

FM1002 Fundamentos del Álgebra abstracta

Profesores: Sebastián Tapia, Sebastián Reyes Rizzo, Leslie Jiménez

Auxiliares: Nicolás Cornejo, Camilo Carvajal, Jordan Urrea, Pablo Araya, Bruno Moreno, Ignacio Fierro



Para estudiantes de Educación Básica y Media.

Resumen Contenidos Control 2

1. **Relacion:** Dado un conjunto A no vacío, llamaremos relación a un conjunto $\mathcal{R} \subseteq A \times A$. Denotaremos $a\mathcal{R}b$ cuando se tenga que $(a, b) \in \mathcal{R}$ y diremos que $a \not\mathcal{R}b$ cuando $(a, b) \notin \mathcal{R}$. Definiremos las siguientes propiedades de relaciones, las cuales no siempre se cumplen:

- a) **Refleja:** Una relación $\mathcal{R}$ será una relación refleja en A , si y solo si

$$(\forall x \in A) x\mathcal{R}x$$

- b) **Simétrica:** Una relación $\mathcal{R}$ será una relación simétrica en A , si y solo si

$$(\forall x, y \in A) x\mathcal{R}y \Rightarrow y\mathcal{R}x$$

- c) **Antisimétrica:** Una relación $\mathcal{R}$ será una relación antisimétrica en A , si y solo si

$$(\forall x, y \in A) (x\mathcal{R}y \wedge y\mathcal{R}x \Rightarrow x = y)$$

- d) **Transitiva:** Una relación $\mathcal{R}$ será una relación transitiva en A , si y solo si

$$(\forall x, y, z \in A) (x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z)$$

En base a estas propiedades definiremos algunas relaciones importantes:

- a) **Relación de orden** Una relación $\mathcal{R}$ se dirá que es relación de orden en A , si y solo si, $\mathcal{R}$ es una relación refleja, antisimétrica y transitiva. Las relaciones de orden se pueden separar en dos grupos:

- i) **Orden total** Una relación de orden, se dirá orden total, si y solo si se cumple que

$$(\forall x, y \in A) x\mathcal{R}y \vee y\mathcal{R}x$$

- ii) **Orden Parcial** Una relación de orden, se dirá orden parcial, si y solo si, no es orden total.

- b) **Relación de equivalencia** Una relación $\mathcal{R}$ se dirá que es relación de equivalencia en A , si y solo si, $\mathcal{R}$ es una relación refleja, simétrica y transitiva. A las relaciones de equivalencia se les pueden definir las clases de equivalencia y el conjunto cociente.

- i) **Clases de equivalencia** Dado un elemento $a \in A$, definimos la clase de equivalencia de a asociada a $\mathcal{R}$ como el conjunto:

$$[a]_{\mathcal{R}} = \{x \in A : x\mathcal{R}a\}$$

- II) **Conjunto cuociente** Al conjunto de las clases de equivalencia de una relación de equivalencia $\mathcal{R}$ se le llama conjunto cuociente y está dado por:

$$A/\mathcal{R} = \{[a]_{\mathcal{R}} : a \in A\}$$

2. **Congruencia Módulo:** Se define en $\mathbb{Z}$ la relación $\equiv_p$ por:

$$x \equiv_p y \Leftrightarrow \exists k \in \mathbb{N}, x - y = kp$$

y se lee "*x es congruente con y en módulo p*". En otras palabras $x \equiv_p y$ si p divide a $(x - y)$, lo que equivale a que $(x - y)$ sea múltiplo de p. Por ejemplo:

$$16 \equiv_5 1, \text{ pues } (16-1) = 15 = 3 \cdot 5;$$

$$\text{o bien } 1 \equiv_5 16, \text{ pues } (1-16) = -15 = -3 \cdot 5.$$

La relación $\equiv_p$ es relación de equivalencia. A su conjunto cuociente se le llamará $\mathbb{Z}_p$.

Podemos ver que para $p=2$, $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, y para $p=3$, $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$, así, generalizando podemos notar que para $p \in \mathbb{Z}$ se cumple que: $\mathbb{Z}_p = \{[0]_p, [1]_p, [2]_p, \dots, [p-1]_p\}$.

Propiedades de congruencia: Sean $a, b, d, e \in \mathbb{N}$, tal que $a \equiv_p b$ y $d \equiv_p e$, se cumple que:

a) $(\forall c \in \mathbb{Z}) a + c \equiv_p b + c.$

b) $(\forall c \in \mathbb{Z}) ac \equiv_p bc.$

c) $a + d \equiv_p b + e.$

d) $ad \equiv_p be.$

e) $(\forall n \in \mathbb{N}) a^n \equiv_p b^n.$