Grupos y Anillos. Grado en Matemáticas. 2010-11. Examen de junio. Soluciones

1. **Enunciar el Teorema de la Correspondencia para anillos y grupos y demostrarlo en uno de los dos casos.** Ver los apuntes.

2. **Demostrar que todo grupo cíclico es isomorfo al grupo aditivo del anillo $\mathbb{Z}/n\mathbb{Z}$ para algún $n \in \mathbb{Z}$ y utilizarlo para demostrar que los subgrupos y grupos cociente de un grupo cíclico son cíclicos.**

Sea G un grupo cíclico y g un generador de G. Consideremos la aplicación

$$\begin{array}{rcl} f : \mathbb{Z} & \to & G \\ n & \mapsto & g^n \end{array}$$

Esta aplicación es un homomorfismo de $(\mathbb{Z}, +)$ a G pues

$$f(n+m) = g^{n+m} = g^n g^m = f(n)f(m).$$

f es suprayectiva pues g genera G y $\ker(f) = n\mathbb{Z}$ para algún $n \in \mathbb{Z}$ pues todos los subgrupos de $\mathbb{Z}$ son de esa forma. Por el Primer Teorema de Isomorfía tenemos $G = \text{Im}\ (f) \cong \mathbb{Z}/\ker(f) = \mathbb{Z}/n\mathbb{Z}$.

De la primera parte se deduce que para demostrar que todo subgrupo y todo cociente de un grupo cíclico G es cíclico basta demostrarlo para los grupos de la forma $\mathbb{Z}/n\mathbb{Z}$. Por el Teorema de la Correspondencia los subgrupos de $\mathbb{Z}/n\mathbb{Z}$ son de la forma $d\mathbb{Z}/n\mathbb{Z}$, con d un divisor de n. Este grupo es cíclico, generado por $d + n\mathbb{Z}$ y el cociente $(\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z})$ es isomorfo a $\mathbb{Z}/d\mathbb{Z}$, por el Segundo Teorema de Isomorfía, con lo que también es cíclico.

3. **Sean A un anillo e I un ideal de A. Sea $I[X]$ el conjunto de los polinomios con coeficientes en I. Demostrar que $I[X]$ es un ideal primo de $A[X]$ si y sólo si I es un ideal primo de A.**

Vamos a dar dos soluciones:

<u>Solución 1</u>. Consideremos el homomorfismo $F : A[X] \to (A/I)[X]$ que asocia el polinomio $\sum_{i=0}^n a_i X^i$ con coeficientes en A con el polinomio $\sum_{i=0}^n (a_i + I)X^i$ con coeficientes en A/I. Claramente F es suprayectivo y su núcleo es $I[X]$. Aplicando el Primer Teorema de Isomorfía deducimos que $(A/I)[X] \cong A[X]/I[X]$. Por tanto I es un ideal primo de A si y sólo si A/I es un dominio si y sólo si $(A/I)[X]$ es un dominio si y sólo si $A[X]/I[X]$ es un dominio si y sólo si $I[X]$ es un ideal primo de $A[X]$.

<u>Solución 2</u>. Supongamos que $I[X]$ es un ideal primo de $A[X]$. Entonces $I[X] \neq A[X]$ y por tanto $I \neq A$. Si $a, b \in A$ con $ab \in I$, entonces considerando a y b como polinomios de grado cero tenemos que $ab \in I[X]$. Como $I[X]$ es primo $a \in I[X]$ ó $b \in I[X]$. Eso implica que $a \in I$ ó $b \in I$.

Recíprocamente, supongamos que I es un ideal primo de A. Como $I \neq A$, tenemos que $I[X] \neq A[X]$. Sean $P, Q \in A[X] \setminus I[X]$ y pongamos $P = \sum_{i=0}^n p_i X^i$ y $Q = \sum_{i=0}^m q_i X^i$ con $p_i, q_i \in A$ para todo i. Entonces existen i_0 y j_0 tales que $p_{i_0} \notin I$ y $q_{j_0} \notin I$. Elegimos i_0 y j_0 mínimos con esta propiedad, es decir suponemos que $p_i \in I$ para todo $0 \le i < i_0$ y $q_j \in I$ para todo $0 \le j < j_0$. Entonces el coeficiente $i_0 + j_0$ de PQ es

$$a = p_0 q_{i_0+j_0} + p_1 q_{i_0+j_0-1} + \cdots + p_{i_0-1} q_{j_0+1} + p_{i_0} q_{j_0} + p_{i_0+1} q_{j_0-1} + \cdots + p_{i_0+j_0-1} q_1 + p_{i_0+j_0} q_0.$$

Los i_0 sumandos están en I por que $p_0, p_1, \ldots, p_{i_0-1}$ lo están. Los últimos j_0 sumandos también están en I por que lo están $q_0, q_1, \ldots, q_{j_0-1}$. Sin embargo, $p_{i_0} q_{j_0} \notin I$, pues I es un ideal primo de A. Eso implica que $a \notin I$, con lo que $PQ \notin I[X]$.

4. **Calcular el máximo común divisor y mínimo común múltiplo de $11 + 16i$ y $8 + i$ en $\mathbb{Z}[i]$.**

$$\frac{11+16i}{8+i} = \frac{(11+16i)(8-i)}{(8+i)(8-i)} = \frac{104+117i}{65} = \frac{8}{5} + \frac{9}{5}i.$$

Poniendo $a = 11 + 16i$, $b = 8 + i$ y $q = 2 + 2i$ tenemos $r = a - bq = -3 - 2i$. Continuando con el algoritmo de Euclides tenemos $b/r = -2 + i$. Por tanto $\text{mcd}(a, b) = r = -3 - 2i$ y $\text{mcm}(a, b) = \frac{ab}{\text{mcd}(a,b)} = -38 - 21i$.

5. **Demostrar que** $\delta(a+b\sqrt{2}) = |a^2-2b^2|$ **es una función euclídea en** $\mathbb{Z}[\sqrt{2}]$**. Encontrar infinitos elementos invertibles de** $\mathbb{Z}[\sqrt{2}]$**.**

Sabemos que la aplicación $\delta : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}$ satisface

1. Si $x \in \mathbb{Z}[\sqrt{2}]$ entonces $\delta(x) \in \mathbb{Z}$.
2. $\delta(xy) = \delta(x)\delta(y)$ para todo $x, y \in \mathbb{Q}(\sqrt{2})$;
3. $\delta(x) = 0$ si y sólo si $x = 0$.

(1) es obvio, y para comprobar (2) y (3) se se puede aplicar que $\delta(x) = x\sigma(x)$, donde $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ y σ es un automorfismo de $\mathbb{Q}(\sqrt{2})$. Por tanto, si $a, b \in \mathbb{Z}[\sqrt{2}] \setminus \{0\}$ con $a|b$, entonces $0 < \delta(a) \le \delta(b)$.

Por otro lado, $\frac{a}{b} = x_1 + x_2\sqrt{2}$ con $x_1, x_2 \in \mathbb{Q}$. Elegimos dos enteros q_1, q_2 que estén lo más próximos posible a x_1 y x_2 respectivamente. Eso implica que $|x_1 - q_1|, |x_2 - q_2| \le \frac{1}{2}$. Por tanto si ponemos $q = q_1 + q_2\sqrt{2}$ entonces

$$\delta\left(\frac{a}{b} - q\right) = |(x_1 - q_1)^2 - 2(x_2 - q_2)^2| \le \frac{1}{4} + 2\frac{1}{4} = \frac{3}{4} < 1.$$

Sea $r = a - bq \in \mathbb{Z}[\sqrt{2}]$. Entonces

$$\delta(r) = \delta(b)\delta\left(\frac{a}{b} - q\right) < \delta(b).$$

Esto prueba que δ es una función euclídea en $\mathbb{Z}[\sqrt{2}]$.

Una vez que sabemos que δ es una función euclídea en $\mathbb{Z}[\sqrt{2}]$ sabemos que las unidades de $\mathbb{Z}[\sqrt{2}]$ son los elementos x con $\delta(x) = 1$. Por ejemplo, $\delta(1 + \sqrt{2}) = |1 - 2| = 1$. Eso implica que $u = 1 + \sqrt{2}$ es una unidad de $\mathbb{Z}[\sqrt{2}]$. Como $u > 1$ tenemos $u^n > 1$ para todo $n \ge 1$ y por tanto u tiene orden infinito. Concluimos que $\langle u \rangle$ contiene infinitas unidades de $\mathbb{Z}[\sqrt{2}]$.

6. **Sean** G_1 **y** G_2 **dos grupos,** $N_1 \trianglelefteq G_1$ **y** $N_2 \trianglelefteq G_2$**. Demostrar que** $(G_1 \times G_2)/(N_1 \times N_2) \cong G_1/N_1 \times G_2/N_2$**.**

Consideremos la aplicación $f : G \to G_1/N_1 \times G_2/N_2$ dada por $f(g) = (gN_1, gN_2)$. Es fácil ver que f es un homomorfismo suprayectivo y que su núcleo es $N_1 \times N_2$. Aplicando el Primer Teorema de Isomorfía deducimos que $(G_1 \times G_2)/(N_1 \times N_2) \cong G_1/N_1 \times G_2/N_2$.

7. **Calcular los subgrupos de** S_4**.**

Comenzamos calculando los subgrupos cíclicos que serán de los siguientes tipos:

<u>De orden 1</u>: Sólo el grupo trivial.

<u>De orden 2</u>: Los generados por transposiciones:

$$\langle(1, 2)\rangle, \quad \langle(1, 3)\rangle, \quad \langle(1, 4)\rangle, \quad \langle(2, 3)\rangle, \quad \langle(2, 4)\rangle, \quad \langle(3, 4)\rangle;$$

y por elementos de tipo $[2, 2]$:

$$\langle(1, 2)(3, 4)\rangle, \quad \langle(1, 3)(2, 4)\rangle, \quad \langle(1, 4)(2, 3)\rangle.$$

<u>De orden 3</u>: Los generados por 3-ciclos. Aquí hay que tener en cuenta que $(1, 2, 3)$ y $(1, 3, 2)$ son inversos y por tanto sólo salen los siguiente subgrupos de orden 3:

$$\langle(1, 2, 3)\rangle, \quad \langle(1, 2, 4)\rangle, \quad \langle(1, 3, 4)\rangle, \quad \langle(2, 3, 4)\rangle.$$

<u>Cíclicos de orden 4</u>: Los generados por 4 ciclos. Como $(1, 2, 3, 4)$ es inverso de $(1, 4, 2, 3)$ sólo tenemos los siguientes subgrupos cíclicos de orden 4:

$$\langle(1, 2, 3, 4)\rangle, \quad \langle(1, 2, 4, 3)\rangle, \quad \langle(1, 3, 2, 4)\rangle.$$

Vamos con los subgrupos no cíclicos. Todos los subgrupos tienen orden 1, 2, 3, 4, 6, 8, 12 ó 24. Como los de órdenes 1, 2 y 3 son cíclicos y S_4 es el único subgrupo de orden 24, sólo nos tenemos que preocupar por los de órdenes 4, 6, 8 y 12.

<u>No cíclicos de orden 4</u>. Si H es un subgrupo no cíclico de orden 4, entonces está formado por la identidad y tres elementos de orden 2. Estos elementos serán o bien trasposiciones o producto de dos transposiciones disjuntas y H tiene que tener al menos dos trasposiciones o dos elementos de tipo $[2,2]$. Consideramos estos dos casos separadamente.

1) H tiene dos transposiciones σ y τ diferentes. Entonces $H = \{1, \sigma, \tau, \sigma\tau\}$. Supongamos que σ y τ no son disjuntas. Por simetría, podemos suponer que $\sigma = (1,2)$ y $\tau = (1,3)$. Eso implicaría que $(1,2,3) = (1,3)(1,2) \in H$, en contra de que H no contiene elementos de orden 3. Por tanto, σ y τ son disjuntas y H es uno de los siguientes grupos:

$$\langle (1,2),(3,4) \rangle, \quad \langle (1,3),(2,4) \rangle, \quad \langle (1,4),(2,3) \rangle.$$

2) H tiene dos elementos de tipo $[2,2]$. Por simetría podemos suponer que $\sigma = (1,2)(3,4)$ y $\tau = (1,3)(2,4)$. Entonces $\sigma\tau = (1,4)(2,3)$ y por tanto H es el siguiente grupo

$$V = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

<u>De orden 6</u>. Sea H un subgrupo de orden 6. Sus elementos tendrán todos orden 2 ó 3. Si H contiene un 3-ciclo, también contiene a su inverso. Por tanto el número de tres ciclos que tiene es par. Si tiene cuatro 3-ciclos, por simetría podemos suponer que contiene a $(1,2,3)$ y $(1,2,4)$. Pero estos dos elementos generan A_{12}, en contra de que H tiene orden 6. Por tanto, H tiene un máximo de dos 3-ciclos. Eso implica que H tiene al menos tres elementos de orden 2 de los que o bien dos son trasposiciones o dos son del tipo $[2,2]$. Sin embargo en este segundo caso H contendría a V, que es un subgrupo de orden 4, lo que no es posible. Por tanto H contiene dos trasposiciones σ y τ. Si σ y τ son dos trasposiciones disjuntas entonces $\langle \sigma, \tau \rangle$ es un subgrupo de H orden 4 lo que no es posible. Por tanto, σ y τ no son disjuntas y por simetría podemos suponer que si $\sigma = (1,2)$ y $\tau = (1,3)$. Entonces H contiene a $\langle \sigma, \tau \rangle = S_3$ y, como H tiene 6 elementos deducimos que $H = S_3$. Considerando las diferentes opciones para σ y τ obtenemos cuatro subgrupos de orden 6 isomorfos todos a S_3:

$$\langle (1,2)(1,3) \rangle, \quad \langle (1,2)(1,4) \rangle, \quad \langle (1,3)(1,4) \rangle, \quad \langle (2,3)(2,4) \rangle.$$

<u>De orden 8</u>. Sea H un subgrupo de orden 8. Todos sus elementos tendrán orden 2 ó 4.

Supongamos que H no tiene elementos de orden 4. Entonces todos los elementos de H son o transposiciones o producto de transposiciones disjuntas. Como de estas últimas sólo hay 3, H tiene que tener al menos cuatro trasposiciones. Pero dos de ellas serían no disjuntas y su producto sería un 3-ciclo, lo que nos lleva a una contradicción. Por tanto H contiene un 4-ciclo. Por simetría supongamos que $\sigma = (1,2,3,4) \in H$. Entonces $\langle \sigma \rangle$ es un subgrupo de orden 2 de H y por tanto es normal. Sea $\tau \in H \setminus \langle \sigma \rangle$. Supongamos primero que τ es un 4-ciclo. Probando con los posibles valores de τ, que son $(1,2,4,3), (1,3,2,4), (1,3,4,2)$ y $(1,4,2,3)$, observamos que en todos ellos $\sigma^\tau \notin \langle \sigma \rangle$, en contra de que $\langle \sigma \rangle$ es un subgrupo normal de H. Por tanto los cuatro elementos de $H \setminus \langle \sigma \rangle$ tienen orden 2 y necesariamente uno de ellos es una trasposición. Por tanto podemos suponer que τ es una trasposición. Pero $\langle (1,2),(1,2,3,4) \rangle = S_4$. Eso implica que $\tau \neq (1,2)$. Por simetría, τ tampoco puede ser $(2,3)$, ni $(3,4)$ ni $(1,4)$. En conclusión $\tau = (1,3)$ ó $(2,4)$. En ambos casos $H = \langle (1,3),(1,2,3,4) \rangle$. Cambiando los papeles del 4-ciclo obtenemos tres subgrupos de orden 8:

$$\langle (1,3),(1,2,3,4) \rangle, \quad \langle (1,4),(1,2,4,3) \rangle, \quad \langle (1,2),(1,3,2,4) \rangle.$$

<u>De orden 12</u>. Si H es un subgrupo de orden 12 distinto de A_4, entonces $H \cap A_4$ tiene orden 6. Sin embargo hemos visto que todos los subgrupos de orden 6 tienen un 2-ciclo y por tanto no están contenidos en A_4. En conclusión el único subgrupo de orden 12 es A_4.