ESTRUCTURAS ALGEBRAICAS. Problemas. 21 de Septiembre.

Ejercicio 8. Hoja 1. (Transitividad de índices) Si $H \leq K \leq G$ comprobad que $[G : H] = [G : K][K : H]$.

Solución:

Tenemos que $G = \bigcup_{i \in I} g_i K$ con $g_i \in G$ e $|I| = [G : K]$, siendo las clases $g_i H$ disjuntas entre ellas. Por otro lado, tenemos que $K = \bigcup_{j \in J} k_j H$ con $k_j \in K$ y $|J| = [K : H]$, siendo las clases $k_j H$ disjuntas entre sí. Entonces tenemos que

$$G = \bigcup_{i \in I} g_i K = \bigcup_{i \in I} g_i \left(\bigcup_{j \in J} k_j H \right) = \bigcup_{(i,j) \in I \times J} g_i k_j H.$$

Veamos que las clases $g_i k_j H$ son disjuntas entre sí. Supongamos que no fuera así, es decir, que $g_i k_j H \cap g_l k_m H \neq \emptyset$. Entonces $g_i k_j H = g_l k_m H$. Así, las clases $g_i k_j H \subset g_i K$ y $g_m k_l H \subset g_l K$ tienen intersección no vacía. Por lo que, $g_i K = g_l K$. Pero estas las seleccionamos disjuntas, por tanto, $g_i = g_l$. Entonces $k_j H = k_m H$, de nuevo, estas eran clases disjuntas, por lo que, $k_j = k_m$. Concluimos que $g_i k_j = g_j k_l$ y, en consecuencia, $G = \bigcap_{(i,j) \in I \times J} g_i k_j H$ es una partición de G. Finalmente, observamos que

$$[G : H] = |I \times J| = |I||J| = [G : K][K : H].$$

Ejercicio 9. Hoja 1. Sean $H \leq K \leq G$. ¿Cuántos elementos puede tener K si $|H| = 4$ y $|G| = 24$?

Solución:

El Teorema de Lagrange nos dice que $|H| \mid |K|$ y $|K| \mid |G|$, es decir, $4 \mid |K|$ y $|K| \mid 24$. La primera condición se traduce en que $|K|$ es múltiplo de 4, es decir, que podemos escribir $|K| = 4k$, para algún entero positivo k. Junto con la segunda condición, tenemos que $4k \mid 24$, es decir, $k \mid 6$. Por tanto, $k \in \{1, 2, 3, 6\}$ y, en consecuencia, $|K| \in \{4, 8, 12, 24\}$.

Ejercicio 10. Hoja 1. Sea G un grupo y sean subgrupos H y K de G. Encontrad todos los posibles órdenes de $H \cap K$ cuando:

(a) $|H| = 16$ y $|K| = 20$;

(b) $|H| = |K| = 7$

(c) $|H| = 15$ y $|K| = 14$;

Solución:

(a) El Teorema de Lagrange nos dice que $|H \cap K|$ divide a $|H| = 16$ y divide a $|K| = 20$. Por lo que, $|H \cap K|$ es un divisor común de 16 y 20. Observamos que $\text{mcd}(16, 20) = 4$. Por tanto, los posibles órdenes de $|H \cap K|$ son $1, 2$ o 4.

En el grupo $\mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ podemos dar ejemplos de cada uno de los tres casos:

- Para $|H \cap K| = 1$, consideramos

$$H = \mathbb{Z}/16\mathbb{Z} \times \{[0]\}, \quad K = \{[0]\} \times \mathbb{Z}/20\mathbb{Z}, \quad H \cap K = \{([0], [0])\}$$

- Para $|H \cap K| = 2$, consideramos

$$H = \langle [2] \rangle \times \langle [10] \rangle, \quad K = \{[0]\} \times \mathbb{Z}/20\mathbb{Z}, \quad H \cap K = \langle ([0], [10]) \rangle$$

- Para $|H \cap K| = 4$, consideramos

$$H = \langle [4] \rangle \times \langle [5] \rangle, \quad K = \{[0]\} \times \mathbb{Z}/20\mathbb{Z}, \quad H \cap K = \langle ([0], [5]) \rangle$$

(b) El Teorema de Lagrange nos dice que $|H \cap K|$ divide a $|H| = |K| = 7$. Por lo que, $|H \cap K|$ es un divisor de 7. Por tanto, los posibles órdenes de $|H \cap K|$ son 1 o 7.

Podemos dar ejemplos de cada uno de los casos:

- Para $|H \cap K| = 1$, consideramos en $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$

$$H = \mathbb{Z}/7\mathbb{Z} \times \{[0]\}, \quad K = \{[0]\} \times \mathbb{Z}/7\mathbb{Z}, \quad H \cap K = \{([0], [0])\}$$

- Para $|H \cap K| = 7$, necesariamente se tiene $H = K$.

(c) El Teorema de Lagrange nos dice que $|H \cap K|$ divide a $|H| = 15$ y divide a $|K| = 14$. Por lo que, $|H \cap K|$ es un divisor común de 15 y 14. Observamos que $\operatorname{mcd}(15, 14) = 1$. Por tanto, el único orden posible de $|H \cap K|$ es 1.

Ejercicio 11. Hoja 1. Sea G un grupo, se define el centro de G como $\mathbf{Z}(G) = \{g \in G \mid gx = xg \text{ para todo } x \in G\}$. Demostrad que $\mathbf{Z}(G) \trianglelefteq G$.

Solución:

Comprobamos que $\mathbf{Z}(G)$ es un subgrupo:

(S1) Sean $g, h \in \mathbf{Z}(G)$. Para todo $x \in G$, tenemos que

$$ghx \underset{g \in \mathbf{Z}(G)}{=} hxg \underset{h \in \mathbf{Z}(G)}{=} xgh \implies gh \in \mathbf{Z}(G).$$

(S2) Sea e el elemento identidad de G. Claramente, tenemos que $ex = xe$. Por lo que, $e \in \mathbf{Z}(G)$.

(S3) Sea $g \in \mathbf{Z}(G)$. Para todo $x \in G$, tenemos que

$$g^{-1}x = (x^{-1}g)^{-1} \underset{g \in \mathbf{Z}(G)}{=} (gx^{-1})^{-1} = xg^{-1} \implies g^{-1} \in \mathbf{Z}(G).$$

Veamos que $\mathbf{Z}(G)$ es un subgrupo normal de G. Sean $g \in \mathbf{Z}(G)$ y $x \in G$. Para todo $y \in G$, tenemos que

$$xgx^{-1}y \underset{g \in \mathbf{Z}(G)}{=} xx^{-1}yg = yg = ygxx^{-1} \underset{g \in \mathbf{Z}(G)}{=} yxgx^{-1} \implies xgx^{-1} \in \mathbf{Z}(G).$$

Lema 1.79 Sean G y H grupos. Sean $g \in G$ y $h \in H$, de forma que (g,h) es un elemento de $G \times H$. Demostrar que $\mathrm{o}((g,h)) = \mathrm{mcm}(\mathrm{o}(g), \mathrm{o}(h))$.

Solución:

Caso finito. Supongamos que $\mathrm{o}(g) = n$ y $\mathrm{o}(h) = m$. Entonces

$$(g,h)^{nm} = (g^{nm}, h^{nm}) = ((g^n)^m, (h^m)^n) = (e_G^m, e_H^n) = (e_G, e_H).$$

Por lo que, (g,h) tiene orden finito, digamos $\mathrm{o}((g,h)) = k$. Entonces:

$$(e_G, e_H) = (g,h)^k = (g^k, h^k) \implies \mathrm{o}(g) \mid k \quad \text{y} \quad \mathrm{o}(h) \mid k$$

Como k es el menor entero con esa condición, concluimos que $k = \mathrm{mcm}(\mathrm{o}(g), \mathrm{o}(h))$.

Caso infinito. Supongamos que $\mathrm{o}(g) = \infty$ (o bien $\mathrm{o}(h) = \infty$), entonces $g^n \neq e_G$ (resp. $h^n \neq e_H$) para todo entero positivo n. Entonces $(g,h)^n \neq (e_G, e_H)$ para todo entero positivo n. Por tanto, $\mathrm{o}((g,h)) = \infty$.

Ejercicio 14. Hoja 1. Hallad todos los elementos del grupo $S_3 \times \mathbb{Z}/2\mathbb{Z}$ y determinad el orden de cada uno. Hallad los elementos de orden 9 del grupo $S_3 \times \mathbb{Z}/3\mathbb{Z}$.

Solución:

Elementos de $S_3 \times \mathbb{Z}/2\mathbb{Z}$. Recordamos que $S_3 = \{(1), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$. En S_3, el elemento identidad tiene orden 1, los $2-$ciclos tienen orden 2 y los $3-$ciclos tienen orden 3. En $\mathbb{Z}/2\mathbb{Z}$, el elemento neutro tiene orden 1 y el elemento $[1]_2$ tiene orden 2.

Aplicando el resultado del Lema 1.79, tenemos que:

- El elemento $((1), [0]_2)$ tiene orden 1.
- Los elementos $((1,2), b), ((1,3), b), ((2,3), b), ((1), [1]_2)$, con $b \in \mathbb{Z}/2\mathbb{Z}$ cualquiera, tienen orden 2.
- Los elementos $((1,2,3), [0]_2), ((1,3,2), [0]_2)$ tienen orden 3.
- Los elementos $((1,2,3), [1]_2), ((1,3,2), [1]_2)$ tienen orden 6.

Elementos de orden 9 de $S_3 \times \mathbb{Z}/3\mathbb{Z}$. En $\mathbb{Z}/3\mathbb{Z}$, el elemento identidad tiene orden 1 y los elementos $[1]_3$ y $[2]_3$ tienen orden 3. Vemos que $\mathrm{mcm}(\mathrm{o}(\sigma), \mathrm{o}(b)) \in \{1,2,3,6\}$, para todo $\sigma \in S_3$, $b \in \mathbb{Z}/3\mathbb{Z}$. Entonces, como consecuencia del Lema 1.79, concluimos que no existe ningún elemento de orden 9 en $S_3 \times \mathbb{Z}/3\mathbb{Z}$.

Ejercicio 15. Hoja 1. Sea G un grupo, decide razonadamente si cada una de las siguientes afirmaciones es verdadera o falsa:

a) $H \leq G$ y H conmutativo implica $H \trianglelefteq G$.

b) $H \leq G$ y $|H| = 2$ implica $H \trianglelefteq G$.

c) Si $H \trianglelefteq K$ y $K \trianglelefteq G$, entonces $H \trianglelefteq G$.

d) Si $H \trianglelefteq G$ y $|H| = m$ entonces H es el único subgrupo de G de orden m.

Solución:

(a) *Falso.* Sean $G = S_3$ y $H = \langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \rangle$. Claramente, H es un subgrupo conmutativo de G. Sin embargo, no es un grupo normal:

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \notin H.$$

Afirmación. El enunciado es cierto si H conmuta con todos los elementos de G, es decir, si $H \leq Z(G)$.

(b) *Falso.* Sean $G = D_8$ y $H = \langle s \rangle$. Claramente, H es un subgrupo de G con orden 2. Sin embargo, no es un grupo normal:

$$rsr^{-1} = sr^{-1}r^{-1} = sr^{-2} = sr^2 \notin H.$$

Afirmación. El enunciado es cierto si el índice $[G : H] = 2$, es decir, si $|G/H| = 2$. Ver Lema 3.31.

(c) *Falso.* Sean $G = D_8$, $K = \langle s, r^2 \rangle$ y $H = \langle s \rangle$. Observamos que

- H es un subgrupo normal de K, puesto que $H \subseteq K$ y $[K : H] = \frac{4}{2} = 2$.
- K es un subgrupo normal de G, puesto que $K \subseteq G$ y $[G : K] = \frac{8}{4} = 2$.
- Sin embargo, H no es normal en G, como hemos visto en el apartado (b).

Por tanto, la propiedad de un subgrupo de ser normal no es transitiva en general.

(d) *Falso.* Sea $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Observamos que en G existen exactamente 3 subgrupos de orden 2:

$$\langle ([0], [1]) \rangle, \quad \langle ([1], [0]) \rangle \quad \text{y} \quad \langle ([1], [1]) \rangle.$$

Todos ellos son normales por ser subgrupos de un grupo abeliano, pero todos ellos son distintos.

Ejercicio 20. Hoja 1. Sean $g, h \in G$ de orden finito con $(o(g), o(h)) = 1$. Demostrad que si $gh = hg$ entonces $o(gh) = o(g)o(h)$.

Solución:

Denotamos $\mathrm{o}(g) = m$ y $\mathrm{o}(h) = n$. Como $gh = hg$, tenemos que $(gh)^m = g^m h^m$. Por lo que, tenemos que

$$(gh)^{mn} = g^{mn} h^{mn} = (g^m)^n (h^n)^m = e^n e^m = e.$$

Entonces $o(gh)$ divide a mn. Sea $r = o(gh)$. Tenemos que $g^r h^r = e$. Tomando la potencia m-ésima, tenemos que $h^{rm} = e$, entonces $n|rm$. Pero $(m, n) = 1$, por lo que, $n|r$. Del mismo modo, tomando la potencia n-ésima, tenemos que $g^{rn} = e$, entonces $m|rn$. Pero $(n, m) = 1$, por lo que, $m|r$. Finalmente, como $(m, n) = 1$ y r es dividido por ambos, se tiene que $mn|r$. Concluimos entonces que $r = mn$.

Ejercicio 22. Hoja 1. Encontrad el número de generadores de los grupos cíclicos de órdenes $6, 8, 12$ y 60.

Solución:

Sabemos que todo grupo cíclico de orden n es isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Además, sabemos que $[1]_n$ es un generador de $\mathbb{Z}/n\mathbb{Z}$, es decir, todo elemento $[k]_n = k \cdot [1]_n$. También, sabemos que $[k]_n$ es un generador de $\mathbb{Z}/n\mathbb{Z}$ si y solo si $\mathrm{mcd}(k, n) = 1$. Por tanto, tenemos que

$$|\{\text{Generadores de } \ C_n\}| = |\{k \in \mathbb{N} : k \leq n, \mathrm{mcd}(k, n) = 1\}| = \varphi(n)$$

siendo φ la función de Euler. En los casos del enunciado, se tiene:

- *Generadores de C_6*. Tenemos
$$\varphi(6) = \varphi(2)\varphi(3) = (2-1)(3-1) = 2 \text{ generadores.}$$
- *Generadores de C_8*. Tenemos
$$\varphi(8) = \varphi(2^3) = (2-1)2^{3-1} = 4 \text{ generadores.}$$
- *Generadores de C_{12}*. Tenemos
$$\varphi(12) = \varphi(2^2)\varphi(3) = (2-1)2^{2-1}(3-1) = 4 \text{ generadores.}$$
- *Generadores de C_{60}*. Tenemos
$$\varphi(60) = \varphi(2^2)\varphi(3)\varphi(5) = (2-1)2^{2-1}(3-1)(5-1) = 16 \text{ generadores.}$$

Ejercicio 24. Hoja 1. Mostrad que en un grupo cíclico finito G de orden n, la ecuación $x^m = 1$ tiene exactamente m soluciones para cada m que divide a n. ¿Qué ocurre si $1 < m < n$ y m no divide a n?

Solución:

$(m|n)$ Sea g un generador de G. Como m divide a n, podemos escribir $n = sm$ para algún entero no nulo s. En primer lugar, observamos que el elemento g^s es una solución de la ecuación $x^m = e$, puesto que
$$(g^s)^m = g^{sm} = g^n = e.$$
Observamos que todo elemento del subgrupo generado por g^s también es solución de la ecuación. Cada elemento de $\langle g^s \rangle$ se escribe de la forma $(g^s)^k$ para algún $k \in \{1, ..., o(g^s)\}$. Comprobamos que

$$((g^s)^k)^m = g^{skm} = (g^{sm})^k = (g^n)^k = e^k = e, \qquad \text{para todo } k \in \{1, ..., o(g^s)\}.$$

Por lo que, $\langle g^s \rangle$ pertenece al conjunto de soluciones de la ecuación $x^m = e$. Sabemos que

$$o(g^s) = \frac{n}{(n, s)} = \frac{n}{s} = m.$$

Por tanto, ya hemos encontrado m soluciones de la ecuación $x^m = e$.

Veamos que no existen más soluciones. Supongamos que h es una solución de $x^m = e$. Como G es cíclico, podemos escribir $h = g^k$ para algún entero k. Entonces tenemos que $g^{km} = (g^k)^m = h^m = e$. Por lo que, eligiendo k suficientemente grande, se tiene que $n|km$. En consecuencia, $km = jn$ para algún entero j y se tiene $k = \frac{jn}{m} = js$. Por tanto, tenemos

$$g^k = g^{js} = (g^s)^j$$

y se tiene $g^k \in \langle g^s \rangle$. Entonces concluimos que el conjunto de soluciones es $\langle g^s \rangle$ y existen exactamente m soluciones para la ecuación $x^m = e$ en G.

($m \nmid n$) Sea g un generador de G. Denotamos por d al máximo común divisor de m y n, de forma que $n = sd$ y $m = kd$ para s, k enteros no nulos. En primer lugar, observamos que g^s es una solución de la ecuación $x^m = e$, puesto que

$$(g^s)^m = (g^s)^{kd} = (g^{sd})^k = (g^n)^k = e^k = e.$$

Observamos que todo elemento del subgrupo generado por g^s también es solución de la ecuación. Cada elemento de $\langle g^s \rangle$ se escribe como $(g^s)^t$ para algún $t \in \{1, ..., \mathrm{o}(g^s)\}$. Comprobamos que

$$((g^s)^t)^m = g^{stm} = g^{stkd} = (g^n)^{tk} = e^{tk} = e, \quad \text{para todo } t \in \{1, ..., \mathrm{o}(g^s)\}.$$

Por lo que, $\langle g^s \rangle$ pertenece al conjunto de soluciones de la ecuación $x^m = e$. Por la Proposición 2.40, sabemos que

$$\mathrm{o}(g^s) = \frac{n}{(n, s)} = \frac{n}{s} = d.$$

Por tanto, ya hemos encontrado d soluciones de la ecuación $x^m = e$.

Veamos que no existen más soluciones. Supongamos que h es una solución de $x^m = e$. Como G es cíclico, podemos escribir $h = g^t$ para algún entero t. Entonces tenemos que $g^{tm} = (g^t)^m = h^m = e$. Por lo que, eligiendo t suficientemente grande, se tiene que $n|tm$. En consecuencia, $tm = jn$ para algún entero j y se tiene $m|jn$. Como $(m, n) = d$, entonces $k|j$. Por lo que, $j = rk$ para algún entero r y, en consecuencia, $tm = rkn = rksd = rsm$ lo que implica que $t = sr$. Por tanto, tenemos

$$g^t = g^{sr} = (g^s)^r$$

y se tiene $g^t \in \langle g^s \rangle$. Entonces concluimos que el conjunto de soluciones es $\langle g^s \rangle$ y existen exactamente d soluciones para la ecuación $x^m = e$ en G.

Ejercicio 27. Hoja 1. Sea A un grupo abeliano. Demostrad que $A_{\mathrm{tor}} := \{a \in A \mid o(a) < \infty\} \leq A$. Comprobad que $\{M \in \mathrm{GL}_2(\mathbb{R}) \mid o(M) < \infty\}$ no es un subgrupo de $\mathrm{GL}_2(\mathbb{R})$.

Solución:

Comprobamos que A_{tor} es un subgrupo de A:

(S1) Sean $a, b \in A_{\mathrm{tor}}$. Denotamos $\mathrm{o}(a) = r$ y $\mathrm{o}(b) = s$. Entonces, como A es abeliano, tenemos

$$(ab)^{rs} = (a^r)^s (b^s)^r = e^s e^r = e.$$

Por lo que, $\mathrm{o}(ab) < \infty$ y $ab \in A_{\mathrm{tor}}$.

(S3) Sea $a \in A_{\mathrm{tor}}$. Sabemos, por el Ejercicio 1.74, que $\mathrm{o}(a^{-1}) = \mathrm{o}(a) < \infty$ y $a^{-1} \in A_{\mathrm{tor}}$.

El siguiente ejemplo nos demuestra que A_{tor} puede no ser un subgrupo de A, si A no es abeliano. En $\text{Gl}_2(F)$, consideramos las matrices:

$$M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 0 & 2 \\ 2^{-1} & 0 \end{pmatrix}.$$

Tenemos que

$$M_1, M_2 \neq I, \quad M_1^2 = M_2^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Por lo que, $\text{o}(M_1) = \text{o}(M_2) = 2 < \infty$. Sin embargo, se tiene que

$$M_1 M_2 = \begin{pmatrix} 2^{-1} & 0 \\ 0 & 2 \end{pmatrix} \implies (M_1 M_2)^n = \begin{pmatrix} 2^{-n} & 0 \\ 0 & 2^n \end{pmatrix} \neq I \quad \text{para todo } n \in \mathbb{N}.$$

Por tanto, $M_1 M_2$ tiene orden infinito y el conjunto $\{M \in \text{Gl}_2(F) : \text{o}(M) < \infty\}$ no es cerrado para la operación de $\text{Gl}_2(F)$ y no es un subgrupo.

Ejercicio 29. Hoja 1. Considerando las matrices reales $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \in \text{GL}_2(\mathbb{R})$, demostrad que el producto de elementos de orden finito no tiene por qué resultar un elemento de orden finito.

Solución:

Sean $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ y $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Observamos que

$$A^4 = I, \quad B^3 = I, \quad (AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Por tanto, A y B tienen orden finito, pero AB tiene orden infinito.

Ejercicio 32. Hoja 1. Sea $N \trianglelefteq G$ con $|G/N| = n$. Demostrad que si $x \in G$ satisface $x^m = 1$ y $(n, m) = 1$, entonces $x \in N$.

Solución:

Sea $x \in G$ tal que $x^m = 1$ con $(m, n) = 1$. Como $|G/N| = n$, tenemos que $\text{o}(xN) | n$. Por otro lado, como N es normal en G, tenemos $(xN)^m = x^m N = N$. Esto implica que $\text{o}(xN) | m$. Pero $(n, m) = 1$, por lo que, $\text{o}(xN) = 1$, es decir, $xN = N$. Concluimos entonces que $x \in N$.

Ejercicio 34. Hoja 1. Dad un grupo G y $N \trianglelefteq G$ tales que N y G/N sean cíclicos pero G no lo sea.

Solución:

El grupo $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, que no es cíclico pues todos sus elementos no triviales tienen orden 2, pero $|G| = 4$. Consideramos el subgrupo cíclico $N = \langle ([1], [0]) \rangle$. N es normal por ser un subgrupo de un grupo abeliano. Observamos que el grupo G/N tiene orden 2, por lo que es cíclico.