Teoría de Galois

Segundo examen parcial. Jueves, 14 de noviembre de 2019

APELLIDOS: ______________________________
NOMBRE: ____________ DNI/NIE: ____________ PROFESORA: ____________

1. (12 puntos) Sea L el cuerpo de escisión (o descomposición) de $x^{12}-3$ sobre $\mathbb{Q}$.

a) Describe L y demuestra que $\mathbb{Q}(i) \subseteq L$.

Las raíces de $x^{12}-3$ son $\sqrt[12]{3}\,\zeta^k$ (donde $\zeta = e^{\frac{2\pi i k}{12}}$) para $k=0,1\ldots 11$.

Luego $L = \mathbb{Q}(\sqrt[12]{3}\,\zeta^k,\ k=0,1\ldots 11)$.

Como $\sqrt[12]{3} \in \cancel{\mathbb{Q}}\ L$, $\sqrt[12]{3}^{-1} \cdot \sqrt[12]{3}\,\zeta \in L \Rightarrow \zeta \in L$.

y en realidad, $L = (\sqrt[12]{3}, \zeta)$. con $\zeta = e^{\frac{2\pi i}{12}} = e^{\pi/6\, i}$

Como $\zeta^2 = e^{2\pi/6\, i} = \frac{1}{2} + \frac{\sqrt{3}}{2} i \Rightarrow L = \mathbb{Q}(\sqrt[12]{3}, \sqrt{3} i)$

y como $(\sqrt[12]{3})^6 = \sqrt{3} \in L$, tenemos que

$L = \mathbb{Q}(\sqrt[12]{3}, i)$, luego $\mathbb{Q}(i) \subset L$.

⊛ Como $[L:\mathbb{Q}] = 24 = [L:\mathbb{Q}[i]]\,[\mathbb{Q}[i]:\mathbb{Q}] \Rightarrow$
$\Rightarrow [L:\mathbb{Q}[i]] = 12 \Rightarrow Irr(\sqrt[12]{3}, L)$ tiene grado 12.
y es divisor de $x^{12}-3 \Rightarrow \underset{Irr(\sqrt[12]{3},L)}{\overset{\|}{x^{12}-3}}$ es irreducible $/\mathbb{Q}(i)$.

b) Calcula el grado de $L/\mathbb{Q}(i)$ y concluye que $x^{12}-3$ es irreducible sobre $\mathbb{Q}(i)$.

Sabemos que:

$$\begin{tikzcd} & \mathbb{Q}(i) \arrow[dr] & \\ \mathbb{Q} \arrow[ur, "2"] \arrow[dr, "12"'] & & L = \mathbb{Q}(\sqrt[12]{3}, i) \\ & \mathbb{Q}(\sqrt[12]{3}) \arrow[ur, "a"'] & \end{tikzcd}$$

y: $[\mathbb{Q}(i):\mathbb{Q}] = 2$ porque x^2+1 es irred$/\mathbb{Q}$ ($\pm i \notin \mathbb{Q}$);
$[\mathbb{Q}(\sqrt[12]{3}):\mathbb{Q}] = 12$ porque $x^{12}-3$ es irred$/\mathbb{Q}$ (por Eisenstein con $p=3$). En consecuencia $[L:\mathbb{Q}(\sqrt[3]{2})] = a \leq 1$
y como $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, se tiene que x^2+1 es irreducible sobre $\mathbb{Q}(\sqrt[3]{2})$ por lo que $a = 2 \Rightarrow [L:\mathbb{Q}] = 24$ ⊛

c) Decide si la extensión $L/\mathbb{Q}$ es simple y, en caso afirmativo, determina un elemento $\alpha \in L$ tal que $L = \mathbb{Q}(\alpha)$.

$L = \mathbb{Q}(\sqrt[12]{3}, i)/\mathbb{Q}$ es finita y separable (por ser $\mathbb{Q}$ un cuerpo perfecto. Por lo tanto, por el teorema del elemento primitivo, $\exists\, \gamma \in L$ tq $L = \mathbb{Q}(\gamma)$.
Usando el algoritmo de la demostración del teorema cuando el cuerpo base es infinito, basta encontrar c adecuado para que $\sqrt[12]{3} + ci$ sea un elemento primitivo. Para buscar c, miramos a las raíces de: $Irr(\sqrt[12]{3}, \mathbb{Q}) = x^{12}-3$, y a las de $Irr(i,\mathbb{Q}) = x^2+1$

- $\alpha = \sqrt[12]{3}$, $a_i = \sqrt[12]{3}\,\xi^i$ $i = 1 \ldots 11$ como en (a);
- $\beta = i$ $b_1 = -i$

y ahora hace falta que $c \neq \dfrac{a_i - \alpha}{i-(-i)} = \dfrac{\sqrt[12]{3}\,(\xi^i - 1)}{2i} \in \mathbb{C}\setminus\mathbb{R}$
ya que $\{\xi^i\}_{i=1\ldots11} = \{\pm\frac{1}{2} \pm \frac{\sqrt{3}}{2}i;\ -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i;\ \pm i;\ \frac{\sqrt{3}}{2} \pm \frac{1}{2}i;\ -\frac{\sqrt{3}}{2} \pm \frac{1}{2}i;\ -1\}$
basta tomar $c = 1$.

2. **(12 puntos)** Responde razonadamente a las siguientes preguntas sobre cuerpos de característica p:

a) Determina el número de raíces distintas de $f(x) = x^{15} + 3x^5 + 2 \in \mathbb{F}_5[x]$ en su cuerpo de escisión (o descomposición).

Tenemos que $a^5 = a \ \forall a \in \mathbb{F}_5$, además $\mathbb{F}_5[x] \to \mathbb{F}_5[x]$, $f \mapsto f^5$ es un isomorfismo de anillos. Por tanto:

$f(x) = x^{15} + 3x^5 + 2 = (x^3)^5 + (3x)^5 + 2^5 = (x^3+3x+2)^5$.

Sea $p(x) = x^3+3x+2 \in \mathbb{F}_5[x]$, entonces f tiene tantas raíces distintas en su cuerpo de escisión como p (ambos polinomios tienen el mismo cuerpo de escisión, de hecho).

Notamos que $p(0)=2$, $p(1)=1$, $p(2)=1$, $p(3)=-2$ y $p(4)=-2$ luego p no tiene raíces en $\mathbb{F}_5$ y por tener grado 3 es irreducible. Como $\mathbb{F}_5$ es perfecto, p es separable (también f lo es) así que tiene 3 raíces distintas en su cuerpo de escisión $\Rightarrow f$ tiene 3 raíces distintas en su cuerpo de escisión

b) Sea E el cuerpo de escisión (o descomposición) del polinomio f del apartado **a)**. Calcula el grado de la extensión $E/\mathbb{F}_5$ y determina si es normal o separable.

El cuerpo de descomposición de f sobre $\mathbb{F}_5$, como ya hemos notado, coincide con el de p sobre $\mathbb{F}_5$.

Sea $K = \mathbb{F}_5[x]/(x^3+3x+2)$, por Kronecker tiene una raíz de p, concretamente $\bar{x} \in K$ es raíz de p.

Además $|K| = 5^3$ (por el algoritmo de la div. cada elemento de K tiene un único representante con grado menor que 3). Por tanto $K \cong \mathbb{F}_{5^3}$ es el cuerpo de descomposición de $x^{5^3} - x$ (por el Teorema de Clasificación/Caracterización de cuerpos finitos). En particular $K/\mathbb{F}_5$ es normal, y p se escinde en K. Como $\bar{x} \in K$ es raíz de p y $K = \mathbb{F}_5(\bar{x})$ tenemos que K es el cuerpo de escisión de p.

Luego $K = E$ y podemos calcular $|E:\mathbb{F}_5|$ según $\begin{cases} |E:\mathbb{F}_5| = 3 & \text{por cardinales } (E \cong \mathbb{F}_5{}^3 \text{ como } \mathbb{F}_5\text{-esp. vect}) \\ |E:\mathbb{F}_5| = |\mathbb{F}_5(\bar{x}):\mathbb{F}_5| = \partial \operatorname{Irr}(\mathbb{F}_5, \bar{x}) = \partial(x^3+3x+2) = 3 \end{cases}$

$E/\mathbb{F}_5$ es normal (por ser el cuerpo de escisión de f).

$E/\mathbb{F}_5$ es separable por ser una ext alg sobre un cuerpo perfecto.

c) Halla un generador del grupo multiplicativo del cuerpo $K = \mathbb{F}_3[x]/(x^2+x+2)$.

$x^2+x+2 \in \mathbb{F}_3[x]$ no tiene raíces en $\mathbb{F}_3$ y por tanto es irreducible

$K = \mathbb{F}_3[x]/(x^2+x+2)$ es un cuerpo

$= \{0, 1, 2, x, 2x, x+1, x+2, 2x+1, 2x+2\}$

en el que se cumple $x^2 = -x-2 = 2x+1$.

$|K| = 9$, luego $|K^\times| = 8$

y buscamos un elemento $\xi \in K^\times$ cuyo orden multiplicativo sea 8. Como $o(\xi) \mid |K^\times| = 8$ basta encontrar un elemento cuyo orden sea mayor que 4.

x, $x^2 = 2x+1$, $x^3 = 2x+2$, $x^4 = 2 \neq 1$

Por tanto, $\langle x \rangle = K^\times$

(otro generador es $x+1$, por ejemplo, de hecho $K^\times$ tiene 4 generadores distintos, que son concretamente

x

$x^3 = 2x+2$

$x^5 = 2x$

$x^7 = x+1$).

3. (**16 puntos**) Determina si las siguientes afirmaciones son verdaderas o falsas, aportando demostraciones o contraejemplos, en cada caso:

a) Existe un polinomio irreducible en $\mathbb{F}_{11}[x]$ de grado 22. VERDADERO

Sabemos que existe un cuerpo con 11^{22} elementos: $\mathbb{F}_{11^{22}}$ que es el cuerpo de descomposición de $x^{11^{22}}-x$ sobre $\mathbb{F}_{11}$. Luego $\mathbb{F}_{11} \subset \mathbb{F}_{11^{22}}$ y $[\mathbb{F}_{11^{22}} : \mathbb{F}_{11}] = 22$.

Como $\mathbb{F}_{11}$ es perfecto, la extensión $\mathbb{F}_{11^{22}}/\mathbb{F}_{11}$ es separable. Como también es finita, el Teorema del elemento primitivo dice que $\exists\ \theta \in \mathbb{F}_{11^{22}}$ tq. $\mathbb{F}_{11^{22}} = \mathbb{F}_{11}[\theta]$. Por el teorema de caracterización de elementos algebraicos $\mathbb{F}_{11}[\theta] \simeq \mathbb{F}_{11}[x]/\langle Irr(\theta, \mathbb{F}_{11})\rangle$ por lo que $\deg(Irr(\theta, \mathbb{F}_{11})) = 22$, y ese es el polinomio buscado.

b) Existen exactamente 3 isomorfismos distintos entre los cuerpos: VERDADERO

$$L = \mathbb{F}_2[t]/(t^3+t+1) \quad \text{y} \quad \mathbb{F}_2[y]/(y^3+y^2+1) = M$$

Como t^3+t+1 y y^3+y^2+1 son irreducibles sobre $\mathbb{F}_2$, tanto L como M son cuerpos. Y como ambos tienen grado 3, $|L| = |M| = 2^3 \Rightarrow L \simeq M \simeq \mathbb{F}_{2^3}$ el cuerpo con 8 elementos. Sabemos que $\mathbb{F}_{2^3}$ es el cuerpo de descomposición de $x^{2^3}-x\ /\mathbb{F}_2$, luego $\mathbb{F}_{2^3} \simeq L$ es normal sobre $\mathbb{F}_2 \Rightarrow L$ contiene las 3 raíces de t^3+t+1, siendo una de ellas $\bar{t}$.
Por otro lado como $L \simeq M$, M también contiene las 3 raíces de t^3+t+1. Además estas 3 raíces son distintas por ser $\mathbb{F}_2$ perfecto y t^3+t+1 irreducible (por tanto separable $/\mathbb{F}_2$). Sean $\alpha_1, \alpha_2, \alpha_3 \in M$ las 3 raíces de t^3+t+1. Entonces $M \simeq \mathbb{F}_2(\alpha_1) \simeq \mathbb{F}_2(\alpha_2) \simeq \mathbb{F}(\alpha_3)$ y como $L = \mathbb{F}_2[\bar{t}]$, hay 3 isomorfismos entre L y M los $\mathbb{F}_2$-isomorfismos $\bar{t} \to \alpha_i$, $i = 1, 2, 3$.

c) Sea $E = \mathbb{Q}(\sqrt[8]{5}, i)$ y sea $L = \mathbb{Q}(\sqrt{5}) \subset E$. Entonces la extensión E/L es normal y separable.

Verdadero

Sea $f(x) = x^4 - \sqrt{5} \in L[x]$, las raíces de f son exactamente $\{\pm\sqrt[8]{5}, \pm\sqrt[8]{5}\, i\}$ y luego el cuerpo de escisión de f sobre L es

$$L(f) = L(\sqrt[8]{5}, \sqrt[8]{5}\, i) = \mathbb{Q}(\sqrt{5}, \sqrt[8]{5}, i)$$

$$(\sqrt[8]{5})^4 = \sqrt{5} \longrightarrow = \mathbb{Q}(\sqrt[8]{5}, i)$$

Por tanto E/L es normal

E/L es separable por ser alg sobre un cuerpo ~~con~~ de característica 0 ($\operatorname{car}(L) = 0$)

$\mathbb{Q} \subseteq$

d) Sea $E = \mathbb{Q}(\sqrt[8]{5}, i)$ y sea $L = \mathbb{Q}(\sqrt{5}) \subset E$. Sea $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ el $\mathbb{Q}$-automorfismo de L definido por $\sigma(\sqrt{5}) = -\sqrt{5}$. Entonces σ se puede extender a un automorfismo de $\mathrm{Gal}(E/\mathbb{Q})$.

Falso

$\mathbb{Q} \subset L \subset E$

normal: $x^4 - \sqrt{5}$ por 8.c)

normal: cuerpo de escisión de $x^2 - 5$

Notemos que $E/\mathbb{Q}$ no es normal pues el pol $x^8 - 5 \in \mathbb{Q}[x]$ (irred. por Eisenstein para $p = 5$) tiene una raíz en E pero no se escinde, puesto que $\sqrt{2} \notin E$ y las raíces de $x^8 - 5$ son $\{\pm\sqrt[8]{5}, \pm\sqrt[8]{5}\, i, \sqrt[8]{5}\,(\pm\sqrt{2}/2 \pm \sqrt{2}/2\, i)\}$

Así que no se pueden aplicar los resultados sobre extensión de automorfismos.

- Supongamos que $\tilde{\sigma}: E \to E$ extiende a σ. Entonces $\tilde{\sigma}(\sqrt[8]{5})$ tiene que ser otra raíz de $x^8 - 5$ que esté contenida en E: $\tilde{\sigma}(\sqrt[8]{5}) = \sqrt[8]{5}\, i^k$ con $k = 0, 1, 2, 3$.
Entonces $-\sqrt{5} = \tilde{\sigma}(\sqrt{5}) = \tilde{\sigma}((\sqrt[8]{5})^4) = (\sqrt[8]{5}\, i^k)^4 = \sqrt{5}$ #
- De otra forma: Como $\tilde{\sigma}^*(x^4 - \sqrt{5}) = x^4 + \sqrt{5}$, $\tilde{\sigma}(\sqrt[8]{5})$ tiene que ser raíz de $x^4 + \sqrt{5}$; pero $x^4 + \sqrt{5}$ no tiene NINGUNA raíz en E.