

Tema 2

Relaciones Binarias

1. Equivalencia

(1.1) Sea n un entero positivo. Una *relación n -aria* entre los elementos de un conjunto A es un subconjunto del producto cartesiano $\underbrace{A \times \cdots \times A}_n$. A n se le llama *aridad* de la relación.

Una relación unaria, resp. binaria, resp. ternaria, etc. entre los elementos de A es un subconjunto de A , resp. de $A \times A$, resp. de $A \times A \times A$, etc.

Si R es una relación binaria entre los elementos de A , esto es, $R \subseteq A \times A$, entonces el hecho de que el par (a, b) sea un elemento de R también se denota aRb , y se lee “ a está relacionado con b ”.

(1.2) Una relación binaria R entre los elementos del conjunto A se dice que es

(1.2.1) *reflexiva* si aRa para todo $a \in A$;

(1.2.2) *simétrica* si bRa siempre que aRb ;

(1.2.3) *antisimétrica* si $a = b$ siempre que aRb y bRa ;

(1.2.4) *transitiva* si aRc siempre que aRb y bRc ;

(1.2.5) *conexa* si para todo $a, b \in A$, o bien $a = b$, o bien aRb , o bien bRa .

(1.3) Sea R una relación binaria entre los elementos de un conjunto.

Se dice que R es una relación de *equivalencia* si es reflexiva, simétrica y transitiva.

Se dice que R es una relación de *orden* (o de orden parcial) si es reflexiva, antisimétrica y transitiva. Se dice que es de *orden total* si además es conexa.

(1.4) Ejemplos.

- La relación definida por

$$aRb \Leftrightarrow a = b$$

entre los elementos de \mathbb{Z} es una relación de equivalencia y de orden parcial.

- La relación definida por

$$aRb \Leftrightarrow a \leq b$$

entre los elementos de \mathbb{Z} es una relación de orden parcial.

- La relación definida por

$$aRb \Leftrightarrow a \text{ divide a } b,$$

donde “ a divide a b ” significa que existe $n \in \mathbb{Z}$ tal que $b = an$, es una relación de equivalencia entre los elementos de $\mathbb{N} - \{0\}$.

2. Conjunto cociente

Sea R una relación de equivalencia entre los elementos de A .

(2.1) Si a es un elemento de A , se llama clase de a y se denota por \bar{a}^R (o por \bar{a} si dejar de mencionar a R no provoca confusión) al conjunto de todos los elementos de A que están relacionados con a :

$$\bar{a}^R = \{b : b \in A \text{ y } aRb\}.$$

(2.2) Las clases de equivalencia tienen las siguientes propiedades:

(2.2.1) $a \in \bar{a}$ para todo elemento a de A , y por lo tanto $\bar{a} \neq \emptyset$.

(2.2.2) Si $a, b \in A$, entonces o bien $\bar{a} = \bar{b}$, o bien $\bar{a} \cap \bar{b} = \emptyset$.

(2.2.3) $\bigcup_{a \in A} \bar{a} = A$.

(2.3) Al conjunto formado por las clases de los elementos de A se le llama *conjunto cociente* y se denota por A/R .

(2.4) Una *partición* de un conjunto A es una familia $\{A_i\}_{i \in I}$ de subconjuntos de A de manera que

(2.4.1) $A_i \neq \emptyset$ para todo $i \in I$;

(2.4.2) $\bigcup_{i \in I} A_i = A$;

(2.4.3) $A_i \cap A_j = \emptyset$ si $i \neq j$;

(2.5) El conjunto cociente A/R es una partición de A .

3. Equipotencia

(3.1) En cualquier conjunto cuyos elementos sean conjuntos se puede definir la relación binaria

$$A \sim B \Leftrightarrow \text{existe una aplicación } f : A \rightarrow B \text{ biyectiva.}$$

Esta relación es una relación de equivalencia, y se llama *equipotencia* de conjuntos. En efecto,

(3.1.1) “ \sim ” es reflexiva porque para todo conjunto A , la aplicación identidad $1_A : A \rightarrow A$ es una biyección.

(3.1.2) “ \sim ” es simétrica puesto que si $A \sim B$, esto es, si existe una aplicación biyectiva $f : A \rightarrow B$, entonces la aplicación inversa $f^{-1} : B \rightarrow A$ también es biyectiva, y por eso $B \sim A$.

(3.1.3) “ \sim ” es transitiva porque si $A \sim B$ y $B \sim C$, esto es, si existen aplicaciones biyectivas $f : A \rightarrow B$ y $g : B \rightarrow C$ entonces la composición $g \circ f : A \rightarrow C$ es biyectiva (ver ejercicio) y por lo tanto $A \sim C$.

(3.2) A las clases de equivalencia de la relación de equipotencia se les llama *cardinales*. El cardinal de un conjunto A es la clase de equivalencia de A bajo la relación de equipotencia, y se denota por $|A|$.

Los cardinales se suelen denotar por letras griegas minúsculas ($\alpha, \beta, \gamma, \dots$).

(3.3) Consideremos, para cada $n \in \mathbb{N}$, el conjunto

$$I_n = \begin{cases} \emptyset, & n = 0; \\ \{1, \dots, n\}, & n > 0. \end{cases}$$

Es fácil ver que $I_n \sim I_m$ si, y sólo si $n = m$.

Un conjunto A es finito si existe $n \in \mathbb{N}$ tal que $A \sim I_n$. Se dice entonces que su cardinal es n , y en este caso el cardinal se corresponde con el número de elementos de A .

(3.4) Se dice que el cardinal α es menor o igual que el cardinal β (se escribe $\alpha \leq \beta$) si para algún A y algún B tales que $|A| = \alpha$ y $|B| = \beta$ existe una aplicación inyectiva $f : A \rightarrow B$.

Se dice que α es estrictamente menor que β (se escribe $\alpha < \beta$) si $\alpha \leq \beta$ pero $\alpha \neq \beta$.

(3.5) Si A es un conjunto, entonces $|A| < |\mathcal{P}(A)|$.

En efecto, la aplicación

$$\begin{aligned} f : A &\rightarrow \mathcal{P}(A) \\ a &\mapsto f(a) = \{a\} \end{aligned}$$

es una aplicación inyectiva, así que $|A| \leq |\mathcal{P}(A)|$.

Supongamos que $|A| = |\mathcal{P}(A)|$. Entonces existe una aplicación $g : A \rightarrow \mathcal{P}(A)$ biyectiva. Consideremos el conjunto

$$B = \{a : a \in A, a \notin g(a)\}.$$

Como g es sobreyectiva, existe $b \in A$ tal que $g(b) = B$.

Si $b \in B$, entonces $b \notin g(b) = B$ — una contradicción.

Si por el contrario $b \notin B$, entonces $b \notin g(b)$, así que $b \in B$ — una contradicción.

Luego $|A| \neq |\mathcal{P}(A)|$.

(3.6) El cardinal de \mathbb{N} se denota por \aleph_0 y se denomina *cardinal del numerable* (\aleph es la primera letra del alfabeto hebreo, y se llama *alef*). De cualquier conjunto que tenga como cardinal a \aleph_0 se dice que es numerable.

(3.7) El cardinal del conjunto de los enteros es el cardinal de los naturales.

En efecto, consideremos la aplicación

$$\begin{aligned} f: \mathbb{N} &\longrightarrow \mathbb{Z} \\ n &\longmapsto f(n) = (-1)^n \lfloor \frac{n+1}{2} \rfloor, \end{aligned}$$

donde $\lfloor x \rfloor$ indica el mayor entero menor o igual que x .

Esta aplicación es biyectiva, así que $|\mathbb{N}| = |\mathbb{Z}|$.

(3.8) El cardinal del conjunto de los números racionales es \aleph_0 .

Por una parte, dado que la aplicación inclusión

$$\begin{aligned} i: \mathbb{N} &\longrightarrow \mathbb{Q} \\ n &\longmapsto n \end{aligned}$$

es inyectiva, se tiene que $|\mathbb{N}| \leq |\mathbb{Q}|$.

Por otra parte, dado que todo número racional admite una única representación a/b donde $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$ y a y b son primos entre sí, podemos considerar la aplicación

$$\begin{aligned} \mathbb{Q} &\longrightarrow \mathbb{Z} \times \mathbb{Z}^+ \\ q &\longmapsto (a, b), \text{ donde } q = a/b, b > 0 \text{ y m.c.d.}(a, b) = 1. \end{aligned}$$

Esta aplicación es inyectiva, por lo que $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}^+|$.

Veamos que $|\mathbb{Z} \times \mathbb{Z}^+| = |\mathbb{N}|$. El producto cartesiano $\mathbb{Z} \times \mathbb{Z}^+$ tiene como elementos a los pares de la siguiente tabla:

	0	1	-1	2	-2	...
1	(0,1)	(1,1)	(-1,1)	(2,1)	(-2,1)	...
2	(0,2)	(1,2)	(-1,2)	(2,2)	(-2,2)	...
3	(0,3)	(1,3)	(-1,3)	(2,3)	(-2,3)	...
4	(0,4)	(1,4)	(-1,4)	(2,4)	(-2,4)	...
...

Consideremos la aplicación $g: \mathbb{Z} \times \mathbb{Z}^+ \longrightarrow \mathbb{N}$ que *recorre toda la tabla desde la esquina superior izquierda*, esto es, que asigna a cada par (a, b) el número natural que le corresponde según ese orden (por ejemplo, $g(0, 1) = 0$, $g(1, 1) = 1$, $g(0, 2) = 2$, $g(-1, 1) = 3$, $g(1, 2) = 4$, $g(0, 3) = 5$, ...). La aplicación g es biyectiva, y por lo tanto $|\mathbb{Z} \times \mathbb{Z}^+| = |\mathbb{N}|$.

(3.9) El cardinal de \mathbb{R} es estrictamente mayor que \aleph_0 .

Por un lado, como la aplicación inclusión $i: \mathbb{N} \longrightarrow \mathbb{R}$ es inyectiva, se tiene que $\aleph_0 \leq |\mathbb{R}|$.

Supongamos que $|\mathbb{R}| = \aleph_0$.

Entonces $]0, 1[= \aleph_0$, porque $|\mathbb{R}| =]0, 1[$ ya que las aplicaciones

$$\begin{aligned}]0, 1[&\longrightarrow]-1, 1[&]-1, 1[&\longrightarrow \mathbb{R} \\ x &\longmapsto 2x - 1 & x &\longmapsto \frac{x}{(x+1)(1-x)} \end{aligned}$$

son biyectivas.

Eso quiere decir que existe una biyección $f: \mathbb{N} \longrightarrow]0, 1[$. Todos los elementos de $]0, 1[$ son de la forma

$$0.a_1a_2a_3a_4a_5a_6a_7\dots,$$

(un desarrollo decimal único e infinito formado por dígitos $a_i \in \{0, \dots, 9\}$). Sea $b = 0.b_1b_2b_3\dots$, donde para cada $i \in \mathbb{N}$, el dígito b_{i+1} es distinto al $(i+1)$ -ésimo dígito de $f(i)$. Entonces $b \in]0, 1[$ y como f es sobreyectiva, existe un elemento n de \mathbb{N} tal que $f(n) = b$. Pero el $(n+1)$ -ésimo dígito de b es distinto del $(n+1)$ -ésimo dígito del desarrollo decimal de $f(n)$, y por lo tanto $f(n) \neq b$ — una contradicción.

Luego $|\mathbb{R}| \neq \aleph_0$.

El cardinal de \mathbb{R} se denota por \mathfrak{c} y se denomina *cardinal del continuo*.

4. Congruencia

(4.1) Sea m un entero no nulo.

Consideremos la relación binaria en \mathbb{Z} definida por

$$a \equiv b \Leftrightarrow m|(a-b).$$

Esta relación es de equivalencia.

En efecto,

(4.1.1) “ \equiv ” es reflexiva, porque si $a \in \mathbb{Z}$, entonces $a - a = 0$ y $m|0$, así que $a \equiv a$.

(4.1.2) “ \equiv ” es simétrica, porque si $a \equiv b$, entonces $m|(a-b)$, es decir, existe $n \in \mathbb{Z}$ tal que $a - b = nm$. Pero también $-n \in \mathbb{Z}$, y $b - a = -nm$, así que $b \equiv a$.

(4.1.3) “ \equiv ” es transitiva, porque si $a \equiv b$ y $b \equiv c$, entonces existen $n, n' \in \mathbb{Z}$ tales que $a - b = nm$ y $b - c = n'm$. Sumando,

$$a - c = a - b + b - c = nm + n'm = (n + n')m,$$

lo que implica que $a \equiv c$.

Esta relación se llama *congruencia módulo m* . Si $a \equiv b$, entonces se dice que a y b son *congruentes módulo m* , y también se denota por $a \equiv b \pmod{m}$ o por $a \equiv b (m)$. A m se le llama *módulo de la congruencia*.

(4.2) Dado $m \neq 0$, tenemos que $-m \neq 0$ y podemos considerar la relación de congruencia módulo $-m$ en \mathbb{Z} . Para cualesquiera a y b enteros se tiene que

$$m|(a-b) \Leftrightarrow -m|(a-b).$$

Por lo tanto la congruencia módulo m y la congruencia módulo $-m$ son la misma relación de equivalencia, y no se pierde generalidad al estudiar congruencias con módulos positivos solamente.

(4.3) Si $m = 1$, entonces cualesquiera enteros a y b son congruentes módulo 1, puesto que $a - b$ siempre es múltiplo de 1. En ese caso, el conjunto cociente está formado por una única clase de equivalencia: la clase del cero $\bar{0} = \mathbb{Z}$.

(4.4) Si $m > 0$, entonces el conjunto cociente \mathbb{Z}/\equiv , que también se denota por \mathbb{Z}_m , es

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\},$$

Para cualquier entero a existe $q \in \mathbb{Z}$ y $0 \leq r < m$ tales que $a = qm + r$ (q es el cociente y r es resto de la división de a entre m). Entonces $a - r = qm$, de donde se tiene que $\bar{a} = \bar{r}$.

A los elementos del conjunto cociente \mathbb{Z}_m se les llama *clases de resto módulo m* .

A todo conjunto de m enteros que representen a las m clases de \mathbb{Z}_m se le llama *sistema completo de residuos módulo m* . Por ejemplo, $\{0, 1, \dots, m-1\}$ es un sistema completo de residuos módulo m , y $\{m, m+1, \dots, 2m-1\}$ también.

En un sistema completo de residuos módulo m no puede haber dos enteros congruentes, porque entonces habría al menos una clase que no está representada por los elementos de ese sistema (si dos enteros son congruentes módulo m , entonces representan a la misma clase).

(4.5) Si a es un entero tal que a y m son primos entre sí y $\{b_1, \dots, b_m\}$ es un conjunto completo de residuos módulo m , entonces $\{ab_1, \dots, ab_m\}$ también es un sistema completo de residuos módulo m .

Para comprobar que lo anterior es cierto basta verificar que si $i \neq j$, entonces $ab_i \not\equiv ab_j$, porque entonces las clases de los enteros ab_1, \dots, ab_m son distintas dos a dos, y como en \mathbb{Z}_m hay sólo m clases, se tiene que $\mathbb{Z}_m = \{\overline{ab_1}, \dots, \overline{ab_m}\}$.

En efecto, si $i \neq j$ y suponemos que $ab_i \equiv ab_j$, entonces $m | a(b_i - b_j)$, pero como a y m son primos entre sí (no tienen factores primos en común) se tiene que $m | (b_i - b_j)$, pero esto implica que $b_i \equiv b_j$, lo que contradice que $\{b_1, \dots, b_m\}$ es un sistema completo de residuos módulo m .

Luego $ab_i \not\equiv ab_j$ si $i \neq j$, así que $\{ab_1, \dots, ab_m\}$ también es un sistema completo de restos módulo m .

(4.6) Sean a, a', b y b' enteros de manera que $a \equiv b$ y $a' \equiv b'$. Entonces existen n y n' enteros tales que $a - b = nm$ y $a' - b' = n'm$, lo que implica que

(4.6.1) $a + a' \equiv b + b'$, porque

$$a + a' - b - b' = a - b + a' - b' = nm + n'm = (n + n')m;$$

(4.6.2) y $aa' \equiv bb'$, porque

$$aa' - bb' = aa' - ba' + ba' - bb' = nma' + bn'm = (na' + bn')m.$$