**Algebra Lineal 1, agsto-dic, 2003.**

---

## Tarea num. 4 – soluciones

1. Determina para cada una de las siguientes relaciones $R$ en un conjunto $X$ si la relación es (1) reflexiva (2) simétrica (3) transitiva. En caso que se cumplen las 3 propiedades, o sea $R$ es una relación de equivalencia, describe la partición asociada.

   (a) $X = \mathbb{R}$, $R = \{(x, y) \mid x \leq y\}$.

   **Respuesta:** (1) $x \leq x$, $\forall x \in \mathbb{R} \implies R$ es reflexiva. (2) $1 \leq 2$ pero $2 \not\leq 1 \implies R$ no es simétrica. (3) $\forall x, y \in \mathbb{R}, x \leq y, y \leq z \implies x + y \leq y + z \implies x \leq z$ (restando $y$) $\implies R$ es transitiva. ($R$ no es una relación de equivalencia porque no es simétrica). □

   (b) $X = \mathbb{R}$, $R = \{(x, y) \mid (x - y) \in \mathbb{Z}\}$.

   **Respuesta:** (1) $x - x = 0 \in \mathbb{Z}$, $\forall x \in \mathbb{R} \implies R$ es reflexiva. (2) $(x, y) \in R \implies x - y = n \in \mathbb{Z} \implies y - x = -n \in \mathbb{Z} \implies (y, x) \in R \implies R$ es simétrica. (3) $(x, y)$, $(y, z) \in R \implies x - y = n \in \mathbb{Z}, y - z = m \in \mathbb{Z} \implies x - z = (x - y) + (y - z) = m + n \in \mathbb{Z} \implies (x, z) \in R \implies R$ es transitiva. Así que $R$ es una relación de equivalencia.

   Sea $x \in \mathbb{R} \implies [x] = \{x + n \mid n \in \mathbb{Z}\} \sim \mathbb{Z}$. Luego, $[0, 1) \to \mathbb{R}/R$, $x \mapsto [x]$, es una biyección. Así que cada clase de equivalencia es infinita (numérable), y el conjunto de clases de equivalencia es infinito (pero no numerable, ya que $[0, 1)$ no es numerable).

   (c) $X = \mathbb{Z}$, $R = \{(x, y) \mid x$ divide a $y\}$. (Definición: $x$ divide a $y$ si $x \neq 0$ y existe un $r \in \mathbb{Z}$ tal que $y = xr$. Notacion: $x|y$.)

   **Respuesta:** (1) $0 \not| \ 0$ así que $R$ no es reflexiva. (2) $1|2$ pero $2 \not| \ 1 \implies R$ no es simétrica. (3)Si $x|y$, $y|z \implies x \neq 0$, $y \neq 0$ y $\exists r, s \in \mathbb{Z}$ tal que $y = rx$, $z = sy \implies z = qx$, con $q = rs \in \mathbb{Z} \implies x|z \implies R$ es transitivo.

   (d) $X = \mathbb{Z} \setminus \{0\}$, $R = \{(x, y) \mid x$ divide a $y\}$.

   **Respuesta:** (1) $\forall x \in \mathbb{Z}, x = x1$, así que si $x \neq 0 \implies x|x \implies R$ es reflexiva. (2) $R$ no es simétrica y (3) sí es transitiva (por las mismas demostraciones como en el inciso anterior).

   (e) $X = P(A)$, donde $A$ es un conjunto, $R = \{(B, C) \mid B \sim C\}$.

   **Respuesta:** (1) $\forall B \subset A, B \sim B$ (usando la función indentidad $1_B : B \to B) \implies (B, B) \in R \implies R$ es reflexiva. (2) Si $(B, C) \in R \implies B \sim C \implies$ existe una función biyectiva $f : B \to C \implies f^{-1} : C \to B$ es biyectiva (su inversa es $f$) $\implies C \sim B \implies (C, B) \in R \implies R$ es simétrica. (3) Si $(B, C), (C, D) \in R \implies B \sim C, C \sim D \implies$ existen funciones biyectivas $f : B \to C, g : C \to D \implies g \circ f : B \to D$ es biyectiva (su inversa es $f^{-1} \circ g^{-1}) \implies B \sim D \implies (B, D) \in R \implies R$ es transitiva. Así que $R$ es una relación de equivalencia.

   Para $A$ general es dificil describir en detalle la partición de $P(A)$ en clases de equivalencia, pero sí se puede describir la partición en caso que $A$ es finito o numerable.

   Si $A$ es finito, $\#A = n \in \mathbb{N}$, entonces todos sus subconjuntos son finitos, con número de elementos $\leq n$, y dos de ellos son equivalentes ssi tienen el mismo número de elementos (ver tarea 2). Esto implica que si $B \in P(A)$, $k = \#B \implies [B] = \{C \subset A \mid \#C = k\} = P_k(A)$. Así que obetenemos una partición de $P(A)$ en $n + 1$ clases: $P_0(A), P_1(A), \ldots, P_n(A)$. Además, el número de elementos en cada clase de equivalencia está dado por los coeficientes binomiales, $\#P_k(A) = \binom{n}{k}$.

   Para $A = \mathbb{N}$ (o cualquer otro conjunto numerable) tenemos para cada $k \in \mathbb{N}$ la clase de equivalencia $P_k(A)$ (el conjunto de todos los subconjuntos de $A$ con $k$ elementos). Luego, cada subconjunto infinito de un conjunto numerable es numerable (¡ejercicio!), así que todos los subconjuntos infinitos forman una sola clase de equivalencia, $[A]$, y la partición es $P(A) = [A] \cup \bigcup_{k=0}^{\infty} P_k(A)$. Tenemos entonces la siguiente situación: para $A$ numerable el conjunto de las clases de equivalencia $P(A)/\sim$ es numerable, una de las clases, $P_0(A)$, es finita (contiene solo un elemento, el conjunto vacio), todas las clases $P_k(A)$, $k \geq 1$, son numerable (demostración similar a la que se dió en clase de que $\mathbb{Q}$ es numerale), y una clase, $[A]$, es infinita pero no numerable (si fuera nuemrable entonces todo $P(A)$

lo fuera, como unión numerable de conjuntos nuemrables o finitos, pero sabemos que $P(A)$ no es numerable, ya que ningun conjunto es equivalente a su conjunto potencia).

Nota: para un conjunto $A$ mas "grande"(infinito no numerable), la descripción de la partición de $P(A)$ en clases de equivalencia es muy dificil y desde un cierto punto de vista imposible de dar. Si tomamos por ejemplo el conjunto de los números reales $A = \mathbb{R}$, entonces tenemos como antes todas las clases $P_k(\mathbb{R})$ formadas por los subconjuntos finitos de $\mathbb{R}$, luego una clase de los sub-conjuntos numerables $[\mathbb{N}]$; luego, como $\mathbb{R}$ es infinito no numerable tenemos la clase $[\mathbb{R}] \neq [\mathbb{N}]$ de los subconjuntos equivalentes a $\mathbb{R}$, pero queda la duda si hay otros conjuntos infinitos $A \subset \mathbb{R}$, no numerable y que no son equivalentes a $\mathbb{R}$. La afirmación que tal subconjuntos de $\mathbb{R}$ no existen es conocida como *la hipotesis del continuo* y fue anunciada por George Cantor (el fundador de la teoría de conjuntos) en 1878. Esta afirmación se quedaba sin demostración por muhcos años, hasta el trabajo de Kurt Gödel (1940) y Paul Cohen (1963) en donde se demostró que en algun sentido la pregunta es irrespondible, ya que es independiente de las axiomas usuales de la teoría de conjuntos.

2. Para cada $n \in \mathbb{N}$, $n \geq 2$, definimos el conjunto $n\mathbb{Z} := \{nx \mid x \in \mathbb{Z}\}$ y una relación en $\mathbb{Z}$ por $R_n := \{(x, y) \mid (x - y) \in n\mathbb{Z}\}$. En otras palabras: $xR_ny$ ssi $n|(x - y)$.

   Notación: $xR_ny$ se denota por $x \equiv y \pmod{n}$ ("$x$ y $y$ son congruentes modulo $n$").

   (a) Demuestra que congruencia modulo $n$ es una relación de equivalencia.

   **Demostración:** (1) $\forall x \in \mathbb{Z}, x - x = 0 \in n\mathbb{Z} \implies x \equiv x \pmod{n} \implies R_n$ es reflexiva.

   (2) $\forall x, y \in \mathbb{Z}, x \equiv y \pmod{n} \implies (x - y) \in n\mathbb{Z} \implies \exists k \in \mathbb{Z}$ tal que $x - y = nk \implies y - x = nk = n(-k) \in n\mathbb{Z} \implies y \equiv x \pmod{n} \implies R_n$ es simétrico.

   (3) $\forall x, y, z \in \mathbb{Z}, x \equiv y$ y $y \equiv z \pmod{n} \implies \exists k, l \in \mathbb{Z}$ tal que $x - y = nk, y - z = nl \implies x - z = (x - y) + (y - z) = nk + nl = n(k + l) \in n\mathbb{Z} \implies x \equiv z \pmod{n} \implies R_n$ es transitivo. □

   Notación: el conjunto de las clases de equivalencia mod $n$, o sea $\mathbb{Z}/R_n$, se denota por $\mathbb{Z}/n\mathbb{Z}$ o simplemente por $\mathbb{Z}_n$ (se lee: $\mathbb{Z}$ mod $n$).

   (b) Demuestra que $\#(\mathbb{Z}/n\mathbb{Z}) = n$ (o sea, que hay $n$ clases de equivalencia mod $n$).

   **Demostración:** sea $f : \{0, 1, 2, \dots, n - 1\} \to \mathbb{Z}/n\mathbb{Z}$ la función dada por $f(x) = [x]$. Demostramos que $f$ es una biyección:

   Si $0 \leq x, y \leq n - 1, f(x) = f(y) \implies x \equiv y \pmod{n} \implies (x - y) \in n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$. Por otro lado, como $0 \leq x, y \leq n - 1 \implies -n + 1 \leq x - y \leq n - 1 \implies x - y = 0 \implies x = y$. Así que $f$ es inyectiva.

   Sea $[x] \in \mathbb{Z}/n\mathbb{Z}$. Sea $m := \max\{k \mid kn \leq x\}$. Por la definición de $k$, $r := x - kn$ satisface $0 \leq r < n$. Así que $r \in \{0, 1, 2, \dots, n - 1\}$ y $f(r) = [r] = [x]$, ya que $x - r = kn \implies x \equiv r \pmod{n}$. Así que $f$ es suprayectiva.

   Concluimos entonces que $f$ es una biyección, así que $\#(\mathbb{Z}/n\mathbb{Z}) = \#\{0, 1, \dots, n - 1\} = n$. La última igualdad se deja como ejercicio (muy facil). □

3. (a) Sea $A$ un anillo. Demuestra que para cada tres elementos $a, b, c \in A$, $a + c = b + c \implies a = b$.

   **Demostración:** Si $c \in A \implies \exists c' \in A$ tal que $c + c' = 0$ (Ax. 4) $\implies (a + c) + c' = (b + c) + c' \implies a + (c + c') = b + (c + c')$ (Ax. 2) $\implies a + 0 = b + 0 \implies a = b$ (Ax. 3). □

   (b) Sea $F$ un campo. Demuestra que para cada tres elementos $a, b, c \in F$, $c \neq 0$, $ac = bc \implies a = b$. □

   **Demostración:** Si $c \in F, c \neq 0 \implies \exists c' \in F$ tal que $cc' = 1$ (Ax. 8) $\implies (ac)c' = (bc)c' \implies a(cc') = b(cc')$ (Ax. 6) $\implies a1 = b1 \implies a = b$ (Ax. 7). □

   (c) (Opcional) Decide si el inciso anterior sigue siendo cierto en cualquer anillo (si es cierto – hay que demostrarlo, si no – hay que dar un contra-ejemplo).

   **Respuesta:** El inciso anterior no es cierto en general (aunque hay anillos que no son campos, como $\mathbb{Z}$, en donde sí es cierto). Un ejemplo es $A = \mathbb{Z}/4\mathbb{Z}$ con la estructura de anillo heredada de $\mathbb{Z}$ (esto lo vamos a ver mas tarde en el curso). En este anillo tenemos $[2][2] = [0][2] = 0$, aunque $[2] \neq [0]$. Mas general, tenemos tales ejemplos en todos los anillos $\mathbb{Z}/n\mathbb{Z}$ (los eneteros mod $n$), donde $n$ no es primo.