

Ejercicio 1. Sea  $f = (x^3 - 2)(x^2 - 3) \in \mathbb{Q}[x]$  y  $K$  el cuerpo de descomposición de  $f$ :

- Comprobar que  $i + \sqrt{3} \in K$ .
- Calcular  $[K : \mathbb{Q}]$ .

Antes de resolver el ejercicio, necesitamos conocer cuál es su cuerpo de descomposición; puesto que  $f = gh \in \mathbb{Q}[x]$  siendo  $g = x^3 - 2 \in \mathbb{Q}[x]$  y  $h = x^2 - 3 \in \mathbb{Q}[x]$ , resolviendo ambas ecuaciones  $g=0$  y  $h=0$  obtenemos que, las raíces de  $f$  son

$$R = \left\{ \sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}, \sqrt{3}, -\sqrt{3} \right\}$$

donde  $\omega \in \mathbb{C}$  es una raíz cúbica primitiva de la unidad, seáse  $\omega = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$ . Por tanto, podemos ya asegurar, puesto que  $\text{UreR}$  resalgárico sobre  $\mathbb{Q}$  que  $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}, \sqrt{3}, -\sqrt{3}) = K$ . Es trivial que  $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ ; pero veamos que  $K = \mathbb{Q}(i\sqrt{3}, \sqrt[3]{2}, \sqrt{3})$

i) La inclusión  $K \subseteq \mathbb{Q}(i\sqrt{3}, \sqrt[3]{2}, \sqrt{3})$  es clara

ii) Ahora bien, como  $i\sqrt{3} = 2\omega - 1 \in \mathbb{Q}(\omega)$  se tiene que  $\mathbb{Q}(i\sqrt{3}, \sqrt[3]{2}, \sqrt{3}) \subseteq K$

Por tanto, se da la igualdad. Veamos ahora que  $K = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{2})$ ; sin embargo, esto es trivial entonces,  $K = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{2})$ .

a) Este ejercicio ya es trivial.

b) Una forma de hacer esto es aplicar el Teorema de la Torre:

$$[\text{Ue. } \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})] [\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}]$$

Calcularemos cada uno de los grados:

i) Como  $i \notin \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$  tenemos que  $x^2 + 1 \in \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})[x]$  es irreducible en  $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})[x]$  de donde  $[\text{Ue. } \mathbb{Q} : \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})] = 2$ .

ii) Veamos que  $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}] = 6$ ; puesto que  $\sqrt{3}$  y  $\sqrt[3]{2}$  ambas son raíz de  $f$  y  $\deg f = 6$  tenemos que  $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}] \leq 6$ . Ahora bien, sabemos bien que  $x^3 - 2 \in \mathbb{Q}[x]$  es irreducible por el criterio de Eisenstein para  $p=2$  de donde  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ . De forma análoga  $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ . Aplicando el Teorema de la Torre obtenemos que

$$6 \geq [\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})] \cdot 3$$

$$6 \geq [\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] \cdot 2$$

De donde se da la igualdad.

Por tanto,  $[\text{Ue. } \mathbb{Q}] = 12$ .

Ejercicio 2. Sea  $f = x^3 - 3x + 1 \in \mathbb{Q}[x]$  siendo  $\alpha$  una raíz real de  $f$ . Probar que el cuerpo de descomposición de  $f$  sobre  $\mathbb{Q}$  es  $\mathbb{Q}(\alpha)$ .

Veamos que  $f \in \mathbb{Q}[x]$  es irreducible en  $\mathbb{Q}[x]$ ; como  $f \in \mathbb{Z}[x]$  tenemos que, sus únicas raíces racionales posibles son  $1$  y  $-1$ ; sin embargo,  $f(1) = -1$  y  $f(-1) = 3$ . Por tanto,  $f = \text{Irr}(\alpha, \mathbb{Q})$  de donde tenemos que  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ .

Sea ahora  $K$  el cuerpo de descomposición de  $f$ ; claramente se tiene que  $\mathbb{Q}(\alpha) \subseteq K$ ; además,

el toro de la Torre nos dice que

$$[u: \mathbb{Q}] = [u: \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha): \mathbb{Q}] = 3 \cdot [\mathbb{Q}(\alpha): \mathbb{Q}]$$

Por tanto, si conseguimos probar que  $[\mathbb{Q}(\alpha): \mathbb{Q}] = 3$  tendríamos la igualdad. Ahora bien, puesto que  $\alpha$  es un elemento de características 0 y  $f$  es irreducible, en particular,  $f$  es separable; por tanto,  $\mathbb{Q}(\alpha)$  es una extensión de Galois. Entonces, el problema se reduce a probar, gracias a la teoría de Galois, que  $|\text{Aut}(u)| = 3$ . Puesto que  $\deg f \geq 3$  tenemos que  $|\text{Aut}(u)| \leq S_3$ ; además, como  $f$  es irreducible se tiene que  $\text{Aut}(u)$  es un subgrupo transitivo de  $S_3$ , es decir,  $A_3 \circ S_3$ .

Por tanto, el problema vuelve a reducirse a probar que  $\Delta(f) \in \mathbb{Q}$ , pero

$$\text{Disc}(f) = -4p^3 - 27q^2 = -4 \cdot (-3)^3 - 27 = 4 \cdot 27 - 27 = 3 \cdot 27 = 81 \in \mathbb{Q}[x] \text{ como cabría esperar}$$

$$\Delta(f) = \sqrt{\text{Disc}(f)} = 9 \in \mathbb{Q}[x]$$

En definitiva, tenemos probado que  $u = \mathbb{Q}(\alpha)$ .

**Ejercicio 3.** Sea  $F$  un cuerpo con  $\text{car}(F) = 3$  y con un elemento  $a \in F$  con  $F = \mathbb{F}_3(a)$  con  $a^4 + a - 1 = 0$ .

- Diseñar  $\text{Aut}(F)$  y evaluarlos en  $a^2$ .
- Calcular el cardinal de  $\mathbb{F}_3(a^2)$ .

Buscamos usar la teoría de cuerpos finitos; para ello, veamos si  $f = x^4 + x - 1 \in \mathbb{F}_3[x]$  es irreducible; puesto que  $f(0) = 2$ ,  $f(1) = 1$ ,  $f(2) = 2$  tenemos que no tiene raíces en  $\mathbb{F}_3$ , si además no tuviera factores irreducibles de orden 2 sería irreducible. Los posibles factores de orden 2 son  $\{x^2 + 1, x^2 + 2x + 1, x^2 + 2x + 2\}$  y ninguno de ellos divide a  $f$ . Por tanto, como  $f$  es irreducible tenemos que su cuerpo de descomposición es isomorfo a  $\mathbb{F}_{81}$ .

Veamos que  $\mathbb{F}_3(a) \cong \mathbb{F}_{81}$ ; para ello, como  $\mathbb{F}_3 \leq \mathbb{F}_3(a)$  es una extensión de cuerpos finitos tenemos que es de Galois y, en particular, normal. Entonces, como  $\mathbb{F}_3(a)$  contiene una raíz,  $a$ , debe contener todos, de donde  $\mathbb{F}_3 \leq \mathbb{F}_3(a)$ . Como trivialmente  $\mathbb{F}_3(a) \leq \mathbb{F}_{81}$ , tenemos la igualdad.

Además, sabemos que, como  $f = \text{Ir}(a, \mathbb{F}_3)$  tenemos que  $[\mathbb{F}_3(a) : \mathbb{F}_3] = 4$  y  $\{1, a, a^2, a^3\}$  es  $\mathbb{F}_3$ -base de  $\mathbb{F}_{81}$ .

- Con todo lo estudiado anteriormente, junto a que, de la teoría sabemos que  $\text{Aut}(\mathbb{F}_{81})$  es un grupo cíclico de orden  $[\mathbb{F}_3(a) : \mathbb{F}_3] = 4$  generado por el automorfismo de Frobenius,  $\tau(a) = a^3$ , podemos ya asegurar que  $\{1, \tau, \tau^2, \tau^3\} = \text{Aut}(\mathbb{F}_{81})$ .

Evaluando en  $a^2$ , sabiendo que  $a^4 + a - 1 = 0$  y  $\{1, a, a^2, a^3\}$  es  $\mathbb{F}_3$ -base de  $\mathbb{F}_3(a)$ .

$$\tau(a^2) = a^2$$

$$\Rightarrow \tau(a^2) = a^6 = a^4 a^2 = (a^4 + 1)a^2 = 2a^3 + a^2 \neq 0 \text{ por ser } a^2 \text{ y } a^3 \text{ LI.}$$

$$\begin{aligned} \Rightarrow \tau^2(a^2) = (\tau(a^2))^3 &= (a^2)^6 = (a^4)^3 = (a^4 + 1)^3 = (4a^2 + 4a + 1)(2a + 1) = (a^2 + a + 1)(2a + 1) = \\ &= 2a^3 + 3a^2 + 3a + a^2 + a + 1 = 2a^3 + 1 \neq 0 \text{ por ser } a^3 \text{ y } 1 \text{ LI.} \end{aligned}$$

$$\Rightarrow \tau^3(a^2) = \tau(\tau(a^2)) = \tau(\tau^2(a^2)) = \tau(2a^3 + 1) = (2a^3 + 1)^3 = (2a^3 + 1)^2(2a^3 + 1) = (a^2 + a + 1)(2a^3 + 1)$$

$$= 2a^3 + 2a^2 + 2a + 1 \neq 0 \text{ pues } \{1, a, a^2, a^3\} \text{ es } \mathbb{F}_3\text{-base de } \mathbb{F}_3$$

b) Para ello, cabe recordar que  $\mathbb{F}_3(a^2) \leq \mathbb{F}_3(a)$ ; por tanto, es claro que  $[\mathbb{F}_3(a^2)]$  divide a 81. Buscamos ahora probar que  $\mathbb{F}_3(a) \cong \mathbb{F}_3(a^2)$ ; para ello, bastará probar que  $[\mathbb{F}_3(a^2) : \mathbb{F}_3] = [\mathbb{F}_3(a) : \mathbb{F}_3]$ ; usando ahora la conexión de Galois y el Teorema de la Torre sabemos que

$$[\mathbb{F}_3(a) : \mathbb{F}_3] = [\mathbb{F}_3(a) : \mathbb{F}_3(a^2)][\mathbb{F}_3(a^2) : \mathbb{F}_3] \Leftrightarrow [\mathbb{F}_3(a^2) : \mathbb{F}_3] = \frac{[\mathbb{F}_3(a) : \mathbb{F}_3]}{[\mathbb{F}_3(a) : \mathbb{F}_3(a^2)]}$$

como, por la conexión de Galois  $[\mathbb{F}_3(a) : \mathbb{F}_3] = 4 = |\text{Aut}(\mathbb{F}_3(a))|$ , buscamos ver cuál es el grado de la extensión de  $[\mathbb{F}_3(a) : \mathbb{F}_3(a^2)]$  que por la conexión de Galois se reduce a divisores  $|\text{Aut}_{\mathbb{F}_3(a^2)}(\mathbb{F}_3(a))|$ ; puesto que, en el apartado anterior vimos que la idéntidad era el único que dejaba fija a  $a^2$  tenemos que  $[\mathbb{F}_3(a^2) : \mathbb{F}_3] > 4$  de donde necesariamente  $|\mathbb{F}_3(a^2) : \mathbb{F}_3| = 3 = \frac{[\mathbb{F}_3(a^2) : \mathbb{F}_3]}{[\mathbb{F}_3(a^2) : \mathbb{F}_3(a^2)]} = 81$ .

**Ejercicio 4.** Responda razonadamente si las siguientes afirmaciones son verdaderas o falsas.

a) Si  $F \leq E \leq K$  con  $F \leq E$  y  $E \leq K$  extensiones de Galois, entonces  $F \leq K$  es de Galois.

b) Si  $z \in \mathbb{C}$  tiene grado 4 sobre  $\mathbb{Q}$  entonces  $z$  es construible.

a) Veamos que es falsa; para ello, consideremos la torre de cuerpos  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{e}) \subseteq \mathbb{Q}(\sqrt[4]{e})$ , veamos que  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{e})$  no es de Galois. Consideremos  $\text{In}_1(\sqrt[4]{e}, \mathbb{Q}) = x^4 - e$ , claramente es irreducible por el criterio de Eisenstein para  $p=2$ . Ahora bien, si  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{e})$  fuera de Galois, como  $\sqrt[4]{e}$  es raíz de su irredicible debería contener todas las raíces y por tanto a una raíz cuarta de la unidad

b) Esta afirmación discutimos en clase su falsedad, buscamos un elemento de grado 4 sobre  $\mathbb{Q}$  que no sea constructible con regla y compás, es decir, que toda extensión de Galois sea de grado una potencia de 2.

Para ello, consideramos el polinomio  $x^4+x+1$  que es irreducible en  $\mathbb{Q}[x]$  por no tener raíces en  $\mathbb{Q}$  y tener factores irreducibles de grado 2. Ahora bien, como  $f$  es irreducible sabemos que su grupo de Galois es isomorfo a un subgrupo transitivo de  $S_4$ , séase:  $S_4$ ,  $A_4$ ,  $D_4$  o  $V$ . Para descartar casuísticas, obteniendo la cónica reducida vemos que es factor  $x^3 - 4x - 1$  cuyo discriminante es 229 que es un número primo, por tanto, tenemos que dicho grupo de Galois es  $S_4$  o  $D_4$ . Además, como  $f$  es irreducible en  $\mathbb{Q}[x]$  por no tener raíces, se cumple que el grupo de Galois de  $f$  es  $S_4$ .

Sea ahora  $F$  el celd de  $\mathbb{Q}$  y  $K$  el celd de  $f$  tenemos que  $\mathbb{Q} \subseteq$  es de Galois y  $F \subseteq K$  de donde, por un teorema visto en clase tenemos que

No entiendo como seguir.

