Algebra Lineal 1, agsto-dic, 2003.

Tarea num. 4
(Para el 5 sept, 2003)

Definiciones:

- Una *relación* en un conjunto X es un subconjunto $R \subset X \times X$. Cuando $(a,b) \in R$ escribimos aRb ("a y b estan relacionados según R").
- Una relación R en un conjunto X es una *relación de equivalencia* si es (1) reflexiva: $\forall x \in X, xRx$; (2) simétrica: $\forall x, y \in X, xRy \Rightarrow yRx$; (3) transitiva: $\forall x, y, z \in X$, $xRy, yRz \Rightarrow xRz$.
- Si R es una relación de equivalencia en X y $x \in X$ entonces la *clase de equivalencia de* x (según R) se define por $[x] := \{y \in X \mid xRy\}$. El conjunto de las clases de equivalencia según R se denota por X/R; se lee: X modulo R (ó X mod R).
- Una *partición* de un conjunto X es una familia $\{X_i\}_{i \in I}$ de subconjuntos de X tal que (1) $\bigcup_{i \in I} X_i = X$, (2) $\forall i, j \in I$, $i \neq j \Rightarrow X_i \cap X_j = \emptyset$.
- Un *campo* es un conjunto F con dos operaciones $s : F \times F \to F$ y $p : F \times F \to F$ ("producto" y "suma"), denotados por $x + y = s(x,y)$ y $xy = p(x,y)$, y dos elementos distintos denotados por $0, 1 \in F$, tal que los siguienetes 9 propiedades ("axiomas") se cumplen (1) $\forall x, y \in F : x + y = y + x$ (2) $\forall x, y, z \in F : (x+y)+z = x+(y+z)$ (3) $\forall x \in F : 0+x = x$ (4) $\forall x \in F\ \exists y \in F : x+y = 0$. (5) $\forall x, y \in F : xy = yx$ (6) $\forall x, y, z \in F : (xy)z = x(yz)$ (7) $\forall x \in F : 1x = x$ (8) $\forall x \in F$, $x \neq 0 \Rightarrow \exists y \in F : xy = 1$. (9) $\forall x, y, z \in F : (x+y)z = xz + yz$.
  Si se cumplen todas las propiedades excepto (posiblemente) la propiedad (8) decimos que tenemos un *anillo*. (Nota: todo campo es un anillo, pero al reves no).

Problemas

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) $X = \mathbb{R}$, $R = \{(x,y) \mid x \leq y\}$.
   (b) $X = \mathbb{R}$, $R = \{(x,y) \mid (x-y) \in \mathbb{Z}\}$.
   (c) $X = \mathbb{Z}$, $R = \{(x,y) \mid x \text{ divide a } y\}$. (Definición: x divide a y si $x \neq 0$ y existe un $r \in \mathbb{Z}$ tal que $y = xr$. Notacion: $x|y$.)
   (d) $X = \mathbb{Z} \setminus \{0\}$, $R = \{(x,y) \mid x \text{ divide a } y\}$.
   (e) $X = P(A)$, donde A es un conjunto, $R = \{(B,C) \mid B \sim C\}$.
   (f) $X = P(A)$, $R = \{(B,C) \mid B \subset C\}$.

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.

   Notación: el conjunto de la 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 $\#(\mathbb{Z}_n/n\mathbb{Z}) = n$ (o sea, hay n clases de equivalencia mod n).

   Sugerencia: Demuestra que la función $f : \{1, 2, \ldots, n\} \to \mathbb{Z}/n\mathbb{Z}$, $f(x) = [x]$, es una biyección.

3. (a) Sea A un anillo. Demuestra que para cada tres elementos $a, b, c \in A$, $a + c = b + c \Rightarrow a = b$.
   (b) Sea F un campo. Demuestra que para cada tres elementos $a, b, c \in F$, $c \neq 0$, $ac = bc \Rightarrow a = b$.
   (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).