Grupos y Anillos. Grado en Matemáticas. 2012-13. Examen de junio. Problemas resueltos

Todas las preguntas tienen un valor de 1.5 puntos menos la última que vale 1 punto.

1. **Dar la lista completa de todos los polinomios irreducibles de $\mathbb{Z}_2[X]$ de grado menor que 5. Construir cuerpos con 4, 8 y 16 elementos.**

   Todos los polinomios de grado 1 son irreducibles y sólo tenemos dos: X y $X+1$. Los polinomios de grado mayor que 1 que sean irreducibles no pueden tener raíces. Por tanto su término independiente ha de ser 1 (para que el 0 no sea raíz) y el número de coeficientes diferentes de 0 ha de ser impar (para que el 1 no sea raíz). Los únicos polinomios de grado menor que 5 que satisfacen esto son X^2+X+1, X^3+X^2+1, X^3+X+1, X^4+X^3+1, X^4+X^2+1, X^4+X+1 y $X^4+X^3+X^2+X+1$. Ninguno de ellos tiene raíces en $\mathbb{Z}_2$. Los tres primeros han de ser irreducibles pues no tienen raíces y su grado es 2 ó 3. Si uno de los de grado 4 fuera reducible tendría que ser producto de dos polinomios irreducibles de grado 2. Cómo X^2+X+1 es el único polinomio irreducible de grado 2 el único que no es irreducible es $(X^2+X+1)^2 = X^4+X^2+1$. En conclusión los polinomios irreducibles de grado menor que 5 son X, $X+1$, X^2+X+1, X^3+X^2+1, X^3+X+1, X^4+X^3+1, X^4+X+1 y $X^4+X^3+X^2+X+1$. Para construir cuerpos con 2^n elementos se toma el cociente $\mathbb{Z}_2[X]/(P)$ con P un polinomio irreducible de grado n. Así $\mathbb{Z}_2[X]/(X^2+X+1), \mathbb{Z}_2[X]/(X^3+X+1)$ y $\mathbb{Z}_2[X]/(X^4+X+1)$ son cuerpos con 4, 8 y 16 elementos respectivamente.

2. **Sea p un número primo y sea $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, p \nmid b\}$.**

   ***a*) Demostrar que $\mathbb{Z}_{(p)}$ es un subanillo de los números racionales.**

   ***b*) Demostrar que los ideales no nulos de $\mathbb{Z}_{(p)}$ son todos de la forma $\mathbb{Z}_{(p)}p^n$ para algún $n \geq 0$.**

   ***c*) ¿Cuáles son los elementos invertibles de $\mathbb{Z}_{(p)}$? ¿Y los irreducibles?**

   ***d*) ¿Es $\mathbb{Z}_{(p)}$ DFU? ¿Y DIP? ¿Y dominio euclídeo? ¿Cómo serán las factorizaciones en $\mathbb{Z}_{(p)}$?**

   ***e*) ¿Cuál es el cuerpo de fracciones de $\mathbb{Z}_{(p)}$?**

   ***f*) Demostrar que $\mathbb{Z}_{(p)}/\mathbb{Z}_{(p)}p^n \cong \mathbb{Z}/\mathbb{Z}p^n$ para todo $n \geq 0$.**

   (a) Claramente $1 = \frac{1}{1} \in \mathbb{Z}_{(p)}$. Si $x, y \in \mathbb{Z}_{(p)}$ entonces $x = \frac{a}{b}$ e $y = \frac{c}{d}$ con $a, b, c, d \in \mathbb{Z}$ y $p \nmid b, d$. Entonces $p \nmid bd$ y por tanto $x - y = \frac{ad-bc}{bd} \in \mathbb{Z}_{(p)}$ y $xy = \frac{ac}{bd} \in \mathbb{Z}_{(p)}$. Esto prueba que $\mathbb{Z}_{(p)}$ es subanillo de $\mathbb{Q}$.

   (b) Sea I un ideal no nulo de $\mathbb{Z}_{(p)}$. Sea $\frac{a}{b}$ un elemento no nulo de I con $a, b \in \mathbb{Z}$ y $p \nmid b$. Pongamos $a = a_1 p^m$ con $p \nmid a_1$. Entonces $\frac{b}{a_1} \in \mathbb{Z}_{(p)}$ y por tanto $p^m = \frac{b}{a_1}\frac{a}{b} \in I$. Esto demuestra que $p^k \in I$ para algún $k \geq 0$. Sea $n = \min\{k \geq 0 : p^k \in I\}$. Entonces $\mathbb{Z}_{(p)}p^n \subseteq I$. Para demostrar la otra inclusión observamos que hemos visto arriba que si $\frac{a}{b} = \frac{a_1 p^m}{b} \in I$, con $p \nmid m$ entonces $p^m \in I$. Por la elección de n tenemos que $m \geq n$ y por tanto $\frac{a}{b} = \frac{a_1 p^{m-n}}{b} p^n \in \mathbb{Z}_{(p)}p^n$. Esto demuestra que $I \subseteq \mathbb{Z}_{(p)}p^n$, con lo que $I = \mathbb{Z}_{(p)}p^n$.

   (c) y (d) Claramente si a y b son enteros que no son múltiplos de p, entonces $\frac{a}{b}, \frac{b}{a} \in \mathbb{Z}_{(p)}$. En tal caso $\frac{a}{b} \in \mathbb{Z}_{(p)}^*$. Sin embargo si $p \nmid b$ pero $p \mid a$ entonces $\frac{b}{a} \notin \mathbb{Z}_{(p)}^*$. Por tanto las unidades de $\mathbb{Z}_{(p)}$ son las fracciones $\frac{a}{b}$ con a y b enteros que no son múltiplos de p.

   En el apartado (b) hemos visto que todos los ideales no nulos de $\mathbb{Z}_{(p)}$ son de la forma $\mathbb{Z}_{(p)}p^n$ para algún n. En particular son principales. Luego $\mathbb{Z}_{(p)}$ es DIP y por tanto también es DFU. Además $\mathbb{Z}_{(p)}p^n \subseteq \mathbb{Z}_{(p)}p^m$ si y sólo si $m \leq n$. Luego el único ideal maximal es $\mathbb{Z}_{(p)}p$. Eso implica que los irreducibles de $\mathbb{Z}_{(p)}$ son los elementos que generen este ideal que son precisamente los asociados de p. Luego los irreducibles de $\mathbb{Z}_{(p)}$ son los

elementos de la forma $\frac{ap}{b}$ con a y b enteros coprimos con p. Por tanto las factorizaciones en $\mathbb{Z}_{(p)}$ son todas de la forma $\frac{a}{b}p^n$ con $p \nmid a, b$.

Vamos a ver que $\mathbb{Z}_{(p)}$ es un dominio euclídeo. La función euclídea que elegimos es $\delta(\frac{a}{b}) =$ mayor $n \geq 0$ tal que $p^n \mid a$ (suponiendo que $a, b \in \mathbb{Z}$ y $p \nmid b$). Está claro que $\delta(xy) = \delta(x) + \delta(y)$, con lo que si $x \mid y$ en $\mathbb{Z}_{(p)}$ entonces $\delta(x) \leq \delta(y)$. Sean $x, y \in \mathbb{Z}_{(p)}$ y pongamos $\delta(x) = n$ y $\delta(y) = m$. Si $n < m$ entonces tomando $q = 0$ y $r = y$ tenemos $x = qy + r$ y $\delta(r) < \delta(y)$. Supongamos que $n \geq m$. Entonces $x = \frac{ap^n}{b}$ e $y = \frac{cp^m}{d}$ con $a, b, c, d \in \mathbb{Z}$ y $p \nmid bd$. Tomando $q = \frac{adp^{n-m}}{bc} \in \mathbb{Z}_{(p)}$ y $r = 0$ tenemos $x = qy + r$.

(e) Como $\mathbb{Z} \subseteq \mathbb{Z}_{(p)} \subseteq \mathbb{Q}$ y $\mathbb{Q}$ es el cuerpo de fracciones de $\mathbb{Z}$, deducimos que $\mathbb{Q}$ también es el cuerpo de fracciones de $\mathbb{Z}_{(p)}$.

(f) Consideramos el homomorfismo $f : \mathbb{Z} \to \mathbb{Z}_{(p)} \to \mathbb{Z}_{(p)}/\mathbb{Z}_{(p)}p^n$, que se obtiene de componer una inclusión con una proyección. Primero vemos que f es suprayectivo. En efecto, sea $x = \frac{a}{b}$ con $p \nmid a$. Como p^n y b son coprimos existen $u, v \in \mathbb{Z}$ tales que $up^n + vb = 1$. Entonces $p \nmid v$ y $x - va = \frac{a - vab}{b} = \frac{au}{b}p^n \in \mathbb{Z}_{(p)}p^n$. Por tanto $f(va) = va + \mathbb{Z}_{(p)}p^n = x + \mathbb{Z}_{(p)}p^n$. Esto demuestra que f es suprayectiva. Ahora calculamos el núcleo de f. Claramente $\mathbb{Z}p^n \subseteq \ker(f) = \mathbb{Z} \cap \mathbb{Z}_{(p)}p^n$. Además, si $m = \frac{a}{b}p^n$ con $a, b, m \in \mathbb{Z}$ y $p \nmid b$ entonces $p^n | m$. Luego $\ker(f) = \mathbb{Z}p^n$. Sólo falta aplicar el Primer Teorema de Isomorfía para deducir que $\mathbb{Z}/(p^n) \cong \mathbb{Z}_{(p)}/\mathbb{Z}_{(p)}p^n$.

3. Sea G un grupo finito y sea H un subgrupo de G. Se llama exponente de G, denotado $\mathbf{Exp}(G)$, al menor entero positivo n tal que $g^n = 1$ para todo $g \in G$. Demostrar

a) **$\mathbf{Exp}(G)$ es el mínimo común múltiplo de los órdenes de los elementos de G.**

b) **$\mathbf{Exp}(H)$ divide a $\mathbf{Exp}(G)$.**

c) **Si H es normal en G entonces $\mathbf{Exp}(G/H)$ divide a $\mathbf{Exp}(G)$.**

d) **Para todo entero $n \geq 2$,**

$$\mathbf{Exp}(S_n) = \begin{cases} \mathbf{Exp}(S_{n-1}), & \textbf{si } n \textbf{ no es potencia de un primo}; \\ p\mathbf{Exp}(S_{n-1}), & \textbf{si } n \textbf{ es potencia de un primo } p. \end{cases}$$

Sea $e = \mathrm{Exp}(G)$.

a) Sea m el mínimo común múltiplo de los órdenes de los elementos de G. Si $g \in G$ entonces $1 = g^e$ y por tanto e es múltiplo del orden de g. Luego e es múltiplo de m. Por otro lado, $g^m = 1$ para todo $g \in G$, con lo que $e \leq m$. De $e \leq m$ y $m | e$ deducimos que $e = m$.

b) De (a) deducimos que $\mathrm{Exp}(H)$ (= mínimo común múltiplo de los órdenes de los elementos de H) divide al mínimo común múltiplo de los órdenes de los elementos de G y éste es $\mathrm{Exp}(G)$.

c) Si $g \in G$ entonces $g^e = 1$ y por tanto $(gH)^e = g^e H = 1$. Luego e es múltiplo de los órdenes de los elementos de G/H, con lo que del apartado (a) deducimos que $\mathrm{Exp}(G/H)$ divide a e.

d) Vamos a ver primero que $\mathrm{Exp}(S_n) = \mathrm{mcm}\{k : k \leq n\}$. En efecto, para cada $k \leq n$, S_n tiene un k-ciclo. Como cada k-ciclo tiene orden k, deducimos que k divide a $\mathrm{Exp}(S_n)$ para todo $k \leq n$ y por tanto $m := \mathrm{mcm}\{k : k \leq n\}$ divide a $\mathrm{Exp}(S_n)$. Por otro lado, el orden de un elemento g de S_n es el mínimo común múltiplo de las componentes de su tipo. Como estas componentes son menores o iguales que n deducimos que $g^m = 1$. En conclusión $m = \mathrm{Exp}(S_n)$.

Por tanto $\mathrm{Exp}(S_n) = \mathrm{mcm}(n, \mathrm{Exp}(S_{n-1}))$. Si n no es potencia de primo entonces $n = n_1 n_2$ con n_1 coprimos y menores que n. Luego $n = \mathrm{mcm}(n_1, n_2)$ divide a $\mathrm{Exp}(S_{n-1})$ y por

tanto $\mathrm{Exp}(S_n) = \mathrm{Exp}(S_{n-1})$. Si $n = p^m$ con p primo entonces p^{m-1} divide a $\mathrm{Exp}(S_{n-1})$ pero p^m no divide a ningún $k < n$. Eso implica que $\mathrm{Exp}(S_n) = \mathrm{mcm}(p^m, \mathrm{Exp}(S_{n-1})) = p\mathrm{Exp}(S_{n-1})$.

4. Sea $A = \mathbb{Z}_{12}[X]/(X^2)$ y si $f \in \mathbb{Z}_{12}[X]$ entonces $\overline{f}$ denota su imagen en A. Demostrar

***a*) Todo elemento de A tiene la forma $\overline{a + bX}$ con $a, b \in \mathbb{Z}_{12}$**

***b*) A tiene 48 unidades (elementos invertibles).**

***c*) Obtener las descomposiciones primaria e invariante del grupo de unidades de A.**

(a) Si $n \geq 2$ entonces $\overline{X^n} = \overline{0}$. Por tanto $\overline{a_0 + a_1X + a_2X^2 + \cdots + a_nX^n} = \overline{a_0 + a_1X}$.

(b) Para simplificar la notación a partir de ahora no escribimos las barras para los elementos de A. Vamos a ver cómo es la multiplicación en A:

$$(a + bX)(c + dX) = ac + (ad + bc)X.$$

Por tanto $a+bX$ es invertible si y sólo si existen $c, d \in \mathbb{Z}_{12}$ tales que $ac = 1$ y $ad+bc = 0$. Eso implica que a es invertible en $\mathbb{Z}_{12}$. Recíprocamente si a es invertible en $\mathbb{Z}_{12}$ entonces $(a + bX)(a^{-1} - ba^{-2}X) = 1$. Por tanto los elementos invertibles son los de la forma $a + bX$ con $a \in \mathbb{Z}_{12}^* = \{\pm 1, \pm 5\}$ y $b \in \mathbb{Z}_{12}$. Esto nos da un total de 48 unidades.

(c) Vamos a calcular una fórmula para las potencias de $a + bX$. Para eso observamos que $(a+bX)^2 = a^2+2abX$, $(a+bX)^3 = a^3+3abX$, ... Es decir $(a+bX)^n = a^n+nabX$. Por tanto $(a + bX)^n = 1$ si y sólo si $a^n = 1$ y $nab = 0$. Como $a^2 = 1$ para todo $a \in \mathbb{Z}_{12}^*$ y $12b = 0$ para todo $b \in \mathbb{Z}_{12}$, deducimos que $u^{12} = 1$ para todo $u \in A^*$. Luego el orden de cada elemento divide a 12. Además $1 + X$ tiene orden 12. Eso implica que el mayor de la lista de los divisores elementales de A^* es 12. Eso nos deja sólo dos posibles listas de factores invariantes: [12,4] ó [12,2,2]. La buena va a ser la segunda pues los elementos de $\mathbb{Z}_{12}^*$ forman un subgrupo de A^* isomorfo a $\mathbb{Z}_2^2$ que no interseca a $\langle 1 + X\rangle$. Luego $A^* = \langle 1 + X\rangle \oplus \mathbb{Z}_{12}^* \cong \mathbb{Z}_{12} \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Otra alternativa para ver esto es observar que en $\mathbb{Z}_{12} \times \mathbb{Z}_4$ hay sólo tres elementos de orden 2 mientras que en $\mathbb{Z}_{12} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ hay siete. Para ver que A^* es isomorfo a $\mathbb{Z}_{12} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ basta encontrar en A^* cuatro elementos de orden 2. Por ejemplo $-1, 5, -5$ y $(X + 1)^6 = 1 + 6X$ tienen orden 2 y son diferentes. Luego la lista de factores invariantes de A^* es $[12, 2, 2]$. Entonces los divisores elementales son $[4, 2, 2, 3]$.

5. Sean $D_n = \langle R, S\rangle$, el grupo diédrico donde R es la rotación de ángulo $2\pi/n$ y S una simetría. Sea $N = \langle R^2\rangle$. Demostrar que N es el menor subgrupo normal de G tal que G/N es abeliano. Calcular $[G : N]$.

Tenemos $(R^2)^R = R^2 \in N$ y $(R^2)^S = R^{-2}$. Por tanto $N \trianglelefteq D_n$. Además el orden de R^2 es

$$\frac{n}{\gcd(2, n)} = \begin{cases} n, & \text{si } 2 \nmid n; \\ \frac{n}{2}, & \text{si } 2 \mid n. \end{cases}$$

Por tanto $[G : N] = 2$ si n es impar y $[G : N] = 4$ en caso contrario. Como todos los grupos de orden 2 ó 4 son abelianos, G/N es abeliano. Sea H un subgrupo normal de G tal que G/H es abeliano. Entonces $RSH = SRH$, o lo que es lo mismo $R^2 = RSR^{-1}S^{-1} \in H$. Por tanto $N \subseteq H$.