}$. Da definição de classe de equivalência temos yRa e yRb. Como R é relação de equivalência temos aRy e bRy. Pela propriedade transitiva segue que aRb, como queríamos.

ii) Precisamos mostrar que $\overline{a} \subseteq \overline{b}$ e que $\overline{b} \subseteq \overline{a}$. Para a primeira inclusão seja $y \in \overline{a}$. Daí yRa. Mas, por hipótese, $\overline{a} \cap \overline{b} \neq \emptyset$, assim pelo item anterior segue que aRb. Logo, como yRa e aRb, segue que yRb, ou seja, $y \in \overline{b}$. Daí $\overline{a} \subseteq \overline{b}$. Agora para provar a segunda inclusão seja $x \in \overline{b}$. Então xRb. Novamente, $\overline{a} \cap \overline{b} \neq \emptyset$ e então pelo item anterior segue que aRb. Assim uma vez que R é uma relação de equivalência temos bRa e de xRb obtemos xRa, ou seja, $x \in \overline{a}$. Com isso $\overline{b} \subseteq \overline{a}$. Portanto $\overline{a} = \overline{b}$, como queríamos.

■

Corolário 3.1.2 Seja R uma relação de equivalência sobre um conjunto não vazio A. Dados a, $b \in A$ então $\overline{a} \cap \overline{b} = \emptyset$ ou $\overline{a} = \overline{b}$.

Definição 3.1.4 Seja R uma relação de equivalência sobre um conjunto não vazio A. O conjunto de todas as classes de equivalência determinadas por R será denotado por A/R e é chamado de **conjunto quociente** de A por R.

■ **Exemplos 3.3** Do Exemplo 3.2 temos:
1) $A/R_1 = \{\overline{1}\}$
2) $A/R_3 = \{\overline{1}, \overline{3}, \overline{4}\}$
3) $A/R_4 = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$
4) $\mathbb{Z}/R = \{\overline{0}, \overline{1}\}$

Definição 3.1.5 Seja C uma classe de equivalência de uma relação de equivalência R. Qualquer elemento $y \in C$ é chamado **representante** de C.

Proposição 3.1.3 Seja A um conjunto não vazio e R uma relação de equivalência em A. Então A é a união disjunta das classes $\overline{b}$, $b \in A$, ou seja,

$$X = \bigcup_{b \in A} \overline{b}.$$

Prova: Para todo $b \in A$ temos, pela definição de classe de equivalência, que $\overline{b} \subseteq A$. Logo $\bigcup_{b \in X} \overline{b} \subseteq X$. Agora seja $x \in A$. Logo $x \in \overline{x}$ e daí $x \in \bigcup_{b \in A} \overline{b}$. Assim $X \subseteq \bigcup_{a \in X} \overline{a}$. Portanto, $X = \bigcup_{b \in X} \overline{b}$. ■

Definição 3.1.6 Sejam $a, b \in \mathbb{Z}$, $b \neq 0$. Dizemos que b **divide** a quando existe um inteiro k tal que $a = bk$. Nesse caso escrevemos $b \mid a$. Quando b **não divide** a, escrevemos $b \nmid a$.

■ **Exemplos 3.4**
1) Os inteiros 1 e -1 dividem qualquer número inteiro a, pois $a = 1a$ e $a = (-1)(-a)$.
2) O número 0 não divide nenhum inteiro b, pois não existe $a \in \mathbb{Z}$ tal que $b = 0a$.
3) Para todo $b \neq 0$, b divide $\pm b$.
4) Para todo inteiro $b \neq 0$, b divide 0, pois $0 = b0$.
5) $3 \nmid 8$.
6) $17 \mid 51$.

Proposição 3.1.4
i) $a \mid a$, para todo $a \in \mathbb{Z}$.
ii) Se $a \mid b$ e $b \mid a$, $a, b > 0$ então $a = b$.
iii) Se $a \mid b$ e $b \mid c$, então $a \mid c$.
iv) Se $a \mid b$ e $a \mid c$, então $a \mid (bx + cy)$, para todos $x, y \in \mathbb{Z}$.

Prova:
i) Imediata.
ii) De fato, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $a = lb$. Assim $b = klb$, isto é, $b(1 - kl) = 0$. Como $b \neq 0$ então $1 - kl = 0$. Daí $kl = 1$ e então $k = \pm 1$ e $l = \pm 1$. Mas $a > 0$ e $b > 0$, logo $k = l = 1$. Logo $a = b$.
iii) De fato, existem $k, l \in \mathbb{Z}$ tais que $b = ka$ e $c = bl$. Assim $c = kal = (kl)a$, ou seja, $a \mid c$.
iv) Temos $b = ka$ e $c = al$, com $k, l \in \mathbb{Z}$. Daí $bx + cy = (ka)x + (al)y = a(kx + ly)$ e como $kx + ly \in \mathbb{Z}$ segue que $a \mid (bx + cy)$.

■

Definição 3.1.7 Sejam $a, b \in \mathbb{Z}$, dizemos que a **é congruente à** b **módulo** m se $m \mid (a - b)$. Neste caso, escrevemos $a \equiv_m b$ ou $a \equiv b \pmod{m}$.

■ **Exemplos 3.5**
1) $5 \equiv 2 \pmod{3}$, pois $3 \mid (5 - 2)$.
2) $3 \equiv 1 \pmod{2}$, pois $2 \mid (3 - 1)$.
3) $3 \equiv 9 \pmod{2}$, pois $2 \mid (3 - 9)$.

Proposição 3.1.5 A congruência módulo m é uma relação de equivalência em $\mathbb{Z}$.

Prova:

i) Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$ pois $m \mid (a-a)$.

ii) Se $a \equiv b \pmod{m}$, então $m \mid (a-b)$. Daí existe $k \in \mathbb{Z}$, tal que $(a-b) = km$. Agora, $(b-a) = -(a-b) = -(km) = (-k)m$, ou seja, $m \mid (b-a)$. Daí $b \equiv a \pmod{m}$.

iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $m \mid (a-b)$ e $m \mid (b-c)$. Assim, $m \mid [(a-b)+(b-c)]$. Logo, $m \mid (a-c)$, isto é, $a \equiv c \pmod{m}$.

Portanto a congruência módulo m é uma relação de equivalência. ■

Teorema 3.1.6 A relação de congruência módulo m satisfaz as seguintes propriedades:

i) $a_1 \equiv b_1 \pmod{m}$ se, e somente se, $a_1 - b_1 \equiv 0 \pmod{m}$.

ii) Se $a_1 \equiv b_1 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, então $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.

iii) Se $a_1 \equiv b_2 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, então $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

iv) Se $a \equiv b \pmod{m}$, então $ax \equiv bx \pmod{m}$, para todo $x \in \mathbb{Z}$.

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

Prova: Provemos o item iii).

Como $a_1 \equiv b_2 \pmod{m}$ e $a_2 \equiv b_2 \pmod{m}$, existem $k, l \in \mathbb{Z}$ tais que

$$a_1 - b_1 = km$$
$$a_2 - b_2 = lm,$$

isto é,

$$a_1 = b_1 + km$$
$$a_2 = b_2 + lm,$$

Assim

$$\begin{aligned} a_1 a_2 &= (b_1 + km)(b_2 + lm) \\ &= b_1 b_2 + b_1 lm + b_2 km + klm^2 \\ &= b_1 b_2 + \underbrace{(lb_1 + kb_2 + klm)}_{\in \mathbb{Z}} m \end{aligned}$$

Ou seja, $a_1 a_2 - b_1 b_2 = pm$, onde $p = lb_1 + kb_2 + klm \in \mathbb{Z}$. Portanto, $a_1 a_2 \equiv b_1 b_2 \pmod{m}$. ■

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

$$\overline{n} = C(n) = \{x \in \mathbb{Z} \mid x \equiv n \pmod{m}\}.$$

Denotaremos $C(n)$ por $R_m(n)$ ou $\overline{n}$, quando não houver possibilidade de confusão.
Por exemplo, fixando $m > 1$

$$R_m(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = mk, k \in \mathbb{Z}\} = m\mathbb{Z}$$
$$R_m(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{m}\} = \{x \in \mathbb{Z} \mid x = 1 + km, k \in \mathbb{Z}\}$$
$$R_m(n) = \{x \in \mathbb{Z} \mid x = n + km, k \in \mathbb{Z}\}$$

Proposição 3.1.7 As classes de equivalência definidas pela congruência módulo m são determinadas pelos restos da divisão inteira por m. Em outras palavras, $R_m(n)$ é o conjunto dos números inteiros cujo resto na divisão inteira por m é n.

Corolário 3.1.8 $R_m(k) = R_m(l)$ se, e somente se, $k \equiv l \pmod{m}$.

■ **Exemplos 3.6** 1) Se $m = 2$, então os possíveis restos na divisão inteira por 2 são 0 e 1. Logo, existem duas classes de equivalência, a saber

$$R_2(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{2}\} = \{x \in \mathbb{Z} \mid x = 2k, k \in \mathbb{Z}\}$$
$$R_2(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{2}\} = \{x \in \mathbb{Z} \mid x = 1+2k, k \in \mathbb{Z}\}.$$

2) Se $m = 3$, então os possíveis restos da divisão inteira são 0, 1 e 2. Daí

$$R_3(0) = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k, k \in \mathbb{Z}\}$$
$$R_3(1) = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k+1, k \in \mathbb{Z}\}$$
$$R_3(2) = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod{3}\} = \{x \in \mathbb{Z} \mid x = 3k+2, k \in \mathbb{Z}\}$$

Proposição 3.1.9 Na relação de equivalência módulo m existem m classes de equivalência.

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

■ **Observaçao 3.3** Fixado m inteiro positivo, denotaremos

$$R_m(0) = \overline{0}$$
$$R_m(1) = \overline{1}$$
$$\vdots$$
$$R_m(m-1) = \overline{m-1}$$

O conjunto quociente desta relação será denotado por $\frac{\mathbb{Z}}{m\mathbb{Z}}$ ou $\mathbb{Z}_m$. Assim

$$\mathbb{Z}_m = \frac{\mathbb{Z}}{m\mathbb{Z}} = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}.$$

Queremos definir um meio de somar e multiplicar os elementos de $\mathbb{Z}_m$. Por exemplo, em $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ temos que a soma de pares é par, soma de par com ímpar é ímpar e a soma de ímpares é par. Assim podemos escrever

$\oplus$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

Para multiplicação, temos

$\otimes$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Definição 3.1.8 Dados $\overline{a}, \overline{b} \in \mathbb{Z}_m$ definimos

$$\overline{a} \oplus \overline{b} = \overline{a+b} \tag{3.1}$$
$$\overline{a} \otimes \overline{b} = \overline{ab}. \tag{3.2}$$

Proposição 3.1.10 As operações de soma e produto definidas em (3.1) e (3.2) são independentes dos representantes das classes.

Prova: Dadas duas classes em $\mathbb{Z}_m$ com representantes diferentes, $\overline{a}_1 = \overline{a}_2$, $\overline{b}_1 = \overline{b}_2$, com $a_1 \neq a_2$ e $b_1 \neq b_2$, temos:

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

■

■ **Exemplo 3.1** A some e a multiplicação em $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ são dadas nas tabelas abaixo:

Tabela 3.1: Soma e multiplicação em $\mathbb{Z}_4$

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

$\otimes$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Bibliografia

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

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

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

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

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