Teoría de Galois **3º de Matemáticas**
Curso 2012-2013 17 de enero de 2013

Examen Final

Apellidos y Nombre ______________________________

D.N.I. ______________ Firma ______________________

1) (2.5 puntos) Escribir razonadamente todos los polinomios mónicos irreducibles de grado 3 en $\mathbb{F}_3[x]$.

2) (3 puntos) Sean los cuerpos $L = \mathbb{Q}(\zeta)$ y $M = \mathbb{Q}(\zeta + \zeta^3 + \zeta^9)$ con $\zeta = e^{2\pi i/13}$. Probar que $\mathcal{G}\big(L/\mathbb{Q}\big) = \langle \sigma \rangle$ con $\sigma(\zeta) = \zeta^2$. Hallar $\mathcal{G}(L/M)$ y deducir cuáles son los grados $[L : M]$ y $[M : \mathbb{Q}]$.

3) (3 puntos) Decidir razonadamente si las siguientes afirmaciones son verdaderas o falsas:

a) $\cos\dfrac{2\pi}{7}$ es raíz de un polinomio de tercer grado en $\mathbb{Q}[x]$.

b) La extensión $\mathbb{Q}(\pi)/\mathbb{Q}(\pi^3 + 2013)$ es normal.

c) Si $L/\mathbb{Q}$ es una extensión de grado 6 con $\mathbb{Q} \subset L \subset \mathbb{R}$ entonces L no contiene irracionales construibles con regla y compás.

4) (1.5 puntos) Sabiendo que $\mathcal{G}(L/\mathbb{Q}) \cong S_5$ donde L es el cuerpo de descomposición de cierto polinomio $P \in \mathbb{Q}[x]$, probar que L tiene un subcuerpo propio M tal que L/M es una extensión radical.

---

1) El polinomio genérico de este tipo es $P = x^3 + ax^2 + bx + c$ con $a, b, c \in \mathbb{F}_3$, y es irreducible si y sólo si $P(0), P(1), P(2) \neq 0$, es decir, $c \neq 0$, $a + b + c \neq 2$ y $a - b + c \neq 1$ en $\mathbb{F}_3$. Dando valores a c y a b y despejando a, se obtiene:

c	b	a	
1	0	$\neq 1, 0$	$\to x^3 + 2x^2 + 1$
	1	$\neq 0, 1$	$\to x^3 + 2x^2 + x + 1$
	2	$\neq 2, 2$	$\to x^3 + 2x + 1$, $x^3 + x^2 + 2x + 1$
2	0	$\neq 0, 2$	$\to x^3 + x^2 + 2$
	1	$\neq 2, 0$	$\to x^3 + x^2 + x + 2$
	2	$\neq 1, 1$	$\to x^3 + 2x + 2$, $x^3 + 2x^2 + 2x + 2$

2) Sabemos que $\mathcal{G}(L/\mathbb{Q}) = \{\sigma_j \ : \ 1 \leq j \leq 12\}$ con $\sigma_j(\zeta) = \zeta^j$. Si comprobamos que que $\sigma = \sigma_2$ tiene orden 12, se deducirá $\mathcal{G}\big(L/\mathbb{Q}\big) = \langle \sigma \rangle$. Para ello basta comprobar que σ^1, σ^2, σ^3, σ^4 y σ^6 no son la identidad (el orden de un elemento divide al orden del grupo) y aplicando estos automorfismos a ζ, esto se sigue de $\zeta^2, \zeta^4, \zeta^8, \zeta^{16}, \zeta^{64} \neq \zeta$. Los automorfismos de $\mathcal{G}(L/M)$ son aquellos de $\mathcal{G}(L/\mathbb{Q})$ que dejan fijo $\alpha = \zeta + \zeta^3 + \zeta^9$. Como $\{\zeta^j \ : \ 1 \leq j < 13\}$ forman una base de $L/\mathbb{Q}$, las únicas posibilidades, aparte de la identidad, es que ζ vaya a ζ^3 o a ζ^9. Se comprueba fácilmente $\sigma_3(\alpha) = \sigma_9(\alpha) = \alpha$ y por tanto $\mathcal{G}(L/M) = \{\mathrm{Id}, \sigma_3, \sigma_9\}$. De aquí $[L : M] = 3$ y $[M : \mathbb{Q}] = [L : \mathbb{Q}]/[L : M] = 12/3 = 4$.

3) La primera es verdadera y las otras dos falsas.

a) $[\mathbb{Q}(e^{2\pi i/7}):\mathbb{Q}]=6$ y $\big[\mathbb{Q}(e^{2\pi i/7}):\mathbb{Q}(\cos\frac{2\pi}{7})\big]=2$ porque $e^{2\pi i/7}$ es raíz de $x^2-2x\cos\frac{2\pi}{7}+1$ y claramente no está en $\mathbb{Q}(\cos\frac{2\pi}{7})$. Entonces $\big[\mathbb{Q}(\cos\frac{2\pi}{7}):\mathbb{Q}\big]=3$ que es el grado del polinomio mínimo sobre $\mathbb{Q}$.

b) El polinomio $x^3-\pi^3\in\mathbb{Q}(\pi^3)[x]=\mathbb{Q}(\pi^3+2013)[x]$ es irreducible porque $\pi\not\in\mathbb{Q}(\pi^3)$, ya que $\pi=P(\pi^3)/Q(\pi^3)$ contradiría que π es trascendente, y $\pi e^{\pm 2\pi i/3}\not\in\mathbb{Q}(\pi^3)$. No es normal porque este polinomio irreducible tiene una raíz en $\mathbb{Q}(\pi)$ pero no todas.

c) Por ejemplo, $L=\mathbb{Q}(\sqrt[6]{2})$ cumple $[L:\mathbb{Q}]=6$ y $\sqrt{2}=\big(\sqrt[6]{2}\big)^3$ es un irracional en L construible con regla y compás.

4) Sea $\tau\in\mathcal{G}(L/\mathbb{Q})$ un elemento de orden 2 (existe, porque los hay en S_5, por ejemplo trasposiciones) y sea $M=\langle\tau\rangle'$, entonces $[L:M]=2$. Por tanto $\tau\in\mathcal{G}(L/M)\cong\mathbb{Z}_2$ y el teorema de Galois implica que L/M es radical (o directamente $L=M(\sqrt{\alpha})$ con $\alpha\in M$ sin apelar a este teorema).