

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

- Calcular razonadamente  $[K : \mathbb{Q}(\sqrt{3})]$ .
- Describir los elementos del grupo  $\text{Aut}_{\mathbb{Q}(\sqrt{3})}(K)$ .
- Calcular todas las subextensiones de la extensión  $\mathbb{Q}(\sqrt{3}) \leq K$ .
- Dar todas las subextensiones de  $\mathbb{Q}(\sqrt{3}) \leq K$  que contienen al número  $\sqrt{3} + i$ .

*Entendemos que busquemos información de la situación del problema; consideramos  $F = \mathbb{Q}(\sqrt{3})$ , puesto que  $f$  es un polinomio de la forma  $x^3 - a \in F[x]$  con  $a \neq 0$  tenemos que es separable.*

*Usando un poco de la teoría del apartado de extensiones cíclicas, consideramos  $w \in \mathbb{C}$  una raíz cubica primitiva de la unidad, sabemos  $w = \frac{-1+i\sqrt{3}}{2} \in \mathbb{C}$ , y  $r = \sqrt[3]{2} \in \mathbb{R}$  raíz de  $f$ . Usando dicha teoría tenemos que  $F(w, r) = K$ . Además, estamos ante una extensión radical, información que podría ser útil en algún momento.*

Por tanto, hemos probado que  $K = \mathbb{Q}(\omega, \sqrt[3]{2}, \sqrt{3}) = \mathbb{Q}(\omega, \sqrt[3]{2}, \sqrt{3})$ ; en otras ocasiones hemos visto que  $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \beta)$  en cuyo caso  $[K : \mathbb{Q}(\alpha, \beta)] = 6$ . Si probáramos ahora que  $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{3})$  tendríamos que  $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 3$  puesto que  $x^3 - 2 \in \mathbb{Q}(\sqrt{3})[x]$  sería irreducible.

De hecho, el Lema de la Torre nos dice que, como  $\sqrt[3]{2}\sqrt{3}$  son raíces de  $h = (x-2)(x-3)$  tenemos que

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

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

por tanto, como queríamos probar  $x=3, y=2$ . De hecho, se podría haber realizado por reducción al absurdo llegando a 213.

- Ahora bien, con todo lo probado y gracias a que  $x^2+1 \in \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})[x]$  es irreducible en  $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})[\sqrt{3}]$  puesto que en ese cuerpo no hay números complejos obfuscantes, en virtud del Lema de la Torre que  $[K : F] = 6$
- Para ello, habría que confirmar todo la paraformalia de otros exámenes sobre las propiedades de extensión; sabemos que las raíces de  $f$  son  $r_j = \sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}$  y las de  $\text{Irr}(i, F(\sqrt[3]{2}))$  son  $i, -i$ . Por tanto, aplicando la tercera proposición de extensión y puesto que  $F \leq K$  es de grado tenemos que  $|\text{Aut}_F(K)| = 6$  y es un subgrupo de  $S_3$ ; entonces  $\text{Aut}_F(K) \cong S_3$ .
- Usando ahora la biología de la primera proposición de extensión tenemos que

$$\text{Aut}_F(K) = \{\eta_{jk} : j=0,1,2 ; k=0,1\} : \quad \eta_{jk} : K \longrightarrow K$$

$$\begin{aligned} \sqrt[3]{2} &\longmapsto w^j\sqrt[3]{2} & j=0,1,2 \\ i &\longmapsto (-)^k i & k=0,1 \end{aligned}$$

- Para ello, como  $\text{Aut}_F(K) \cong S_3$  tenemos que no hay elementos de orden 6, hay un subgrupo de orden 3 que será isomórfico a  $\mathbb{Z}_3$  y habrá 3 grupos de orden 2. Calcularemos los órdenes de los

elementos

$$\begin{matrix} \zeta_{200} & \zeta_1 & \zeta_{10} & \zeta_{11} & \zeta_{20} & \zeta_{21} \\ 1 & 2 & 3 & 4 & 3 & 2 \end{matrix}$$

Por tanto, los subgrupos son  $\{\text{Aut}_F(K)\}, \langle \zeta_{20} \rangle, \langle \zeta_{11} \rangle, \langle \zeta_{21} \rangle, \langle \zeta_{10} \rangle = \langle \zeta_{20} \rangle^2$ . Sus generadores correspondientes son las subextensiones correspondientes:

i) Claramente, la conocida de Galois nos dice que la subextensión de  $\langle \zeta_{20} \rangle$  es  $K^{(\zeta_{20})}$ ; como  $\langle \zeta_{20} \rangle$  dejó fijo todo  $K$  tenemos que  $K \subseteq K^{(\zeta_{20})}$  además, como  $[K : K^{(\zeta_{20})}] = |\langle \zeta_{20} \rangle| = 1$  se da la igualdad.

ii) Como  $\text{Aut}_F(K)$  no dejó fija  $\sqrt[3]{2}$  vio i tenemos que  $K^{(\text{Aut}_F(K))} \supseteq F$ , tenemos que  $[K : K^{(\text{Aut}_F(K))}] = 6$ ; pero el lema de la Torre juntando la conocida de Galois nos dice que

$$6 \cdot [K : F] = [K : K^{(\text{Aut}_F(K))}] \cdot [K^{(\text{Aut}_F(K))} : F] \stackrel{(i)}{=} 6 \cdot g = 12 \text{ lo que da la igualdad}$$

$$g \in \mathbb{N} \text{ usando que } [K : K^{(\text{Aut}_F(K))}] = \frac{|\text{Aut}_F(K)|}{|\langle \zeta_{20} \rangle|} = 6 \text{ gracias a la conocida de Galois.}$$

Análogamente se obtiene que  $K^{(\zeta_{11})} = F(\sqrt[3]{2}), K^{(\zeta_{21})} = F(i), K^{(\zeta_{10})} = F(w\sqrt[3]{2})$  y  $K^{(\zeta_{20})} = F(w\sqrt[3]{2})$

d) Puesto que todas las subextensiones vienen dadas por un subgrupo del grupo de Galois; de hecho, por todos aquellos elementos de  $K$  que permanecen fijos por uno de los subgrupos del grupo de Galois tenemos que buscar aquellos subgrupos cuyos generadores dejan fija a  $\sqrt[3]{2}$ . Ahora bien, como todos ellos son  $\mathbb{Q}(\sqrt[3]{2})$ -lineales por construcción, buscamos aquellos que deje fija a  $i$ . Igualmente, buscamos aquellos subgrupos que contengan a  $\mathbb{Q}(i)$ ; estos son  $K$  y  $F(i)$  puesto que  $\zeta_{11}$  y  $\zeta_{21}$  no dejan fija a  $i$ .

**Ejercicio 2.** Consideremos una raíz cúbica primitiva de la unidad  $w \in \mathbb{C}$ . Decidir razonadamente si  $\mathbb{Q}(w) = \mathbb{Q}(\frac{1}{w+1})$ .

Puesto que  $w \in \mathbb{C}$  es una raíz cúbica de la unidad, la podemos considerar de la siguiente forma:

$$w = \frac{-1 + i\sqrt{3}}{2}$$

de donde se deduce que  $\mathbb{Q}(w) = \mathbb{Q}(\sqrt[3]{2})$ . Ahora bien, puesto que  $\mathbb{Q}(\frac{1}{w+1}) \subseteq \mathbb{Q}(w)$  trivialmente por la estructura de cuerpo bastaría probar que  $\mathbb{Q}(w) \subseteq \mathbb{Q}(\frac{1}{w+1})$

$$\text{Ahora bien } \frac{1}{w+1} = \frac{1}{\frac{-1 + i\sqrt{3}}{2} + 1} = \frac{2}{-1 + i\sqrt{3}} = \frac{2(1 - i\sqrt{3})}{(-1 + i\sqrt{3})(1 - i\sqrt{3})} = \frac{2 - 2i\sqrt{3}}{4} = \frac{1 - i\sqrt{3}}{2} = \frac{1}{2} - \frac{i\sqrt{3}}{2} = -w$$

entonces  $\mathbb{Q}(\frac{1}{w+1}) = \mathbb{Q}(-w) = \mathbb{Q}(w)$  de donde se tiene la igualdad; por tanto, la respuesta es afirmativa.

**Ejercicio 3.** Sea  $g = x^3 + x^2 - 1 \in \mathbb{F}_3[x]$  y  $F$  un cuerpo de descomposición sobre  $\mathbb{F}_3$  de  $g$ .

- Describir los elementos del grupo  $\text{Aut}(F)$  y calcular todos los subcuerpos de  $F$ .
- Si  $\alpha_1, \alpha_2, \alpha_3 \in F$  son las raíces de  $g$ , decidir si  $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 \in \mathbb{F}_3$ .
- Resolver la ecuación  $x^2 + 1 = 0$  en  $F$ .

$$2+1-1=2$$

La estrategia es la siguiente, intuitivamente podemos ver que  $g$  es irreducible en  $\mathbb{F}_3[x]$  de forma que, como  $F$  es cuerpo de descomposición tendremos que  $F = \mathbb{F}_3$  de donde tenemos que  $\mathbb{F}_3 \leq F$  es una extensión de Galois por ser de cuerpos finitos.

Siguiendo ese supuesto, tendríamos que el grupo de Galois,  $\text{Aut}(F)$ , sería cíclico de orden 3 cuyo generador sería el automorfismo de Frobenius de la extensión  $\mathbb{F}_3 \leq \mathbb{F}_{27}$  dado por

$$\tau(a) = a^3 \quad \forall a \in \mathbb{F}_9$$

obteniendo así que  $\text{Aut}(F) = \{\text{id}, \tau, \tau^2\} = \{\text{id}, \tau, \tau \circ \tau\}$

a) Con todo el razonamiento anterior, sólo debemos estudiar la irreductibilidad de  $g$ , si log suerte, el razonamiento anterior nos da el resultado. Estudiemos si las raíces en  $\mathbb{F}_3 = \{0, 1, 2\}$

$$g(0) = 2 \quad g(1) = 1 \quad g(2) = 2$$

Por tanto, ha habido suerte y  $\text{Aut}(F) = \{\text{id}, \tau, \tau^2\}$ . Además, si  $a \in F$  es raíz de  $g$  tenemos que  $\mathbb{F}_3(a) \cong F$  pues  $\mathbb{F}_3 \leq \mathbb{F}_3(a)$  es Galois y  $\mathbb{F}_3(a) \leq F$ . De hecho, como  $\text{Irr}(a, \mathbb{F}_3) = g$  tenemos que  $[\mathbb{F}_3(a) : \mathbb{F}_3] = 3$  de donde  $\{1, a, a^2\}$  es una  $\mathbb{F}_3$ -base de  $F$ . Cosa añadida, también tenemos gracias al automorfismo de Frobenius que  $a^3$  y  $a^9$  son raíces de  $g$ .

Para calcular los subcuerpos usaremos la presentación de  $F$  como  $\mathbb{F}_{27}$  sobre  $\mathbb{F}_3$ . De hecho, habrá tantos subcuerpos como subgrupos del grupo de Galois en virtud de la conmutatividad de Galois.

Como  $\text{Aut}(F)$  es cíclico de orden 3, el Teorema de Lagrange nos asegura que no hay subgrupos propios pues  $\text{Div}(3) = \{1, 3\}$ .

b) Para resolver el problema usaremos las identidades de Cardano-Vietta, que nos aseguran que

$$\alpha_1 + \alpha_2 + \alpha_3 = -1 = 2 \in \mathbb{F}_3$$

$$\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3 = 0 \in \mathbb{F}_3$$

Como  $(x_1^2 + x_2^2 + x_3^2)^2 = (x_1 + x_2 + x_3)^2 + 2(x_1 x_2 + x_1 x_3 + x_2 x_3)$ , aplicando lo obtenido tenemos que  $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = -1 + 2 \cdot 0 = 1 \in \mathbb{F}_3$

c) Puesto que  $\mathbb{F}_{27}$  contiene todas las raíces del polinomio  $x^2 + x \in \mathbb{F}_3[x]$  y este polinomio se escribe como el producto de todos los polinomios irreducibles de grado divisor de 2, tenemos que una ecuación  $p=0$  con  $p \in \mathbb{F}_3[x]$  irreducible tendría solución en  $\mathbb{F}_{27}$  si y solo si  $\deg p \mid 3$ .

Vemos que  $p = x^2 + x \in \mathbb{F}_3[x]$  es irreducible, puesto que  $p(0) = 1, p(1) = 2$  y  $p(2) = 4$  tenemos que es irreducible y como  $\mathbb{F}_3$  no tiene soluciones.

**Ejercicio 4.** Decidir razonadamente sobre la veracidad de las siguientes afirmaciones:

- $\sqrt{32} - \sqrt{16} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ .
- Si  $F \leq K$  es una extensión de Galois y  $\alpha \in K$  es tal que  $\sigma(\alpha) \neq \alpha$  para todo  $\sigma \in \text{Aut}_F(K)$  distinto de la identidad, entonces  $K = F(\alpha)$ .
- Si  $f \in \mathbb{Q}[x]$  es un polinomio de grado 3 y tiene una raíz construible, entonces  $f$  es reducible.
- Sea  $F$  un cuerpo de descomposición de  $f = x^2 + x + 1 \in \mathbb{F}_5[x]$  y  $\alpha \in F$  una raíz de  $f$ . Para  $g = \text{Irr}(\alpha + 1, \mathbb{F}_5)$  se tiene que  $g(\alpha) = 3\alpha$ .

c) Si el polinomio fuese irreducible tendríamos que, si  $K$  es su cuerpo de descomposición, entonces la extensión sería de Galois y por tanto,  $\deg f$  dividiría a  $|\text{Aut}(K)|$  entonces tendríamos que  $|\text{Aut}(K)|$  no podría ser una potencia de 2, por lo que ninguna raíz sería constructible.

Por tanto, tenemos probado usando el contrapositivo que la afirmación es cierta.

a) Puesto que  $\sqrt{2}\sqrt[3]{2} = \sqrt[3]{8} = \sqrt[3]{2}$  tenemos que  $\sqrt[3]{2} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ , necesariamente  $\sqrt[3]{2} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ . Sea ahora  $\alpha = \sqrt[3]{2} - \sqrt[3]{16}$ , buscamos probar que  $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ ; juntando,  $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{16})$ . Como anteriormente nos hizo probar la multiplicación, probaremos la división  $\frac{\sqrt{2}}{\sqrt[3]{2}} = \sqrt[3]{2}$  porque  $\sqrt[3]{2} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$  lo que nos da que la afirmación es cierta.

b) Tenemos que esta afirmación es cierta, trataremos de probar, puesto que  $F$  sí es cierta, que  $K \subseteq F(\alpha)$ ; para ello, probaremos que el subgrupo del grupo de Galois de la extensión,  $\text{Aut}_{F(\alpha)}(K)$ , coincide con la identidad. En cuyo caso, tenemos la igualdad en virtud de la conexión de Galois.

Ahora bien, dicho autómorfismo nos asegura que el subgrupo asociado a  $F(\alpha)$  es

$$\text{Aut}_{F(\alpha)}(K) = \{ \sigma \in \text{Aut}(K) : \sigma(\alpha) = \alpha \}$$

puesto que  $\sigma(\alpha) = \alpha$  tiene  $\sigma \in \text{Aut}_F(K)$  dicho subgrupo es equivalente a

$$\text{Aut}_{F(\alpha)}(K) = \{ \sigma \in \text{Aut}_F(K) : \sigma(\alpha) = \alpha \}$$

Ahora bien, como por hipótesis  $\sigma(\alpha) = \alpha$  tenemos lo que queríamos.

d) Veamos una idea poco creativa de la vieja, que nos puede ayudar; si  $\beta = \alpha + i$ , buscamos hallar su polinomio irreducible. Para ello, usaremos que se llama so fraca y so cónica (suma y producto simétrico de conjugados). Como los conjugados de  $\alpha$  son  $\alpha$  y  $\alpha^5$  equivale al autómorfismo de Frobenius de la extensión de Galois dada por  $\mathbb{F}_5 \hookrightarrow F$  (esto se puede argumentar como en el ejercicio 3) tenemos que

$$(\alpha+i) + (\alpha^5+i) = (\alpha+\alpha^5)+2i$$

de lo que tenemos es reconstruir ese polinomio con Cardano-Vieta

y como  $\alpha$  y  $\alpha^5$  son las raíces de las relaciones de Cardano-Vieta nos dice que  $\alpha + \alpha^5 = -1 = 4$

$$(\alpha+i)(\alpha^5+i) = (\alpha\alpha^5 + i\alpha^5 + i\alpha + i^2) = -1 + i\alpha + i\alpha^5 - 1 = -2 + i(\alpha + \alpha^5)$$

Es de grado 2 porque la subextensión correspondiente debe tener un subgrupo del grupo de Galois que es de orden 2 por ser irreducible y trivalente.

Por otro lado, tomamos el producto de  $(\alpha+i)(\alpha^5+i)$ ;  $P = \alpha^6 + \alpha^5 + \alpha + i$ . Ahora bien, como  $i$  es raíz de  $x^2 + 1$  tenemos que, si multiplicamos por  $(i-1)$  obtenemos que  $i^3 = 1$  y por tanto  $i^2 = -1$  por lo que  $P = 1 + (\alpha + \alpha^5) + i = 1 + (-1) + i = i$ .

Veamos ahora que el polinomio  $g = x^2 - 5x + P = x^2 + 4x + 1$  es irreducible y  $\alpha + i$  es raíz simple. Como ya hemos visto en  $\mathbb{F}_5$  es irreducible y  $g(\alpha + i) = (\alpha + i)^2 + 4(\alpha + i) + 1 = \alpha^2 + 4\alpha + 1 + 4\alpha + 4 + 1 = 0$

Veamos ahora que  $g(\alpha) = 3\alpha$ ; puesto que  $g(\alpha) = \alpha^2 + 4\alpha + 1 = \alpha^2 + \alpha + 1 + 3\alpha = 3\alpha$ .