

Ejercicio 1 (5 puntos). Sea  $f = x^4 + 3x^2 - 2 \in \mathbb{Q}[x]$  y  $K$  su cuerpo de descomposición.

1. Demostrar que  $f$  tiene una raíz real positiva  $\alpha$  tal que  $\alpha \notin \mathbb{Q}(\alpha^2)$ . → para esto basta usar que  $x^2 - 17$  es irreducible en  $\mathbb{Q}[x]$  por ser 17 primo  
 $\Rightarrow f, \sqrt{17} \in \mathbb{Q}$ -base de  $\mathbb{Q}(\alpha^2) \Rightarrow x = \alpha + b\sqrt{17} \in \mathbb{Q}(\sqrt{17})$
2. Demostrar que  $i\sqrt{2} \in K$  y calcular  $[K : \mathbb{Q}]$ .
3. Calcular  $Aut(K)$  definiendo explícitamente todos sus elementos.
4. Calcular los subgrupos de  $Aut(K)$  correspondientes por la conexión de Galois con los subcuerpos  $\mathbb{Q}(\alpha^2)$  y  $\mathbb{Q}(i\sqrt{2})$  de  $K$ , listando sus elementos.
5. Decidir razonadamente cuál es el grado del polinomio

$$g = Irr(\alpha + i\sqrt{2}, \mathbb{Q})$$

¿Es  $g$  resoluble por radicales? ¿Son las raíces complejas de  $f$  constructibles con regla y compás?

Antes de todo, como siempre haremos, vamos a estudiar cuál es el cuerpo de descomposición de  $f \in \mathbb{Q}[x]$ . Puesto que la ecuación  $f=0$  es bicuadrática al resolverla obtenemos que sus raíces son, tomando  $\alpha = \sqrt{\frac{-3+i\sqrt{17}}{2}}$  y  $\beta = i\sqrt{\frac{3+\sqrt{17}}{2}}$ , las siguientes:  $R = \{\alpha, -\alpha, \beta, -\beta\}$ . Por tanto, sabemos ya que  $K = \mathbb{Q}(\alpha, \beta)$ .

1. Claramente, tenemos que  $\alpha > 0$  puesto que  $\sqrt{17} > 4 > 3$ . Queda por ver que  $\alpha \notin \mathbb{Q}$ , para ello, bastará probar que  $f = Irr(\alpha, \mathbb{Q})$ ; pero, en virtud del criterio de Eisenstein aplicado al primo  $p=2$ , se tiene que  $f$  es irreducible y podemos concluir que  $\alpha$  tiene raíces en  $\mathbb{Q}$ .

Por tanto, podemos concluir que así obtiene lo pedido.

2. Probemos que  $\mathbb{Q}(i\sqrt{2}) \subseteq \mathbb{Q}(\alpha, \beta)$ ; para ello, bastará probar que  $i\sqrt{2} \in \mathbb{Q}(\alpha, \beta)$ , pero tenemos que

$$\sqrt{2} = i\sqrt{\frac{(i\sqrt{17}-3)(i\sqrt{17}+3)}{4}} = i\sqrt{\frac{17-9}{4}} = i\sqrt{2}$$

de donde se obtiene dicha inclusión.

De dicha inclusión se obtiene que  $\mathbb{Q}(\alpha, i\sqrt{2}) \subseteq \mathbb{Q}(\alpha, \beta)$ ; si conseguimos probar la otra inclusión tendremos que  $K = \mathbb{Q}(\alpha, i\sqrt{2})$  lo que nos facilitará las cuentas. Como  $i\sqrt{2} = \alpha\beta$  y  $\alpha \in \mathbb{Q}(\alpha, i\sqrt{2})$  es fácil ver que  $\beta = \frac{i\sqrt{2}}{\alpha}$  de donde se tiene la igualdad.

Buscamos ahora calcular el grado de la extensión  $\mathbb{Q} \subseteq K$  y, para ello, aplicaremos el Teorema de la Torre obteniendo que

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)] [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

Calcularemos cada uno de los índices.

(i)  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$  puesto que ya vimos que  $f = Irr(\alpha, \mathbb{Q})$  de donde, aplicando que  $\alpha$  es algebraico sobre  $\mathbb{Q}$  existe un único polinomio monólico irreducible del cual es raíz que nos asegura que  $\alpha$  es irracional.

(ii)  $[K : \mathbb{Q}(\alpha)] \geq 2$ ; esto es así debido a que  $i\sqrt{2}$  es raíz del polinomio  $x^2 + 2 \in \mathbb{Q}(\alpha)[x]$  porque tenemos que  $[i\sqrt{2} : \mathbb{Q}(\alpha)] \leq 2$  y como  $i\sqrt{2} \in \mathbb{Q}(\alpha)$  por ser  $\alpha$  real tenemos la igualdad.

Por tanto,  $[K : \mathbb{Q}] = 8$ .

3. Aunque no es necesario para obtener este apartado, recalcaremos que  $\alpha \in K$  es una extensión de Galois por ser  $K$  cuerpo de descomposición de un polinomio irreducible en característica 0 y así podemos recordar que se nos pide calcular el grupo de Galois de la extensión.

Pronto que, teniendo los únicos homomorfismos posibles al ser  $\mathbb{Q}$  el cuerpo primo de los cuadros el siguiente esquema:

$$\begin{array}{ccc} \mathbb{Q} & \xrightarrow{i} & K \\ & \searrow i & \downarrow \\ & & K \end{array}$$

Si consideramos ahora el polinomio  $f \in \mathbb{Q}[x]$  tenemos que, como  $f' = f$  se descompone como producto de polinomios lineales sobre  $K$  al ser este su cuerpo de descomposición, la tercera proposición de extensión nos asegura que  $|\text{Aut}(K)| = |\text{Ex}(i, i)| = [K : \mathbb{Q}(\alpha)] = 8$ .

Considerando ahora el siguiente esquema, el polinomio  $f \in \mathbb{Q}[x]$  que vienes que era irreducible

$$\begin{array}{ccc} \mathbb{Q} & \xrightarrow{i} & K \\ & \searrow i & \downarrow \\ & & \mathbb{Q}(\alpha) \end{array}$$

y de  $\mathbb{Q}(\alpha)$  raíz de  $f' = f$ . La primera proposición de extensión nos asegura que hay una correspondencia biyectiva entre las raíces de  $f' = f$  en  $K$  y  $\text{Ex}(i, i)$  dada por:  $\text{Ex}(i, i) \longrightarrow R$

$$R \longmapsto \gamma^{(R)}$$

este resultado nos permite obtener los homomorfismos  $\gamma_j : \mathbb{Q}(\alpha) \longrightarrow K$  dados por

$$\gamma_j(\alpha) = (-i)^j \alpha \text{ para } j=0,1 \quad \text{y} \quad \gamma_j(\alpha) = (-i)^j \beta \text{ para } j=2,3.$$

Ahora bien, cada uno de estos homomorfismos puede extenderse ahora, de nuevo por la primera proposición de extensión, a los automorfismos más allá lugar al grupo de Galois dado por

$$\text{Aut}(K) = \{\gamma_{ju} : j=0,1,2,3 \wedge u=0,1\}$$

donde lo único nuevo es que  $\gamma_{ju}(\sqrt[4]{2}) = u^{-1} \sqrt[4]{2}$ . Implicitamente hemos usado que el polinomio  $x^2 + 2 \in \mathbb{Q}(\alpha)[x]$  es invariante por  $\gamma_j \forall j \in \{0,1,2,3\}$  y que  $p = \text{Irr}(\sqrt[4]{2}, \mathbb{Q}(\alpha))$ .

4. La coerción de Galois nos asegura que, al ser los automorfismos que los subgrupos buscados son  $\text{Aut}_{\mathbb{Q}(\sqrt[4]{2})}(K)$  y  $\text{Aut}_{\mathbb{Q}(\sqrt[4]{7})}(K)$ ; por tanto, buscamos cuáles de los elementos de  $\text{Aut}(K)$  dejan fijos a  $\alpha^2$  ó a  $i\sqrt[4]{2}$ . Procedemos por partes:

i) Para el caso  $\sqrt[4]{2}$ ; como  $|\text{Aut}_{\mathbb{Q}(\sqrt[4]{2})}(K)| = [K : \mathbb{Q}(\sqrt[4]{2})] = 4$  por lo visto anteriormente y en virtud de la coerción de Galois buscamos 4 elemeatos que únicamente sea

$$\{\gamma_{j0} : j=0,1,2,3\}$$

ii) Para el caso  $\alpha^2$ ; como  $\alpha(\alpha^2) = \mathbb{Q}(\sqrt[4]{7})$  y  $[\mathbb{Q}(\sqrt[4]{7}) : \mathbb{Q}] = 2$ , el lema de la Torre nos dice que  $[K : \mathbb{Q}] = [\mathbb{Q} : \mathbb{Q}(\sqrt[4]{7})][\mathbb{Q}(\sqrt[4]{7}) : \mathbb{Q}] = 4 \Rightarrow [K : \mathbb{Q}(\sqrt[4]{7})] = 4$  deducido de la coerción de Galois nos da que  $|\text{Aut}_{\mathbb{Q}(\alpha^2)}(K)| = 4$ . Se tiene que:

$$\gamma_{ju}(\alpha^2) = (\gamma_{ju}(\alpha))^2 \quad ; \quad \gamma_{ju}(\alpha) = \begin{cases} (-i)^j \beta & \text{si } j=2,3 \Rightarrow (\gamma_{ju}(\alpha))^2 = \beta^2, j=2,3 \\ (-i)^j \alpha & \text{si } j=0,1 \Rightarrow (\gamma_{ju}(\alpha))^2 = \alpha^2, j=0,1 \end{cases}$$

de donde se deduce que  $\text{Aut}_{\mathbb{Q}(\alpha^2)}(K) = \{\gamma_{ju} : j=0,1; u=0,1\}$

5. Puesto que  $g = \text{Irr}(\alpha + i\sqrt{2}, \mathbb{Q})$  tenemos que  $[\mathbb{Q}(\alpha + i\sqrt{2}) : \mathbb{Q}] = |\text{Aut}_{\mathbb{Q}(\alpha + i\sqrt{2})}(\mathbb{K})|$ . Buscando ahora probar que  $\mathbb{Q}(\alpha + i\sqrt{2}) = \mathbb{Q}(\alpha, i\sqrt{2})$ ; tenemos que  $\mathbb{Q}(\alpha + i\sqrt{2}) \subseteq \mathbb{Q}(\alpha, i\sqrt{2})$  y para probar la otra inclusión probaremos que  $\text{Aut}_{\mathbb{Q}(\alpha + i\sqrt{2})}(\mathbb{K}) = \langle \eta_{\alpha, i\sqrt{2}} \rangle$  puesto que, en ese caso, la conexión de Galois nos asegura que  $[\mathbb{K} : \mathbb{Q}(\alpha + i\sqrt{2})] = 1$ .

a) Es claro que, necesitamos que  $\alpha = 0$  pues  $\gamma_{\alpha}(i\sqrt{2}) = e^{i\frac{\pi}{2}}i\sqrt{2}$   $\forall \alpha \in \mathbb{C}$

ii) Además,  $\gamma_{\alpha}(\alpha) = \alpha$  si y sólo si  $j = 0$

Por tanto, tenemos ya que  $\mathbb{Q}(\alpha + i\sqrt{2}) = \mathbb{K}$  de donde el grupo de Galois de  $g$  es  $\text{Aut}(\mathbb{K})$ . Como todo grupo de 8 elementos es resoluble tenemos que  $g$  es resoluble por radicales. Además, como  $\mathbb{Q}$  tiene de Galois con  $\mathbb{K}$  cuerpo de descomposición de  $g$  tenemos que todas las raíces son construibles con regla y compás.

**Ejercicio 2** (3 puntos). Sea  $\eta \in \mathbb{C}$  una raíz decimocuarta primitiva de la unidad.

1. Calcular el decimocuarto polinomio ciclotómico  $\phi_{14}$ .
2. Calcular, definiendo explícitamente todos sus elementos,  $\text{Aut}(\mathbb{Q}(\eta))$  y todos sus subgrupos.
3. Calcular, expresando sus generadores en función de  $\eta$ , todos los subcuerpos de  $\mathbb{Q}(\eta)$ .

Puesto que  $\eta \in \mathbb{C}$  es una raíz decimocuarta primitiva de la unidad sabemos que  $\eta$  es raíz del polinomio  $x^{14}-1 \in \mathbb{Q}[x]$ , polinomio cuyas raíces son las raíces decimocuartas de la unidad; de hecho, sabemos ya que  $[\mathbb{Q}(\eta) : \mathbb{Q}] = \Phi(14) = 6$  donde  $\Phi(n)$  es el cuerpo de descomposición de  $x^n - 1$ . Además, el polinomio  $\Phi_{14}$  es irreducible en  $\mathbb{Q}[x]$  y da lugar a la decimocuarta extensión ciclotómica que es de Galois con grupo de Galois isomorfo a los cuadrados de  $\mathbb{Z}_{14}$ .

1. Para calcular dicho polinomio bastará usar la recursión vista en teoría dada por

$$\Phi_{14} = \frac{x^{14}-1}{\Phi_2 \Phi_7}$$

donde  $\Phi_1 = x+1$  y  $\Phi_2 = x+1$ . Además, si usas fijas  $x^{14}-1 = (x^7-1)(x^7+1)$  deduce

$$\Phi_{14} = \frac{(x^7-1)(x^7+1)}{x+1} \Phi_7$$

pero  $(x^7-1) = \Phi_7 \Phi_1$  deduce  $\Phi_{14} = \frac{x^7+1}{x+1} = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$

2. Alguna brev, puesto que  $\text{Aut}(\mathbb{Q}(\eta)) \cong U(\mathbb{Z}_{14})$  tenemos que sus elementos son los siguientes

$$\tau_j : \mathbb{Q}(\eta) \longrightarrow \mathbb{Q}(\eta)$$

$$z \longmapsto z^j$$

para  $j \in U(\mathbb{Z}_{14}) = \{1, 3, 5, 9, 11, 13\}$ . Calcularemos el orden de cada elemento

$$\begin{array}{cccccc} \tau_1 & \tau_3 & \tau_5 & \tau_9 & \tau_{11} & \tau_{13} \\ 1 & 6 & 6 & 3 & 3 & 2 \end{array}$$

Tenemos que  $\text{Aut}(\mathbb{Q}(\eta)) = \langle \tau_3 \rangle$  que tiene un subgrupo de cada cardinal divisor de 6 en virtud del Teorema de Lagrange, y estos son  $\langle \tau_9 \rangle$  y  $\langle \tau_{13} \rangle$ .

3. Veremos a hora que subextensiones de  $\mathbb{Q}(\eta)$  se corresponden con cada uno de los subgrupos del grupo de Galois.

i) Puesto que  $\langle \eta_{20} \rangle$  es  $K$ -lineal (tenemos que  $K \subseteq K^{\langle \eta_{20} \rangle}$  deducido, como  $[K : K^{\langle \eta_{20} \rangle}] = 1$ ) seda la igualdad.

ii) Como  $\langle \tau_3 \rangle$  es  $\mathbb{Q}$ -lineal pero no dejó fijo a ninguna raíz decimal o carta primitiva de la unidad tenemos que  $\mathbb{Q} \subseteq K^{\langle \tau_3 \rangle}$  equivale a la conexidad de Galois. Además, como  $[K : K^{\langle \tau_3 \rangle}] = |\langle \tau_3 \rangle| = 6$  el lema de la torre nos dice que  $[K^{\langle \tau_3 \rangle} : \mathbb{Q}] = 1$  como queríamos probar.

iii) Estudiaremos la órbita de  $\eta$  por la acción de  $\tau_4$

$$\eta \longrightarrow \eta^8 \longrightarrow \eta^{16} \longrightarrow \eta$$

como  $\tau_4(\eta_i) = \eta_i$  con orden multiplicativo 2 tenemos que  $\mathbb{Q}(\eta^8) = \mathbb{Q}$  pero esto nos permite obtener que  $\eta^8 = -\eta^4$ ,  $\eta^{16} = -\eta^{12} = -\eta^4$  y  $-\eta^{32} = -\eta^8 = \eta$  ya que  $\eta^8 = 1$ . Por lo que podemos ver que  $\eta - \eta^4 - \eta^8$  queda fijo por  $\tau_4$  dando lugar a que  $\mathbb{Q}(\eta - \eta^4 - \eta^8) \subseteq K^{\langle \tau_4 \rangle}$  y como la conexidad de Galois nos asegura que  $[K : K^{\langle \tau_4 \rangle}] = |\langle \tau_4 \rangle| = 3$  obtenemos por el lema de la Torre que seda la igualdad.

iv) Análogamente, calculando la órbita de  $\eta$  por  $\tau_3$  tenemos que

$$\eta \longrightarrow \eta^3 \longrightarrow \eta^{27} = \eta$$

pero  $\eta^3 = \eta^7 \eta^6 = -\eta^6$ , deducido  $-\eta^{28} = -\eta^8 = \eta$ . Además, usando que  $\eta^3 = \eta^9$  tenemos que  $\eta^{18} = \eta^1$  de donde  $\eta + \eta^{-1}$  queda fijo por  $\tau^3$  pues  $\tau^3(\eta + \eta^{-1}) = \eta + \eta^{-1}$ . Faltaría probar que  $\eta + \eta^{-1} \notin \mathbb{Q}$  pero  $\Phi_4 = \text{Irr}(\eta, \mathbb{Q})$  de donde  $\eta + \eta^{-1} = \eta - \eta^6 = -\eta^5 + \eta^4 - \eta^3 + \eta^2 + 1$  y como  $\{1, \omega, \omega^2, \omega^3, \omega^5, \omega^7\}$  es una  $\mathbb{Q}$ -base de  $\mathbb{Q}(\eta)$  tenemos lo que queríamos.

Por lo tanto combinando con lo anterior tenemos que  $K^{\langle \tau_3 \rangle} = \mathbb{Q}(\eta + \eta^{-1})$ .

**Ejercicio 3** (2 puntos). Vimos en clase que  $\mathbb{F}_{64} = \mathbb{F}_2(a)$  con  $a$  satisfaciendo la ecuación  $a^6 + a + 1 = 0$ , y que  $a$  es un elemento primitivo del  $\mathbb{F}_{64}$ . Calcular, expresándolas en función de  $a$ , las raíces en  $\mathbb{F}_{64}$  del polinomio  $h = x^3 + x + 1 \in \mathbb{F}_2[x]$ .

Primero de todo, puesto que  $\mathbb{F}_{64}$  contiene todas las raíces del polinomio  $x^{64} - x \in \mathbb{F}_2[x]$  y este polinomio se factoriza como el producto de todos los irreducibles de grado divisor de 6 bastará probar que  $h$  es irreducible en  $\mathbb{F}_2[x]$  para saber que dicha ecuación tiene solución en  $\mathbb{F}_{64}$ .

En dicho caso, si  $b \in \mathbb{F}_{64}$  fuese una raíz de  $h$  tenemos que  $\mathbb{F}_2(b)$  es cuerpo de descomposición de  $h$  puesto que  $\mathbb{F}_2 \subseteq \mathbb{F}_2(b)$  es una extensión de Galois al ser de cuerpos finitos, lo que nos dice que es normal y como contiene una raíz de  $h$  debe contener las demás. Ahora bien, sabemos de la teoría de cuerpos finitos que  $\mathbb{F}_8$  es el cuerpo de descomposición de  $h$  por lo que el Teorema de Unicidad del cuerpo de descomposición nos da que  $\mathbb{F}_2(b) \subseteq \mathbb{F}_8$ .

En ese caso, como  $[\mathbb{F}_2(b) : \mathbb{F}_2] = 3$  tenemos que  $\{1, b, b^2\}$  es una  $\mathbb{F}_2$ -base de  $\mathbb{F}_2(b)$  y como  $b^3 + b + 1 = 0$

tenemos que  $\alpha(b)=7$  pues sabemos que  $b \in \mathbb{F}_3^\times$  y  $\alpha(b) \in \{1, 7\}$ .

Por tanto, buscamos un elemento de orden multiplicativo 7 sobre  $\mathbb{F}_{3^4}^\times$ , dicho elemento puede ser  $a^9$ , pero  $h(a^9) \neq 0$  por lo que, el autodominio de Frobenius de la extensión  $\mathbb{F}_2 \subset \mathbb{F}_2(a)$  o  $\mathbb{F}_2 \subset \mathbb{F}_2(b)$  (es el mismo) nos dice que  $a^{18}$  y  $a^{36}$  son las raíces que buscamos pues son del polinomio  $x^3+x^2+1 \in \mathbb{F}_2[x]$  también irreducible.

Por tanto, los elementos que serán raíces de  $h$  son los elementos restantes de  $\mathbb{F}_2(b)^\times$ , a saber, estos son  $b^3, b^5$  y  $b^6$  que se corresponden con  $a^{27}, a^{45}$  y  $a^{54}$ .

$\xrightarrow{\text{multiplicar por } 9 \text{ porque es el círculo generado por } a^9}$

Quedó por probar que  $h$  es irreducible en  $\mathbb{F}_2[x]$  pero  $h(0)=1=h(1)$  luego se tiene el acuchido y el ejercicio está resuelto.