Álgebra II — **3º de Matemáticas**
Curso 2012-2013 — 17 de mayo de 2013

Examen Ordinario

Apellidos y Nombre _____

D.N.I. _____ Firma _____

$\square + \square + \square + \square = \square$

1) (2.5 puntos) Explica con tus palabras qué es un ideal en un anillo (conmutativo) y pon un ejemplo. Decide si el ideal $I = \langle x^2, y^2 \rangle$ es principal en $\mathbb{Q}[x, y]$.

2) (2.5 puntos) Decidir razonadamente si las siguientes afirmaciones son verdaderas o falsas:
a) El grupo de Galois sobre $\mathbb{Q}$ del cuerpo de descomposición de $\big(x^{2013} - 2012\big)\big(x^{2012} - 2013\big)$ es un grupo soluble.
b) Si un polinomio de grado 4 no tiene raíces en $\mathbb{Q}\big(\sqrt{2}\big)$ entonces es irreducible sobre $\mathbb{Q}\big(\sqrt{2}\big)$.

3) (3 puntos) Sea L el cuerpo de descomposición de $x^3 - 7 \in \mathbb{Q}[x]$. Calcula razonadamente el grupo de Galois de la extensión $L/\mathbb{Q}$ e indica cuántos subcuerpos propios tiene (no hace falta hallarlos).

4) (2 puntos) Sean $L = \mathbb{Q}\big(e^{2\pi i/13}\big)$, $\alpha_1 = \cos\frac{2\pi}{13}$ y $\alpha_2 = i\,\mathrm{sen}\,\frac{2\pi}{13}$. Demuestra que $[L : \mathbb{Q}(\alpha_j)] \leq 2$ para $j = 1, 2$. Prueba también que L sólo tiene un subcuerpo M con $[L : M] = 2$ y deduce finalmente que $L = \mathbb{Q}(\alpha_2)$.

---

1) Un ideal I en un anillo conmutativo $(R, +, \cdot)$ es un subgrupo de $(R, +)$ que tiene la propiedad de que cualquier elemento de I multiplicado por otro de R vuelve a estar en I. Por ejemplo, los pares son un ideal de los enteros porque $\mathsf{par} \pm \mathsf{par} = \mathsf{par}$ y $\mathsf{par} \cdot \mathsf{entero} = \mathsf{par}$.

Si el ideal $I = \langle x^2, y^2 \rangle$ fuera principal, existiría $P \in \mathbb{Q}[x, y]$ tal que $\langle P \rangle = \langle x^2, y^2 \rangle$. En particular $P \mid x^2$ y $P \mid y^2$. Esto implica $P = r \in \mathbb{Q} - \{0\}$ y $r = Ax^2 + By^2$ con $A, B \in \mathbb{Q}[x, y]$ es una contradicción tomando por ejemplo $y = 0$.

2) a) [V] El polinomio es claramente soluble por radicales: sus raíces son $e^{2\pi ik/2013}\,\sqrt[2013]{2012}$, $e^{2\pi ik/2012}\,\sqrt[2013]{2013}$; entonces el teorema de Galois asegura que el grupo es soluble.
a) [F] $(x^2+1)(x^2+2)$ tiene raíces complejas $\pm i, \pm i\sqrt{2} \notin \mathbb{Q}\big(\sqrt{2}\big)$ y obviamente no es irreducible.

3) Las raíces de $P = x^3 - 7$ son $\omega^j \sqrt[3]{7}$, $j = 0, 1, 2$ con $\omega = e^{2\pi i/3} = (-1 + i\sqrt{3})/2$. Por consiguiente $L = \mathbb{Q}\big(\sqrt[3]{7}, \omega\big)$. Se tiene $[\mathbb{Q}\big(\sqrt[3]{7}\big) : \mathbb{Q}] = 3$ porque P es irreducible sobre $\mathbb{Q}$ (por el criterio de Eisenstein) y $[L : \mathbb{Q}\big(\sqrt[3]{7}\big)] = 2$ porque ω es raíz de $x^2 + x + 1$ y obviamente $\omega \notin \mathbb{Q}\big(\sqrt[3]{7}\big)$ (es complejo). Así pues $[L : \mathbb{Q}] = 6$.

Por la teoría sabemos que existe $\sigma \in \mathcal{G}(L/\mathbb{Q})$ con $\sigma\big(\sqrt[3]{7}\big) = \omega\sqrt[3]{7}$ (pues ambas son raíces de P) y componiendo con la conjugación τ, si fuera necesario, podemos suponer $\sigma(\omega) = \omega$. Además $\tau\big(\sqrt[3]{7}\big) = \sqrt[3]{7}$ y $\tau(\omega) = \overline{\omega} = \omega^2$. Con todo esto, los automorfismos Id, σ, σ^2, τ, $\tau\sigma$, $\tau\sigma^2$ son distintos y como hay tantos como $[L : \mathbb{Q}] = 6$, conforman todo el grupo de Galois. No es conmutativo porque por ejemplo $\tau\sigma\big(\sqrt[3]{7}\big) = \tau\big(\omega\sqrt[3]{7}\big) = \omega^2\sqrt[3]{7} \neq \sigma\tau\big(\sqrt[3]{7}\big) = \sigma\big(\sqrt[3]{7}\big) = \omega\sqrt[3]{7}$, entonces $\mathcal{G}(L/\mathbb{Q}) \cong S_3$.

Los subgrupos de orden 2 de S_3 están generados por las trasposiciones $(1,2)$, $(1,3)$, $(2,3)$ y los de orden 3 por cualquier 3-ciclo, por ejemplo $(1,2,3)$. Por el teorema fundamental de la teoría de Galois hay tantos subgrupos propios como subcuerpos propios, esto es, cuatro.

4) Sea $\zeta = e^{2\pi i/13}$, entonces $\zeta + \zeta^{-1} = 2\alpha_1$ y $\zeta - \zeta^{-1} = 2\alpha_2$, por tanto ζ es raíz de las ecuaciones $x^2 - 2\alpha_1 x + 1$ y $x^2 - 2\alpha_2 x - 1$, lo cual prueba $[L : \mathbb{Q}(\alpha_j)] \leq 2$. Sabemos que $\mathcal{G}(L/\mathbb{Q}) \cong \mathbb{Z}_{13}^* \cong \mathbb{Z}_{12}$ y los grupos cíclicos sólo tienen un subgrupo de cada orden, entonces por el teorema fundamental de la teoría de Galois, sólo puede haber un subcuerpo con $[L : M] = 2$, por tanto un $[L : \mathbb{Q}(\alpha_j)]$ es 1 y el otro es 2. Como $\alpha_1 \in \mathbb{R}$, no puede ser $[L : \mathbb{Q}(\alpha_1)] = 1$ y se concluye $[L : \mathbb{Q}(\alpha_2)] = 1$.