

SOLUCIONES DEL SEGUNDO PARCIAL DE MATEMÁTICA DISCRETA 2.
26 DE JUNIO DE 2009

Ejercicio 1. Sea G un grupo abeliano finito, $s \in \mathbb{Z}$. Definimos la función $\psi : G \rightarrow G$ como $\psi(x) = x^s$.

1. Mostrar que ψ es un morfismo de grupos:

$$\psi(xy) = (xy)^s = x^s y^s \text{ (donde la última igualdad se verifica por ser } G \text{ abeliano).}$$

2. Probar que si s y $|G|$ son coprimos, entonces ψ es biyectiva:

Inyectividad: Si $\psi(x) = \psi(y) \Rightarrow x^s = y^s$.

Por Bezout existen $\alpha, \beta \in \mathbb{Z}$ tales que $\alpha s + \beta |G| = 1$. Como $x^{|G|} = e$ se tiene que:

$$x = x^1 = x^{\alpha s + \beta |G|} = (x^s)^\alpha \cdot (x^{|G|})^\beta = (x^s)^\alpha = (y^s)^\alpha = (y^s)^\alpha \cdot (y^{|G|})^\beta = y^{\alpha s + \beta |G|} = y$$

Lo que prueba la inyectividad de ψ .

Como $\psi : G \rightarrow G$ es inyectiva y G finito entonces ψ es una biyección.

3. Probar que si s y $|G|$ no son coprimos, entonces ψ no es biyectiva:

Sea $d = \text{mcd}(s, |G|)$ y consideramos p primo tal que $p|d$. Como $d|s$ resulta que $p|s$ (o sea $s = kp$, con $k \in \mathbb{Z}$). De igual forma $p|d$ implica $p||G|$, luego por Cauchy existe $H < G$ con $|H| = p$. Por Lagrange resulta que $h^p = e$ para todo $h \in H$ y por lo tanto $h^s = (h^p)^k = e^k = e$. Para ver que ψ no es inyectiva nos basta con tomar dos elementos distintos de H (ambos van a parar a e con ψ).

4. Sea $h : S_3 \rightarrow S_3$ definida como $h(\sigma) = \sigma^2$. ¿Es h un morfismo?:

Si h fuese morfismo, $h(ab) = h(a)h(b), \forall a, b \in S_3$, es decir $(ab)^2 = a^2 b^2, \forall a, b \in S_3$ y esto implicaría que S_3 es abeliano, lo cual sabemos que es falso. Entonces h no es un morfismo.

(Para una prueba directa basta con un contraejemplo, se pueden tomar por ejemplo $a = (1 \ 2)$ y $b = (1 \ 3)$, resulta $h(ab) \neq h(a)h(b)$).

Ejercicio 2.

1. Sea $H < G$ de orden m y $g \in G$, probar que $K = gHg^{-1}$ también es un subgrupo de G . ¿Cuál es el cardinal de K ? (justifique su respuesta):

i) No vacío: $e = geg^{-1} \in K$ pues $e \in H$.

ii) Cerrado por producto: Si $k_1 = gh_1g^{-1}$ y $k_2 = gh_2g^{-1}$ con $h_1, h_2 \in H$ resulta que $k_1 k_2 = gh_1 h_2 g^{-1} \in K$ (pues $h_1 h_2 \in H$).

- iii) Cerrado por inverso: Si $k = ghg^{-1}$ con $h \in H$ entonces $g^{-1} = (ghg^{-1})^{-1} = gh^{-1}g^{-1} \in K$ (pues $h^{-1} \in H$).

El cardinal de K es el mismo que el de H , para verlo alcanza encontrar una biyección entre ambos conjuntos. Consideramos $\varphi : H \rightarrow K$ tal que $\varphi(h) = ghg^{-1}$.

φ es sobreyectiva por definición de K . Como $\varphi(h_1) = \varphi(h_2) \Rightarrow gh_1g^{-1} = gh_2g^{-1} \Rightarrow h_1 = h_2$ (esto último es por la cancelativa por izquierda y por derecha en un grupo), por lo tanto φ es la biyección buscada.

2. Sea G un grupo y H y K dos subgrupos distintos de G , supongamos que $|H| = |K| = m$ y sea q el menor divisor primo de m . Probar que $|H \cap K| \leq m/q$.

Como $H \cap K < H \Rightarrow |H \cap K|$ divide a $|H| = m$, si $|H \cap K| = m$ entonces $H \cap K = H \Rightarrow H \subset K$, pero al tener el mismo cardinal resultaría $H = K$ lo cual es absurdo.

Por consiguiente $|H \cap K|$ es un divisor de m menor que m así que $|H \cap K| \leq m/q$ como queríamos probar.

3. Sea G un grupo de orden n y p el menor divisor primo de n , sea $H < G$ con $[G : H] = p$. Supongamos además que p^2 no divide a n . Probar que $H \triangleleft G$:

Sea $n = pm$, como $p^2 \nmid n$ resulta $p \nmid m$. Sea q el menor divisor primo de m . Como $[G : H] = p$ tenemos que $|H| = m$.

Supongamos que $H \not\triangleleft G$ entonces existe $g \in G$ tal que $gHg^{-1} \neq H$. Llamemos $K = gHg^{-1}$.

Por la primera parte $K < G$, $|H| = |K| = m$ y por nuestra suposición $H \neq K$. Por la segunda parte $|H \cap K| \leq m/q$. Luego tenemos que:

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{m^2}{|H \cap K|} \geq \frac{m^2}{m/q} = qm$$

Pero $q|n$ (pues $q|m$) y $q \neq p$ (pues $p \nmid m$) así que $q > p$ lo cual implicaría que $|HK| \geq qm > pm = n$ lo cual es absurdo pues $HK \subset G$ y $|G| = n$. Por lo tanto H es normal.

Ejercicio 3.

1. Sea $n \in \mathbb{Z}^+$ impar y sea $b \in \mathbb{Z}$ tal que $2 \leq b \leq n-1$. Si $b^{n-1} \equiv 1 \pmod{n}$ y $b^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$, para cada factor primo p de $n-1$, demostrar que n es primo:

Para probar que n es primo basta chequear que $\varphi(n) = n-1$.

Por un lado $\varphi(n) \leq n-1$ por definición.

Sea s el orden de b en \mathbb{Z}_n^* .

Como $b^{n-1} \equiv 1 \pmod{n} \Rightarrow s|n-1$

Como $b^{(n-1)/p} \not\equiv 1 \pmod{n} \Rightarrow s \nmid (n-1)/p$ para todo primo $p|n$.

Por lo tanto $s = n-1$, por Lagrange resulta que $s|\varphi(n)$ lo cual implica $\varphi(n) \geq n-1$, luego $\varphi(n) = n-1$ y por lo tanto n es primo.

2. Hallar un b que verifique las condiciones del ítem anterior si $n = 71$. (Sug.: usar que $7^5 \equiv 51 \pmod{71}$)

Tomemos $b = 7$.

$$7^{10} \equiv (51)^2 \equiv (-20)^2 \equiv 45 \pmod{71}.$$

$$7^{14} \equiv (-10) \cdot 7^{15} \equiv (-10) \cdot (-20)^3 \equiv 45 \cdot 58 \equiv 26 \cdot 13 \equiv 54 \pmod{71}.$$

$$7^{35} \equiv (51)^7 \equiv (-20)^7 \equiv -(2)^{14} \cdot 5^7 \equiv -1 \pmod{71} \text{ (en la última congruencia se usó que } 2^6 = 64 \equiv -7 \pmod{71} \text{ y que } 5^3 \equiv -17 \pmod{71}\text{)}.$$

$$\text{Finalmente } 7^{70} \equiv (7^{35})^2 \equiv (-1)^2 \equiv 1 \pmod{71}.$$

3. Resolver: $x^{15} \equiv 51 \pmod{71}$:

Por la parte anterior 7 es raíz primitiva módulo 71 así que $x \equiv 7^t \pmod{71}$ con $0 \leq t < 70$. Se tiene que:

$$x^{15} \equiv 7^{15t} \equiv 7^5 \Leftrightarrow 15t \equiv 5 \pmod{70} \Leftrightarrow 3t \equiv 1 \pmod{14} \Leftrightarrow t \equiv 5 \pmod{14}$$

Luego $t = 14s + 5$ con $0 \leq t < 70$ implica que $t \in \{5, 19, 33, 47, 61\}$. Así que las soluciones son los $x \equiv 7^5, 7^{19}, 7^{33}, 7^{47}, 7^{61} \pmod{71}$.