Universidad Autónoma de Madrid Curso 2019-20

Matemáticas/ Ingeniería Informática-Matemáticas

Teoría de Galois

Tercer examen parcial. Jueves, 19 de diciembre de 2019

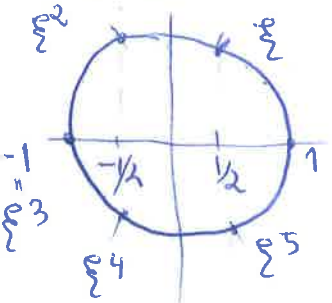
APELLIDOS: ______________________________

NOMBRE: ____________ DNI/NIE: ____________ PROFESORA: ____________

1. **(16 puntos)** Sea $f(x) = x^6 - 3 \in \mathbb{Q}[x]$.

a) Calcula $E = \mathbb{Q}(f)$ y muestra que $i \in E$.

Las raíces de f (en $\mathbb{C}$) son $\{\alpha\xi^j \mid 0 \leq j \leq 5\}$ donde $\alpha = \sqrt[6]{3} \in \mathbb{R}_{>0}$ y ξ es una raíz sexta de la unidad primitiva, p.ej: $\xi = 1/2 + \sqrt{3}/2\, i$.



(Notamos que ξ^2 y $\xi^4 = \overline{\xi^2}$ son las raíces primitivas cúbicas de la unidad, $\xi^5 = \overline{\xi}$ es otra raíz primitiva sexta de la unidad y $\xi^3 = -1$).

Entonces $E = \mathbb{Q}(\alpha, \alpha\xi^j \mid j=1..5) = \mathbb{Q}(\alpha, \xi^j)$

$= \mathbb{Q}(\alpha, \xi) = \mathbb{Q}(\alpha, \sqrt{3}i) = \mathbb{Q}(\alpha, i)$

$\alpha^3 = \sqrt{3} \in \mathbb{Q}(\alpha)$

Por tanto, $i \in E$. además, podemos notar que $|E:\mathbb{Q}| = |E:\mathbb{Q}(\alpha)||\mathbb{Q}(\alpha):\mathbb{Q}|$

$$= \underbrace{|\mathbb{Q}(\alpha)(i):\mathbb{Q}(\alpha)|}_{2 = \partial \mathrm{Irr}(\mathbb{Q}(\alpha), i)} \underbrace{|\mathbb{Q}(\alpha):\mathbb{Q}|}_{6 = \partial \mathrm{Irr}(\mathbb{Q}, \alpha) = x^6 - 3}$$

x^2+1 no tiene raíces en $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$

(Eisenstein $p=3$)

b) Sea $K = \mathbb{Q}(i)$, calcula el grado de E/K.

Por 1.a) $|E:\mathbb{Q}| = 12$, por el Teorema de Transitividad de Grados $|E:K| = 12/|K:\mathbb{Q}| = 12/2 = 6$

$K = \mathbb{Q}(i)$ $\mathrm{Irr}(i, \mathbb{Q}) = x^2+1$

También podríamos haber argumentado de la siguiente forma: $E = K(\alpha)$, E/K es una extensión simple y $|E:K| = \partial \mathrm{Irr}(K, \alpha) \leq 6$ (pues $\mathrm{Irr}(K,\alpha) \mid x^6 - 3$)

Por otro lado $K(\sqrt{3})/K$ y $K(\sqrt[3]{3})/K$ son subextensiones de E/K de grado 2 y 3 respectivamente (grados coprimos) luego $6 \mid |E:K| \Rightarrow |E:K| = 6$.

c) Describe los elementos de Gal(E/K) y sus órdenes. Sea $G = Gal(E/K)$. Como E/K es de Galois, $|G| = 6$. Como $K(\sqrt[3]{3})/K$ no es normal, sabemos que G no es abeliana por la caract. de ext normales en términos de grupos de Galois. (La razón por la que $K(\sqrt[3]{3})/K$ no es normal es que $\sqrt{3} \notin K(\sqrt[3]{3})$ y, por tanto, x^3-3 que es irreducible sobre K no se escinde en $K(\sqrt[3]{3})$) $\Rightarrow G \cong S_3$

Cada $\tau \in G$ queda determinado por $\tau(\alpha)$, y por ser x^6-3 irreducible sobre K, dado $j = 0, \ldots, 5$ existe $\tau_j \in G$ tal que $\tau_j(\alpha) = \alpha\xi^j$. Con esto ya tenemos los 6 elementos de G que podemos escribir en una tabla. Para calcular $o(\tau_j)$ necesitamos conocer $\tau_j(\xi)$. Notemos que $\xi = 1/2 + \alpha^3/2\, i$.

G	α	$\alpha^3=\sqrt{3}$	ξ	ord
$1_E=\tau_0$	α	$\sqrt{3}$	ξ	1
τ_1	$\alpha\xi$	$-\sqrt{3}$	ξ^5	2
τ_2	$\alpha\xi^2$	$\sqrt{3}$	ξ	3
τ_3	$\alpha\xi^3=-\alpha$	$-\sqrt{3}$	ξ^5	2
τ_4	$\alpha\xi^4$	$\sqrt{3}$	ξ	3
τ_5	$\alpha\xi^5$	$-\sqrt{3}$	ξ^5	2

Luego $\tau_j(\xi) = \begin{cases} \xi & j \text{ par} \\ \xi^5 & j \text{ impar} \end{cases}$

$\alpha \xrightarrow{\tau_1} \alpha\xi \xrightarrow{\tau_1} \alpha\xi\xi^5 = \alpha$ $\quad o(\tau_1) = 2$

$\alpha \xrightarrow{\tau_2} \alpha\xi^2 \xrightarrow{\tau_2} \alpha\xi^4 \xrightarrow{\tau_2} \alpha\xi^6 = \alpha$ $\quad o(\tau_2) = 3$

$\alpha \xrightarrow{\tau_3} \alpha\xi^3 \xrightarrow{\tau_3} \alpha$ $\quad o(\tau_3) = 2$

$\alpha \xrightarrow{\tau_4} \alpha\xi^4 \xrightarrow{\tau_4} \alpha\xi^2 \xrightarrow{\tau_2} \alpha\xi^6 = \alpha$ $\quad o(\tau_4) = 3$

$\alpha \xrightarrow{\tau_5} \alpha\xi^5 \rightarrow \alpha\xi^5(\xi^5)^{-1} = \alpha$ $\quad o(\tau_5) = 2$

* OTRA FORMA: subir por la extensión normal $K(\sqrt{3})$ notando que $x^3-6 = (x^3-\sqrt{3})(x^3+\sqrt{3})$

d) Determina todas las subextensiones de E/K indicando aquellas que se corresponden con extensiones normales sobre K.

Los cálculos en el apartado 1c) nos permiten concluir que $G = \langle\tau_2\rangle \rtimes \langle\tau_3\rangle$ donde $\tau_2^{\tau_3} = \tau_4 = \tau_2^{-1}$ ($G \cong S_3 = D_6$ "D_3")

Como $\langle\tau_2\rangle \trianglelefteq G$ $|\langle\tau_2\rangle| = 3$, $\langle\tau_2\rangle \in Syl_3(G)$ es el único subgp de orden 3 y es normal, por el TFTG se corresponde con la única subextensión de E/K de grado 2 sobre K (y, por tanto, normal). Como $K(\sqrt{3})/K$ es de grado 2 tenemos que $K(\sqrt{3}) = E^{\langle\tau_2\rangle} = E^{\tau_2}$

Por otro lado, G tiene 3 subgrupos de orden 2, por T$^{\text{a}}$ de Sylow todos ellos son conjugados, de hecho:

$$\langle\tau_1\rangle = \langle\tau_3\rangle^{\tau_2}, \quad \langle\tau_3\rangle, \quad \langle\tau_5\rangle = \langle\tau_3\rangle^{\tau_4}.$$

Notemos que $\tau_3(\alpha^2) = \alpha^2 = \sqrt[3]{3}$, luego $E^{\langle\tau_3\rangle} = K(\sqrt[3]{3})$ y

$E^{\langle\tau_1\rangle} = \tau_2(K(\sqrt[3]{3})) = K(\sqrt[3]{3}\,\xi^4)$

$E^{\langle\tau_5\rangle} = \tau_4(K(\sqrt[3]{3})) = K(\sqrt[3]{3}\,\xi^2)$

son las 3 subext. de grado 3 sobre K (ninguna de ellas es normal).

2. (12 puntos) Cuestiones. Responde de manera razonada a las siguientes preguntas, enunciando en cada caso los teoremas o resultados que utilices.

a) Sea E/K una extensión abeliana con $E = K(f)$ donde $f \in K[x]$ es irreducible, demuestra que $E = K(\alpha)$ para cualquier raíz α de f.

Primero observamos que:

$$K \hookrightarrow \underbrace{K[x]/\langle f(x)\rangle}_{L} \simeq K(\alpha) \hookrightarrow E$$

Si $L \subsetneq E$, entonces $Gal(E/L) < Gal(E/K)$ no sería normal ya que L/K no es normal si $K(\alpha) \subsetneq E$. Pero $Gal(E/K)$ es abeliano, y por lo tanto todos sus subgrupos son normales. En consecuencia $L = E$.

b) Considera un polinomio $p(x) \in \mathbb{F}_5[x]$ irreducible de grado 12 y E su cuerpo de descomposición (o escisión) sobre $\mathbb{F}_5$. Decide cuál es la clase de isomorfía de $\mathrm{Gal}(E/\mathbb{F}_5)$.

El cuerpo de descomposición de $p(x)/_{\mathbb{F}_5}$ es $E \simeq \mathbb{F}_5[x]/\langle p(x)\rangle$ que tiene grado 12 sobre $\mathbb{F}_5$.

La extensión $E/\mathbb{F}_5$ es Galois, por ser $\mathbb{F}_5$ perfecto, luego $12 = |E:\mathbb{F}_5| = |Gal(E/\mathbb{F}_5)|$.

Sabemos que $Fr: E \to E,\ \alpha \to \alpha^5$ es un automorfismo de $E/\mathbb{F}_5$. Si Θ es un generador del grupo multiplicativo E^*, entonces $E^* = \langle \Theta \rangle$ y $|\Theta| = 5^{12}-1$. En consecuencia $|Fr| = 12$ (porque basta iterar $Fr(\Theta)$ para calcular el orden del automorfismo); y por lo tanto $Gal(E/\mathbb{F}_5) \simeq C_{12}$.

c) Demuestra que todo polinomio con coeficientes racionales de grado 4 es resoluble por radicales.

Sea $p(x) \in \mathbb{Q}[x]$ un polinomio de grado 4 y sea E su cuerpo de descomposición $/\mathbb{Q}$

Sea o no irreducible sobre $\mathbb{Q}$, como $p(x)$ tiene como mucho 4 raíces distintas, se tiene que $Gal(E/\mathbb{Q}) \leq S_4$.

Como S_4 es resoluble $\Rightarrow$ $Gal(E/\mathbb{Q})$ también por ser subgrupo de un resoluble $\Rightarrow$ $E/\mathbb{Q}$ es una extensión radical. (por el Gran Teorema de la T^{a} de Galois).

3. **(12 puntos)** Determina si las siguientes afirmaciones son verdaderas o falsas, aportando demostraciones o contraejemplos, en cada caso:

a) Sea E/K una extensión finita, entonces $|\mathrm{Gal}(E/K)| = |E : K|$.

FALSO

Sea $K = \mathbb{Q}$; $E = \mathbb{Q}(\sqrt[3]{2})$. Entonces $[E : \mathbb{Q}] = 3$ porque $x^3 - 2 = \mathrm{Irr}(\sqrt[3]{2}, \mathbb{Q})$ y $E \cong \mathbb{Q}[x]/_{\langle x^3-2\rangle}$.

Si $\varphi \in \mathrm{Gal}(E/\mathbb{Q})$ entonces $\varphi(\sqrt[3]{2})$ tiene que ser otra raíz de x^3-2. Pero las otras raíces de x^3-2 no son reales y como $E \subseteq \mathbb{R}$ no están en E. Luego $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$ y como $\sqrt[3]{2}$ genera $E/\mathbb{Q} \Rightarrow \mathrm{Gal}(E/\mathbb{Q}) = \{id\}$

Luego $|\mathrm{Gal}(E/\mathbb{Q})| = 1 < [E : \mathbb{Q}] = 3$.

b) Sea $\alpha = \sqrt[3]{2} \in \mathbb{R}$, existe un número natural n tal que $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\xi)$ donde ξ es una raíz n-ésima de la unidad.

FALSO Primero observamos que $\mathbb{Q}(\xi)/\mathbb{Q}$ es el cuerpo de descomposición de $x^n - 1/\mathbb{Q}$. Luego $\mathbb{Q}(\xi)/\mathbb{Q}$ es Galois. Cada automorfismo $\varphi \in \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ viene dado por $\varphi(\xi) = \xi^i$ para algún $i \in \{1, \ldots, n-1\}$.

Luego si $\varphi, \psi \in \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$, se tiene que $\varphi(\xi) = \xi^i$, $\psi(\xi) = \xi^k$ para ciertos $i, k \in \{1 \ldots n-1\}$ de donde se deduce que $\varphi \circ \psi = \psi \circ \varphi$

$\Rightarrow \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ es abeliano. Como todo subgrupo de un grupo abeliano es normal, $\mathbb{Q}(\xi)/\mathbb{Q}$ no puede tener extensiones intermedias que no sean normales $/\mathbb{Q}$. Luego $\mathbb{Q}(\sqrt[3]{2}) \not\subset \mathbb{Q}(\xi)$ nunca porque $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ no es normal.

c) Sea E el cuerpo de descomposición (o escisión) de $x^{11}-1$ sobre $\mathbb{Q}$. Entonces $E/\mathbb{Q}$ tiene exactamente dos subextensiones propias. VERDADERO

$$x^{11}-1=(x-1)\underbrace{(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)}_{\text{ciclotómico irreducible}/\mathbb{Q}}$$

$\Rightarrow E=\mathbb{Q}(\zeta)$ con $\zeta=e^{2\pi i/11}$ es el cuerpo de descomposición de $x^{11}-1/\mathbb{Q}$ y $|E:\mathbb{Q}|=10$.

Como $\mathbb{Q}$ es perfecto, $E/\mathbb{Q}$ es Galois y

$$|Gal(E/\mathbb{Q})|=10.$$

Como $E=\mathbb{Q}(\zeta)$, por el mismo argumento que en (b), $Gal(E/\mathbb{Q})$ es abeliano, luego necesariamente isomorfo a C_{10} (*). Como C_{10} es cíclico, para cada d, $1<d<10$, con $d|10$, tiene exactamente un subgrupo con orden d. Así, C_{10} tiene un subgrupo H de orden 5 y otro N, de orden 2. Por el Teorema Fundamental de la Tª de Galois, estos dos subgrupos están en correspondencia biyectiva con las subextensiones propias de $E/\mathbb{Q}$, que por tanto sólo pueden ser dos.

(*) C_{10} es el único grupo abeliano de orden 10 salvo isomorfismo.