Álgebra III

Examen I

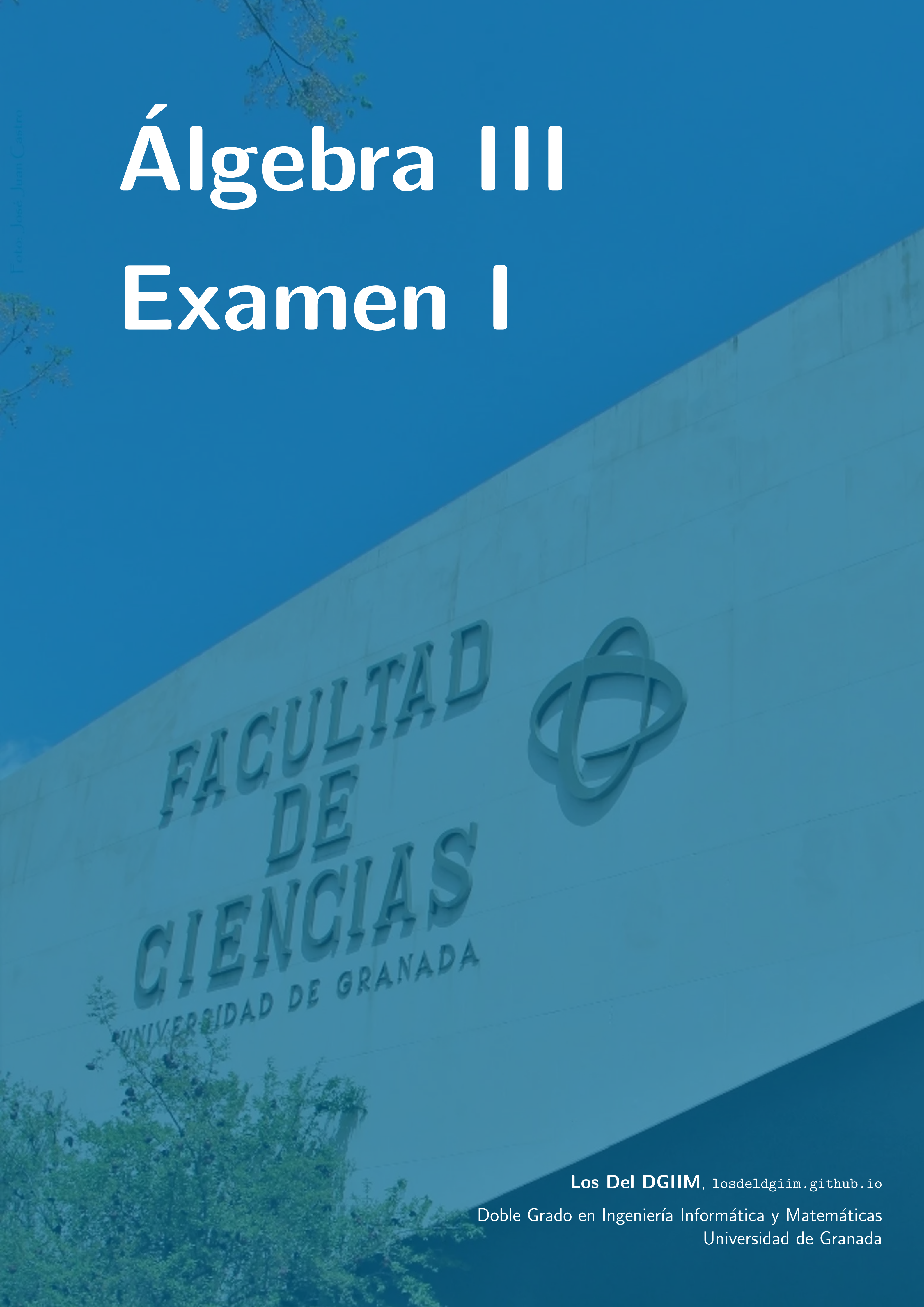

Foto: José Juan Castro

Los Del DGIIM, `losdeldgiim.github.io`

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Álgebra III
Examen I

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán

Granada, 2025

Asignatura Álgebra III.

Curso Académico 2025/26.

Grado Doble Grado en Ingeniería Informática y Matemáticas.

Grupo Único.

Profesor José Gómez Torrecillas.

Descripción Segundo examen sorpresa.

Fecha 20 de noviembre de 2025.

Duración Una hora.

Ejercicio 1. Calcular $\phi_9 \in \mathbb{Q}[x]$.

Solución.
Sabemos que:
$$x^9 - 1 = \prod_{d \in Div(9)} \phi_d = \phi_1\phi_3\phi_9$$
Por lo que:
$$\phi_9 = \frac{x^9 - 1}{\phi_1\phi_3}$$
Tenemos que $\phi_1 = x - 1$, y para ϕ_3 tenemos que las raíces cúbicas de la unidad son:
$$\{1, w, w^2\}$$
con w y w^2 las raíces cúbicas primitivas de la unidad. $1, w, w^2$ son todas las raíces dle polinomio $x^3 - 1$, y queremos quitar 1 como raíz, por lo que dividimos entre $x - 1$, obteniendo:
$$x^3 - 1 = (x - 1)(x^2 + x + 1)$$
Con w y w^2 las raíces de $x^2 + x + 1$, por lo que este polinomio es ϕ^3. Así:
$$\phi_9 = \frac{x^9 - 1}{\phi_1\phi_3} = \frac{x^9 - 1}{(x - 1)(x^2 + x + 1)} = \frac{x^9 - 1}{x^3 - 1}$$
Y vemos que:
$$x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$$
de donde deducimos que $\phi_9 = x^6 + x^3 + 1$.

Ejercicio 2. Sea $\zeta \in \mathbb{C}$ una raíz primitiva novena de la unidad, calcular todos los subcuerpos de $\mathbb{Q}(\zeta)$.

Solución.
Sabemos que $\mathbb{Q} \leqslant \mathbb{Q}(\zeta)$ es de Galois, que $\mathrm{Aut}(\mathbb{Q}(\zeta)) \cong \mathcal{U}(\mathbb{Z}_9)$ y que:
$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(9) = 6$$
Además, vimos que los elementos de $\mathrm{Aut}(\mathbb{Q}(\zeta))$ son:
$$\mathrm{Aut}(\mathbb{Q}(\zeta)) = \{\tau_1, \tau_2, \tau_4, \tau_5, \tau_7, \tau_8\}$$
y que vienen determinados por:
$$\zeta \xmapsto{\tau_j} \zeta^j \qquad \forall j \in \mathcal{U}(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$$
Si calculamos el orden de τ_2 vemos que:
$$\zeta \xmapsto{\tau_2} \zeta^2 \xmapsto{\tau_2} \zeta^4 \xmapsto{\tau_2} \zeta^8$$
por lo que el orden de τ_2 no es ni 1 ni 2 ni 3, luego ha de ser un elemento de orden 6, con lo que $\langle\tau_2\rangle = \mathrm{Aut}(\mathbb{Q}(\zeta))$. Una vez conocemos el generador del grupo es sencillo calcular los órdenes del resto de elementos:

- Para los elementos de orden 2 (sabemos que solo hay uno, puesto que el grupo es cíclico y por tanto solo puede haber un subgrupo de orden 2, que están en correspondencia biunívoca con los elementos de orden 2), vemos que τ_2^3 es un elemento de orden 2, y como:
$$\zeta \xmapsto{\tau_2^3} \zeta^8$$
vemos por tanto que $\tau_2^3 = \tau_8$
- Para los elementos de orden 3 (sabemos que hay 2, y que una vez obtenido uno el otro es su cuadrado) tenemos que τ_2^2 será un elemento de orden 3, y como:
$$\zeta \xmapsto{\tau_2^2} \zeta^4$$
tenemos por tanto que $\tau_2^2 = \tau_4$, y el otro elemento de orden 3 será τ_4^2, que verifica:
$$\zeta \xmapsto{\tau_4} \zeta^4 \xmapsto{\tau_4} \zeta^{16} = \zeta^7$$
- Sabemos que el orden de τ_1 es uno, y el resto de elementos que no hemos considerado serán de orden 6.

Tenemos así que los órdenes de los elementos son:

τ_1	τ_2	τ_4	τ_5	τ_7	τ_8
1	6	3	6	3	2

Y podemos ya por tanto determinar todos los subgrupos de $\operatorname{Aut}(\mathbb{Q}(\zeta))$:

$$\begin{tikzcd}
 & Aut(\mathbb{Q}(\zeta)) = \langle \tau_2 \rangle = \langle \tau_5 \rangle \arrow[dl, dash] \arrow[dr, dash] & \\
\langle \tau_4 \rangle = \langle \tau_7 \rangle \arrow[dr, dash] & & \langle \tau_8 \rangle \arrow[dl, dash] \\
 & \langle \tau_1 \rangle &
\end{tikzcd}$$

Para calcular todos los subcuerpos de $\mathbb{Q}(\zeta)$ lo que hacemos es buscar las subextensiones de $\mathbb{Q} \leqslant \mathbb{Q}(\zeta)$ que son correspondientes mediante la conexión de Galois a los subgrupos $\langle \tau_4 \rangle$ y $\langle \tau_8 \rangle$ de $\operatorname{Aut}(\mathbb{Q}(\zeta))$. Para ello, una opción es buscar los elementos que dejan fijos τ_4 y τ_8:

- Para la subextensión asociada a $\langle \tau_4 \rangle$, como $|\langle \tau_4 \rangle| = 3$ tenemos por tanto que:
$$(\operatorname{Aut}(\mathbb{Q}(\zeta)) : \langle \tau_4 \rangle) = 2$$
y por la conexión de Galois:
$$2 = (\operatorname{Aut}(\mathbb{Q}(\zeta)) : \langle \tau_4 \rangle) = [K^{\langle \tau_4 \rangle} : \mathbb{Q}]$$

Por lo que basta buscar una subextensión de $\mathbb{Q} \leqslant K^{\langle \tau_4 \rangle}$ con grado 2 sobre $\mathbb{Q}$.

Observemos que si ζ es una raíz novena primitiva de la unidad tenemos entones que ζ^3 es una raíz cúbica de la unidad, que ha de ser primitiva, pues $\zeta^3 \neq 1$. De esta forma, vemos que ζ^3 es raíz del polinomio irreducible:

$$\phi_3 = x^2 + x + 1$$

de donde $[\mathbb{Q}(\zeta^3) : \mathbb{Q}] = 2$. Si aplicamos ahora τ_4 a ζ_3 vemos que:

$$\zeta^3 \xmapsto{\tau_4} \zeta^{12} = \zeta^3$$

de donde $\mathbb{Q} \leqslant \mathbb{Q}(\zeta^3) \leqslant K^{\langle \tau_4 \rangle}$, y viendo el grado de $\mathbb{Q}(\zeta^3)$ la única posibilidad es $\mathbb{Q}(\zeta^3) = K^{\langle \tau_4 \rangle}$.

- Para la subextensión asociada a $\langle \tau_8 \rangle$, como $|\langle \tau_8 \rangle| = 2$ tenemos que:

$$[K^{\langle \tau_8 \rangle} : \mathbb{Q}] = (\mathrm{Aut}(\mathbb{Q}(\zeta)) : \langle \tau_8 \rangle) = 3$$

Por lo que basta buscar una subextensión de $\mathbb{Q} \leqslant K^{\langle \tau_8 \rangle}$ con grado 3 sobre $\mathbb{Q}$.

Opción 1. Observemos que:

$$\zeta^9 = 1 \quad \Longrightarrow \quad \zeta^8 = \zeta^{-1}$$

Si calculamos $\tau_8(\zeta^8)$ vemos que:

$$\zeta^8 \xmapsto{\tau_8} \zeta^{64} = \zeta$$

y recordemos que:

$$\zeta \xmapsto{\tau_8} \zeta$$

por lo que vemos que el elemento $\zeta + \zeta^8$ queda fijo por τ_8:

$$\zeta + \zeta^8 \xmapsto{\tau_8} \zeta^8 + \zeta$$

Así, tenemos que:

$$\mathbb{Q} \leqslant \mathbb{Q}(\zeta + \zeta^8) \leqslant K^{\langle \tau_8 \rangle}$$

Como $[K^{\langle \tau_8 \rangle} : \mathbb{Q}] = 3$, será $[\mathbb{Q}(\zeta + \zeta^8) : \mathbb{Q}] \in \{1, 3\}$, de donde bien:

$$\mathbb{Q}(\zeta + \zeta^8) = \mathbb{Q} \quad \text{ó} \quad \mathbb{Q}(\zeta + \zeta^8) = K^{\langle \tau_8 \rangle}$$

Por reducción al absurdo, supuesto que $\mathbb{Q}(\zeta + \zeta^8) = \mathbb{Q}$, tendremos entonces que $\zeta + \zeta^8 \in \mathbb{Q}$. En este caso, usando el ejercicio anterior vimos que $\phi_9 = x^6 + x^3 + 1$, de donde:

$$\zeta^6 = -1 - \zeta^3$$

Usando esta relación vemos que:

$$\mathbb{Q} \ni \zeta + \zeta^8 = \zeta + \zeta^2 \zeta^6 = \zeta + \zeta^2(-1 - \zeta^3) = \zeta - \zeta^2 - \zeta^5$$

Pero como $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$ tenemos que el conjunto $\{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$ son $\mathbb{Q}-$linealmente independientes, por lo que no puede ser $\zeta - \zeta^2 - \zeta^5 \in \mathbb{Q}$, hemos llegado a una contradicción, de donde teníamos que:

$$K^{\langle \tau_8 \rangle} = \mathbb{Q}(\zeta + \zeta^8)$$

Opción 2. Como $[\mathbb{Q}(\zeta):\mathbb{Q}] = 6$, tenemos que una $\mathbb{Q}-$base de $\mathbb{Q}(\zeta)$ es:

$$\{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$$

Así, buscamos las condiciones que ha de cumplir cualquier elemento de $\mathbb{Q}(\zeta)$ para quedar fijo por τ_8. De esta forma, sean $a, b, c, d, e, f \in \mathbb{Q}$, calculamos:

$$\begin{aligned} a + b\zeta + c\zeta^2 + d\zeta^3 + e\zeta^4 + f\zeta^5 &\xmapsto{\tau_8} a + b\zeta^8 + c\zeta^{16} + d\zeta^{24} + e\zeta^{32} + f\zeta^{40} \\ &= a + b\zeta^8 + c\zeta^7 + d\zeta^6 + e\zeta^5 + f\zeta^4 \end{aligned}$$

Si imponemos que el elemento sea igual a su imagen, buscamos igualar término a término usando que las potencias de ζ hasta 5 son una $\mathbb{Q}-$base. Sin embargo, vemos que nos aparecen potencias de ζ mayores que 5. Conseguiremos reducirlas si recordamos el ejercicio anterior, pues sabemos que ζ es raíz de ϕ_9, con lo que:

$$\zeta^6 + \zeta^3 + 1 = 0 \quad \Longrightarrow \quad \zeta^6 = -1 - \zeta^3$$

así, tenemos que:

$$\begin{aligned} &a + b\zeta + c\zeta^2 + d\zeta^3 + e\zeta^4 + f\zeta^5 \\ &= a + b\zeta^8 + c\zeta^{16} + d\zeta^{24} + e\zeta^{32} + f\zeta^{40} \\ &= a + b\zeta^8 + c\zeta^7 + d\zeta^6 + e\zeta^5 + f\zeta^4 \\ &= a + b\zeta^2(-1-\zeta^3) + c\zeta(-1-\zeta^3) + d(-1-\zeta^3) + e\zeta^5 + f\zeta^4 \\ &= (a-d) + \zeta(-c) + \zeta^2(-b) + \zeta^3(-d) + \zeta^4(-c+f) + \zeta^5(-b+e) \end{aligned}$$

Y si usamos que el conjunto anterior era una base, podemos igualar coeficiente a coeficiente, obteniendo las relaciones:

$$\left.\begin{array}{l} a = a - d \\ b = -c \\ c = -b \\ d = -d \\ e = -c + f \\ f = -b + e \end{array}\right\} \quad \Longleftrightarrow \quad \left\{\begin{array}{l} b = -c \\ d = 0 \\ e = -c + f \\ f = -b + e \end{array}\right.$$

Si probamos a tomar $a = 0 = d$, $b = 1$, $c = -1$ nos queda:

$$\left\{\begin{array}{l} e = 1 + f \\ f = -1 + e \end{array}\right.$$

por lo que una elección es tomar $f = 0$ y $e = 1$. Obtenemos por tanto el elemento:

$$\zeta - \zeta^2 + \zeta^4$$

que ya sabemos que queda fijo por τ_8, pero que comprobamos para ver que no nos hayamos equivocado en ninguna cuenta:

$$\begin{aligned} \zeta - \zeta^2 + \zeta^4 &\xmapsto{\tau_8} \zeta^8 - \zeta^{16} + \zeta^{32} \\ &= \zeta^8 - \zeta^7 + \zeta^5 \\ &= \zeta^2(-1-\zeta^3) - \zeta(-1-\zeta^3) + \zeta^5 \\ &= -\zeta^2 \cancel{-\zeta^5} + \zeta + \zeta^4 \cancel{+\zeta^5} \end{aligned}$$

Efectivamente, tenemos así que:

$$\mathbb{Q} \leqslant \mathbb{Q}(\zeta - \zeta^2 + \zeta^4) \leqslant K^{\langle \tau_8 \rangle}$$

Con $[K^{\langle \tau_8 \rangle} : \mathbb{Q}] = 3$, por lo que tenemos:

$$\mathbb{Q} = \mathbb{Q}(\zeta - \zeta^2 + \zeta^4) \quad \text{ó} \quad K^{\langle \tau_8 \rangle} = \mathbb{Q}(\zeta - \zeta^2 + \zeta^4)$$

Por reducción al absurdo, suponemos que $\mathbb{Q}(\zeta - \zeta^2 + \zeta^4) = \mathbb{Q}$, con lo que tenemos que:

$$\zeta - \zeta^2 + \zeta^4 \in \mathbb{Q}$$

Pero teníamos que $\{\zeta, \zeta^2, \zeta^4\}$ eran $\mathbb{Q}-$linealmente independientes, por lo que hemos llegado a una contradicción, luego tenemos que:

$$K^{\langle \tau_8 \rangle} = \mathbb{Q}(\zeta - \zeta^2 + \zeta^4)$$

Hemos obtenido así todos los subcuerpos de $\mathbb{Q}(\zeta)$, obteniendo: