Repaso sobre relaciones de equivalencia. Los enteros módulo m

Sergio A. Carrillo
sacarrillot@unal.edu.co

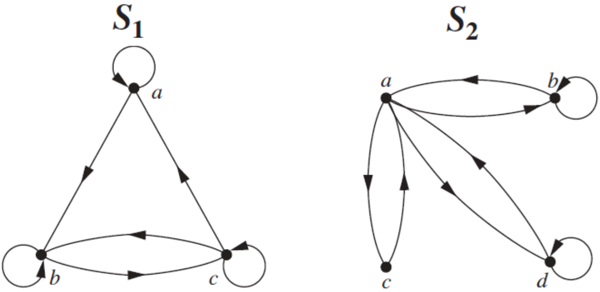
Repaso sobre relaciones de equivalencia

Una relación $\mathcal{R} \subseteq A \times A$ es de *equivalencia* si es reflexiva, simétrica y transitiva. Recordemos que $\mathcal{R}$ es:

- *Reflexiva* si para todo $a \in A$, $a\mathcal{R}a$. De manera equivalente $\Delta_A = \{(a, a) \in A \times A \ : a \in A\} \subseteq \mathcal{R}$. En términos de grafos dirigidos, cada nodo debe tener un bucle.
- *Simétrica* si para todo $x, y \in A$, $x\mathcal{R}y$ implica que $y\mathcal{R}x$.
- *Transitiva* si para todo $x, y, z \in A$, las condiciones $x\mathcal{R}y$ y $y\mathcal{R}z$ implican que $x\mathcal{R}z$.

Ejemplos

Determine si las relaciones dadas por los siguientes grafos son reflexivas, simétricas, transitivas.



Ejemplos

Determine si las relaciones sobre el conjunto $\{1, 2, 3, 4\}$ son reflexivas, simétricas, transitivas.

$$
\begin{aligned}
R_1 &= \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\},\\
R_2 &= \{(1, 1), (1, 2), (2, 1)\},\\
R_3 &= \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\},\\
R_4 &= \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\},\\
R_5 &= \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\},\\
R_6 &= \{(3, 4)\}.
\end{aligned}
$$

Clases de equivalencia

Sea $\sim$ una relación de equivalencia sobre $A \neq \emptyset$ y $x, y \in A$. Recordemos que

$$[x] = \{a \in A : x \sim a\} \qquad \text{es la clase de } x.$$

1. $x \sim y$ si y solo si $[x] = [y]$.
2. Si $x \not\sim y$, entonces $[x] \cap [y] = \emptyset$.
3. $A = \bigcup_{x \in A} [x]$.

Denotaremos por

$$A/\sim := \{[x] : x \in A\}$$

al *cociente* de A respecto a $\sim$. Note que tenemos la proyección

$$\pi : A \to A/\sim, \qquad \pi(a) = [a].$$

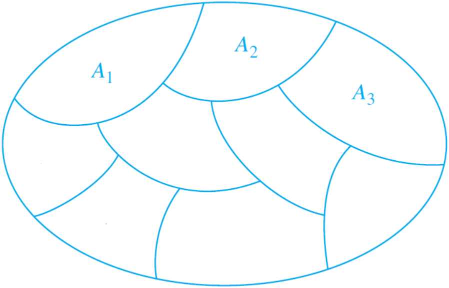
Resulta que $A/\sim$ es una partición de A.

Particiones

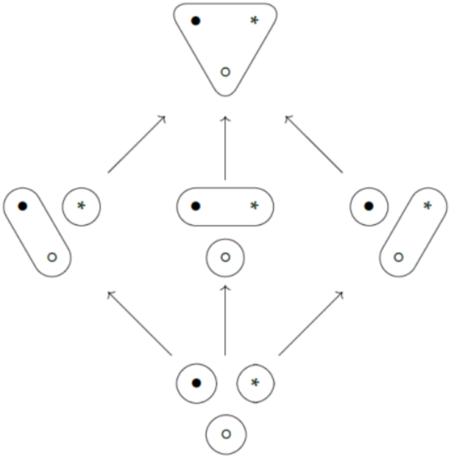
Una partición de un conjunto $A \neq \emptyset$ es una familia $\mathcal{F}$ de subconjuntos de A tales que:

1. Si $A_i, A_j \in \mathcal{F}$ y $A_i \neq A_j$, entonces $A_i \cap A_i = \emptyset$ (la familia es disjunta dos a dos).
2. $A = \bigcup_{B \in \mathcal{F}} B$.

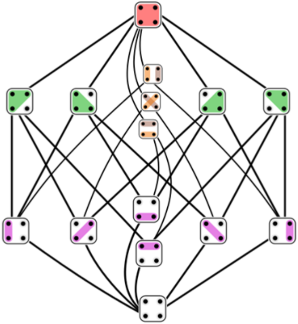
Los elementos $B \in \mathcal{F}$ a veces se llaman bloques de la partición.



Particiones de un conjunto de 3 elementos



Particiones de un conjunto de 4 elementos



Los números de Bell B_n cuentan el número de relaciones de equivalencia (particiones) sobre un conjunto de n elementos.

$$B_1 = 1, B_2 = 2, B_3 = 5, B_4 = 15.$$

Un ejemplo fundamental

Dada una aplicación $f : A \to B$, considere la relación sobre A dada por

$$a \sim a' \quad \text{si y solo si } f(a) = f(a').$$

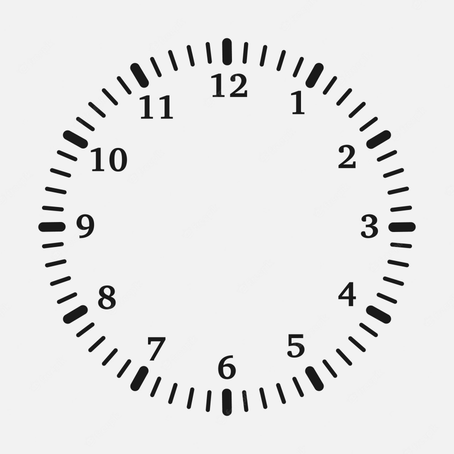
Esta es una relación de equivalencia. Además existe una única aplicación inyectiva $\overline{f} : A/\sim \to B$ dada por $\overline{f}([a]) = f(a)$, es decir, el diagrama conmuta,

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\pi"'] & B \\
A/\sim \arrow[ur, "\overline{f}"'] &
\end{tikzcd}$$

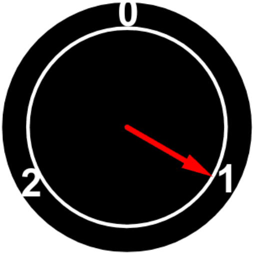
donde $\pi : A \to A/\sim$ es la proyección canónica.

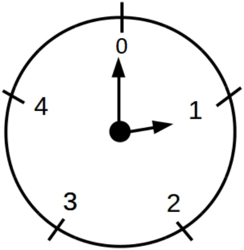
Introducción a congruencias

¿Cómo contamos las horas?



Relojes módulo 3 y 5





Congruencias

Definición

Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{N}^+$. Decimos que a *es congruente a* b *módulo* m si m divide a $(a - b)$. En este caso escribiremos

$$a \equiv b \mod m.$$

Según la definición de divisibilidad, esto equivale a que exista $k \in \mathbb{Z}$ tal que $a = b + km$.

Se comprueba que $(\equiv \mod m)$ es una relación de equivalencia sobre $\mathbb{Z}$.

Los posibles representantes

Ejemplo (Pares e impares)

$$0 \equiv 2 \equiv 4 \equiv 6 \equiv 8 \equiv 10 \equiv \cdots \equiv -2 \equiv -4 \equiv \cdots \pmod 2,$$
$$1 \equiv 3 \equiv 5 \equiv 7 \equiv 9 \equiv 11 \equiv \cdots \equiv -1 \equiv -3 \equiv \cdots \pmod 2.$$

Ejemplo ($m = 3$)

$$0 \equiv 3 \equiv 6 \equiv 9 \equiv \cdots \equiv -3 \equiv -6 \equiv \cdots \pmod 3,$$
$$1 \equiv 4 \equiv 7 \equiv 10 \equiv \cdots \equiv -2 \equiv -5 \equiv \cdots \pmod 3,$$
$$2 \equiv 5 \equiv 8 \equiv 11 \equiv \cdots \equiv -1 \equiv -4 \equiv \cdots \pmod 3.$$

¿Cómo hallar un representante?

Dados $a \in \mathbb{Z}$ y $m \in \mathbb{N}^+$, si dividimos a por m obtenemos

$$a = qm + r, 0 \leq r < m.$$

Por definición,

$$a \equiv r \pmod{m}.$$

Así el resto de la división nos da un representante en el conjunto

$$\{0, 1, 2, \ldots, m-1\}.$$

El cociente se suele escribir

$$\mathbb{Z}/m\mathbb{Z} = \{[0], [1], [2], \ldots, , [m-1]\}$$

y se denomina el conjunto de enteros, módulo m.

Operaciones con congruencias

Teorema

Sean $a, b, c, d \in \mathbb{Z}$ *y* $m \in \mathbb{N}^+$ *tales que* $a \equiv b \pmod{m}$ *y* $c \equiv d \pmod{m}$. *Entonces*

$$a + c \equiv b + d \pmod{m}, \qquad ac \equiv bd \pmod{m}.$$

Corolario

La suma $+ : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ *y el producto* $+ : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ *está bien definidas.*

Ejemplos

$$50 + 41 \equiv 1 + 6 \equiv 7 \equiv 0 \pmod{7}.$$

$$501 \cdot 22 \equiv 3 \cdot 4 \equiv 12 \equiv 0 \pmod{6}.$$

$$\begin{aligned} 5^7 &\equiv (5^2)^2 \cdot 5^2 \cdot 5 \equiv 25^2 \cdot 25 \cdot 5 \equiv 7^2 \cdot 7 \cdot 5 \\ &\equiv 49 \cdot 35 \equiv 4 \cdot (-1) \equiv 5 \pmod{9}. \end{aligned}$$

La idea es dar la respuesta en el conjunto $\{0, 1, \ldots, m-1\}$, módulo m.