

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

- Describe todos los elementos de $\text{Aut}(K)$.
- Comprueba que $w \in K$, con $w = -1/2 + i\sqrt{3}/2$.
- Calcula $\text{Aut}_{\mathbb{Q}(w)}(K) \cap \text{Aut}_{\mathbb{Q}(\sqrt{3})}(K)$.
- Calcula los subcuerpos de K de grado 4.

Sabes de cada, vamos a estudiar qué es K ; para ello, se ve que $f = gh$ con $g = x^4 + 1 \in \mathbb{Q}[x]$ y $h = x^2 - 3 \in \mathbb{Q}[x]$. Es claro que, tanto g como h son irreducibles en $\mathbb{Q}[x]$ pues si aplicásemos Eisenstein a h con $p=3$ y vemos que g no tiene raíces en \mathbb{Q} (las posibles son ± 1) y tenemos factores de grado 2 (el único posible es $x^2 + x + 1$ y solo es).

También es claro que, las raíces de h son $R_h = \sqrt[3]{3}, -\sqrt[3]{3}$. Para el caso de g , buscamos números complejos tales que al elevarlos a la cuarta obtenemos -1 , uno de ellos es $\sqrt[4]{1} = \sqrt{1}$, entonces otro de ellos es $-\sqrt[4]{1}$; pero, si nos damos cuenta $\sqrt[4]{1}$ es la raíz octava primitiva de la unidad, de donde deducimos, si $w = \sqrt[4]{1}$, que $R_g = \{w, w^3, w^5, w^7\}$ donde $w = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$.

Por tanto, tenemos ya que $R_f = R_h \cup R_g$ de donde deducimos que $K = \mathbb{Q}(\sqrt{3}, w)$. Tratemos de simplificar esto; vemos que $K = \mathbb{Q}(\sqrt{3}, i\sqrt{2}, \sqrt{2})$; claramente, se tiene que $K \subseteq \mathbb{Q}(\sqrt{3}, i\sqrt{2}, \sqrt{2})$. Para la otra inclusión basta ver que

$$\begin{aligned}\sqrt{2} &= \frac{4+4w^2}{4w} = \frac{1+w^2}{w} \in \mathbb{Q}(w) \\ i\sqrt{2} &= w - \frac{\sqrt{2}}{w} \in \mathbb{Q}(w)\end{aligned}$$

Por tanto, ya tenemos que $K = \mathbb{Q}(\sqrt{3}, i\sqrt{2}, \sqrt{2})$; además, con un razonamiento análogo se obtiene que $K = \mathbb{Q}(i, \sqrt{3}, \sqrt{2})$.

a) Una vez hecho este estudio, podemos ya aplicar la primera proposición de extensión; para ello, consideramos la situación del esquema y el polinomio $p = x^2 - 2 \in \mathbb{Q}[x]$ claramente irreducible cuyas raíces en K

$\mathbb{Q} \xrightarrow{i} K$ son $R = \{\sqrt{2}, -\sqrt{2}\}$. Dicha proposición nos asegura que $E(x, i)$ está en biyección con R de la siguiente manera:

$$\begin{aligned}\eta_j: \mathbb{Q}(\sqrt{2}) &\longrightarrow K \quad \text{para } j=0,1 \\ \sqrt{2} &\longmapsto (-1)^j \sqrt{2}\end{aligned}$$

Pasamos ahora, usando un tema de la primera proposición de extensión a extender, de nuevo, cada una de las anteriores según el esquema; vemos entonces que $p = x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$ es irreducible; supongamos

$\mathbb{Q}(\sqrt{2}) \xrightarrow{j} K$ que no lo fuera, en ese caso $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ de donde $\exists a, b \in \mathbb{Q}$ tales que $\sqrt{3} = a + b\sqrt{2}$ de donde $\sqrt{2} = \frac{3 - a^2 - 2b^2}{2ab} \in \mathbb{Q}$ lo cual

ya vemos que no era cierto. Por tanto, como $R = \{\sqrt{3}, -\sqrt{3}\}$ son las raíces de p en K obtenemos de forma análoga que; los $E(x, j)$ son

$$\begin{aligned}\eta_{jn}: \mathbb{Q}(\sqrt{2}, \sqrt{3}) &\longrightarrow K \\ \sqrt{2} &\longmapsto (-1)^j \sqrt{2} \quad j=0,1 \\ \sqrt{3} &\longmapsto (-1)^n \sqrt{3} \quad n=0,1\end{aligned}$$

De forma análoga se obtiene que $\text{Aut}(u) = \{\gamma_{jkl} : j=0,1; u=0,1; l=0,1\}$ con

$$\begin{aligned}\gamma_{jkl} : u &\longrightarrow u \\ \sqrt{2} &\longrightarrow (-i)^j \sqrt{2} \\ \sqrt{3} &\longrightarrow (-i)^k \sqrt{3} \\ i &\longrightarrow (-i)^l i\end{aligned}$$

b) Despues del trabajo previo realizado, puesto que $K = \mathbb{Q}(i, \sqrt{3}, \sqrt{2})$ esto es final

c) Puesto que $w = \frac{1}{2} + \frac{i\sqrt{3}}{2}$ buscamos aquellos elementos de $\text{Aut}(u)$ que dejan fijo a $i\sqrt{3}$ y a $\sqrt{3}$, gracias a que

$$\gamma_{jkl}(\sqrt{3}) = (-i)^k \sqrt{3} \text{ obtenemos que } \text{Aut}_{\mathbb{Q}(\sqrt{3})}(u) = \{\gamma_{jkl} : j=0,1; l=0,1\}$$

$$\gamma_{jkl}(i\sqrt{3}) = \gamma_{jkl}(i)\gamma_{jkl}(\sqrt{3}) = (-i)^l i (-i)^k \sqrt{3} \text{ obtenemos que } \text{Aut}_{\mathbb{Q}(w)}(u) = \{\gamma_{jkl} : j=0,1; u=l\}$$

Por tanto tenemos que $\text{Aut}_{\mathbb{Q}(w)}(u) \cap \text{Aut}_{\mathbb{Q}(\sqrt{3})}(u) = \{\gamma_{j00} : j=0,1\}$

d) Si $E \subseteq K$ de grado 4 entonces tenemos que $[E : \mathbb{Q}] = 4$ de donde, usando la correspondencia de Galois para $\mathbb{Q}(E)$ sabemos que

$$|\text{Aut}(u)| = [u : \mathbb{Q}] = [u : E] \cdot [E : \mathbb{Q}] = |\text{Aut}_E(u)| \cdot 4 \Leftrightarrow |\text{Aut}_E(u)| = 2$$

Gracias a que el grado de E es divisible por 2.

Es decir, buscamos aquellos subcampos de K cuyo subgrupo dentro del grupo de Galois de $\mathbb{Q} \subseteq u$ sea de orden 2. Los órdenes de los elementos son:

$$\begin{matrix} \gamma_{000} & \gamma_{001} & \gamma_{010} & \gamma_{011} & \gamma_{100} & \gamma_{101} & \gamma_{110} & \gamma_{111} \\ 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{matrix}$$

por tanto, dichos subgrupos son todos esos subgrupos de orden 2. Usando la correspondencia de Galois sabemos que:

•) Puesto que γ_{001} deja fijo a $\sqrt{3}$ y a $\sqrt{2}$ tenemos que $(\mathbb{Q}(\sqrt{3}, \sqrt{2}))^{\gamma_{001}} = K^{(\gamma_{001})}$; ademas, como

$$[u : \mathbb{Q}] = [u : K^{(\gamma_{001})}] \cdot [K^{(\gamma_{001})} : \mathbb{Q}] \wedge [u : K^{(\gamma_{001})}] = 1 \cdot \gamma_{001} > 1 > 2$$

tenemos que $[K^{(\gamma_{001})} : \mathbb{Q}] = 4$ de donde, como $[\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}] = 4$ (ya lo vimos) obtenemos la igualdad.

De manera análoga se obtiene que $K^{(\gamma_{010})} = \mathbb{Q}(i, \sqrt{2})$, $K^{(\gamma_{011})} = \mathbb{Q}(\sqrt{2})$, $K^{(\gamma_{100})} = \mathbb{Q}(\sqrt{3}, i)$...

Ejercicio 2. Sea $f = x^3 + 3x^2 - x + 1 \in \mathbb{Q}[x]$ con α, β raíces reales de f . Calcular $[\mathbb{Q}(\alpha + \beta) : \mathbb{Q}]$.

Para este ejercicio, puesto que, como las únicas raíces posibles de f son $-1, \pm \sqrt{2}$ como polinomio en $\mathbb{R}[x]$, vemos que f es irreducible en $\mathbb{Q}[x]$ pues $f(-1) = 4$ y $f(\pm \sqrt{2}) = 4$. Sea además, γ la raíz restante de f , las relaciones de Cardano-Vieta nos dice que $\alpha + \beta + \gamma = \frac{-3}{1} = -3$ de donde se deduce que

$$\alpha + \beta = -3 - \gamma$$

Este acierto es útil pues decuivierta que $\mathbb{Q}(\alpha+\beta) \cong \mathbb{Q}(\beta) = \mathbb{Q}(\gamma)$; por tanto, bastará con comprobar

$$[\mathbb{Q}(\gamma):\mathbb{Q}]$$

No obstante, como $\text{Irr}(\gamma, \mathbb{Q}) = f$ tenemos fácilmente que $[\mathbb{Q}(\gamma):\mathbb{Q}] = \deg f = 3$.

Ejercicio 3. Sea F un cuerpo con $\text{car}(F) = 2$, $a \in F$ con $F = \mathbb{F}_2(a)$ y $a^6 = a^5 + 1$.

- Calcular $\text{Aut}(F)$.
- Encontrar un elemento b y expresarlo en función de a para que $|\mathbb{F}_2(b)| = 8$.

Antes de nada, debemos saber cuál es $\mathbb{F}_2(a)$; para ello, puesto que $\mathbb{F}_2 \leq \mathbb{F}_2(a)$ es de grado 2 para ser una extensión de cuerpos finitos tenemos que $\mathbb{F}_2(a)$ es el cuerpo de descomposición de $f = x^6+x^5+1$ por ser a raíz de f .

Si conseguimos probar que f es irreducible tendríamos que $[\mathbb{F}_2(a):\mathbb{F}_2] = 6$, que $\mathbb{F}_2(a) \cong \mathbb{F}_{64}$ y que $\{1, a, a^2, a^3, a^4, a^5\}$ es una \mathbb{F}_2 -base de $\mathbb{F}_2(a)$. Por último, tendríamos que $\text{Aut}(\mathbb{F}_2(a))$ es el círculo de orden 6 generado por el automorfismo de Frobenius

$$\varepsilon(a) = a^2 \quad \text{y en } \mathbb{F}_2(a). \quad \{1, \text{id}, \varepsilon, \varepsilon^2 = \varepsilon_4, \varepsilon^3 = \varepsilon_8, \varepsilon^4, \varepsilon^5\}$$

- Por tanto, cosa lo visto antes, sólo debemos probar que f es irreducible en $\mathbb{F}_2[x]$; puesto que $f(0) = f(1) = 1$, f no tiene raíces en \mathbb{F}_2 ; veamos que no tiene factores de grado 2 ni de grado 3. Las posibilidades son $\{x^3+x+1, x^3+x^2+1, x^3+x^2+x\}$; se deja al lector realizar las divisiones pertinentes. Como f es irreducible en $\mathbb{F}_2[x]$; en particular, $f \in \text{Irr}(a, \mathbb{F}_2)$ de donde obtenemos lo mencionado al principio.

- Puesto que $|\mathbb{F}_2(b)| = 8$, sabemos que, de esta forma $\langle b \rangle = (\mathbb{F}_2(b))^*$ y además, por la información del enunciado tenemos que $\mathbb{F}_2(b) \leq \mathbb{F}_{64}$ de donde $(\mathbb{F}_2(b))^* \leq (\mathbb{F}_{64})^* = \langle a \rangle$. Entonces, buscamos un elemento en $\mathbb{F}_2(a)^*$ cuyo orden multiplicativo sea 7; por ejemplo a^9 ; otras posibilidades son, puesto que dicho elemento será raíz de x^3+x+1 o de x^3+x^2+1 , gracias al automorfismo de Frobenius a^{18} ó a^{36} . También, puesto que $\text{gcd}(x^3+x+1, x^3+x^2+1) = 1$, no tendrán raíces comunes y a^{27}, a^{54} y a^{45} son otras posibilidades.

Este ejercicio estaría bien si probáramos que $\text{ord}(a) = 63$; pero esto se dejó al lector, basta con ver que $a \neq 1, a^3 \neq 1, a^9 \neq 1, a^{27} \neq 1$ usando que $\{1, a, a^2, a^3, a^4, a^5\}$ es una \mathbb{F}_2 -base de $\mathbb{F}_2(a)$ y que $a^6 = a^5 + 1$.