Pauta Control 2 MA11A ALGEBRA

30 de Mayo de 1996

P1.-

(i) Probemos que R es una relación refleja, simétrica y transitiva (0.2 ptos.)
Refleja: Sea $n \in \mathbb{Z}$. Como $f(n) = f(n)$ entonces se tiene directamente que $n\ R\ n$, siendo la relación refleja (0.6 ptos.).
Simétrica: Sean $n, m \in \mathbb{Z}$ y supongamos que $n\ R\ m$, es decir $f(n) = f(m)$. Como la igualdad es simétrica entonces también se tiene que $f(m) = f(n)$ que es equivalente con $m\ R\ n$, probando así que R es simétrica (0.6 ptos.).
Transitiva: Sean $n, m, l \in \mathbb{Z}$ tales que $n\ R\ m$ y $m\ R\ l$. Por definición se tiene entonces que $f(n) = f(m)$ y $f(m) = f(l)$. Pero la igualdad es transitiva, luego $f(n) = f(l)$, lo que equivale a decir que $n\ R\ l$. Esto prueba que R es transitiva (0.6 ptos.).

(ii) Como $0 + 0 = 0$ entonces se tiene que $f(0 + 0) = f(0)$. Usando en la expresión anterior la propiedad de f se tiene que $f(0) + f(0) = f(0)$. Despejando se concluye que $f(0) = 0$ (0.5 ptos.).

(iii) Como $m - m = 0$ entonces $f(m - m) = f(0)$. Usando la parte anterior y la propiedad de f se tiene $f(m) + f(-m) = 0$. Despejando se concluye que $f(-m) = -f(m)$ (0.5 ptos).

(iv) Probemos primero que si f es inyectiva entonces $f^{-1}(\{0\}) = \{0\}$. Para ello tomemos un entero $n \in f^{-1}(\{0\})$, lo que equivale a decir que $f(n) = 0$. Pero de la parte (ii) sabemos que $f(0) = 0$, entonces $f(n) = f(0)$. Luego usando la inyectividad de f se concluye que $n = 0$ probando que la única preimagen de 0 por f es el 0 (1.5 ptos.).

Probemos ahora la recíproca. Es decir, si $f^{-1}(\{0\}) = \{0\}$ entonces f es inyectiva. Tomemos entonces $n, m \in \mathbb{Z}$ tales que $f(n) = f(m)$. Entonces se tiene que $f(n) - f(m) = f(n - m) = 0$. Pero estamos suponiendo que 0 es la única preimagen de 0 por f, luego $n - m = 0$ y entonces $n = m$. Esto último prueba que f es inyectiva (1.5 ptos.).

P2.-
(i) Sean A y B subconjuntos estables de E, es decir $f^{-1}(f(A)) = A$ y $f^{-1}(f(B)) = B$. Probemos que $A \cup B$ es estable. Sabemos que $f(A \cup B) = f(A) \cup f(B)$ y por otro lado $f^{-1}(f(A) \cup f(B)) = f^{-1}(f(A)) \cup f^{-1}(f(B))$. Usando la estabilidad de A y B, y juntando las igualdades anteriores se tiene que $f^{-1}(f(A \cup B)) = A \cup B$. Esto prueba que $A \cup B$ es estable (1.5 ptos.).

Probemos finalmente que $A \cap B$ es estable. Notemos que sólo es cierto en general que $f(A \cap B) \subseteq f(A) \cap f(B)$ lo que nos obliga a probar dos inclusiones. La primera, $A \cap B \subseteq f^{-1}(f(A \cap B))$, es directa de las definiciones de conjunto imagen y preimagen (0.5 ptos.). La inclusión contraria es necesario probarla. Sea $y \in f^{-1}(f(A \cap B))$. Entonces $f(y) \in f(A \cap B) \subseteq f(A) \cap f(B)$, lo que implica que $f(y) \in f(A)$ y $f(y) \in f(B)$, o equivalentemente $y \in f^{-1}(f(A))$ y $y \in f^{-1}(f(B))$. Pero A y B son estables, luego $y \in A$ y $y \in B$. Hemos probado que $f^{-1}(f(A \cap B)) = A \cap B$ (1 pto.).

(ii) Probemos que R^* es una relación de orden, es decir es refleja, antisimétrica y transitiva (0.2 ptos.).
Refleja: Sea $f \in \mathcal{F}$. Como R es refleja entonces para cada $a \in A$, $f(a)Rf(a)$. Es decir R^* es refleja (0.5 ptos).
Antisimétrica: Sean f y g en $\mathcal{F}$. Supongamos que $fR^*g \ \wedge \ gR^*f$. Entonces para cada $a \in A$ se tiene que $f(a)Rg(a)$ y $g(a)Rf(a)$. Pero R es antisimétrica, luego $f(a) = g(a)$ en cada $a \in A$. Como el dominio y recorrido de las funciones f y g son los mismos entonces la igualdad anterior prueba que $f = g$ y la relación es antisimétrica (0.8 ptos.).
Transitiva: Sean f, g y h funciones en $\mathcal{F}$. Supongamos que fR^*g y gR^*h. Es decir para cada elemento $a \in A$ se tiene $f(a)Rg(a)$ y $g(a)Rh(a)$. Luego por transitividad de R, $f(a)Rh(a)$. Hemos probado que R^* es transitiva (0.5 ptos.).

Supongamos ahora que A y B poseen al menos 2 elementos. Es decir $A = \{a, b\} \cup \bar{A}$ y $B = \{c, d\} \cup \bar{B}$. Definamos las funciones f y g en $\mathcal{F}$ por: $f(a) = c, f(b) = d, \forall\ \bar{a} \in \bar{A}, f(\bar{a}) = c$ y $g(a) = d, g(b) = c, \forall\ \bar{a} \in \bar{A}, f(\bar{a}) = c$. Las funciones f y g no son comparables por R^*. En efecto, si lo fuesen entonces $f(a)Rg(a)$ y $f(b)Rg(b)$, lo que implica que $c = d$, que es una contradicción (1 pto.).

P3.-

(i) Si x es solución de $x^2 = 1 \ (mod \ n)$ entonces existe un entero k tal que $x^2 - 1 = k \ n$, o bien factorizando, $(x-1)(x+1) = k \ n$. Notar que $k \in I\!N$ puesto que $x^2 - 1 > 0$ en soluciones no triviales. Esto prueba que n divide a $(x-1)(x+1)$ (2 ptos.).

(ii) Supongamos que n es un número primo y que x es solución no trivial de la ecuación. Entonces n divide a $(x+1)(x-1)$. Esto implica que n divide a $x+1$ o bien a $x-1$. Es decir x es solución trivial de la ecuación, lo que es una contradicción (2 ptos.).

(iii) Como x es solución no trivial de la ecuación entonces n no puede dividir a $x+1$ ni a $x-1$. Pero del punto (i) n divide a $(x+1)(x-1)$, lo que implica que p o q debe dividir a $x+1$ pero no ambos. Esto prueba que $MCD(n, x+1) \in \{p, q\}$.