Entrega Grupo 3

Íñigo Alemany Sánchez, Alberto Almagro Sánchez,
Juan Carlos Llamas Núñez, Enrique Rey Gisbert, Pablo Torre Piñana

1. *Sea $u := \sqrt{2+\sqrt{2+\sqrt{2}}}$. Demostrar que $\mathbb{Q}(u)|\mathbb{Q}$ es una extensión de Galois y calcular el grupo de Galois $G(\mathbb{Q}(u) : \mathbb{Q})$.*

Un polinomio anulador de u es $P(\mathtt{t}) = \left(\left(\mathtt{t}^2-2\right)^2-2\right)^2-2 = \mathtt{t}^8-8\mathtt{t}^6+20\mathtt{t}^4-16\mathtt{t}^2+2$, que es mónico y además irreducible en $\mathbb{Z}[\mathtt{t}]$ por el Criterio de Eisenstein con el primo 2, lo que es equivalente a su irreducibilidad en $\mathbb{Q}[\mathtt{t}]$ por el Lema de Gauss. Por tanto, se tiene que P es el polinomio mínimo de u sobre $\mathbb{Q}$.

Además, si $\delta_1,\delta_2,\delta_3 \in \{-1,1\}$, tenemos que $\delta_1\sqrt{2+\delta_2\sqrt{2+\delta_3\sqrt{2}}}$ es también raíz de P para cualquier combinación de los δ_i, ya que $(\delta_i)^2=1$. Por tanto, para ver que la extensión $\mathbb{Q}(u)|\mathbb{Q}$ es de Galois, debemos probar que las 8 raíces se pueden escribir en función de u. Nos centraremos únicamente en aquellas tales que $\delta_1=1$, ya que las otras se pueden obtener multiplicando la expresión resultante por -1.

Comenzamos hallando las expresiones de $\sqrt{2}$, $r := \sqrt{2+\sqrt{2}}$ y $s := \sqrt{2-\sqrt{2}}$, que nos serán útiles más adelante:

$$r = u^2-2$$
$$\sqrt{2} = r^2-2 = u^4-4u^2+2$$
$$s = \frac{\sqrt{2}}{r} = \frac{u^4-4u^2+2}{u^2-2} \overset{(*)}{=} \frac{u^8-8u^6+21u^4-20u^2+4}{u^2-2} = u^6-6u^4+9u^2-2$$

En $(*)$ hemos hecho uso de que u es raíz de P, es decir, $-2 = u^8-8u^6+20u^4-16u^2$. Para aplicar la igualdad hemos sumado y restado 2 en el numerador y sustituido el -2.

Con esto, podemos calcular el resto de raíces positivas de P, que denotaremos por:

$$v := \sqrt{2-\sqrt{2+\sqrt{2}}} \qquad w := \sqrt{2+\sqrt{2-\sqrt{2}}} \qquad x := \sqrt{2-\sqrt{2-\sqrt{2}}}$$

Entonces, la expresión de v será:

$$v = \frac{s}{u} = \frac{u^6-6u^4+9u^2-2}{u}$$

Podemos calcular w teniendo en cuenta que $w = \sqrt{2+s}$, por lo que, como $u>0$, se tiene:

$$w = \sqrt{2+s} = \sqrt{2+(u^6-6u^4+9u^2-2)} = \sqrt{u^6-6u^4+9u^2} = \left|u^3-3u\right| = u\left|u^2-3\right|$$

Como $\sqrt{2} > 1$, tenemos que $r = \sqrt{2+\sqrt{2}} > \sqrt{2} > 1$, por lo que $u^2 = 2 + r > 3$, y por tanto:

$$w = u\left|u^2 - 3\right| = u\left(u^2 - 3\right) = u^3 - 3u$$

Finalmente, podemos obtener x a partir de la expresión de w:

$$x = \frac{r}{w} = \frac{u^2 - 2}{u^3 - 3u}$$

Puesto que hemos podido escribir todas las raíces positivas en función de u, concluimos que $v, w, x \in \mathbb{Q}(u)$, por lo que $\mathbb{Q}(u)$ es un cuerpo de descomposición de P, y por tanto la extensión $\mathbb{Q}(u)|\mathbb{Q}$ es de Galois.

Pasamos ahora a calcular el grupo de Galois $G(\mathbb{Q}(u) : \mathbb{Q})$. Sea f el $\mathbb{Q}$-automorfismo de $\mathbb{Q}(u)$ tal que $f(u) = -w = -u^3 + 3u$. Veamos que el orden de f es 8, por lo que $G(\mathbb{Q}(u) : \mathbb{Q})$ será cíclico de orden 8, es decir, isomorfo a $\mathbb{Z}_8$. Para ello, calculamos:

$$\begin{aligned}
f(w) &= f\left(u^3 - 3u\right) = f(u)^3 - 3f(u) = -w^3 + 3w = v \\
f(v) &= f\left(\frac{w^2 - 2}{u}\right) = \frac{f(w^2 - 2)}{f(u)} = \frac{f(w)^2 - 2}{-w} = \frac{v^2 - 2}{-w} = \frac{\sqrt{2+\sqrt{2}}}{\sqrt{2+\sqrt{2-\sqrt{2}}}} = x \\
f(x) &= f\left(\frac{u^2 - 2}{w}\right) = \frac{f(u)^2 - 2}{f(w)} = \frac{w^2 - 2}{v} = \frac{\sqrt{2-\sqrt{2}}}{\sqrt{2-\sqrt{2+\sqrt{2}}}} = u
\end{aligned}$$

donde la única comprobación que debemos hacer es que efectivamente $v = -w^3 + 3w$:

$$v = -w^3 + 3w = w(3 - w^2) = \left(\sqrt{2+\sqrt{2-\sqrt{2}}}\right)\left(1 - \sqrt{2-\sqrt{2}}\right) > 0$$

Elevando ambos lados al cuadrado (tanto v como $-w^3 + 3w$ son positivos, por lo que mantenemos la equivalencia) obtenemos que:

$$\begin{aligned}
v^2 = 2 - \sqrt{2+\sqrt{2}} &= \left(2 + \sqrt{2-\sqrt{2}}\right)\left(3 - \sqrt{2} - 2\sqrt{2-\sqrt{2}}\right) = \\
&= 2 - \sqrt{2-\sqrt{2}} - \sqrt{2}\sqrt{2-\sqrt{2}}
\end{aligned}$$

Restando 2 en cada lado, multiplicando por -1 y simplificando:

$$\sqrt{2+\sqrt{2}} = \sqrt{2-\sqrt{2}} + \sqrt{2}\sqrt{2-\sqrt{2}} = \sqrt{2-\sqrt{2}}\left(1 + \sqrt{2}\right)$$

Finalmente, dividiendo entre $\sqrt{2-\sqrt{2}}$ llegamos a que:

$$\frac{\sqrt{2+\sqrt{2}}}{\sqrt{2-\sqrt{2}}} = \frac{\sqrt{2+\sqrt{2}}}{\sqrt{2-\sqrt{2}}}\frac{\sqrt{2+\sqrt{2}}}{\sqrt{2+\sqrt{2}}} = \frac{2+\sqrt{2}}{\sqrt{2}} = 1 + \sqrt{2}$$

lo cual es cierto, y por tanto $-w^3 + 3w = v$.

Con esto, y teniendo en cuenta que $f(-k) = -f(k)$ para $k = u, v, w, x$ se comprueba que f tiene orden 8 puesto que hemos probado que:

$$u \xrightarrow{f} -w \xrightarrow{f} -v \xrightarrow{f} -x \xrightarrow{f} -u \xrightarrow{f} w \xrightarrow{f} v \xrightarrow{f} x \xrightarrow{f} u$$

2. *Sea $\mathbb{Q}_f \subset \mathbb{C}$ el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $f(\mathtt{t}) := \mathtt{t}^8 - 2$.*
(i) *Calcular el número de subextensiones de grado 8 de $\mathbb{Q}_f|\mathbb{Q}$.*
(ii) *¿Es diedral el grupo de Galois $G(\mathbb{Q}_f : \mathbb{Q})$?*
(iii) *Encontrar un conjunto finito de generadores de una subextensión $F|\mathbb{Q}$ de $\mathbb{Q}_f|\mathbb{Q}$ tal que el grupo de Galois $G(\mathbb{Q}_f : F)$ sea cíclico de orden 8.*

Para obtener el cuerpo de descomposición del polinomio f sobre $\mathbb{Q}$ calculamos sus raíces. Sea $u := \sqrt[8]{2}$ el único número real positivo cuya potencia octava es 2 y sea $\xi := e^{\frac{2\pi \mathtt{i}}{8}}$ con $\mathtt{i} := \sqrt{-1}$. Entonces las soluciones de $f(\mathtt{t}) = 0$ son $\mathtt{t} = u\xi^j$ con $j = 0, 1, ..., 7$. Por tanto, $\mathbb{Q}_f = \mathbb{Q}(u, u\xi, u\xi^2, u\xi^3, u\xi^4, u\xi^5, u\xi^6, u\xi^7) = \mathbb{Q}(u, \xi)$. En la segunda igualdad, el contenido hacia la derecha es inmediato y el contenido hacia la izquierda se sigue de que $\xi = \frac{u\xi}{u} \in \mathbb{Q}_f$. Queremos probar que $\mathbb{Q}(u, \xi) = \mathbb{Q}(u, \mathtt{i})$, ya que esta elección de representantes nos facilitará el trabajo en lo que sigue. De la igualdad $\xi = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}\mathtt{i} = \frac{u^4}{2} + \frac{u^4}{2}\mathtt{i}$ se obtiene el contenido hacia la derecha y despejando $\mathtt{i}$ como $\mathtt{i} = \xi\frac{2}{u^4} - 1$, el otro contenido.

Estamos ahora interesados en calcular el grado de la extensión $\mathbb{Q}_f|\mathbb{Q}$ para lo que utilizamos la transitividad del grado, es decir, $[\mathbb{Q}(u, \mathtt{i}) : \mathbb{Q}] = [\mathbb{Q}(u, \mathtt{i}) : \mathbb{Q}(u)] \cdot [\mathbb{Q}(u) : \mathbb{Q}]$. El grado de la extensión $\mathbb{Q}(u)|\mathbb{Q}$ es fácil de calcular porque coincide con el grado del polinomio mínimo sobre $\mathbb{Q}$ de u. Veamos que $P_{\mathbb{Q},u} = f$. Pero esto es claro porque $f(u) = 0$, $f \in \mathbb{Q}[\mathtt{t}]$, es mónico e irreducible en $\mathbb{Q}[\mathtt{t}]$. Para esto último, f es irreducible en $\mathbb{Z}[\mathtt{t}]$ por el Criterio de Eisenstein para el primo 2 y por el Lema de Gauss también lo es en $\mathbb{Q}[\mathtt{t}]$. Por tanto, $[\mathbb{Q}(u) : \mathbb{Q}] = \deg(f) = 8$. Por otro lado, $[\mathbb{Q}(u, \mathtt{i}) : \mathbb{Q}(u)] \leq [\mathbb{Q}(\mathtt{i}) : \mathbb{Q}] = 2$ y esta desigualdad es en realidad una igualdad porque $\mathbb{Q}(u) \subset \mathbb{R}$ y $\mathbb{Q}(u, \mathtt{i})$ tiene elementos en $\mathbb{C}$. Por tanto, $[\mathbb{Q}(u, \mathtt{i}) : \mathbb{Q}] = 2 \cdot 8 = 16$.

Evidentemente, la extensión $\mathbb{Q}_f|\mathbb{Q}$ es de Galois por ser el cuerpo de descomposición de un polinomio, luego $\operatorname{ord}(G_{\mathbb{Q}}(f)) = 16$. Los automorfismos de $\mathbb{Q}_f = \mathbb{Q}(u, \mathtt{i})$ quedan determinados por las imágenes de u e $\mathtt{i}$. Cada automorfismo transforma estos elementos en raíces de su polinomio irreducible luego tenemos un máximo de $8 \cdot 2 = 16$ candidatos. Como $\operatorname{ord}(G_{\mathbb{Q}}(f)) = 16$ todas estas asignaciones inducen automorfismos en $\mathbb{Q}_f$. Por tanto, $G_{\mathbb{Q}}(f) = \{\rho_{kl} : \ k \in \{0, 1\}, \ l \in \{0, 1, ..., 7\}\}$, donde $\rho_{kl}(\mathtt{i}) = (-1)^k\mathtt{i}$, $\rho_{kl}(u) = u\xi^l$, y por lo anterior,

$$\rho_{kl}(\xi) = \rho_{kl}\left(\frac{u^4}{2} + \frac{u^4}{2}\mathtt{i}\right) = \frac{\rho_{kl}(u)^4}{2} + \frac{\rho_{kl}(u)^4}{2}\rho_{kl}(\mathtt{i}) = \frac{(u\xi^l)^4}{2} + \frac{(u\xi^l)^4}{2}(-1)^k\mathtt{i} =$$
$$\xi^{4l}\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}(-1)^k\mathtt{i}\right) = \xi^{4l}\xi^{1-2k}.$$

Para responder a las tres cuestiones que se preguntan es conveniente calcular el orden de los automorfismos.

$\rho_{0,0}(\mathtt{i}) = \mathtt{i}, \ \rho_{0,0}(u) = u$
$\rho_{0,1}(\mathtt{i}) = \mathtt{i}, \ \rho_{0,1}(u) = u\xi, \ \ \rho_{0,1}(\xi) = \xi^5, \ u \to u\xi \to u\xi^6 \to u\xi^7 \to u\xi^4 \to u\xi^5 \to u\xi^2 \to u\xi^3 \to u$
$\rho_{0,2}(\mathtt{i}) = \mathtt{i}, \ \rho_{0,2}(u) = u\xi^2, \ \ \rho_{0,2}(\xi) = \xi, \ \ u \to u\xi^2 \to u\xi^4 \to u\xi^6 \to u$
$\rho_{0,3}(\mathtt{i}) = \mathtt{i}, \ \rho_{0,3}(u) = u\xi^3, \ \rho_{0,3}(\xi) = \xi^5, \ \rho_{0,3} = \rho_{0,1}^{-1}$
$\rho_{0,4}(\mathtt{i}) = \mathtt{i}, \ \rho_{0,4}(u) = u\xi^4, \ \rho_{0,4}(\xi) = \xi, \ \ u \to u\xi^4 \to u$
$\rho_{0,5}(\mathtt{i}) = \mathtt{i}, \ \rho_{0,5}(u) = u\xi^5, \ \rho_{0,5}(\xi) = \xi^5, \ u \to u\xi^5 \to u\xi^6 \to u\xi^3 \to u\xi^4 \to u\xi \to u\xi^2 \to u\xi^7 \to u$
$\rho_{0,6}(\mathtt{i}) = \mathtt{i}, \ \rho_{0,6}(u) = u\xi^6, \ \rho_{0,6}(\xi) = \xi, \ \ \rho_{0,6} = \rho_{0,2}^{-1}$
$\rho_{0,7}(\mathtt{i}) = \mathtt{i}, \ \rho_{0,7}(u) = u\xi^7, \ \rho_{0,7}(\xi) = \xi^5, \ \rho_{0,7} = \rho_{0,5}^{-1}$

$\rho_{1,0}(\mathtt{i}) = -\mathtt{i},\ \rho_{1,0}(u) = u \qquad \mathtt{i} \to -\mathtt{i} \to \mathtt{i}$
$\rho_{1,1}(\mathtt{i}) = -\mathtt{i},\ \rho_{1,1}(u) = u\xi,\ \ \rho_{1,1}(\xi) = \xi^3,\ u \to u\xi \to u\xi^4 \to u\xi^5 \to u$
$\rho_{1,2}(\mathtt{i}) = -\mathtt{i},\ \rho_{1,2}(u) = u\xi^2,\ \rho_{1,2}(\xi) = \xi^7,\ u \to u\xi^2 \to u$
$\rho_{1,3}(\mathtt{i}) = -\mathtt{i},\ \rho_{1,3}(u) = u\xi^3,\ \rho_{1,3}(\xi) = \xi^3,\ u \to u\xi^3 \to u\xi^4 \to u\xi^7 \to u$
$\rho_{1,4}(\mathtt{i}) = -\mathtt{i},\ \rho_{1,4}(u) = u\xi^4,\ \rho_{1,4}(\xi) = \xi^7,\ u \to u\xi^4 \to u$
$\rho_{1,5}(\mathtt{i}) = -\mathtt{i},\ \rho_{1,5}(u) = u\xi^5,\ \rho_{1,5}(\xi) = \xi^3,\ \rho_{1,5} = \rho_{1,1}^{-1}$
$\rho_{1,6}(\mathtt{i}) = -\mathtt{i},\ \rho_{1,6}(u) = u\xi^6,\ \rho_{1,6}(\xi) = \xi^7,\ u \to u\xi^6 \to u$
$\rho_{1,7}(\mathtt{i}) = -\mathtt{i},\ \rho_{1,7}(u) = u\xi^7,\ \rho_{1,7}(\xi) = \xi^3,\ \rho_{1,7} = \rho_{1,3}^{-1}$

Una vez conocemos los automorfismos del grupo de Galois y sus respectivos órdenes ya podemos responder todas las preguntas.

(i) En primer lugar, se pide calcular el número de subextensiones de grado 8 de $\mathbb{Q}_f|\mathbb{Q}$. Por el Teorema fundamental de la teoría de Galois, existe una biyección entre las subextensiones de $\mathbb{Q}_f|\mathbb{Q}$ y los subgrupos de $G_{\mathbb{Q}}(f)$, por lo que este número de subextensiones de grado 8 será igual al número de subgrupos de orden $2 = \frac{16}{8}$. El número de subgrupos de orden 2 es igual al número de elementos de orden 2, porque cada elemento de orden 2 genera un subgrupo formado por él mismo y la identidad. Como $G_{\mathbb{Q}}(f)$ tiene 5 elementos de orden 2 concluimos que hay 5 subextensiones de grado 8 de $\mathbb{Q}_f|\mathbb{Q}$.

(ii) Después se pregunta si $G_{\mathbb{Q}}(f)$ es diedral. Un argumento sencillo para demostrar que $G_{\mathbb{Q}}(f)$ no es isomorfo a $\mathcal{D}_8$ es contar el número de elementos de orden 2 que hay en cada uno de los grupos y ver que no coinciden. Hemos visto que $G_{\mathbb{Q}}(f)$ tiene 5 elementos de orden 2 y $\mathcal{D}_8$ tiene como elementos de orden 2 las 8 simetrías y la rotación de ángulo π, en total 9. Por tanto $G_{\mathbb{Q}}(f)$ no es isomorfo a $\mathcal{D}_8$.

(iii) Por último, se pide encontrar un grupo finito de generadores de una subextensión $F|\mathbb{Q}$ de $\mathbb{Q}_f|\mathbb{Q}$ tal que $G(\mathbb{Q}_f : F)$ sea cíclico de orden 8. Podemos tomar F de tal forma que $G(\mathbb{Q}_f : F) = \langle \rho_{0,1} \rangle$ con lo que $F = \mathrm{Fix}(\langle \rho_{0,1} \rangle) = \mathbb{Q}(\mathtt{i})$, que efectivamente es una subextensión de grado 2 y $G(\mathbb{Q}_f : F)$ es cíclico de orden 8.

3. (i) *Sea* $\zeta := e^{2\pi \mathtt{i}/5}$, *donde* $\mathtt{i} := \sqrt{-1}$. *Demostrar que* $\sqrt{5} \in \mathbb{Q}(\zeta)$.
(ii) *Sea* $E := \mathbb{Q}(\sqrt{5})$. *Calcular el grado de las extensiones* $E\left(\sqrt[10]{5}\right)|E$ *y* $E\left(e^{2\pi \mathtt{i}/10}\right)|E$.
(iii) *Sea* $f(\mathtt{t}) := \mathtt{t}^{10} - 5$ *y* $\mathbb{Q}_f \subset \mathbb{C}$ *un cuerpo de descomposición de* f *sobre* $\mathbb{Q}$. *Calcular el grado de* $\mathbb{Q}_f|\mathbb{Q}$.
(iv) *¿Cuántas subextensiones de grado* 5 *tiene* $\mathbb{Q}_f|\mathbb{Q}$*?*
(v) *Demostrar que* $\sqrt{3} \notin \mathbb{Q}(\zeta)$.
(vi) *Calcular el polinomio mínimo de* ζ *sobre* $\mathbb{Q}(\sqrt{3})$.

(i) Podemos expresar ζ como $\zeta = \cos\left(\frac{2\pi}{5}\right) + \mathtt{i}\sin\left(\frac{2\pi}{5}\right)$. Sea $u := \zeta + \zeta^{-1}$. Por la fórmula de Euler para ζ y ζ^{-1} sabemos que $u = \zeta + \zeta^{-1} = 2\cos\left(\frac{2\pi}{5}\right) \in \mathbb{Q}(\zeta)$.

Como $\zeta^5 = 1$ y $\zeta \neq 1$, ζ será raíz del polinomio ciclotómico $\Phi_5(\mathtt{t}) = \mathtt{t}^4 + \mathtt{t}^3 + \mathtt{t}^2 + \mathtt{t} + 1$. Sea $h(\mathtt{t}) := \mathtt{t}^{-2} \cdot \Phi_5(\mathtt{t})$, que se anula en ζ ya que ζ no es raíz de $\mathtt{t}^2$. Reescribiendo h llegamos a que:

$h(\mathtt{t}) = \left(\mathtt{t}^2 + \mathtt{t}^{-2}\right) + \left(\mathtt{t} + \mathtt{t}^{-1}\right) + 1$ y, como $\left(\mathtt{t} + \mathtt{t}^{-1}\right)^2 = \mathtt{t}^2 + \mathtt{t}^{-2} + 2$, entonces:

$h(\mathtt{t}) = \left[\left(\mathtt{t} + \mathtt{t}^{-1}\right)^2 - 2\right] + \left(\mathtt{t} + \mathtt{t}^{-1}\right) + 1 = \left(\mathtt{t} + \mathtt{t}^{-1}\right)^2 + \left(\mathtt{t} + \mathtt{t}^{-1}\right) - 1$

Como $h(\zeta) = 0$, deducimos que $h(\zeta) = \left(\zeta + \zeta^{-1}\right)^2 + \left(\zeta + \zeta^{-1}\right) - 1 = 0 \Leftrightarrow u^2 + u - 1 = 0$

Resolviendo la ecuación de segundo grado, tenemos que $u = \frac{-1 \pm \sqrt{5}}{2}$. Dado que u ha de ser positivo, tomamos la solución positiva, obteniendo que $\sqrt{5} = 2u + 1 \in \mathbb{Q}(\zeta)$.

(ii) En primer lugar, $E\left(\sqrt[10]{5}\right) = \mathbb{Q}\left(\sqrt[10]{5}\right)$ ya que $\sqrt{5} \in \mathbb{Q}\left(\sqrt[10]{5}\right)$, pues $\left(\sqrt[10]{5}\right)^5 = \sqrt{5}$. Es decir, $\mathbb{Q}\left(\sqrt{5}\right)|\mathbb{Q}$ es una subextensión de $\mathbb{Q}\left(\sqrt[10]{5}\right)|\mathbb{Q}$. Sabemos que $[\mathbb{Q}\left(\sqrt{5}\right) : \mathbb{Q}] = 2$ ya que el polinomio mínimo de $\sqrt{5}$ sobre $\mathbb{Q}$ es $g_1(\mathtt{t}) := \mathtt{t}^2 - 5$ (es mónico e irreducible por el Criterio de Eisenstein con el primo 5, aplicable a $\mathbb{Q}$ por el Lema de Gauss) y también sabemos que $[\mathbb{Q}\left(\sqrt[10]{5}\right) : \mathbb{Q}] = 10$ ya que el polinomio mínimo de $\sqrt[10]{5}$ sobre $\mathbb{Q}$ es $g_2(\mathtt{t}) := \mathtt{t}^{10} - 5$ que de nuevo es mónico e irreducible argumentando de forma análoga. Por todo lo anterior y la transitividad del grado:

$$[E(\sqrt[10]{5}) : E] = [\mathbb{Q}(\sqrt[10]{5}) : \mathbb{Q}(\sqrt{5})] = \frac{[\mathbb{Q}\left(\sqrt[10]{5}\right) : \mathbb{Q}]}{[\mathbb{Q}\left(\sqrt{5}\right) : \mathbb{Q}]} = \frac{10}{2} = 5$$

Argumentando de forma similar, como $e^{2\pi \mathtt{i}/5} = \left(e^{2\pi \mathtt{i}/10}\right)^2$ y $\sqrt{5} \in \mathbb{Q}\left(e^{2\pi \mathtt{i}/5}\right)$ según lo visto en (i), entonces $\sqrt{5} \in \mathbb{Q}\left(e^{2\pi \mathtt{i}/10}\right)$. Por tanto, $E\left(e^{2\pi \mathtt{i}/10}\right) = \mathbb{Q}\left(e^{2\pi \mathtt{i}/10}\right)$. Sabemos que el polinomio mínimo de $e^{2\pi \mathtt{i}/10}$ sobre $\mathbb{Q}$ es el polinomio ciclotómico $\Phi_{10}(\mathtt{t}) = \mathtt{t}^4 - \mathtt{t}^3 + \mathtt{t}^2 - \mathtt{t} + 1$, que tiene grado $4 = \varphi(10)$, por lo que:

$$[E(e^{2\pi \mathtt{i}/10}) : E] = [\mathbb{Q}(e^{2\pi \mathtt{i}/10}) : \mathbb{Q}(\sqrt{5})] = \frac{[\mathbb{Q}(e^{2\pi \mathtt{i}/10}) : \mathbb{Q}]}{[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}]} = \frac{4}{2} = 2$$

(iii) Sea $r := \sqrt[10]{5}$ la única raíz real positiva de f. El resto de raíces serán de la forma $r \cdot \xi^k$ donde $0 \leq k \leq 9$ y $\xi := e^{2\pi \mathtt{i}/10}$ por lo que el conjunto de raíces de f será $\{r \cdot \xi^k : 0 \leq k \leq 9\}$. Por tanto, un cuerpo de descomposición de f sobre $\mathbb{Q}$ es $\mathbb{Q}_f = \mathbb{Q}(r, \xi)$. Ya sabemos por el apartado anterior que $[E(\xi) : E] = 2$ y $[E(r) : E] = 5$ y como 5 y 2 son coprimos, $[E(r, \xi) : E] = 5 \cdot 2 = 10$. Por último, como $[\mathbb{Q}\left(\sqrt{5}\right) : \mathbb{Q}] = 2$ y $\sqrt{5} \in \mathbb{Q}(\xi)$ concluimos que $[\mathbb{Q}_f : \mathbb{Q}] = [\mathbb{Q}(r, \xi) : \mathbb{Q}] = [E(r, \xi) : \mathbb{Q}] = [E(r, \xi) : E] \cdot [E : \mathbb{Q}] = 10 \cdot 2 = 20$.

(iv) Como la extensión $\mathbb{Q}_f|\mathbb{Q}$ es de Galois, su grado (que es 20) coincide con el orden de $G := G(\mathbb{Q}_f : \mathbb{Q})$. Así que el número de subextensiones de grado 5 coincidirá con el número de subgrupos de G de orden $4 = \frac{20}{5}$. Puesto que $20 = 2^2 \cdot 5$, los subgrupos de G de orden 4 son sus 2-subgrupos de Sylow. Por el tercer Teorema de Sylow, si n_2 es el número de 2-subgrupos de Sylow de G, entonces $n_2 \equiv 1 \mod 2$ y $n_2|5$. Es decir, n_2 es o bien 1, o bien 5.

Veamos por contradicción que $n_2 = 5$. Si $n_2 = 1$, entonces, ese 2-subgrupo de Sylow de G, al que llamaremos H, sería el único subgrupo de G de su grado, por lo que sería normal.

Utilizamos ahora que $\mathbb{Q}(\sqrt[5]{5})|\mathbb{Q}$ es una (de hecho, según hemos supuesto, la única) subextensión de grado 5 de $\mathbb{Q}_f|\mathbb{Q}$. Esto es fácil de comprobar, pues el polinomio

$$g_3(\mathtt{t}) := \mathtt{t}^5 - 5$$

tiene a $\sqrt[5]{5}$ por única raíz real, es mónico, y es irreducible (por el Criterio de Eisenstein con el primo 5, aplicable a $\mathbb{Q}$ por el Lema de Gauss), luego es el polinomio mínimo sobre $\mathbb{Q}$ de $\sqrt[5]{5}$, y $[\mathbb{Q}(\sqrt[5]{5}) : \mathbb{Q}] = 5$. Así que necesariamente $H = G(\mathbb{Q}_f : \mathbb{Q}(\sqrt[5]{5}))$, por ser H el único subgrupo de orden 4 de G, y $\mathbb{Q}(\sqrt[5]{5})|\mathbb{Q}$ la única subextensión de grado 5 de $\mathbb{Q}_f|\mathbb{Q}$.

Por la segunda parte del Teorema Fundamental de la Teoría de Galois, el hecho de que H sea normal es equivalente a que la subextensión $\mathbb{Q}(\sqrt[5]{5})|\mathbb{Q}$ sea de Galois. Pero esto es imposible, pues de ser el caso, se tendría que $\mathbb{Q}_{g_3}$, el cuerpo de descomposición del polinomio g_3 sobre $\mathbb{Q}$, coincide con $\mathbb{Q}(\sqrt[5]{5})$, pero $\mathbb{Q}(\sqrt[5]{5}) \subset \mathbb{R}$, y sabemos que$g_3$ tiene raíces complejas, luego $\mathbb{Q}_{g_3}$ tiene elementos en $\mathbb{C}\backslash\mathbb{R}$ y no pueden coincidir.

Por tanto, $n_2 = 5$, de modo que $\mathbb{Q}_f|\mathbb{Q}$ tiene 5 subextensiones de grado 5, que de hecho son $\mathbb{Q}(\sqrt[5]{5}\zeta^k)|\mathbb{Q}$ con $k = 0, 1, ..., 4$.

(v) Lo probamos por contradicción. Si $\sqrt{3} \in \mathbb{Q}(\zeta)$, entonces, como $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$, tenemos que tanto $\mathbb{Q}(\sqrt{3})|\mathbb{Q}$ como $\mathbb{Q}(\sqrt{5})|\mathbb{Q}$ son subextensiones de grado 2 de $\mathbb{Q}(\zeta)|\mathbb{Q}$, y como sabemos que $\sqrt{3} \notin \mathbb{Q}(\sqrt{5})$, necesariamente

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{5})] \cdot [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

Esto implica que $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\zeta)$ (pues tenemos $\subset$, y la igualdad se sigue de que ambas extensiones tienen el mismo grado sobre $\mathbb{Q}$), lo cual es imposible porque $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \subset \mathbb{R}$ y $\zeta \in \mathbb{C}\backslash\mathbb{R}$, luego $\sqrt{3} \notin \mathbb{Q}(\zeta)$.

(vi) Sabemos que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(5) = 4$, y también que $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Utilizamos el apartado anterior, que nos dice que $\sqrt{3} \notin \mathbb{Q}(\zeta)$, para deducir que $[\mathbb{Q}(\sqrt{3}, \zeta) : \mathbb{Q}(\zeta)] = 2$, pues ha de ser mayor que 1 y menor o igual que 2 (ya que $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$). Gracias a la transitividad del grado, obtenemos que

$$[\mathbb{Q}(\sqrt{3}, \zeta) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \zeta) : \mathbb{Q}(\zeta)] \cdot [\mathbb{Q}(\zeta) : \mathbb{Q}] = 2 \cdot 4 = 8$$

Esto nos sirve para calcular el grado de la extensión $\mathbb{Q}(\sqrt{3}, \zeta)|\mathbb{Q}(\sqrt{3})$, puesto que

$$[\mathbb{Q}(\sqrt{3}, \zeta) : \mathbb{Q}(\sqrt{3})] = \frac{[\mathbb{Q}(\sqrt{3}, \zeta) : \mathbb{Q}]}{[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]} = \frac{8}{2} = 4.$$

Por tanto, puesto que el polinomio ciclotómico asociado al primo 5, Φ_5, tiene grado 4, es mónico y se anula en ζ, ha de ser $P_{\mathbb{Q}(\sqrt{3}),\zeta} = \Phi_5(\mathtt{t}) = \mathtt{t}^4 + \mathtt{t}^3 + \mathtt{t}^2 + \mathtt{t} + 1$.