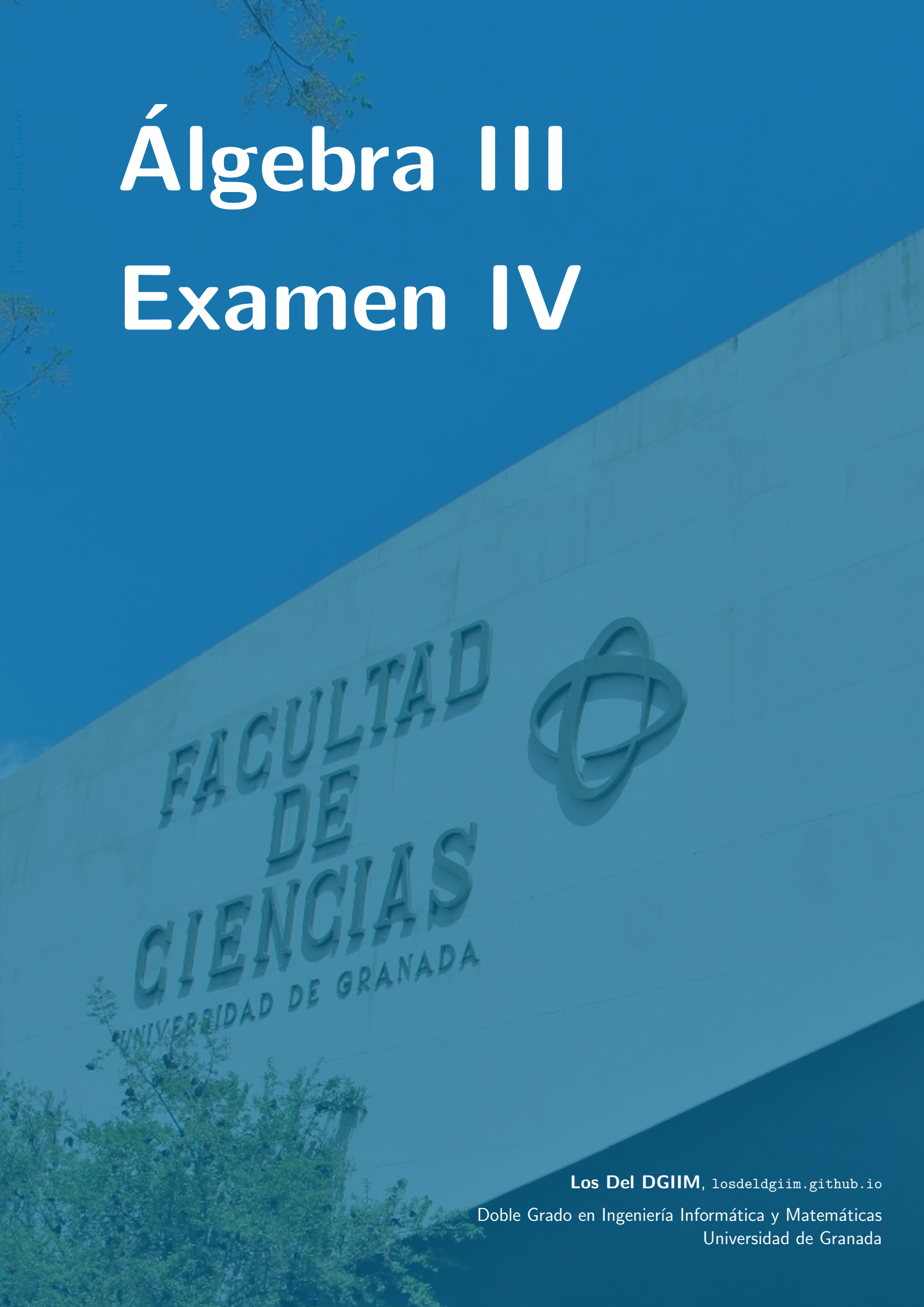
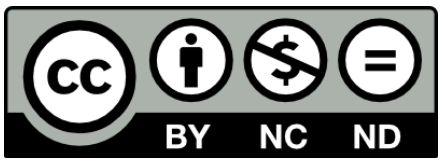
Álgebra III
Examen IV



Los Del DGIIM, losdeldgiim.github.io

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada



Álgebra III
Examen IV

Los Del DGIIM, `losdeldgiim.github.io`

Granada, 2025

Asignatura Álgebra III.

Curso Académico 2023/24.

Grado Doble Grado en Ingeniería Informática y Matemáticas.

Grupo Único.

Profesor José Gómez Torrecillas.

Descripción Examen Ordinario de Incidencias.

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

a) Describe todos los elementos de $\mathrm{Aut}(K)$.

b) Comprueba que $w \in K$, con $w = {}^{-1}/_{2} + i{}^{\sqrt{3}}/_{2}$.

c) Calcula $\mathrm{Aut}_{\mathbb{Q}(w)}(K) \cap \mathrm{Aut}_{\mathbb{Q}(\sqrt{3})}(K)$.

d) Calcula los subcuerpos de K de grado 4.

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

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

a) Calcular $\mathrm{Aut}(F)$.

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

Solución.

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

a) Describe todos los elementos de $\mathrm{Aut}(K)$.

Las raíces de f son $\pm\sqrt{3}, \pm\sqrt{i}, \pm i\sqrt{i}$, donde vemos que:

$$\sqrt{i} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

Así, vemos que $K = \mathbb{Q}\left(\sqrt{3}, \sqrt{i}\right) \leqslant \mathbb{Q}\left(\sqrt{3}, \sqrt{2}, i\right)$, pero esta última inclusión es una igualdad, pues:

$$i = \left(\sqrt{i}\right)^2 \in \mathbb{Q}\left(\sqrt{3}, \sqrt{i}\right) \qquad \sqrt{2} = \frac{\sqrt{i}}{1/2 + i/2} \in \mathbb{Q}\left(\sqrt{3}, \sqrt{i}\right)$$

Tenemos así que $K = \mathbb{Q}\left(\sqrt{3}, \sqrt{2}, i\right)$ y que $\mathbb{Q} \leqslant K$ es de Galois. Si calculamos ahora $[K : \mathbb{Q}]$ por el Lema de la Torre:

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

Vemos que:

- $\left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] = 2$, ya que $x^2 - 3$ es irreducible en $\mathbb{Q}[x]$ por Eisenstein.
- $\left[K : \mathbb{Q}\left(\sqrt{3}, \sqrt{2}\right)\right] = 2$, ya que $x^2 + 1$ es irreducible en $\mathbb{Q}\left(\sqrt{3}, \sqrt{2}\right)[x]$ por ser sus raíces complejas.
- $\left[\mathbb{Q}\left(\sqrt{3}, \sqrt{2}\right) : \mathbb{Q}(\sqrt{3})\right] \leqslant 2$ ya que $x^2 - 2$ tiene por raíz $\sqrt{2}$. Si fuera $\left[\mathbb{Q}\left(\sqrt{3}, \sqrt{2}\right) : \mathbb{Q}\left(\sqrt{3}\right)\right] = 1$ tendríamos entonces que $\sqrt{2} \in \mathbb{Q}\left(\sqrt{3}\right)$, por lo que existirían $a, b \in \mathbb{Q}$ de forma que:

$$\sqrt{2} = a + b\sqrt{3} \implies 2 = a^2 + 2ab\sqrt{3} + 3b^2 \iff \begin{cases} 2 = a^2 + 3b^2 \\ 0 = 2ab \end{cases}$$

De ser $b = 0$ tendríamos que $\sqrt{2} \in \mathbb{Q}$, pero $x^2 - 2$ es irreducible en $\mathbb{Q}[x]$ por Eisenstein, por lo que tiene que ser $a = 0$, de donde:

$$2 = 3b^2 \iff b = \sqrt{\frac{2}{3}}$$

Pero vemos que $\sqrt{2/3} \notin \mathbb{Q}$, ya que el polinomio $3x^2 - 2$ es irreducible en $\mathbb{Q}[x]$ por ser de grado 2 y no tener raíces en $\mathbb{Q}$, ya que sus únicas posibiles raíces son:

$$\pm 1, \pm 2, \pm\frac{1}{3}, \pm\frac{2}{3}$$

y ninguna lo es. Hemos llegado a una contradicción, que viene de suponer que $\left[\mathbb{Q}\left(\sqrt{3}, \sqrt{2}\right) : \mathbb{Q}\left(\sqrt{3}\right)\right] = 1$, por lo que ha de ser 2.

En definitiva, tenemos que x^2-2 es irreducible en $\mathbb{Q}\left(\sqrt{3}\right)[x]$, de donde tenemos:

$$[K:\mathbb{Q}] = 2^3 = 8$$

Para calcular los elementos de $\mathrm{Aut}(K)$ lo que haremos será aplicar varias veces la Proposición de extensión. Comenzamos calculando los homomorfismos $\eta : \mathbb{Q}\left(\sqrt{3}\right) \to K$:

$$\begin{array}{ccc} \mathbb{Q} & \hookrightarrow & K \\ & \searrow & \\ & & \mathbb{Q}(\sqrt{3}) \end{array}$$

Como $x^2-3 \in \mathbb{Q}[x]$ es irreducible y tiene sus dos raíces $(\pm\sqrt{3})$ en K tenemos que hay dos automorfismos, η_j con $j \in \{0,1\}$, que vienen determinados por:

$$\sqrt{3} \overset{\eta_j}{\longmapsto} (-1)^j\sqrt{3}$$

Cada uno de estos homomorfismos puede extenderse a varios homomorfismos $\mathbb{Q}\left(\sqrt{3},\sqrt{2}\right) \to K$:

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{3}) & \xrightarrow{\eta_j} & K \\ & \searrow & \\ & & \mathbb{Q}(\sqrt{3},\sqrt{2}) \end{array}$$

Ya que $x^2-2 \in \mathbb{Q}\left(\sqrt{3}\right)[x]$ es irreducible y tiene sus dos raíces en K, tenemos que cada η_j se extiende a dos homomorfismos $\eta_{j,k}$ con $k \in \{0,1\}$, que vienen determinados por:

$$\sqrt{3} \overset{\eta_{j,k}}{\longmapsto} (-1)^j\sqrt{3}$$
$$\sqrt{2} \overset{\eta_{j,k}}{\longmapsto} (-1)^k\sqrt{2}$$

Cada uno puede extenderse a su vez a homomorfismos $K \to K$:

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{3},\sqrt{2}) & \xrightarrow{\eta_{j,k}} & K \\ & \searrow & \\ & & K \end{array}$$

Ya que $x^2+1 \in \mathbb{Q}\left(\sqrt{3},\sqrt{2}\right)[x]$ es irreducible y tiene sus dos raíces en K, obteniendo para cada $j,k \in \{0,1\}\times\{0,1\}$ los automorfismos $\eta_{j,k,l}$ con $l \in \{0,1\}$ determinados por:

$$\sqrt{3} \overset{\eta_{j,k,l}}{\longmapsto} (-1)^j\sqrt{3}$$
$$\sqrt{2} \overset{\eta_{j,k,l}}{\longmapsto} (-1)^k\sqrt{2}$$
$$i \overset{\eta_{j,k,l}}{\longmapsto} (-1)^l i$$

Así, tenemos que:

$$\mathrm{Aut}(K) = \{\eta_{j,k,l} : j,k,l \in \{0,1\}\}$$

b) Comprueba que $w \in K$, con $w = {}^{-1}/_2 + i{}^{\sqrt{3}}/_2$.
Como $K = \mathbb{Q}\left(\sqrt{3}, \sqrt{2}, i\right)$ es claro que $w \in K$.

c) Calcula $\mathrm{Aut}_{\mathbb{Q}(w)}(K) \cap \mathrm{Aut}_{\mathbb{Q}(\sqrt{3})}(K)$.
Calculamos primero $\mathrm{Aut}_{\mathbb{Q}(w)}(K)$ y $\mathrm{Aut}_{\mathbb{Q}(\sqrt{3})}(K)$:

- Para el primero, vemos que:

$$|\mathrm{Aut}_{\mathbb{Q}(w)}(K)| = (\mathrm{Aut}_{\mathbb{Q}(w)}(K) : \{id\}) = [K : \mathbb{Q}(w)] = \frac{[K:\mathbb{Q}]}{[\mathbb{Q}(w):\mathbb{Q}]} = \frac{8}{2} = 4$$

  Puesto que $\mathrm{Irr}(w, \mathbb{Q}) = \phi_3 = x^2 + x + 1$. Así como que los automorfismos $\eta_{000}, \eta_{010}, \eta_{101}, \eta_{111}$ dejan fijo el elemento w, por lo que:

$$\{\eta_{000}, \eta_{010}, \eta_{101}, \eta_{111}\} \subseteq \mathrm{Aut}_{\mathbb{Q}(w)}(K)$$

  Pero como $|\mathrm{Aut}_{\mathbb{Q}(w)}(K)| = 4$ estos son todos.
- Y para el segundo de forma análoga se tiene que:

$$\left|\mathrm{Aut}_{\mathbb{Q}\left(\sqrt{3}\right)}(K)\right| = \left(\mathrm{Aut}_{\mathbb{Q}\left(\sqrt{3}\right)}(K) : \{id\}\right) = \left[K : \mathbb{Q}\left(\sqrt{3}\right)\right] = \frac{8}{2} = 4$$

  Vemos de la misma forma que:

$$\mathrm{Aut}_{\mathbb{Q}\left(\sqrt{3}\right)}(K) = \{\eta_{000}, \eta_{001}, \eta_{010}, \eta_{011}\}$$

En definitiva, tenemos que:

$$\mathrm{Aut}_{\mathbb{Q}(w)}(K) \cap \mathrm{Aut}_{\mathbb{Q}(\sqrt{3})}(K) = \{\eta_{000}, \eta_{010}\}$$

d) Calcula los subcuerpos de K de grado 4.

Viendo la definición de $\eta_{j,k,l}$ para $j,k,l \in \{0,1\}$ observamos que todos estos elementos son de orden multiplicativo 2. Sea $L \leqslant K$ con $[L:\mathbb{Q}] = 4$, tenemos entonces que $(G = \mathrm{Aut}(K))$:

$$4 = [L:\mathbb{Q}] = [G : \mathrm{Aut}_L(K)] = \frac{|G|}{|\mathrm{Aut}_L(K)|} \quad \Longrightarrow \quad |\mathrm{Aut}_L(K)| = 2$$

Es decir, que cada subcuerpo de grado 4 da un subgrupo de $\mathrm{Aut}(K)$ de orden 2 y sabemos por la conexión de Galois que al revés también sucede esto, por lo que buscamos calcular los subgrupos de $\mathrm{Aut}(K)$ de orden 2, que sabemos que se corresponden con los generados por los elementos de orden 2, obteniendo así 7 subgrupos de orden 2:

$$\langle\eta_{001}\rangle, \quad \langle\eta_{010}\rangle, \quad \langle\eta_{011}\rangle, \quad \langle\eta_{100}\rangle, \quad \langle\eta_{101}\rangle, \quad \langle\eta_{110}\rangle, \quad \langle\eta_{111}\rangle$$

Detallaremos la obtención del subcuerpo asociado al primer subgrupo y el resto son análogos.

- Para $\langle \eta_{001} \rangle$ observamos que $\mathbb{Q}\left(\sqrt{3}, \sqrt{2}\right) \leqslant K^{\langle \eta_{001} \rangle}$, pues $\sqrt{3}$ y $\sqrt{2}$ quedan fijos por este automorfismo. Como tenemos que:

$$\left[K^{\langle \eta_{001} \rangle} : \mathbb{Q}\right] = \frac{|G|}{|\langle \eta_{001} \rangle|} = \frac{8}{2} = 4$$

  Y anteriormente vimos que:

$$\left[\mathbb{Q}\left(\sqrt{3}, \sqrt{2}\right) : \mathbb{Q}\right] = 4$$

  Tenemos por tanto que $\mathbb{Q}\left(\sqrt{3}, \sqrt{2}\right) = K^{\langle \eta_{001} \rangle}$, por lo que $\mathbb{Q}\left(\sqrt{3}, \sqrt{2}\right)$ es un subcuerpo de K de grado 4.
- $K^{\langle \eta_{010} \rangle} = \mathbb{Q}\left(\sqrt{3}, i\right)$.
- $K^{\langle \eta_{011} \rangle} = \mathbb{Q}\left(\sqrt{3}, i\sqrt{2}\right)$.
- $K^{\langle \eta_{100} \rangle} = \mathbb{Q}\left(i, \sqrt{2}\right)$.
- $K^{\langle \eta_{101} \rangle} = \mathbb{Q}\left(i\sqrt{3}, \sqrt{2}\right)$.
- $K^{\langle \eta_{110} \rangle} = \mathbb{Q}\left(\sqrt{6}, i\right)$.
- $K^{\langle \eta_{111} \rangle} = \mathbb{Q}\left(i\sqrt{2}, \sqrt{6}\right)$.

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

Sea γ la tercera raíz de f en un cuerpo de descomposición, en vista de los coeficientes de f y las relaciones de Cardano-Vieta, tenemos que:

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

De donde deducimos que $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha + \beta)$. Observemos que f es irreducible, pues es de grado 3 y no tiene raíces en $\mathbb{Q}$, ya que las únicas posibles son ± 1 y ninguna de ellas es raíz:

$$f(1) = 4, \quad f(-1) = 4$$

Tenemos así que $f = \mathrm{Irr}(\gamma, \mathbb{Q})$, por lo que:

$$3 = [\mathbb{Q}(\gamma) : \mathbb{Q}] = [\mathbb{Q}(\alpha + \beta) : \mathbb{Q}]$$

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

a) Calcular $\mathrm{Aut}(F)$.

Sea $f = x^6 + x^5 + 1 \in \mathbb{F}_2[x]$, estudiemos la irreducibilidad de f:

- f no tiene raíces en $\mathbb{F}_2[x]$, pues $f(0) = 1 = f(1)$, de donde no tiene factores de grado 1 ni factores de grado 5.
- El único polinomio irreducible de grado 2 en $\mathbb{F}_2[x]$ es x^2+x+1, si dividimos f entre él vemos que:

$$x^6 + x^5 + 1 = (x^2 + x + 1)(x^4 + x^2 + 1) + x + 1$$

  Por lo que f no tiene factores de grado 2, luego tampoco de grado 4.

- f puede tener factores de grado 3, y los únicos polinomios irreducibles de grado 3 en $\mathbb{F}_2[x]$ son:

$$x^3 + x^2 + 1, \quad x^3 + x + 1$$

Vemos que:

$$x^6 + x^5 + 1 = (x^3 + x^2 + 1)(x^3 + 1) + x^2$$

Por lo que $x^3 + x^2 + 1$ no es un factor de f, la única posibilidad restante para que f tenga factores de grado 3 es que sea igual a:

$$(x^3 + x + 1)^2 = x^6 + x^2 + 1$$

pero no es el caso, por lo que f no tiene factores de grado 3.

Concluimos que f es irreducible. Tenemos así que $f = \mathrm{Irr}(a, \mathbb{F}_2)$, con lo que:

$$[\mathbb{F}_2(a) : \mathbb{F}_2] = 6 \quad \Longrightarrow \quad \mathbb{F}_2(a) = \mathbb{F}_{64}$$

Sabemos que $\mathrm{Aut}(F)$ es un grupo cíclico de orden 6, generado por el automorfismos de Frobenius $\tau_2 : \mathbb{F}_2(a) \to \mathbb{F}_2(a)$ determinado por $\tau_2(a) = a^2$, con lo que el grupo es:

$$\mathrm{Aut}(F) = \{\tau_1, \tau_2, \tau_4, \tau_8, \tau_{16}, \tau_{32}\}$$

donde τ_j viene dado por $\tau_j(a) = a^j$, para $j \in \{1, 2, 4, 8, 16, 32\}$.

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

Como $[\mathbb{F}_2(a) : \mathbb{F}_2] = 6$, tenemos que $\{1, a, a^2, a^3, a^4, a^5\}$ es una $\mathbb{F}_2-$base de $\mathbb{F}_2(a)$, $\mathbb{F}_2(a)^\times$ es un grupo de orden $63 = 3^2 \cdot 7$, por lo que a puede tener órden $3, 7, 9, 21$ o 63:

- $a^3 \neq 1 \Longrightarrow O(a) \neq 3$.
- $a^7 = a(a^5 + 1) = a^6 + a = a^5 + 1 + a \neq 1 \Longrightarrow O(a) \neq 7$.
- $a^9 = a^2a^7 = a^2(a^5 + a + 1) = a^7 + a^3 + a^2 = a(a^5 + 1) + a^3 + a^2 = a^5 + 1 + a + a^3 + a^2 \neq 1 \Longrightarrow O(a) \neq 9$.
- $a^{21} = a^3(a^9)^2 = a^3(a^5 + a^3 + a^2 + a + 1)^2 = a^3(a^{10} + a^6 + a^4 + a^2 + 1) = a^3(a^4(a^5 + 1) + a^5 + 1 + a^4 + a^2 + 1) = a^3(a + a^3 + 1) = a^4 + a^6 + a^3 = a^4 + a^5 + 1 + a^3 \neq 1 \Longrightarrow O(a) \neq 21$.

Vemos así que $O(a) = 63$. Buscamos un elemento $b \in \mathbb{F}_2(a)$ de forma que $\mathbb{F}_2(b) = \mathbb{F}_8$. Sabemos que $\mathbb{F}_8$ es cuerpo de descomposición de un polinomio de grado 3 sobre $\mathbb{F}_2$, y sabemos que los elementos de $\mathbb{F}_{64}$ son las raíces de $x^{64} - x$, cuyos factores son polinomios irreducibles cuyo grado divide a 6, por lo que tanto las raíces de $x^3 + x + 1$ como de $x^3 + x^2 + 1$ están en $\mathbb{F}_{64}$. Sea $b \in \mathbb{F}_2(a)$ la solución a cualquiera de estas ecuaciones, obtendríamos así que $\mathbb{F}_2(b)$ es cuerpo de descomposición de dicho polinomio, con lo que $\mathbb{F}_8 = \mathbb{F}_2(b)$. Observamos que $\mathbb{F}_2(b)^\times$ es un grupo cíclico de orden 7, por lo que b tiene que tener orden multiplicativo 7. Observamos que elementos de esta forma en $\mathbb{F}_2(a)$ hay 6 (todos y cada uno de los elementos del grupo cíclico de orden 7, menos 1), 3 corresponden a las soluciones de $x^3 + x + 1$ y otros 3 a las de $x^3 + x^2 + 1$.

De esta forma, al tomar cualquier elemento $b \in \mathbb{F}_2(a)$ de orden multiplicativo 3 obtenemos que $\mathbb{F}_2(b) = \mathbb{F}_8$.

Como a tiene orden 63, tomando:

$$b = a^9$$

obtenemos que $O(b) = 7$, por lo que por el razonamiento que hemos mostrado tenemos que $\mathbb{F}_2(b) = \mathbb{F}_8$.