Grupos y Anillos. Grado en Matemáticas. 2011-12. Examen de junio. Teoría

Todas las preguntas tienen un valor de 1.5 puntos.

1. Dar un ejemplo de dos elementos de un dominio que no tengan máximo común divisor.
2. Enunciado del Teorema de Clasificación de Grupos Abelianos Finitamente Generados y esquema de la demostración, sin detalles técnicos.

Grupos y Anillos. Grado en Matemáticas. 2011-12. Examen de junio. Problemas

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

1. **Sean $P = 2\mathbb{Z}[X]$, $I = (1+i)\mathbb{Z}[i]$ y $J = I[X]$, o sea J está formado por los polinomios con coeficientes en I. Demostrar que J es un ideal primo de $\mathbb{Z}[i][X]$ y $\mathbb{Z}[i][X]/J \cong \mathbb{Z}[X]/P \cong \mathbb{Z}_2[X] \cong (\mathbb{Z}[i]/I)[X]$.**

   Por un lado los isomorfismos $\mathbb{Z}[i][X]/J \cong (\mathbb{Z}[i]/I)[X]$ y $\mathbb{Z}[X]/P \cong \mathbb{Z}_2[X]$ se deducen de aplicar el Primer Teorema de Isomorfía a las aplicaciones naturales $\mathbb{Z}[i][X] \to (\mathbb{Z}[i]/I)[X]$ y $\mathbb{Z}[X] \to \mathbb{Z}_2[X]$ dadas por $f(\sum a_i X^i) = \sum \overline{a_i} X^i$ donde $\overline{a}$ representa la clase de a, módulo I y módulo $2\mathbb{Z}$, respectivamente. Para obtener el isomorfismo $\mathbb{Z}[i][X]/J \cong \mathbb{Z}[X]/P$ aplicamos el Tercer Teorema de Isomorfía al anillo $A = \mathbb{Z}[i][X]$, el subanillo $B = \mathbb{Z}[X]$ y el ideal J. Es decir tenemos $(B+J)/J \cong B/(B \cap J)$. Por un lado si $a + bi \in \mathbb{Z}[i]$, entonces $a + bi = (a-b) + (1+i)b \in \mathbb{Z} + I$. Esto demuestra que $\mathbb{Z} + I = \mathbb{Z}[i]$ y de ahí se deduce fácilmente que $\mathbb{Z}[i] = \mathbb{Z}[X] + J = B + J$. Por otro lado $\mathbb{Z} \cap I = 2\mathbb{Z}$. La inclusión $\mathbb{Z} \cap I \supseteq 2\mathbb{Z}$ está clara pues $2 = (1+i)(1-i)$. Por otro lado, si $a \in \mathbb{Z} \cap I$ entonces $1+i$ divide a a en $\mathbb{Z}[i]$ y por tanto $2 = N(1+i)$ divide a $N(a) = a^2$. Por tanto 2 divide a a. Esto da la otra inclusión. Una vez que tenemos $\mathbb{Z} \cap I = 2\mathbb{Z}$, deducimos que $B \cap J = \mathbb{Z}[X] \cap J = 2\mathbb{Z}[X] = P$. Concluimos pues que $\mathbb{Z}[i][X]/J = (B+J)/J \cong B/B \cap J = \mathbb{Z}[X]/P$.
2. **Sean $a = 3 + 4i$ y $A = \mathbb{Z}[i]/(a)$. Calcular la factorización de a en $\mathbb{Z}[i]$ y la característica, los ideales y cardinal de A.**

   Tenemos $N(a) = (3+4i)(3-4i) = 25$ y $N(1+2i) = (1+2i)(1-2i) = 5$. Luego $1+2i$ y $1-2i$ son irreducibles en $\mathbb{Z}[i]$ y $25 = (3+4i)(3-4i) = (1+2i)^2(1-2i)^2$. Uno de los factores irreducibles de esta factorización debe de dividir a $3+4i$. En efecto

$$\frac{3+4i}{1-2i} = \frac{(3+4i)(1+2i)}{5} = \frac{-5+10i}{5} = -1+2i$$

   Por tanto la factorización de a es

$$a = 3+4i = (1-2i)(-1+2i) = -(1-2i)^2.$$

   Como $\mathbb{Z}[i]$ es un DIP, los ideales de (a) son los de la forma (b) con $b|a$. Usando la factorización deducimos que a sólo tiene tres divisores (salvo asociados), a saber 1, $1-2i$ y a. Del Teorema de la Correspondencia deducimos que $A = \mathbb{Z}[i]/(a)$ tiene tres ideales $A, (1-2i)A$ y 0.

   Como hemos visto que a divide a 25, tendremos que $25A = 0$. Por tanto la característica de A divide a 25, pero no es 5 pues (ni 1) pues 5 no es múltiplo de a en $\mathbb{Z}[i]$. Por tanto A tiene característica 25.

   Como la característica de A es 25, los elementos de A tienen todos la forma $x+yi+(a)$ con $0 \le x, y \le 24$. Esto nos da un máximo de 25^2 elementos. Sin embargo, sabemos que $3+4i \equiv 0 \mod (a)$ y por tanto $4i \equiv -3 \mod (a)$. Por otro lado, $4 \cdot 6 = 24 \equiv -1 \mod a$, con lo que $i \equiv (-6)4 \equiv -18 \equiv 7 \mod (a)$. Por tanto $x+yi+(a) = x+7y+(a) = h+(a)$ con $0 \le h \le 24$. Por tanto A tiene exactamente 25 elementos.

3. **Sea $\omega = \frac{-1+\sqrt{-3}}{2}$ y consideremos el grupo multiplicativo G generado por las matrices**

$$a = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \quad \mathbf{y} \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

***a*) Demostrar que a tiene orden 3, b tiene orden 4, $a^b = a^{-1}$ y G tiene orden 12.**

***b*) Calcular los subgrupos de G.**

Observamos que $\omega^3 = 1$ y de ahí se tiene

$$a^3 = \begin{pmatrix} \omega^3 & 0 \\ 0 & \omega^{-3} \end{pmatrix} = I.$$

Por otro lado $b^2 = -I$ con lo que $b^4 = 1$. Luego a y b tienen órdenes 3 y 4 respectivamente. Comprobar $a^b = a^{-1}$, es lo mismo que probar que $ab = ba^{-1}$. Lo cual es fácil pues

$$ab = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \omega \\ -\omega^{-1} & 0 \end{pmatrix}$$

y

$$ba^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{pmatrix} = \begin{pmatrix} 0 & \omega \\ -\omega^{-1} & 0 \end{pmatrix}.$$

Utilizando $a^b = a^{-1}$, se deduce que $(a^i)^b = a^{-i}$ y por tanto $(a^i)^{b^2} = a^i$, para todo i. Utilizando esto se deduce que todo elemento de la forma $b^i a^j$ también tiene la forma $a^{j_1} b^i$ para algún j_1, con lo que todo elemento de G tiene la forma $a^i b^j$ con $0 \leq i \leq 2$ y $0 \leq j \leq 3$. Esto proporciona 12 elementos que es fácil ver que son todos ellos disjuntos.

Para calcular los subgrupos comenzamos calculando los subgrupos cíclicos no triviales:

$$\begin{aligned} \langle a \rangle = \langle a^2 \rangle &= \{1, a, a^2\}. \\ \langle b \rangle &= \{1, b^2\} \\ \langle b \rangle &= \{1, b, b^2, b^3\} \\ \langle ab \rangle &= \{1, ab, b^2, ab^3\} \\ \langle a^2 b \rangle &= \{1, a^2 b, b^2, a^2 b^3\} \\ \langle ab^2 \rangle = \langle a^2 b^2 \rangle &= \{1, ab^2, a^2, b^2, a, a^2 b^2\} \end{aligned}$$

Aparte de estos grupos cíclicos habría que añadir el trivial y G. Vamos a ver que no hay más subgrupos. Si los hubiera no tendrían que ser cíclicos y su orden tendría que ser 4 ó 6. Si hay un subgrupo de orden 4 no cíclico estaría formado por 1 y tres elementos de orden 2. Sin embargo sólo hay un elemento de orden 2, a saber b^2. En conclusión no hay subgrupos de orden 4. Si hubiera un subgrupo H de orden 6 este tendría un elemento de orden 2 y por tanto $b^2 \in H$. Sea $h \in H \setminus \langle b^2 \rangle$, entonces $H = \langle b^2, h \rangle$. Como h^2 está en el centro de G, necesariamente H es abeliano y por tanto H es cíclico de orden 6. Luego tendría un elemento de orden 3. Como los únicos elementos de G de orden 3 son a y a^2, deducimos que $a \in H$. Luego $H = \langle a, b \rangle = \langle ab \rangle$.

4. **Encontrar un subgrupo H de S_4 isomorfo a D_4. Demostrar que H no es normal en S_4.**

Numeramos los vértices de un cuadrado con 1,2,3 y 4 en sentido anti-horario Si miramos cómo actúan los elementos de D_4 en los vértices de un cuadrado observamos que la rotación R produce el 4-ciclo $(1, 2, 3, 4)$ en los vértices y la simetría respecto de la recta que pasa por los vértices 2 y 4 actúa en los vértices como la permutación $(1, 3)$. Por tanto podemos ver D_4 como el subgrupo $H = \langle a = (1, 2, 3, 4), b = (1, 3) \rangle$ de S_4. Observamos que a tiene orden 4, b tiene orden 2 y $a^b = a^{-1}$. Por tanto D_4 es isomorfo a H. Obsérvese que $(1, 2, 3, 4)^{(1,2)} = (2, 1, 3, 4) \notin H$, pues los únicos elementos de orden 4 en H son a y a^{-1}.

5. **Demostrar que todo grupo de orden 15 es abeliano y si G es un grupo arbitrario entonces $[G : Z(G)] \neq 15$.**

Comenzamos demostrando que la segunda parte se deduces de la primera. En efecto, si $[G : Z(G)] = 15$, entonces de la primera parte se deduce que $G/Z(G)$ es abeliano. Analizando las posibles listas de enteros $2 \leq d_n|d_{n+1}|\ldots|d_1$, $15 = d_1 \cdots d_n$, deducimos que la única posibilidad es que $d_1 = 15$, es decir $G/Z(G)$ es cíclico. Eso implicaría que G es abeliano y por tanto $G = Z(G)$, una contradicción.

Vamos pues a demostrar la primera parte, por reducción al absurdo. Supongamos que G es un grupo de orden 15. Por el Teorema de Cauchy G tiene un elemento a de orden 5 y otro b de orden 3. Claramente $G = \langle a, b\rangle$, con lo cual basta demostrar que $ab = ba$. Vamos primero a demostrar que $H = \langle a\rangle$ ó $K = \langle b\rangle$ es normal en G. Supongamos que H no es normal. Entonces $H \cap H^a = 1$ y por tanto $H^a \cap H^{a^2} = (H \cap H^a)^a = 1$ y $H \cap H^{a^2} = (H^{a^2} \cap H^a)^a = 1$. Es decir H, H^a y H^{a^2} sólo tienen el neutro en común, con lo que entre los tres tienen $1 + 3 \cdot 4 = 13$ elementos. Los dos elementos que faltan para completar G tendrían que ser b y b^2, con lo que K sería el único subgrupo de orden 3, y por tanto sería normal como queríamos demostrar. Por tanto H ó K es normal en G. Supongamos que H es normal. Entonces $b^a = b^i$, con $i = 1, 2, 3$ ó 4. Entonces $b = b^{a^3} = b^{i^3}$. Por tanto $i^3 \equiv 1 \mod 5$. Es decir, el orden de la clase de i en $\mathbb{Z}_5^*$ divide a 3. Pero también divide a $4 = |\mathbb{Z}_5^*|$, por el Teorema de Lagrange. Por tanto i tiene orden 1 en $\mathbb{Z}_5^*$, con lo que $a^b = a$. El mismo argumento muestra que si K es normal en G entonces $b^a = b^i$ con $i^5 \equiv 1 \mod 3$, y como $|\mathbb{Z}_3^*|$, necesariamente $i \equiv 1 \mod 3$, o sea $b^a = b$. En cualquiera de los dos casos deducimos que $ab = ba$, como queríamos.