Universidad de la República - Facultad de Ingeniería - IMERL
Matemática Discreta 2, semipresencial

Tercer prueba - 24 de octubre de 2016.

Ejercicio 1. (7 puntos)
Dado $(G, *, e)$ un grupo de orden finito, y sea $g \in G$.

a. Probar que: $o(g)||G|$ (el orden de g divide al orden de G).

b. Demostrar que $g^{|G|} = e$.

c. Demostrar el teorema de Euler.

Sugerencia: utilizar las partes a. y b. considerando $G = U(n)$.

Solución:

a. (3 puntos) Lo primero a observar es que el orden del subgrupo $< g >$ coincide con el orden del elemento $o(g)$ (ver Proposición 3.7.9; en la prueba se podría citar la Proposición enunciándola con precisión o bien demostrarla). Como $< g >$ es subgrupo de G entonces podemos usar el Teorema de Lagrange y obtenemos que $o(g) = | < g > |$ divide a $|G|$.

b. (1 punto) Sabemos que $g^{o(g)} = e$. Por el ítem anterior $o(g)$ divide a $|G|$. O sea existe $k \in \mathbb{N}$ tal que $k.o(g) = |G|$. Entonces $g^{|G|} = g^{k.o(g)} = (g^{o(g)})^k = e^k = e$.

c. (3 puntos) Consideramos $G = U(n)$. Recordamos que $|U(n)| = \varphi(n)$ (función de Euler). Un entero positivo a es un elemento de $U(n)$ si y solo si a es coprimo con n. O sea $a \in U(n)$, si y solo si $\text{mcd}(a, n) = 1$. Utilizando el ítem **b.** se obtiene que $a^{\varphi(n)} = 1$, para todo $a \in \mathbb{N}$ tal que $\text{mcd}(a, n) = 1$.

Ejercicio 2. (8 puntos)
(Ejercicio 13 del Práctico 7; Examen Julio 2012)

a. Probar que si $\phi : G_1 \to G_2$ es un homomorfismo de grupos finitos y $g \in G_1$, entonces $o(\phi(g)) \mid mcd(|G_1|, |G_2|)$.

b. Hallar todos los homomorfismos $\phi : \mathbb{Z}_2 \to U(8)$.

c. Hallar p sabiendo que p es primo, y existe un homomorfismo no trivial $\phi : \mathbb{Z}_{51} \to \mathbb{Z}_p$ tal que $\phi(\overline{17}) = \overline{0}$.

Solución:

a. (3 puntos) Observar primero que $o(\phi(g))$ divide a $|G_2|$, a causa del ítem **a.** del Ejercicio anterior.

Por otro lado si restringimos el homomorfismo ϕ al subgrupo generado por g, se obtiene el homomorfismo $\phi_{|<g>} :< g > \longrightarrow G_2$. Luego, usando el Teorema de órdenes (Teorema 3.9.8), tenemos que $o(g) = | < g > | = |\ker(\phi_{|<g>})| \times |\text{Im}(\phi_{|<g>})|$.

Obsérvese que $\text{Im}(\phi_{|<g>}) =< \phi(g) >$. Concluimos que $o(\phi(g)) = | < \phi(g) > | = |\text{Im}(\phi_{|<g>})|$ divide a $o(g)$. Pero, nuevamente por el ítem **a.** del Ejercicio anterior, se tiene que $o(g)||G_1|$.

Como hemos probado que $o(g)||G_1|$ y que $o(g)||G_2|$, entonces $o(\phi(g)) \mid mcd(|G_1|, |G_2|)$ (Corolario 1.2.9).

b. (2 puntos) En $\mathbb{Z}_2$ tenemos solamente dos elementos $[0], [1]$. En $U(8)$ tenemos $\{1, 3, 5, 7\}$, donde 3, 5 y 7 tienen orden 2. Luego, todo homomorfismo $\phi : \mathbb{Z}_2 \to U(8)$, queda definido por la imagen de $[1]$. Si enviamos $[1]$ a $1 \in U(8)$, entonces obtenemos el homomorfismo trivial. Pero también podemos enviar $[1]$ al 3, 5 o 7 en $U(8)$ porque todos tienen orden 2. O sea, tenemos cuatro homomorfismos posibles (que son cuatro formas de ver a $\mathbb{Z}_2$ como subgrupo de $U(8)$).

c. (3 puntos) Supongamos que $\phi(\overline{3}) = \overline{0}$. Entonces $\phi(\overline{3} + \overline{3} + \overline{3} + \overline{3} + \overline{3} + \overline{3}) = \phi(\overline{3}) + \phi(\overline{3}) + \phi(\overline{3}) + \phi(\overline{3}) + \phi(\overline{3}) + \phi(\overline{3}) = \overline{0}$. O sea $\phi(\overline{18}) = \overline{0}$. Como $\phi(\overline{17}) = \overline{0}$ (por hipótesis), entonces $\phi(\overline{34}) = \overline{0}$. Luego $\phi(\overline{34 + 18}) = \phi(\overline{34}) + \phi(\overline{18}) = \overline{0}$, pero por otro lado $\overline{34 + 18} = \overline{1}$. Entonces $\phi(\overline{1}) = \phi(\overline{34 + 18}) = \overline{0}$. Se concluye que si $\phi(\overline{3}) = \overline{0}$ entonces ϕ es el homomorfismo trivial. Entonces, $\phi(\overline{3})$ no puede ser $\overline{0}$. Pero $o(\overline{3}) = 17$, luego usando el ítem **a.** de este Ejercicio, se tiene que $1 \neq o(\phi(\overline{3}))$ divide a p (primo) y a 17. Luego $o(\phi(\overline{3})) = 17$ y por lo tanto $p = 17$.