ESTRUCTURAS ALGEBRAICAS (8-1-2016)	•	Grado en Matemáticas Curso 2015-2016	•	Examen Ordinario

SOLUCIONES

1. Estudia si las siguientes afirmaciones son verdaderas o falsas. Justifica tu repuesta. (Recuerda que si la afirmación es verdadera hay que dar una demostración mientras que si la afirmación es falsa es suficiente con dar un contraejemplo):

a) (1 punto) La aplicación $F : \mathbb{Z}_{11} \longrightarrow \mathbb{Z}_{11}$ definida por $F(x) = x^{11}$ es un homomorfismo de anillos.

<u>*Solución:*</u> En primer lugar veamos que $F(x) = x$ en $\mathbb{Z}_{11}$. Para ello utilizamos que el grupo multiplicativo de $\mathbb{Z}_{11}$ tiene orden 10, o lo que es lo mismo el Pequeño Teorema de Fermat para $p = 11$ y x coprimo con 11: $x^{10} \equiv 1 \pmod{11}$. Aplicado a nuestra función tenemos $F(x) = x^{11} = x$.

Ahora, tenemos que ver que se respeta tanto la estructura aditiva como la multiplicativa a través de la aplicación F:

• ¿$F(x + y) = F(x) + F(y)$?: $F(x + y) = x + y = F(x) + F(y)$.

• ¿$F(x \cdot y) = F(x) \cdot F(y)$?: $F(x \cdot y) = x \cdot y = F(x) \cdot F(y)$.

<u>*Solución 2:*</u> Sin utilizar que $F(x) = x$ en $\mathbb{Z}_{11}$:

• ¿$F(x + y) = F(x) + F(y)$?

Utilizando el binomio de Newton, tenemos:

$$(x + y)^{11} = \sum_{k=0}^{11} \binom{11}{k} x^{11-k} y^k = x^{11} + \binom{11}{1} x^{10} y + \binom{11}{2} x^9 y^2 + \cdots + \binom{11}{10} x y^{10} + y^{11}.$$

Ahora como $\binom{11}{k} = \dfrac{11 \cdot 10 \cdots (11 - (k - 1))}{k!}$, se tiene que 11 divide a $\binom{11}{k}$ si $k \neq 11, 0$.

Por lo tanto $(x + y)^{11} = x^{11} + y^{11}$ en $\mathbb{Z}_{11}$. Así $F(x + y) = F(x) + F(y)$.

• ¿$F(x \cdot y) = F(x) \cdot F(y)$?

Utilizando que $\mathbb{Z}_{11}$ es conmutativo: $(x \cdot y)^{11} = x^{11} \cdot y^{11}$ y por lo tanto $F(x \cdot y) = x \cdot y = F(x) \cdot F(y)$.

Así la afirmación es <u>Verdadera</u>.

b) (1 punto) Hay 9 grupos abelianos de orden 2000, salvo isomorfismo,

<u>*Solución:*</u> Vamos a utilizar el Teorema de clasificación de grupos abelianos finitos. En nuestro caso a buscar los grupos abelianos de orden $2000 = 2^4 \cdot 5^3$. Para ver cuantos hay basta con ver cada factor potencia de primo y ver como podemos poner la potencia como suma de enteros positivos (denotamos por C_n el grupo cíclico de orden n):

$\boxed{2^4}$	:	$1+1+1+1$	:	$C_2 \times C_2 \times C_2 \times C_2$	$\boxed{5^3}$	:	$1+1+1$	:	$C_5 \times C_5 \times C_5$
	:	$1+1+2$	:	$C_2 \times C_2 \times C_4$		:	$1+2$	:	$C_5 \times C_{25}$
	:	$1+3$	:	$C_2 \times C_8$		:	3	:	C_{125}
	:	$2+2$	:	$C_4 \times C_4$					
	:	4	:	C_{16}					

Por lo tanto tenemos 5 grupos abelianos de orden 2^4 y 3 de orden 5^3. Así hay $15 = 5 \cdot 3$ grupos abelianos de orden 2000.

Si utilizamos la versión del teorema de clasificación en el que nos dice que si G es un grupo abeliano de orden n entonces

$$G \simeq C_{d_1} \times \cdot \times C_{d_s},$$

donde d_i divide a d_{i+1} y $n = d_1 \cdots d_s$. Así podemos denotar por $(d_1, \dots, d_s)$ la clase de isomorfía de G. Entonces las posibles clase de isomorfía en el caso de $n = 2000$ son las tuplas:

$$\begin{array}{lllllllll} (2,10,10,10) & , & (10,10,20) & , & (5,10,40) & , & (5,20,20) & , & (5,5,80)\,, \\ (2,2,10,50) & , & (2,10,100) & , & (10,200) & , & (20,100) & , & (5,400)\,, \\ (2,2,2,250) & , & (2,2,500) & , & (2,1000) & , & (4,500) & , & (2000)\,. \end{array}$$

Así la afirmación es <u>Falsa</u>.

c) (1 punto) El mayor orden que puede tener un elemento de S_{11} es 12.

<u>*Solución:*</u> La afirmación es <u>Falsa</u>. Para ello basta con dar un contraejemplo. Sea $\sigma = (1\,2\,3)$ y $\tau = (4\,5\,6\,7\,8)$. Entonces tenemos que $\sigma, \tau \in S_{11}$ son disjuntas. Por lo tanto el elemento $\sigma\tau \in S_{11}$ cumple

$$|\sigma\tau| = \text{mcm}\{|\sigma|, |\tau|\} = 3 \cdot 5 = 15.$$

---

2. Considera el subconjunto de matrices 2×2 con coeficientes en $\mathbb{Z}$ definido por

$$A = \{aI + bM : a, b \in \mathbb{Z}\}, \quad \textbf{donde} \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \textbf{y} \quad M = \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix}.$$

a) (0.5 puntos) Demuestra que A es un anillo conmutativo y con unidad, con la multiplicación y suma de matrices.

<u>*Solución:*</u> Sabemos que el conjunto de las matrices 2×2 con coeficientes en $\mathbb{Z}$, $M_2(\mathbb{Z})$, forman un anillo no conmutativo con unidad con las operaciones suma y producto habituales de las matrices. Ahora como $A \subset M_2(\mathbb{Z})$, para ver que A es anillo con la suma y producto de matrices, basta con ver que la suma y el producto de matrices son cerrados en A, ya que el resto de las propiedades provienen de $M_2(\mathbb{Z})$. Veámoslo: sean $aI + bM\,, cI + dM \in A$:

$$\begin{aligned} &(aI + bM) + (cI + dM) = (a + c)I + (b + d)M \in A\,, \\ &(aI + bM) \cdot (cI + dM) = (ac)I + (ad)M + (bc)M + bdM^2 = (ac)I + (ad + bc + 2bd)M \in A\,, \end{aligned}$$

donde hemos usado que $M^2 = 2M$.

Por último falta ver que A es conmutativo (la unidad es I que es la misma que la de $M_2(\mathbb{Z})$):

$$(aI+bM)\cdot(cI+dM) = (ac)I+(ad+bc+2bd)M = (ca)I+(da+cb+2db)M = (cI+dM)\cdot(aI+bM).$$

Por lo tanto hemos visto que A es un anillo conmutativo con unidad.

b) (0.75 puntos) Decide cuáles de los siguientes elementos son divisores de cero y/o unidades en A:

$$2I, \qquad I-M, \qquad 2I-M.$$

<u>*Solución:*</u> Sea $aI+bM \in A$, entonces $aI+bM$ es

- divisor de cero si existe $cI+dM \in A$ tal que $(aI+bM)(cI+dM)=0$.
- una unidad si existe $cI+dM \in A$ tal que $(aI+bM)(cI+dM)=I$.

$\boxed{2I}$

- $2I(cI+dM)=0 \Leftrightarrow cI=-dM \Leftrightarrow \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} = \begin{pmatrix} -2d & -d \\ 0 & 0 \end{pmatrix} \Leftrightarrow c=d=0.$
- $2I(cI+dM)=I \Leftrightarrow (1-2c)I=dM \Leftrightarrow \begin{pmatrix} 1-2c & 0 \\ 0 & 1-2c \end{pmatrix} = \begin{pmatrix} 2d & d \\ 0 & 0 \end{pmatrix} \Leftrightarrow d=0, c=\frac{1}{2}.$

Por lo tanto, $2I$ no es ni divisor de cero ni unidad.

$\boxed{I-M}$

- $(I-M)(cI+dM)=0 \Leftrightarrow cI=(c+d)M \Leftrightarrow \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} = \begin{pmatrix} 2(c+d) & c+d \\ 0 & 0 \end{pmatrix} \Leftrightarrow c=d=0.$
- $(I-M)(cI+dM)=I \Leftrightarrow (c-1)I=(c+d)M \Leftrightarrow \begin{pmatrix} c-1 & 0 \\ 0 & c-1 \end{pmatrix} = \begin{pmatrix} 2(c+d) & c+d \\ 0 & 0 \end{pmatrix} \Leftrightarrow$ $c=1, d=-1.$

Por lo tanto, $I-M$ no es divisor de cero, pero si unidad, su inverso es el mismo.

$\boxed{2I-M}$

- $(2I-M)(cI+dM)=0 \Leftrightarrow 2cI=cM \Leftrightarrow \begin{pmatrix} 2c & 0 \\ 0 & 2c \end{pmatrix} = \begin{pmatrix} 2c & c \\ 0 & 0 \end{pmatrix} \Leftrightarrow c=0.$
- $(2I-M)(cI+dM)=I \Leftrightarrow (2c-1)I=cM \Leftrightarrow \begin{pmatrix} 2c-1 & 0 \\ 0 & 2c-1 \end{pmatrix} = \begin{pmatrix} 2c & c \\ 0 & 0 \end{pmatrix} \Leftrightarrow \frac{1}{2}=c=0$.

Por lo tanto, $2I-M$ es divisor de cero, y no puede ser unidad.

Conclusión:

	¿Divisor de cero?	¿Unidad?
$2I$	No	No
$I-M$	No	Si
$2I-M$	Si	No

c) (0.75 puntos) ¿Es maximal el ideal generado por $3I$?

<u>*Solución:*</u> El ideal $\langle 3I\rangle$ es maximal si y sólo si el anillo cociente $A/\langle 3I\rangle$ es un cuerpo. Veamos que ni siquiera es un dominio. Para ello vamos a usar que $(2I-M)M = 0$ en A. Basta con ver que la clase de $2I-M$ y de M en $A/\langle 3I\rangle$ no son la del 0. O equivalentemente, $2I-M, M \notin \langle 3I\rangle$. Supongamos lo contrario, entonces existirán $aI+bM, cI+dM \in A$ tales que

$$2I - M = 3I(aI+bM) \iff (3a-2)I = -(3b+1)M \iff \begin{pmatrix} 3a-2 & 0 \\ 0 & 3a-2 \end{pmatrix} = \begin{pmatrix} -6b-2 & -3b-1 \\ 0 & 0 \end{pmatrix}.$$

$$M = 3I(cI+dM) \iff 3cI = (1-3d)M \iff \begin{pmatrix} 3c & 0 \\ 0 & 3c \end{pmatrix} = \begin{pmatrix} 2-6d & 1-3d \\ 0 & 0 \end{pmatrix}.$$

Necesariamente $a = \frac{2}{3}, d = \frac{1}{3}$, pero $\frac{1}{3}, \frac{2}{3} \notin \mathbb{Z}$. Así hemos visto que la clase de $2I-M$ en $A/\langle 3I\rangle$ es un divisor de cero. Por lo tanto, $\langle 3I\rangle$ no es un ideal maximal de A.

---

3. Sea $\varphi : \mathbb{R} \longrightarrow \mathbb{C}^\times$ la aplicación dada por $\varphi(x) = \cos x + i \operatorname{sen} x$.

a) (1 punto) Demuestra que φ es un homomorfismo de grupos.

<u>*Solución:*</u> Tenemos que ver que $\varphi(x+y) = \varphi(x)\cdot\varphi(y)$ ya que la operación en $\mathbb{R}$ es la suma y en $\mathbb{C}^\times$ es el producto:

$$\begin{aligned} \varphi(x)\cdot\varphi(y) &= (\cos(x) + i\operatorname{sen}(x))(\cos(y) + i\operatorname{sen}(y)) = \\ &= \cos(x)\cos(y) - \operatorname{sen}(x)\operatorname{sen}(y) + i(\operatorname{sen}(x)\cos(y) + \operatorname{sen}(y)\cos(x)) = \\ &= \cos(x+y) + i\operatorname{sen}(x+y) = \\ &= \varphi(x+y). \end{aligned}$$

Aquí sólo hemos utilizado las fórmulas de coseno y seno de la suma de ángulos. Otra forma es ver que $\varphi(x) = e^{ix}$. Entonces

$$\varphi(x+y) = e^{i(x+y)} = e^{ix}e^{iy} = \varphi(x)\varphi(y).$$

b) (1 punto) Calcula el núcleo e imagen de φ.

<u>*Solución:*</u>

$$\operatorname{Ker}(\varphi) = \{x \in \mathbb{R} \mid \varphi(x) = 1\} = \{x \in \mathbb{R} \mid \cos(x) + i\operatorname{sen}(x) = 1\} = \{2k\pi \mid k \in \mathbb{Z}\}.$$
$$\operatorname{Im}(\varphi) = \{\varphi(x) \mid x \in \mathbb{R}\} = \{\cos(x) + i\operatorname{sen}(x) \mid x \in [0, 2\pi]\} = \{z \in \mathbb{C} \mid \|z\| = 1\} = S^1.$$

4. bf Considera el subgrupo de $\mathrm{SL}(3, \mathbb{Z}_3)$ definido como:

$$G = \left\{ m(a,x,y) := \begin{pmatrix} a & \overline{0} & x \\ \overline{0} & a^{-1} & y \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \;\middle|\; x, y \in \mathbb{Z}_3, a \in \mathbb{Z}_3^\times \right\}.$$

a) (0.75 puntos) Calcula $|G|$. Encuentra un subgrupo de G de tamaño 3.

<u>*Solución:*</u> Se tiene $|G| = |\mathbb{Z}_3|^2 |\mathbb{Z}_3^\times| = 3^2 \cdot 2 = 18$ ya que $x, y \in \mathbb{Z}_3, a \in \mathbb{Z}_3^\times$. Ahora vamos a calcular un subgrupo H de G de orden 3. Como 3 es primo este subgrupo deberá de ser cíclico. En primer lugar hay que tener en cuenta que el elemento identidad en este grupo es $m(\overline{1}, \overline{0}, \overline{0})$. Ahora, la matriz $m(\overline{1}, \overline{1}, \overline{0})$ satisface:

$$m(\overline{1},\overline{1},\overline{0})^2 = \begin{pmatrix} \overline{1} & \overline{0} & \overline{1} \\ \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}^2 = \begin{pmatrix} \overline{1} & \overline{0} & \overline{2} \\ \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} = m(\overline{1},\overline{2},\overline{0}) \neq m(\overline{1},\overline{0},\overline{0})$$

$$m(\overline{1},\overline{1},\overline{0})^3 = \begin{pmatrix} \overline{1} & \overline{0} & \overline{1} \\ \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}^3 = \begin{pmatrix} \overline{1} & \overline{0} & \overline{0} \\ \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} = m(\overline{1},\overline{0},\overline{0}).$$

Por lo tanto $H = \langle m(\overline{1}, \overline{1}, \overline{0}) \rangle$ es un subgrupo de orden 3 de G.

b) (0.75 puntos) ¿Tiene G un subgrupo de orden d para cada divisor d de $|G|$?

<u>*Solución 1:*</u> Tenemos $|G| = 18 = 2 \cdot 3^2$. Por lo tanto los posibles divisores de 18 son $1, 2, 3, 6, 9, 18$. Los subgrupos triviales: $\{m(\overline{1}, \overline{0}, \overline{0})\}$ y G tienen ordenes 1 y 18 respectivamente. En el apartado anterior hemos encontrado H de orden 3. Ahora, los Teoremas de Sylow nos dicen que existen subgrupos de G de ordenes 2 y 9 (también 3). Ahora sólo nos queda por ver si hay algún subgrupo o no de orden 6.

Veamos que H es normal. Tenemos que un elemento de H es de la forma $m(\overline{1}, z, \overline{0})$, $z \in \mathbb{Z}_3$. Para demostrar que es normal tenemos que ver $\alpha \cdot m(\overline{1}, z, \overline{0}) \cdot \alpha^{-1} \in H$ para todo $\alpha = m(a, x, y) \in G$:

$$\begin{aligned} m(a,x,y) \cdot m(\overline{1},z,\overline{0}) \cdot m(a,x,y)^{-1} &= \begin{pmatrix} a & \overline{0} & x \\ \overline{0} & a^{-1} & y \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \begin{pmatrix} \overline{1} & \overline{0} & z \\ \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \begin{pmatrix} a & \overline{0} & x \\ \overline{0} & a^{-1} & y \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}^{-1} = \\ &= \begin{pmatrix} \overline{1} & \overline{0} & az \\ \overline{0} & \overline{1} & 0 \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} = m(\overline{1}, az, \overline{0}) \in H. \end{aligned}$$

Así hemos visto que H es normal en G y por lo tanto G/H es un grupo de orden 6. Tenemos una correspondencia entre los subgrupos $K \leq G$ que contienen a H y los subgrupos de $\overline{K} \leq G/H$, de tal forma que $|K| = |\overline{K}| \cdot |H|$.

Por último como G/H es un grupo de orden 6 será isomorfo a C_6 o a S_3. Ambos grupos tienen elementos de orden 2. Por lo tanto tenemos que existe $\overline{K} \leq G/H$ tal que $|\overline{K}| = 2$.

Juntando ese último resultado con la correspondencia entre los subgrupos de G que contienen a H y los subgrupos de G/H tenemos que existe K tal que $|K| = |\overline{K}| \cdot 3$=6.

Conclusión: Existen subgrupos de G de cualquier orden divisor de $|G|$.

Solución 2: Sea $a \in \mathbb{Z}_3^\times$, entonces $a \in \{\pm\overline{1}\}$ y en particular $a^{-1} = a$. Así tenemos:

$$m(a,x,y)\cdot m(b,w,z) = \begin{pmatrix} a & \overline{0} & x \\ \overline{0} & a & y \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \begin{pmatrix} b & \overline{0} & w \\ \overline{0} & b & z \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} ab & \overline{0} & x+aw \\ \overline{0} & ab & y+az \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} = m(ab, x+aw, y+az).$$

Definamos los siguientes subconjuntos:

$$\begin{aligned} H_1 &= \left\{m(\overline{1},\overline{0},\overline{0})\right\}, \\ H_2 &= \left\{m(a,\overline{0},\overline{0})\ a \in \mathbb{Z}_3^\times\right\}, \\ H_3 &= \left\{m(1,x,\overline{0})\ x \in \mathbb{Z}_3\right\}, \\ H_6 &= \left\{m(a,x,\overline{0})\ x \in \mathbb{Z}_3, a \in \mathbb{Z}_3^\times\right\}, \\ H_9 &= \left\{m(\overline{1},x,y)\ x,y \in \mathbb{Z}_3\right\}, \\ H_{18} &= \left\{m(a,x,y)\ x,y \in \mathbb{Z}_3, a \in \mathbb{Z}_3^\times\right\}. \end{aligned}$$

Utilizando la anterior representación del producto de matrices de G se observa que $H_d \leq G$, con $d \,|\, 18$. En particular hemos construido estos subgrupos de forma que $|H_d| = d$ con $d \,|\, |G| = 18$.

c) (0.75 puntos) ¿Es G resoluble?

Solución 1: Utilizamos $H \trianglelefteq G$, para conseguir el troceado H, G/H. Tenemos que H es cíclico de orden 3 y G/H es de orden 6, por lo tanto isomorfo a C_6 o a S_3, ambos resolubles. Por lo tanto G es resoluble.

Solución 2: Sea $s_3 = \#\mathrm{Syl}_3(G)$, entonces el tercer Teorema de Sylow nos asegura que $s_3|2$ y $s_3 \equiv 1 \pmod 3$. Por lo tanto $s_3 = 1$. Así $\mathrm{Syl}_3(G) = \{P\}$ y se tiene que $P \trianglelefteq G$ con $|P| = 9$. Utilizamos $P \trianglelefteq G$, para conseguir el troceado P, G/P. Como G/P tiene orden 2 es cíclico y como $|P| = 9 = 3^2$ sabemos que P es abeliano. Por lo tanto G es resoluble.

d) (0.75 puntos) ¿Son $m(\overline{1},\overline{1},\overline{1})$ y $m(\overline{-1},\overline{1},\overline{0})$ elementos conjugados en G?

Solución 1: Si las matrices $m(\overline{1},\overline{1},\overline{1})$ y $m(\overline{-1},\overline{1},\overline{0})$ fueran conjugados en G, entonces existiría una matriz $m(a,x,y) \in G$ tal que

$$m(a,x,y)\cdot m(\overline{1},\overline{1},\overline{1}) m(a,x,y)^{-1} = m(\overline{-1},\overline{1},\overline{0}).$$

Pero tenemos que para todo $a \in \mathbb{Z}_3^\times$, $x,y \in \mathbb{Z}_3$ se tiene:

$$\begin{pmatrix} a & \overline{0} & x \\ \overline{0} & a^{-1} & y \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \begin{pmatrix} \overline{1} & \overline{0} & 1 \\ \overline{0} & \overline{1} & \overline{1} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \begin{pmatrix} a & \overline{0} & x \\ \overline{0} & a^{-1} & y \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}^{-1} = \begin{pmatrix} \overline{1} & \overline{0} & a \\ \overline{0} & \overline{1} & a^{-1} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \neq \begin{pmatrix} \overline{-1} & \overline{0} & \overline{1} \\ \overline{0} & \overline{-1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} = m(\overline{-1},\overline{1},\overline{0}).$$

Solución 2: Los autovalores de $m(\overline{1},\overline{1},\overline{1})$ son $\{1,1,1\}$ y los de $m(\overline{-1},\overline{1},\overline{0})$ son $\{-1,-1,1\}$. Como tienen autovalores distintos, tenemos que no pueden ser matrices conjugadas.

Solución 3: $m(\overline{1},\overline{1},\overline{1})$ y $m(\overline{-1},\overline{1},\overline{0})$ tienen distinto orden:

$$|m(\overline{1},\overline{1},\overline{1})| = 3 \qquad \text{y} \qquad |m(\overline{-1},\overline{1},\overline{0})| = 2.$$