

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

- Decidir razonadamente si $\sqrt[3]{3} \in K$.
- Describir los elementos del grupo $\text{Aut}_{\mathbb{Q}}(K)$.
- Calcular todos los subcuerpos de K . Señalar cuáles son extensiones de Galois de \mathbb{Q} .
- Calcular el cardinal del grupo $\text{Aut}_{\mathbb{Q}}(K(i))$.

Antes de nada, estudiemos qué es el cuerpo de descomposición de f ; puesto que f es irreducible en $\mathbb{Q}[x]$ en virtud del criterio de Eisenstein para $p=3$ obtenemos que, al estar en característica 0, f es separable y $\mathbb{Q} \leq K$ es de Galois.

Ahora bien, sea $\omega \in \mathbb{C}$ una raíz cúbica primitiva de la unidad. Tenemos que, las raíces de son el conjunto $R = \{-\sqrt[3]{3}, -\omega\sqrt[3]{3}, -\omega^2\sqrt[3]{3}\}$ donde $\omega = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$. Por tanto, en concordancia con que f induce una extensión cónica, $K = \mathbb{Q}(\sqrt[3]{3}, \omega)$; de forma análoga a otros casos podemos deducir que $K = \mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$. Además, puesto que $\mathbb{Q}(\sqrt[3]{3})$ no contiene números complejos ($x+iy \in \mathbb{Q}(\sqrt[3]{3})[x]$ es irreducible) tenemos que, en virtud del lema de la Torre se cumple que

$$[K : \mathbb{Q}] = 6$$

Como $\text{Aut}(K)$ es un subgrupo transitivo de S_3 tenemos que, necesariamente es S_3 , lo cual implica que $\text{Aut}(f) = \langle i\sqrt{3} \rangle = 9 \leqslant 12$.

a) Puesto que $K = \mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$ tenemos que esto es falso; supongamos que fuera cierto; en ese caso, se tendría la siguiente torre de cuerpos $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{3}) \leq \mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$. De hecho, en ese caso, se tendría que $K = \mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$ puesto que $i \in \mathbb{Q}(\sqrt[3]{3})$ de donde $\mathbb{Q}(i) \leq \mathbb{Q}(i\sqrt{3})$. Trivialmente se tiene la otra inclusión.

Ahora bien, como $K = \mathbb{Q}(i, \sqrt[3]{3}, \sqrt{3})$, el lema de la Torre nos dice que

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

•) $[K : \mathbb{Q}(\sqrt[3]{3}, \sqrt{3})] = 2$ puesto que $x^2+1 \in \mathbb{Q}(\sqrt[3]{3}, \sqrt{3})[x]$ es irreducible ya que $i \notin \mathbb{Q}(\sqrt[3]{3}, \sqrt{3})$

•) Puesto que $(x^3-3)(x^2-3) \in \mathbb{Q}[x]$ tiene como raíces a $\sqrt[3]{3}$ y $\sqrt{3}$ se cumple que $[\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}] \leq 6$. De hecho, como $x^3-3 \in \mathbb{Q}[x]$ y $x^2-3 \in \mathbb{Q}[x]$ son irreducibles en $\mathbb{Q}[x]$ por el criterio de Eisenstein tenemos, en virtud del lema de la Torre

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

$$\leq [\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{3}, \sqrt{3}) : \mathbb{Q}(\sqrt[3]{3})][\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3 \cdot K$$

Por tanto, $|\text{Aut}(K)| = 12$ y es un subgrupo transitivo de S_3 cuyo cardinal es 6 !!

b) En virtud de la primera proposición de extensión y contando la paraformalia pertinente que se ha contado en otros ejercicios se obtiene que

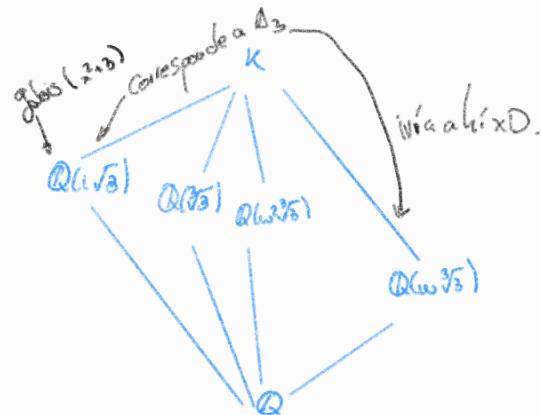
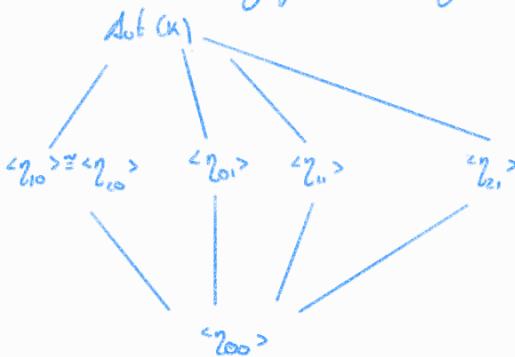
$$\text{Aut}(K) = \{ \gamma_{ju} : j=0,1,2; u=0,1 \}$$

donde $\gamma_{ju} : K \longrightarrow K$ dado por $\gamma_{ju}(\sqrt[3]{3}) = \omega^j \sqrt[3]{3}$, $j=0,1,2$ y $\gamma_{ju}(i\sqrt{3}) = (-1)^u i\sqrt{3}$, $u=0,1$.

c) Para ello, calcularemos todos los órdenes:

$$\begin{matrix} \mathbb{Z}_0 & \mathbb{Z}_{01} & \mathbb{Z}_{10} & \mathbb{Z}_{11} & \mathbb{Z}_{20} & \mathbb{Z}_{21} \\ 1 & 2 & 3 & 4 & 3 & 2 \end{matrix}$$

El retículo de subgrupos es el siguiente



A la derecha aparece el retículo de subcuerpos que se ha identificado usando la teoría de Galois obteniendo una inclusión trivial y la otra razonando por grados usando de nuevo este anti-isomorfismo.

d) Se nos pide calcular el cardinal del grupo de Galois de la extensión $\mathbb{Q} \subseteq \mathbb{K}(i)$ que es de Galois con su cuerpo de descomposición del polinomio $g = f(x^2+1)$. (siguiendo una observación del Teo 2)

Como $\mathbb{K}(i) = \mathbb{Q}(\sqrt{3}, i\sqrt{3})(i) = \mathbb{Q}(i, \sqrt{3}, i\sqrt{3})$ podemos saber si, como en el apartado a), deducir que $\mathbb{Q}(i, \sqrt{3}, i\sqrt{3}) = \mathbb{Q}(i, \sqrt{3}, \sqrt{3})$ obteniendo así que $[\mathbb{K}(i) : \mathbb{Q}] = 6$.

No obstante, este ejercicio puede hacerse con contenido del Teo 1 pues vemos que, si, $F \subseteq \mathbb{K}(i)$ es una extensión y $\mathbb{K}(i)$ es cuerpo de descomposición de $g \in F[x]$, en nuestro caso $\mathbb{Q} = F$, se tiene que

$$|\text{Aut}_F(\mathbb{K}(i))| = |\text{Aut}(\mathbb{K}(i))| \leq [\mathbb{K}(i) : \mathbb{Q}]$$

Ade más, como g es separable tenemos que se da la igualdad.

Ejercicio 2. Consideremos el número real $\alpha = \sqrt{2} + \sqrt{3}$. Decidir razonadamente si $\mathbb{Q}(\alpha) = \mathbb{Q}(\frac{1}{\alpha^2+1})$

En este ejercicio lo que se pide es probar que $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\frac{1}{\alpha^2+1})$ pues la otra inclusión es trivial.

Vemos dicha inclusión; puesto que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ puesto que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ (y con un razonamiento análogo a $\mathbb{Q}(\sqrt{3}, \sqrt{5})$). Además, $\alpha^2 = 5 + 2\sqrt{6}$ de donde $\frac{1}{\alpha^2+1} = \frac{1}{6+2\sqrt{6}} = \frac{6-2\sqrt{6}}{12} = \frac{1}{2} - \frac{\sqrt{6}}{6}$ de donde $\mathbb{Q}(\frac{1}{\alpha^2+1}) = \mathbb{Q}(\sqrt{6})$ cuyo grado sobre \mathbb{Q} es 2. Por tanto, no se da la igualdad.

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

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

Para ello, primero vamos a estudiar, como en otros ejercicios, la irreducibilidad deg; como $g(0) = 0$ tenemos que $g = (x+1)f$ donde $f \in \mathbb{F}_3[x]$ es irreducible en $\mathbb{F}_3[x]$, y a veremos por qué.

Haciendo la división obtenemos que $f = x^2 + 2x + 2$ que no tiene raíces en \mathbb{F}_3 . Sea ahora el cuerpo de descomposición de f , puesto que $g = (x+1)f$ y $g \in \mathbb{F}_3[x]$ tenemos que $F = K$. Además, como $\mathbb{F}_3 \leq K$ es de Galois por ser una extensión de cuerpos finitos y g es irreducible necesariamente $K = \mathbb{F}_q$.

Usando ahora el teorema del ejemplo sabemos que $\exists \alpha \in K$ tal que α es raíz de g ; por tanto, como $\mathbb{F}_3 \leq \mathbb{F}_3(\alpha)$ es una extensión de cuerpos finitos de Galois de donde es acanal y deducimos que $\mathbb{F}_3(\alpha) = K$. Veamos que a tiene orden multiplicativo 8; los posibles órdenes son 1, 2, 4, 8.

Recordemos que, como $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = \deg g = 2$ tenemos que β, α es una \mathbb{F}_3 -base de \mathbb{F}_q y que $\alpha^2 = a+1$:

$$\rightarrow \alpha \neq 1$$

$$\rightarrow \alpha^2 = a+1 \neq 1$$

$$\rightarrow \alpha^4 = (\alpha^2)^2 = (a+1)^2 = a^2 + 2a + 1 = a+1 + 2a+1 = 2 \neq 1$$

Por tanto, $\mathbb{F}_q^\times = \langle \alpha \rangle$.

- a) Con todo lo visto tenemos ya que, puesto que $(\mathbb{F}_3(\alpha))$ es cuerpo de descomposición de g se cumple que $\text{Aut}(\mathbb{F}_3(\alpha)) = \{ \text{id}, \tau \}$
- b) De aquí deducimos que los únicos subcuerpos son \mathbb{F}_3 y $\mathbb{F}_3(\alpha)$.
- c) Usando las relaciones de Cardano-Vieta y suponiendo, sin pérdida de generalidad, que $\alpha_1 = a$ obtenemos que

$$2\alpha_1 + \alpha_2 = 0 \iff \alpha_1 + \alpha_2 = 1 \in \mathbb{F}_3$$

Por tanto, la respuesta es afirmativa.

- d) Puesto que \mathbb{F}_q contiene todas las raíces de $x^8 - x \in \mathbb{F}_3[x]$ y este se escribe como producto de todos los polinomios irreducibles de grado divisor de 8 tenemos que tiene solución; alargabien, sea $b \in \mathbb{F}_3(\alpha)$ una raíz de $h = x^2 + 1$; en ese caso, $\mathbb{F}_3(\alpha)$ es cuerpo de descomposición de h , que es irreducible, de donde deducimos que $\mathbb{F}_3(\alpha) \cong \mathbb{F}_q$; por lo tanto, el orden multiplicativo de α es orden multiplicativo 8. Como α es raíz de h y α^2 también gracias al automorfismo de Frobenius, podemos descartar a α^3 . Probemos con α^5 y α^7 .

$$\begin{aligned} (\alpha^5)^2 + 1 &= \alpha^{10} + 1 = (\alpha^2)^5 + 1 = (\alpha+1)^2(\alpha+1)^2(\alpha+1) + 1 = (\alpha^2 + 2\alpha + 1)(\alpha^2 + 2\alpha + 1)(\alpha+1) + 1 = (\alpha+1 + 2\alpha+1)(\alpha+1+2\alpha+1) + 1 \\ &= \alpha+1 + 1 = \alpha+2 \neq 0 \end{aligned}$$

$$1 + (\alpha^7)^2 = (\alpha^5)^2(\alpha^2)^2 = (\alpha+1)(\alpha+1)^2 + 1 = (\alpha+1)(\alpha^2 + 2\alpha + 1) + 1 = (\alpha+1) \cdot 2 + 1 = 2\alpha + 2 + 1 = 2\alpha$$

Alguna cuenta falla pero es probar y probar.

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

- a) El número real $\sum_{n=1}^8 \sqrt[n]{2}$ es algebraico sobre \mathbb{Q} .
- b) Si K es un cuerpo de descomposición de un polinomio $f \in F[x]$ y $\alpha \in K$, entonces $\text{Irr}(\alpha, F)$ es un divisor de f .
- c) Dada una torre de cuerpos $F \leq E \leq K$, si $F \leq E$ y $E \leq K$ son de Galois, entonces $F \leq K$ es de Galois.
- d) Si $z \in \mathbb{C}$ tiene grado 4 sobre \mathbb{Q} , entonces z es un número construible.

Puesto que c) y d) están hechas en otro examen, no las repito pues ambas son falsas. Para c) $\mathbb{Q} \leq \mathbb{Q}(\sqrt[4]{2}) \leq \mathbb{Q}(\sqrt{2})$ y para d) $x^4 + x + 1$.

b) Puesto que, en ningún momento se dice que α sea raíz de f , buscamos un cuerpo de descomposición de un polinomio que tenga una raíz de otro polinomio. Consideremos el polinomio $f = x^2 - 2$ cuyo campo de descomposición es $\mathbb{Q}(\sqrt{2})$; sabemos que $1 + \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ y, sin embargo, su polinomio irreducible en $\mathbb{Q}[x]$ es $x^2 - 2x - 1 \in \mathbb{Q}[x]$. Claramente $x^2 - 2x - 1$ no divide a f .

a) Puesto que $\bar{\mathbb{Q}}$ es el cuerpo de todos los algebraicos sobre \mathbb{Q} tenemos que la suma de algebraicos es algebraico de grado, como $\sqrt[8]{2}$ es raíz de $x^8 - 2$ para $a = 1, \dots, 8$ tenemos que $\sum_{a=1}^8 \sqrt[8]{2}$ es algebraico sobre \mathbb{Q} .