Teoría de Galois — **3º de Matemáticas**

CURSO 2011-2012 — 19 DE ENERO DE 2012

EXAMEN FINAL

APELLIDOS Y NOMBRE ______________________________

D.N.I. ______________ FIRMA ______________________

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

1) (3 puntos) Decidir razonadamente si las siguientes afirmaciones son verdaderas o falsas:
a) Existe una extensión $L/\mathbb{Q}$ que no es de Galois tal que $[L:\mathbb{Q}]=6$ y $|\mathcal{G}(L/\mathbb{Q})|=2$.
b) El cuerpo de descomposición L de $x^2+1\in\mathbb{F}_3[x]$ tiene 9 elementos.
c) Si $K\subset M\subset L$ y L/K es normal, entonces M/K también es normal.

2) (2 puntos) Sea $\alpha\in\mathbb{C}$ una raíz de x^3-2x-2. Expresar 1, α^2, $(\alpha^2)^2$ y $(\alpha^2)^3$ en términos de la base $\{1,\alpha,\alpha^2\}$ y utilizar el resultado para hallar $P\in\mathbb{Q}[x]$ de grado 3 tal que $P(\alpha^2)=0$. *Indicación*: Buscar una combinación lineal $(\alpha^2)^3+\lambda_2(\alpha^2)^2+\lambda_1\alpha^2+\lambda_0=0$.

3) (3 puntos) Sea $\zeta=e^{2\pi i/5}$ y $L=\mathbb{Q}(\zeta)$.
a) Usando el polinomio mínimo de ζ, deducir que $(2\zeta+2\zeta^4+1)^2=5$.
b) Probar que el único subcuerpo propio de $L/\mathbb{Q}$ es $\mathbb{Q}(\sqrt{5})$.

4) (2 puntos [de dificultad mayor]) Demostrar que $\cos\frac{2\pi}{13}$ es solución de una ecuación de tercer grado con coeficientes en $\mathbb{Q}(\sqrt{q_0})$ para cierto $q_0\in\mathbb{Q}$.

Soluciones

1) Las dos primeras afirmaciones son verdaderas y la última falsa.

a) **V**. Por ejemplo, $L=\mathbb{Q}(\sqrt[6]{2})$. Como $P=x^6-2\in\mathbb{Q}[x]$ es el polinomio mínimo sobre $\mathbb{Q}$ de $\sqrt[6]{2}$, se cumple $[L:\mathbb{Q}]=6$. Cualquier $\sigma\in\mathcal{G}(L/\mathbb{Q})$ debe enviar $\sqrt[6]{2}$ a una raíz de P, entonces las únicas posibilidades son $\sigma_\pm(\sqrt[6]{2})=\pm\sqrt[6]{2}$ (las otras raíces son complejas). Claramente $\sigma_+=\mathrm{Id}$. Por otro lado, σ_- define realmente un $\mathbb{Q}$-automorfismo porque viene de restringir a L un elemento de $\mathcal{G}(M/\mathbb{Q})$ con M el cuerpo raíz de P, ya que $M/\mathbb{Q}$ normal implica que existe un $\mathbb{Q}$-automorfismo que pasa una raíz a cualquier otra.

b) **V**. El polinomio x^2+1 es irreducible en $\mathbb{F}_3[x]$ (porque 0, 1, 2 no son raíces). Sea α una de sus raíces en su cuerpo de descomposición L sobre $\mathbb{F}_3$, entonces $x^2+1=(x-\alpha)(x+\alpha)$ y $L=\mathbb{F}_3(\alpha)$. Como $[\mathbb{F}_3(\alpha):\mathbb{F}_3]=\partial(x^2+1)=2$, se tiene que L es isomorfo a $\mathbb{F}_{3^2}$ (la única extensión de grado 2 de $\mathbb{F}_3$ salvo isomorfismos) que es un cuerpo de 9 elementos.

c) **F**. Por ejemplo $K=\mathbb{Q}$, $M=\mathbb{Q}(\sqrt[4]{2})$, $L=\mathbb{Q}(\sqrt[4]{2},i)$. Se cumple que L/K es normal por ser el cuerpo de descomposición de $P=x^4-2\in\mathbb{Q}[x]$. Sin embargo M/K no es normal porque P es irreducible en $\mathbb{Q}[x]$ y tiene una raíz en M pero no todas las raíces están en M.

2) Sabemos $\alpha^3-2\alpha-2=0$, por tanto $\alpha^4=2\alpha^2+2\alpha$ y $\alpha^6=(2\alpha+2)^2=4\alpha^2+8\alpha+4$. En forma matricial:

$$\begin{pmatrix}1\\ \alpha^2\\ \alpha^4\\ \alpha^6\end{pmatrix}=\begin{pmatrix}1&0&0\\0&0&1\\0&2&2\\4&8&4\end{pmatrix}\begin{pmatrix}1\\ \alpha\\ \alpha^2\end{pmatrix}.$$

Si llamamos f_1, f_2, f_3, f_4 a las filas de la matriz, $f_4 = 4f_1 + 4f_3 - 4f_2$, por consiguiente $\alpha^6 = 4 + 4\alpha^4 - 4\alpha^2$ y $P = x^3 - 4x^2 + 4x - 4$ es el polinomio buscado con $P(\alpha^2) = 0$.

3) Sea P el polinomio ciclotómico, $P = x^4 + x^3 + x^2 + x + 1 = (x^5 - 1)/(x - 1)$.

a) Sabemos que $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$ porque $P(\zeta) = 0$. Entonces

$$\begin{aligned}(2\zeta + 2\zeta^4 + 1)^2 &= 4\zeta^2 + 4\zeta^8 + 1 + 8\zeta^5 + 4\zeta + 4\zeta^4 \\ &= 4\zeta^2 + 4\zeta^3 + 4\zeta + 4\zeta^4 + 9 = -4 + 9 = 5.\end{aligned}$$

b) La extensión $L/\mathbb{Q}$ es de Galois (es cuerpo de descomposición de P) y cada automorfismo $\sigma \in \mathcal{G}(L/\mathbb{Q})$ está determinado por la raíz de P a la que envía ζ. Hay 5 posibilidades, lo que demuestra $\mathcal{G}(L/\mathbb{Q}) = \{\sigma_j \ : \ 1 \le j < 5\}$ con $\sigma_j(\zeta) = \zeta^j$. Como $|\mathcal{G}(L/\mathbb{Q})| = 4$ y σ_2 no tiene orden 2, ya que $\sigma_2\big(\sigma_2(\zeta)\big) = \zeta^4 \ne \zeta$, se tiene $\mathcal{G}(L/\mathbb{Q}) \cong \mathbb{Z}_4$ y sólo hay un subgrupo propio, $\langle\sigma_2^2\rangle$. Consecuentemente sólo hay un subcuerpo propio. Por otro lado, $2\zeta + 2\zeta^4 + 1 = \pm\sqrt{5}$ por a), así pues $\mathbb{Q} \subset \mathbb{Q}\big(\sqrt{5}\big) \subset L$. Claramente $\mathbb{Q}\big(\sqrt{5}\big) \ne \mathbb{Q}$ porque $\sqrt{5} \notin \mathbb{Q}$ y $\mathbb{Q}\big(\sqrt{5}\big) \ne L$ ya que ζ es un número complejo no real.

4) Razonando como en 3b) se tiene que la extensión $L/\mathbb{Q}$ con $L = \mathbb{Q}(\zeta)$, $\zeta = e^{2\pi i/13}$, es de Galois y $\mathcal{G}(L/\mathbb{Q}) = \{\sigma_j \ : \ 1 \le j < 13\}$ con $\sigma_j(\zeta) = \zeta^j$. Se cumple $\langle\sigma_2\rangle = \mathcal{G}(L/\mathbb{Q}) \cong \mathbb{Z}_{12}$ porque $|\mathcal{G}(L/\mathbb{Q})| = 12$ y σ_2 es un elemento de orden mayor que 6 ya que $\sigma_2^6(\zeta) = \zeta^{2^6} = \zeta^{64} = \zeta^{12} \ne \zeta$.

Se tiene $\mathbb{Q}\big(\cos\frac{2\pi}{13}\big) = \langle\sigma_2^6\rangle'$ porque $\cos\frac{2\pi}{13} = (\zeta + \zeta^{-1})/2 = (\zeta + \zeta^{12})/2$ es invariante por σ_2^6 y $[L : \mathbb{Q}\big(\cos\frac{2\pi}{13}\big)] = 2 = |\langle\sigma_2^6\rangle|$, ya que $\zeta \notin \mathbb{Q}\big(\cos\frac{2\pi}{13}\big)$ y $\zeta^2 - 2\zeta\cos\frac{2\pi}{13} + 1 = 0$. Entonces, definiendo $H = \langle\sigma_2^2\rangle$ que es de orden 6, $\mathbb{Q} \subset H' \subset \mathbb{Q}\big(\cos\frac{2\pi}{13}\big)$ y se verifica $[\mathbb{Q}\big(\cos\frac{2\pi}{13}\big) : H'] = [L : H']/[L : \mathbb{Q}\big(\cos\frac{2\pi}{13}\big)] = 6/2 = 3$. Por tanto $\cos\frac{2\pi}{13}$ tiene un polinomio mínimo de grado 3 sobre H'.

Finalmente, $[H' : \mathbb{Q}] = [L : \mathbb{Q}]/|H| = 12/6 = 2$ implica que $H' = \mathbb{Q}(\alpha)$ donde α satisface una ecuación de segundo grado (irreducible) sobre $\mathbb{Q}$, en particular $H' = \mathbb{Q}(\sqrt{q_0})$.