Diciembre 2023

Ejercicio 5. Sean a y b enteros positivos. Considere las siguientes proposiciones:

(i) Si m es un número primo divisor de a que no divide a b y n un número primo divisor de b que no divide a a, entonces $\operatorname{mcd}(\frac{a}{m}, b) = \operatorname{mcd}(a, \frac{b}{n})$. Verdadera

(ii) Si m es un divisor de a que no divide a b y n un divisor de b que no divide a a, entonces $\operatorname{mcd}(\frac{a}{m}, b) = \operatorname{mcd}(a, \frac{b}{n})$.

Entonces elija la opción correcta:

(A) sólo (i) es verdadera

(B) sólo (ii) es verdadera

(C) las dos son verdaderas

(D) las dos son falsas

a y b enteros positivos

(i) m primo tq $m \mid a$ y $m \nmid b$

n primo tq $n \nmid a$ y $n \mid b$

$\operatorname{mcd}(\frac{a}{m}, b) = \operatorname{mcd}(a, \frac{b}{n})$?

$\rightarrow$ $a = \underbrace{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}}_{\text{descomposición en primos}}$ donde alguno de los p_i es m y ninguno de los p_i es n

$a = m^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ donde $p_i \neq n$ para todo $i = 2, \ldots, r$

$\rightarrow$ $b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\alpha_s}$ donde alguno de los q_i es n y ninguno de los q_i es m

$b = n^{\beta_1} q_2^{\beta_2} \cdots q_s^{\alpha_s}$ donde $q_i \neq m$ para todo $i = 2, \ldots, s$

$\rightarrow$ $\operatorname{mcd}(a,b) =$

$a = 2^3 \cdot 5^2 \cdot 7$

$b = 3^2 \cdot 5^3 \cdot 7^2$

divisor de a: $2^2 \cdot 5 \cdot 7$

no divisor de a: $2 \cdot 5 \cdot 11$

$\operatorname{mcd}(a,b) = 5^2 \cdot 7$

$a = 2^3 \cdot 3^0 \cdot 5^2 \cdot 7$

$b = 2^0 \cdot 3^2 \cdot 5^3 \cdot 7^2$

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$$

$$mcd(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_r^{\min\{\alpha_r,\beta_r\}}$$

<u>volviendo al ejercicio</u>

$$a = n^0 m^x p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \qquad x \geq 1$$

$$b = n^y m^0 p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$$

$$mcd(a,b) = n^0 m^0 p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_r^{\min\{\alpha_r,\beta_r\}}$$

$$\frac{a}{m} = n^0 m^{x-1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

$$mcd\left(\frac{a}{m}, b\right) = n^0 m^0 p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_r^{\min\{\alpha_r,\beta_r\}}$$

$$\Rightarrow mcd\left(\frac{a}{m}, b\right) = mcd(a,b)$$

$$mcd\left(a, \frac{b}{n}\right) = n^0 m^0 p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_r^{\min\{\alpha_r,\beta_r\}}$$

$$a = n^0 m^x p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

$$\frac{b}{n} = n^{y-1} m^0 p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$$

entonces $mcd\left(\frac{a}{m}, b\right) = mcd\left(a, \frac{b}{n}\right)$

(ii) a y b enteros positivos

m entero tal que $m \mid a$ y $m \nmid b$

n entero tal que $n \nmid a$ y $n \mid b$

$\Rightarrow mcd\left(\frac{a}{m}, b\right) = mcd\left(a, \frac{b}{n}\right)$?

buscamos un contraejemplo

$a = 12 \qquad b = 27$

$m = 6 \qquad n = 9$

$\text{mcd}\left(\frac{a}{m}, b\right) = \text{mcd}\left(\frac{12}{6}, 27\right) = \text{mcd}(2, 27) = 1$

$\text{mcd}\left(a, \frac{b}{n}\right) = \text{mcd}\left(12, \frac{27}{9}\right) = \text{mcd}(12, 3) = 3$

entonces la afirmación 2 es falsa.

2) (10 puntos) Demostrar que si N es un subgrupo normal de G entonces:

a. G/N es un grupo.

b. El mapa $\pi : G \to G/N$, definido $\pi(g) = gN$, es un homomorfismo sobreyectivo.

c. El kernel de π es N.

N subgrupo normal de G:

$G/N = \{gN : g \in G\}$

a) Queremos probar que G/N es un grupo

① Vamos a definir una operación en G/N

$$\underbrace{(g_1N)}_{\substack{g_1h \,:\, h \in N \\ \underbrace{g_1 e}_{g_1},\, g_1h_1,\, g_1h_2 \ldots}} \cdot (g_2N) = (g_1g_2)N$$

operación del grupo G

→ tenemos que verificar que esta operación está bien definida

es decir, tenemos que ver que

$$\left.\begin{array}{l} \tilde{g}_1 \in g_1N \\ \tilde{g}_2 \in g_2N \end{array}\right\} \Rightarrow \underbrace{(\tilde{g}_1\tilde{g}_2)N = (g_1g_2)N}$$

para probar esto alcanza con ver que

$\tilde{g}_1\tilde{g}_2 \in (g_1g_2)N$

entonces vamos a probar

$$\left.\begin{array}{l}\tilde{g}_1 \in g_1 N \\ \tilde{g}_2 \in g_2 N\end{array}\right] \Rightarrow \underbrace{\tilde{g}_1 \tilde{g}_2 \in (g_1 g_2) N}$$

objetivo:

$\tilde{g}_1 \tilde{g}_2 = g_1 g_2 \bigcirc$ algo en N

tenemos:

$$\tilde{g}_1 \in g_1 N \Rightarrow \tilde{g}_1 = g_1 h_1 \text{ donde } h_1 \in N$$

$$\tilde{g}_2 \in g_2 N \Rightarrow \tilde{g}_2 = g_2 h_2 \text{ donde } h_2 \in N$$

entonces:

$$\tilde{g}_1 \tilde{g}_2 = g_1 \underbrace{h_1 g_2}_{\in N g_2} h_2 = g_1 g_2 \underbrace{\tilde{h}_1 h_2}_{\in N}$$

como N es un subgrupo normal:

$$N g_2 = g_2 N$$

entonces $h_1 g_2 \in N g_2 = g_2 N$

es decir $h_1 g_2 \in g_2 N$

$$\Rightarrow h_1 g_2 = g_2 \tilde{h}_1 \text{ para algún } \tilde{h}_1 \in N$$

(2) Verificamos que la operación

$$(g_1 N)(g_2 N) = (g_1 g_2) N$$

cumple las condiciones de grupo

* asociativa: $((g_1 N)(g_2 N))(g_3 N) = (g_1 N)((g_2 N)(g_3 N))$

$$((g_1 N)(g_2 N))(g_3 N) = ((g_1 g_2) N)(g_3 N)$$

$$= (\underbrace{(g_1 g_2) g_3}) N \quad \text{operación en } G \text{ que es un grupo}$$

$$= (g_1 (g_2 g_3)) N$$

$$= (g_1 N)((g_2 g_3)N)$$
$$= (g_1 N)((g_2 N)(g_3 N))$$

* existencia del neutro: $e_G N$ donde e_G es el neutro de G

$$(gN)(e_G N) = (g e_G)N = gN$$

* existencia de inversos: el inverso de gN es $(g^{-1})N$

$$(gN)(g^{-1}N) = (gg^{-1})N = e_G N = e_{G/N}$$

b) Definimos $\pi : G \longrightarrow G/N$
$$g \longmapsto gN$$

(1) π es un morfismo de grupos

sean $g_1, g_2 \in G$ y queremos probar que

$$\underbrace{\pi(g_1 g_2)}_{\text{operación de } G} = \underbrace{\pi(g_1)\,\pi(g_2)}_{\text{operación de } G/N}$$

$$\pi(g_1 g_2) = (g_1 g_2)N$$

$$\pi(g_1)\pi(g_2) = (g_1 N)(g_2 N) = (g_1 g_2)N$$

$\Rightarrow \pi(g_1 g_2) = \pi(g_1)\pi(g_2)$

$\Rightarrow \pi$ es un morfismo de grupos.

(2) π es sobreyectivo

Sea $gN \in G/N$

por definición $gN = \pi(g)$

$\Rightarrow gN \in \mathrm{Im}(\pi)$

$\Rightarrow \pi$ es sobreyectivo

c) $\pi : G \longrightarrow G/N$

$g \longmapsto gN$

queremos probar que $\ker(\pi) = N$

$g \in \ker(\pi) \iff \pi(g) = e_{G/N}$

$\iff gN = e_G N$

$\iff g \in e_G N$

$\iff g = e_G h$ para algún $h \in N$

$\iff g = h$ para algún $h \in N$

$\iff g \in N$

entonces $\ker(\pi) = N$