Álgebra III
Examen III

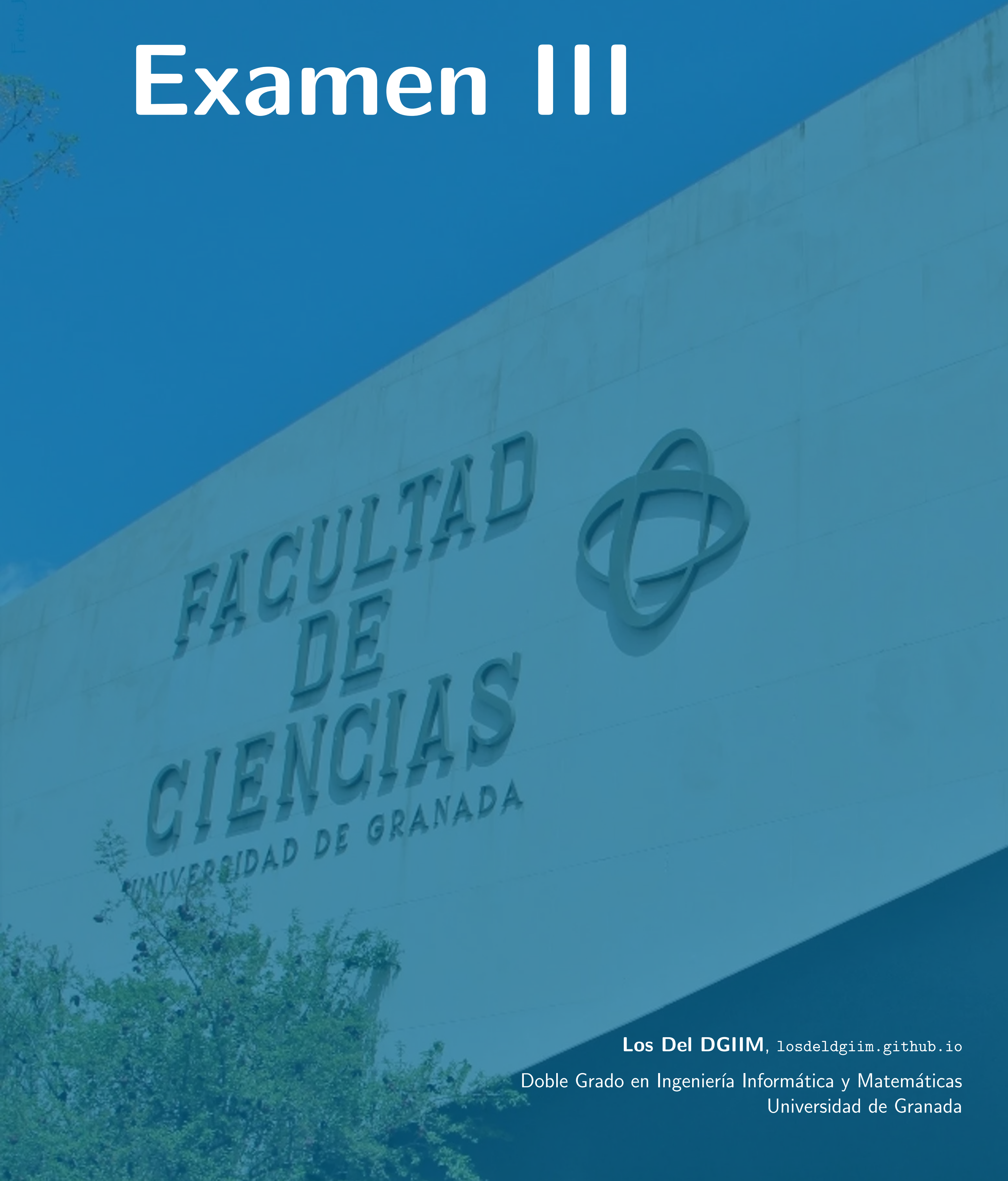

Foto: José Juan Castro

Los Del DGIIM, `losdeldgiim.github.io`

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Álgebra III
Examen III

Los Del DGIIM, `losdeldgiim.github.io`

Granada, 2026

Asignatura Álgebra III.

Curso Académico 2023/24.

Grado Doble Grado en Ingeniería Informática y Matemáticas.

Grupo Único.

Profesor José Gómez Torrecillas.

Descripción Examen Ordinario.

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

a) Comprobar que $i + \sqrt{3} \in K$.

b) Calcular $[K : \mathbb{Q}]$.

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

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

a) Describir $\mathrm{Aut}(F)$ y evaluarlos en a^2.

b) Calcular el cardinal de $\mathbb{F}_3(a^2)$.

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

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

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

Solución.

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

a) Comprobar que $i+\sqrt{3} \in K$.

Las raíces de f son $\pm\sqrt{3}, w^k\sqrt[3]{2}$ para $k=0,1,2$ y donde w es una raíz cúbica primitiva de la unidad. Podemos tomar por ejemplo:

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

Por lo que $K = \mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}\right)$. Vemos que:

$$w = \frac{w\sqrt[3]{2}}{\sqrt[3]{2}} \in \mathbb{Q}\left(\sqrt[3]{2}, w\right)$$

Por lo que $K = \mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}, w\right)$. Más aún, vemos que:

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

Ya que:

$\subseteq$) $w = \frac{-1}{2} + i\frac{\sqrt{3}}{2} \in \mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}, i\right)$.

$\supseteq$) $i = \frac{2}{\sqrt{3}}\left(w+\frac{1}{2}\right) \in \mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}, w\right)$.

Con esta descripción de K es claro que:

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

b) Calcular $[K:\mathbb{Q}]$. Por el Lema de la Torre tenemos que:

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

donde:

- $\left[K:\mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}\right)\right] = 2$ ya que $x^2+1 \in \mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}\right)[x]$ es un polinomio irreducible por ser sus dos raíces complejas.
- Comprobamos ahora que $\left[\mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}\right):\mathbb{Q}\right] = 6$, ya que el Lema de la Torre nos permite escribir:

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

donde:

  - $\left[\mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}\right):\mathbb{Q}\left(\sqrt{3}\right)\right] \leqslant 3$ ya que $\sqrt[3]{2}$ es raíz de x^3-2.
  - $\left[\mathbb{Q}\left(\sqrt{3}\right):\mathbb{Q}\right] = 2$, ya que $\mathrm{Irr}\left(\sqrt{3}, \mathbb{Q}\right) = x^2-3$, que es irreducible por Eisenstein para $p=3$.

    Deducimos por tanto que $\left[\mathbb{Q}\left(\sqrt{3}, \sqrt[3]{2}\right):\mathbb{Q}\right] \leqslant 6$ y es múltiplo de 2.

Aplicando el Lema de la Torre en sentido opuesto y usando que x^3-2 es irreducible en $\mathbb{Q}[x]$ para $p=2$ por Eisenstein vemos que $\left[\mathbb{Q}\left(\sqrt{3},\sqrt[3]{2}\right):\mathbb{Q}\right]$ es múltiplo de 3 también, por lo que no queda más salida que:

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

Así, tenemos que:

$$[K:\mathbb{Q}]=\left[K:\mathbb{Q}\left(\sqrt{3},\sqrt[3]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{3},\sqrt[3]{2}\right):\mathbb{Q}\right]=2\cdot 6=12$$

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

Vemos que f es irreducible en $\mathbb{Q}[x]$ por ser de grado 3 y no tener raíces en $\mathbb{Q}$, ya que las únicas posibles raíces de f en $\mathbb{Q}$ son ± 1 y ninguna de ellas es raíz:

$$f(0)=1,\qquad f(1)=-1$$

Sea K el cuerpo de descomposición de f, como $\mathrm{car}(K)=0$ vemos que $\mathbb{Q}\leqslant K$ es de Galois y si consideramos $G=\mathrm{Aut}_F(K)$ el grupo de Galois de f vemos que G es un “subgrupo” de S_3 que actúa de forma transitiva sobre las raíces de f (por ser f irreducible), por lo que $G\cong S_3$ ó $G\cong A_3$. Si calculamos:

$$\mathrm{Disc}(f)=-4p^3-27q^2=4\cdot 3^3-27=4\cdot 27-27=3\cdot 27=81$$

Vemos que $81=3^4$, de donde $\Delta(f)=\sqrt{81}=3^9=9\in\mathbb{Q}$. Así, vemos que “$G<A_3$”, por lo que $|G|=3$. Así, tenemos que:

$$[K:F]=|G|=3$$

Como α es una raíz de f tenemos claramente que $\mathbb{Q}\leqslant\mathbb{Q}(\alpha)\leqslant K$, y como $[K:F]=3$ tenemos por el Lema de la Torre que bien $\mathbb{Q}(\alpha)=\mathbb{Q}$ o bien $\mathbb{Q}(\alpha)=K$. Como $f=\mathrm{Irr}(\alpha,\mathbb{Q})$ tenemos por tanto que $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$, por lo que la única posibilidad es $K=\mathbb{Q}(\alpha)$.

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

a) Describir $\mathrm{Aut}(F)$ y evaluarlos en a^2.

Sea $f=x^4+x-1\in\mathbb{F}_3[x]$, vemos que f es irreducible en $\mathbb{F}_3[x]$, pues:

- No tiene raíces en $\mathbb{F}_3$:

$$f(0)=-1,\quad f(1)=1,\quad f(2)=2$$

Por lo que no tiene factores de grado 1 ni de grado 3.

- Podría tener factores de grado 2. Para ello, calculamos primero los polinomios mónicos irreducibles de grado 2 en $\mathbb{F}_3[x]$. Sabemos que:

  $$x^{3^2} - x = x^9 - x \in \mathbb{F}_3[x]$$

  factoriza como todos y cada uno de los polinomios mónicos irreducibles de grados 1 y 2, de grado 1 hay 3, por lo que de grado 2 hay $\frac{9-3}{2} = 3$. Buscando entre todos los polinomios de grado 2 que parecen no tener raíces, encontramos que estos son:

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

  Veamos si alguno de estos divide a f:

  $$\begin{aligned} x^4 + x - 1 &= (x^2 + 1)(x^2 + 2) + x \\ x^4 + x - 1 &= (x^2 + x + 2)(x^2 + 2x + 2) + x + 1 \end{aligned}$$

  Vemos en este último caso que tampoco es divisible entre $x^2 + 2x + 2$, por lo que f no tiene factores de grado 2.

Como f es irreducible, vemos que $\text{Irr}(a, \mathbb{F}_3) = f$, por lo que:

$$[\mathbb{F}_3(a) : \mathbb{F}_3] = 4$$

y tenemos por tanto que $\{1, a, a^2, a^3\}$ es una $\mathbb{F}_3-$base de F. En vista de esto último y de la extensión $\mathbb{F}_3 \leqslant \mathbb{F}_3(a)$, vemos que $\text{Aut}(F)$ es un grupo cíclico de orden 4, que estará generado por el automorfismo de Frobenius de la extensión $\mathbb{F}_3 \leqslant \mathbb{F}_3(a)$, que es $\tau : \mathbb{F}_3(a) \to \mathbb{F}_3(a)$ determinado por:

$$\tau(a) = a^3$$

Elevando τ a 2 y 3 obtenemos todos los automorfismos. En definitiva, tenemos que:

$$\text{Aut}(F) = \{\tau_1, \tau_3, \tau_9, \tau_{27}\}$$

donde τ_j viene dado por $\tau_j(a) = a^j$, para $j \in \{1, 3, 9, 27\}$. Si evaluamos cada uno de ellos en a^2 teniendo en cuenta que:

$$a^4 + a - 1 = 0 \iff a^4 = 1 - a$$

Vemos que:

$$\begin{aligned}
\tau_1(a^2) &= a^2 \\
\tau_3(a^2) &= \left(a^2\right)^3 = a^6 = a^2(1 - a) = a^2 - a^3 \\
\tau_9(a^2) &= \left(a^2\right)^9 = a^{18} = a^2\left(a^4\right)^4 = a^2(1 - a)^4 = a^2(1 - a - a^3 + a^4) \\
&= a^2 - a^3 - a^5 + a^6 = a^2 - a^3 - a(1 - a) + a^2(1 - a) \\
&= a^2 - a^3 - a + a^2 + a^2 - a^3 = a^3 + 2a \\
\tau_{27}(a^2) &= \left(a^2\right)^{27} = \left(a^{18}\right)^3 = \left(a^3 + 2a\right)^3 = a^9 + 2a^7 + a^5 + 2a^3 \\
&= a(1 - a)^2 + 2a^3(1 - a) + a(1 - a) + 2a^3 \\
&= a \cancel{- 2a^2} + \cancel{a^3} + \cancel{2a^3} - 2a^4 + a \cancel{- a^2} + 2a^3 \\
&= 2a + 2a^3 - 2a^4 = 2a + 2a^3 - 2(1 - a) = 2a + 2a^3 - 2 + 2a \\
&= -2 + a + 2a^3
\end{aligned}$$

b) Calcular el cardinal de $\mathbb{F}_3(a^2)$.

Como $a^2 \in \mathbb{F}_3(a)$ vemos claramente que $\mathbb{F}_3 \leqslant \mathbb{F}_3(a^2) \leqslant \mathbb{F}_3(a)$ con todas las extensiones de Galois por ser cuerpos finitos, por lo que esta subextensión debe corresponderse por la conexión de Galois con un subgrupo de $\mathrm{Aut}(F)$, concretamente con $\mathrm{Aut}_{\mathbb{F}_3(a^2)}(\mathbb{F}_3(a))$. Sin embargo, en el apartado anterior hemos visto que ningún elemento de $\mathrm{Aut}(\mathbb{F}_3(a))$ distinto de $\tau_1 = id$ deja fijo a^2, por lo que tiene que ser:

$$\mathrm{Aut}_{\mathbb{F}_3(a^2)}(\mathbb{F}_3(a)) = \{\tau_1\}$$

de donde $\mathbb{F}_3(a^2) = \mathbb{F}_3(a)$, y tenemos por tanto que:

$$|\mathbb{F}_3(a^2)| = |\mathbb{F}_3(a)| \overset{(*)}{=} 3^4 = 81$$

donde en $(*)$ usamos que $[\mathbb{F}_3(a) : \mathbb{F}_3] = 4$.

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

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

Es falsa, si consideramos $\mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt{2}\right) \leqslant \mathbb{Q}\left(\sqrt[4]{2}\right)$, tenemos que $\mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt{2}\right)$ es de Galois por ser $\mathbb{Q}\left(\sqrt{2}\right)$ el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio x^2-2, que $\mathbb{Q}\left(\sqrt{2}\right) \leqslant \mathbb{Q}\left(\sqrt[4]{2}\right)$ es de Galois por ser $\mathbb{Q}\left(\sqrt[4]{2}\right)$ cuerpo de descomposición de $x^2-\sqrt{2}$ sobre $\mathbb{Q}\left(\sqrt{2}\right)$ y $\mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt[4]{2}\right)$ no es de Galois, pues el polinomo $x^4-2 \in \mathbb{Q}[x]$ es irreducible por Eisenstein para $p=2$ y sus raíces son $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$, vemos que algunas están en $\mathbb{Q}\left(\sqrt[4]{2}\right)$ y otras no, con lo que $\mathbb{Q} \leqslant \mathbb{Q}\left(\sqrt[4]{2}\right)$ no puede ser una extensión de Galois, al no ser si quiera una extensión normal.

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

Es falsa, pensamos en buscar un polinomio de grado 4 irreducible en $\mathbb{Q}[x]$ para así obtener un elemento de grado 4 como una raíz suya. Para ello, como hemos de buscar un polinomio de grado 4 que sea irreducible, lo escogemos bien pensando en el criterio de reducción para $p=2$, en $\mathbb{F}_2[x]$, sabemos que el polinomio $x^4+x^2+1 = \left(x^2+x+1\right)^2$ no es irreducible y que los polinomios:

$$x^4+x+1, \qquad x^4+x^3+1$$

sí que lo son. Tomamos pues $f = x^4+x+1 \in \mathbb{Q}[x]$, que sabemos que es irreducible por el criterio de reducción para $p=2$. Buscamos calcular su grupo de Galois. Como f es irreducible sabemos que su grupo de Galois será isomorfo a C_4, V, D_4, A_4 o S_4. Para ello, en vista de que f es una cuártica reducida, buscamos su resolvente cúbica, que aplicando la fórmula vista en teoría, sabemos que es (para x^4+px^2+qx+r):

$$g = x^3+2px^2+(p^2-4r)x-q^2 = x^3-4x-1$$

Sabemos ya calcular el discriminante de f:

$$\mathrm{Disc}(f) = \mathrm{Disc}(g) = -4p^3-27q^3 = 4\cdot 4^3-27 = 4^4-27 = 256-27 = 229$$

Como 229 es primo, vemos que $\sqrt{229} \notin \mathbb{Q}$, por lo que G (el grupo de Galois de f) no puede ser isomorfo a A_4 ni a V. Vemos que g es irreducible en $\mathbb{Q}[x]$, por no tener raíces en $\mathbb{Q}$ y que su grupo de Galois es S_3 por ser $\Delta(g) \notin \mathbb{Q}$. Así, sea E el cuerpo de descomposición de g y K el de f, vemos que $\mathbb{Q} \leqslant E$ es de Galois, por lo que aplicando un Teorema de teoría vemos que:

$$\frac{\operatorname{Aut}_F(K)}{\operatorname{Aut}_E(K)} \cong \operatorname{Aut}_F(E) \cong S_3$$

Con $|S_3| = 6$, múltiplo de 3, por lo que $|\operatorname{Aut}_F(K)|$ es múltiplo de 3, por lo que la única opción es $G \cong S_4$. Así, vemos que:

$$[K : F] = |G| = |S_4| = 24 = 2^3 \cdot 3$$

Tenemos la torre:

$$\mathbb{Q} \leqslant \mathbb{Q}(\alpha) \leqslant K$$

Sea L un cuerpo de forma que $\mathbb{Q}(\alpha) \leqslant L$ con $\mathbb{Q} \leqslant L$ de Galois, tenemos entonces que la extensión es normal y α es una raíz de $f = \operatorname{Irr}(\alpha, \mathbb{Q})$, por lo que todas las raíces de f deben estar en L, de donde tiene que ser entonces:

$$\mathbb{Q}(\alpha) \leqslant K \leqslant L$$

Así, tenemos que $[L : \mathbb{Q}]$ es múltiplo de 3 por serlo $[K : \mathbb{Q}]$, de donde $[L : \mathbb{Q}]$ no puede ser una potencia de 2, luego α no es constructible.