| | | |
|---|---|---|
| Nombre: | Juan Carlos | Calificación |
| Apellidos: | Llamas Núñez | |
| DNI/Alias | 11 867 802-D | |
| Titulación | Doble Grado Matemáticas Informática | |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |

**Examen Enero (180 minutos)**: Jueves 13 de Enero de 2022

*Instrucciones:* Se deberá entregar únicamente este block con seis hojas con la solución del ejercicio. Podéis utilizar todas la hojas de sucio que deseéis pero sólo recogeré este block. Deberéis escribir tanto vuestro nombre como el alias con el que queráis que aparezca vuestra calificación. Podéis usar los enunciados de apartados no resueltos para resolver otros siempre que no hagáis bucles.

**Ejercicio.** Sean $L_1 \subset \mathbb{C}$ un cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio ciclotómico $\phi_7$, $L_2 \subset \mathbb{C}$ un cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio ciclotómico $\phi_9$ y $L$ un cuerpo de descomposición de $\phi_7 \cdot \phi_9$.

(1) Demostrar que $L$ es un cuerpo de descomposición de $\phi_{63}$. Demostrar que $[L : Q] = 36$ y que $G(L : \mathbb{Q}) \cong \mathbb{Z}_6 \times \mathbb{Z}_6$.

(2) Encontrar un elemento primitivo de la extansión $L|\mathbb{Q}$ y calcular explícitamente su polinomio mínimo sobre $\mathbb{Q}$.

(3) Encontrar un sistema generador de $G(L : \mathbb{Q})$ formado por dos elementos y construir un isomorfismo entre $G(L : \mathbb{Q})$ y $G(L_1 : \mathbb{Q}) \times G(L_2 : \mathbb{Q})$.

(4) Encontrar una torre cíclica para $G(L : \mathbb{Q})$ y una torre de resolución para $L|\mathbb{Q}$.

(5) Demostrar que $G(L : \mathbb{Q})$ tiene un elemento de orden 1, tres elementos de orden 2, ocho elementos de orden 3 y veinticuatro elementos de orden 6.

(6) Determinar cuántos subgrupos tiene $G(L : \mathbb{Q})$ de ordenes 2, 3 y 6.

(7) Demostrar que $G(L : \mathbb{Q})$ tiene un único subgrupo de orden 4 (isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$), un único subgrupo de orden 9 (isomorfo a $\mathbb{Z}_3 \times \mathbb{Z}_3$), cuatro subgrupos de orden 12 (todos ellos isomorfos a $\mathbb{Z}_2 \times \mathbb{Z}_6$), tres subgrupos de orden 18 (todos ellos isomorfos a $\mathbb{Z}_3 \times \mathbb{Z}_6$).

(8) Demostrar que $L|\mathbb{Q}$ tiene una única subextensión de grado 9 y una única subextensión de grado 4. Encontrar sistemas de generadores para cada una de las subextensiones anteriores.

(9) Demostrar que hay tres subextensiones de $L|\mathbb{Q}$ de grado 2 y encontrar generadores de cada una de ellas.

(10) Encontrar generadores de dos de las subextensiones de grado 3 de $L|\mathbb{Q}$, de dos de las subextensiones de grado 6 de $L|\mathbb{Q}$, de dos de las subextensiones de grado 12 de $L|\mathbb{Q}$ y de dos de las subextensiones de grado 18 de $L|\mathbb{Q}$.

~~4~~

7 Demostrar ~~que hay 4 de orden 12 y 3 de orden~~ 18

~~8 Demostrar que los grados son 4 y 9~~

9 Encontrar la 3ª

~~10~~



0

1) Sea $\eta = e^{\frac{2\pi i}{7}}$, $\xi = e^{\frac{2\pi i}{9}}$ raíces primitivas séptima y novena de la unidad.

Como 7 es primo $\Phi_7(t) = t^6+t^5+t^4+t^3+t^2+t+1$.

Además $\Phi_9(t) = \Phi_{3^2}(t) = \Phi_3(t^{3^{2-1}}) = \Phi_3(t^3) \underset{\substack{\uparrow \\ 3\text{ primo}}}{=} \cancel{\Phi}\, t^6+t^3+1$.

Las raíces de $\Phi_7(t)$ son $\eta^k$ con $k=1\cdots 6$ por ser 7 primo y las raíces de $\Phi_9(t)$ son $\xi^k$ con $mcd(k,9)=1$ y $k\in[1,8]\cap\mathbb{Z}$ es decir $\{\xi, \xi^2, \xi^4, \xi^5, \xi^7, \xi^8\}$.

$L$ es el cuerpo de descomposición de $\Phi_7 \cdot \Phi_9$ por lo que hay que adjuntar todas sus raíces que son todas las de $\Phi_9$ y todas las de $\Phi_7$, es decir

$$L = \mathbb{Q}(\xi, \xi^2, \xi^4, \xi^5, \xi^7, \xi^8, \eta, \eta^2, \eta^3, \eta^4, \eta^5, \eta^6) = \mathbb{Q}(\xi, \eta)$$

Por otro lado $\Phi_{63}(t) = \Phi_{7\cdot 9}(t) = \Phi_{7\cdot 3^2}(t) = \Phi_{7\cdot 3}(t^{7^{1-1}}\cdot t^{3^{2-1}}) = \Phi_{7\cdot 3}(t^3)$.

El cuerpo de descomposición de $\Phi_{63}$ estará generado por las raíces 63 primitivas de la unidad, es decir, si $\alpha = e^{\frac{2\pi i}{63}}$, las raíces de $\Phi_{63}$ son:

$\{\alpha^k : \cancel{1}\leq k\leq 62,\ mcd(k,63)=1\}$, es decir,

$$\mathbb{Q}_{\Phi_{63}} = \mathbb{Q}(\alpha^k : 1\leq k\leq 62, mcd(k,63)=1) = \mathbb{Q}(\alpha)$$

Se pide probar que $L = \mathbb{Q}(\xi,\eta) = \mathbb{Q}(e^{\frac{2\pi i}{9}}, e^{\frac{2\pi i}{7}}) \overset{?}{=} \mathbb{Q}(e^{\frac{2\pi i}{63}}) = \mathbb{Q}(\alpha)$.

$\subseteq$) $e^{\frac{2\pi i}{9}} = (e^{\frac{2\pi i}{63}})^7 \in \mathbb{Q}(e^{\frac{2\pi i}{63}})$ y $e^{\frac{2\pi i}{7}} = (e^{\frac{2\pi i}{63}})^9 \in \mathbb{Q}(e^{\frac{2\pi i}{63}})$.

$\supseteq$) Como $mcd(7,9)=1$, podemos construir una Identidad de Bezut de la forma $7x+9y=1$. Unos posibles valores de $x$ e $y$ son $x=4$ e $y=-3$, ya que $7\cdot 4 - 9\cdot 3 = 1$. Entonces $(e^{\frac{2\pi i}{7}})^{-3}\cdot(e^{\frac{2\pi i}{9}})^4 = e^{2\pi i\left(\frac{-3}{7}+\frac{4}{9}\right)} = e^{2\pi i\left(\frac{-3\cdot 9+4\cdot 7}{63}\right)} = e^{\frac{2\pi i}{63}}$ y, por tanto, $e^{\frac{2\pi i}{63}} \in \mathbb{Q}(e^{\frac{2\pi i}{7}}, e^{\frac{2\pi i}{9}})$

Ahora que sabemos que $L = \mathbb{Q}(\alpha) = \mathbb{Q}(e^{\frac{2\pi i}{63}})$,

$[L:\mathbb{Q}] = \varphi(63) = \varphi(7\cdot 9) = \varphi(7)\cdot\varphi(9) = 6\cdot 3\cdot 2 = 36$ donde $\varphi$ es la función de Euler.

Dejamos pendiente por el momento demostrar que $G(L:\mathbb{Q}) \cong \mathbb{Z}_6 \times \mathbb{Z}_6$.

2) Ya hemos probado en (1) que $L|\mathbb{Q} = \mathbb{Q}(e^{\frac{2\pi i}{63}})|\mathbb{Q}$ así que $e^{\frac{2\pi i}{63}}$ es un elemento primitivo. Sabemos que su polinomio mínimo es el polinomio ciclotómico $\Phi_{63}$ que es mónico, irreducible y lo tiene por raíz.

Habíamos llegado a que $\Phi_{63}(t) = \Phi_{7\cdot 3}(t^3)$ así que únicamente hace falta calcular $\Phi_{21}(t)$.

Utilizamos el apartado (6) de la observación VI.1.10. que dice que si $n$ es un entero positivo y $p$ un primo que no divide a $n$, entonces

$$\Phi_n(t)\cdot\Phi_{pn}(t) = \Phi_n(t^p).$$

Tomando $n=3$, $p=7$. $\quad \Phi_3(t)\cdot\Phi_{7\cdot 3}(t) = \Phi_3(t^7)$

$$\Rightarrow \Phi_{7\cdot 3}(t) = \Phi_{21}(t) = \frac{\Phi_3(t^7)}{\Phi_3(t)} = \frac{t^{14}+t^7+1}{t^2+t+1} = t^{12}-t^{11}+t^9-t^8+t^6-t^4+t^3-t+1$$

Se comprueba dividiendo o mirando en tablas de polinomios ciclotómicos, por ejemplo la de la wikipedia.

Por tanto $\Phi_{63}(t) = \Phi_{21}(t^3) = (t^3)^{12}-(t^3)^{11}+(t^3)^9-(t^3)^8+(t^3)^6-(t^3)^4+(t^3)^3-t^3+1 =$

$= t^{36}-t^{33}+t^{27}-t^{24}+t^{18}-t^{12}+t^9-t^3+1$, que efectivamente tiene grado $36 = [L:\mathbb{Q}]$.

3) Ya hemos visto que $L = \mathbb{Q}(\eta,\xi) = \mathbb{Q}(e^{\frac{2\pi i}{7}}, e^{\frac{2\pi i}{9}})$.

Ahora $L_1 = \mathbb{Q}_{\Phi_7} = \mathbb{Q}(\eta,\eta^2,\eta^3,\eta^4,\eta^5,\eta^6) = \mathbb{Q}(\eta) = \mathbb{Q}(e^{\frac{2\pi i}{7}})$ y

$L_2 = \mathbb{Q}_{\Phi_9} = \mathbb{Q}(\xi,\xi^2,\xi^4,\xi^5,\xi^7,\xi^8) = \mathbb{Q}(\xi) = \mathbb{Q}(e^{\frac{2\pi i}{9}})$

$j\in\{1,2,4,5,7,8\}$

... $\varphi_{ij}(\eta) = \eta^i$, $\varphi_{ij}(\xi) = \xi^j$.

Vamos a calcular $G(L_1:\mathbb{Q}) = G(\mathbb{Q}(e^{\frac{2\pi i}{7}}):\mathbb{Q})$ y
$G(L_2:\mathbb{Q}) = G(\mathbb{Q}(e^{\frac{2\pi i}{9}}):\mathbb{Q})$.

En primer lugar, cabe destacar que ambas extensiones $L_1|\mathbb{Q}$ y $L_2|\mathbb{Q}$ son de Galois por ser los cuerpos de descomposición de los polinomios $\Phi_7$ y $\Phi_9$ respectivamente y también lo es $L|\mathbb{Q}$ por ser el cuerpo de descomposición de $\Phi_{63}$ sobre $\mathbb{Q}$.

Por tanto $\operatorname{ord}(G(L_1:\mathbb{Q})) = [L_1:\mathbb{Q}]$, $\operatorname{ord}(G(L_2:\mathbb{Q})) = [L_2:\mathbb{Q}]$ y $\operatorname{ord}(G(L:\mathbb{Q})) = [L:\mathbb{Q}] = 36$.

El grado de las extensiones de $L_1|\mathbb{Q}$ y $L_2|\mathbb{Q}$ es:
$[L_1:\mathbb{Q}] = [\mathbb{Q}(e^{\frac{2\pi i}{7}}):\mathbb{Q}] = \varphi(7) = 6$ y $[L_2:\mathbb{Q}] = [\mathbb{Q}(e^{\frac{2\pi i}{9}}):\mathbb{Q}] = \varphi(9) = 3\cdot 2 = 6$.

Sabemos que ambos grupos son abelianos por tratarse de grupos de Galois de polinomios ciclotómicos y como solamente hay un grupo abeliano de orden 6, concluimos que $G(L_1:\mathbb{Q}) \cong G(L_2:\mathbb{Q}) \cong \mathbb{Z}_6$.

Si construimos el isomorfismo $\Psi: G(L:\mathbb{Q}) \longrightarrow G(L_1:\mathbb{Q})\times G(L_2:\mathbb{Q})$ ya habremos probado lo que nos quedaba del apartado (1), que era ver que $G(L:\mathbb{Q}) \cong \mathbb{Z}_6 \times \mathbb{Z}_6$.

Primero vamos a ver cuáles son los elementos del grupo de Galois $G(L:\mathbb{Q})$. Ya hemos visto que la extensión era de Galois y que $\operatorname{ord}(G(L:\mathbb{Q})) = 36$. Los $\mathbb{Q}$-automorfismos de $L$ quedan determinados por las imágenes de sus generadores $\eta = e^{\frac{2\pi i}{7}}$ y $\xi = e^{\frac{2\pi i}{9}}$ y estas imágenes pueden ser cada una de las raíces de sus respectivos polinomios mínimos, es decir, $\Phi_7$ y $\Phi_9$ respectivamente. Tenemos por tanto $6\cdot 6$ candidatos así que todos son válidos y $G(L:\mathbb{Q}) = \{\varphi_{ij} : i\in\{1,2,3,4,5,6\},\ j\in\{1,2,4,5,7,8\}\}$ verificando $\varphi_{ij}(\eta) = \eta^i$, $\varphi_{ij}(\xi) = \xi^j$.

Veamos que $\varphi_{31}$ y $\varphi_{12}$ son generadores de $G(L:\mathbb{Q})$.
Efectivamente, el primero deja fijo $\xi$ y nótese que $3+7\mathbb{Z}$ genera $(\mathbb{Z}_7^*,\cdot)$.
Además, el segundo deja fijo $\eta$ y $2+9\mathbb{Z}$ genera $(\mathbb{Z}_9^*,\cdot)$.
Por tanto, dado $\varphi_{ij}$ con $i\in\{1,\dots,6\}$, $j\in\{1,2,4,5,7,8\}$ existen $a,b\in\mathbb{Z}$ tales que $(3+7\mathbb{Z})^a=(i+7\mathbb{Z})$ y $(2+9\mathbb{Z})^b=(j+9\mathbb{Z})$ por lo que

$$\varphi_{ij}=\varphi_{31}^{a}\cdot\varphi_{12}^{b}.$$

Efectivamente,
$$(\varphi_{31}^{a}\varphi_{12}^{b})(\eta)=\varphi_{12}^{b}(\varphi_{31}^{a}(\eta))=\varphi_{12}^{b}(\eta^{i})=\eta^{i}=\varphi_{ij}(\eta) \text{ y}$$
$$(\varphi_{31}^{a}\varphi_{12}^{b})(\xi)=\varphi_{12}^{b}(\varphi_{31}^{a}(\xi))=\varphi_{12}^{b}(\xi)=\xi^{j}=\varphi_{ij}(\xi).$$

Por tanto $G(L:\mathbb{Q})=<\varphi_{31},\varphi_{12}>$.

Es claro que el isomorfismo buscado es:

$$\Psi: G(L:\mathbb{Q})\longrightarrow G(L_1:\mathbb{Q})\times G(L_2:\mathbb{Q})$$
$$\varphi\longmapsto(\varphi|_{L_1},\varphi|_{L_2}).$$

Por el Corolario IV.2.8 apartado (2), como $r=2$, esto es un isomorfismo si y solo si $L_1\cap L_2=\mathbb{Q}$, es decir $\mathbb{Q}(e^{\frac{2\pi i}{7}})\cap\mathbb{Q}(e^{\frac{2\pi i}{9}})=\mathbb{Q}$.

Pero por el Corolario IV.2.7,

$$\underset{36}{\underset{\shortparallel}{[L:\mathbb{Q}]}}\cdot[L_1\cap L_2:\mathbb{Q}]=\underset{6}{\underset{\shortparallel}{[L_1:\mathbb{Q}]}}\cdot\underset{6}{\underset{\shortparallel}{[L_2:\mathbb{Q}]}}.$$

Por tanto $[L_1\cap L_2:\mathbb{Q}]=1$ y esto significa que $L_1\cap L_2=\mathbb{Q}$ lo que termina de justificar que $\Psi$ es isoformismo.

Dejamos por ahora el ejercicio 4 para más adelante.

5) Vamos a calcular explícitamente el orden de los 36 automorfismos porque pueden sernos útiles posteriormente

$\varphi_{1,j}$ $\eta \to \eta$

$j=1$ $\xi \to \xi$ 1

$j=2$ $\xi \to \xi^2 \to \xi^4 \to \xi^8 \to \xi^7 \to \xi^5 \to \xi$ 6

$j=4$ $\xi \to \xi^4 \to \xi^7 \to \xi$ 3

$j=5$ $\xi \to \xi^5 \to \xi^7 \to \xi^8 \to \xi^4 \to \xi^2 \to \xi$ 6

$j=7$ $\xi \to \xi^7 \to \xi^4 \to \xi$ 3

$j=8$ $\xi \to \xi^8 \to \xi$ 2

$\varphi_{2,j}$ $\eta \to \eta^2 \to \eta^4 \to \eta$

$j=1$ $\xi \to \xi$ 3

$j=2$ $\xi \to \xi^2 \to \xi^4 \to \xi^8 \to \xi^7 \to \xi^5 \to \xi$ 6

$j=4$ $\xi \to \xi^4 \to \xi^7 \to \xi$ 3

$j=5$ $\xi \to \xi^5 \to \xi^7 \to \xi^8 \to \xi^4 \to \xi^2 \to \xi$ 6

$j=7$ $\xi \to \xi^7 \to \xi^4 \to \xi$ 3

$j=8$ $\xi \to \xi^8 \to \xi$ 6

$\varphi_{3,j}$ $\eta \to \eta^3 \to \eta^2 \to \eta^6 \to \eta^4 \to \eta^5 \to \eta$

$j=1$ $\xi \to \xi$ 6

$j=2$ $\xi \to \xi^2 \to \xi^4 \to \xi^8 \to \xi^7 \to \xi^5 \to \xi$ 6

$j=4$ $\xi \to \xi^4 \to \xi^7 \to \xi$ 6

$j=5$ $\xi \to \xi^5 \to \xi^7 \to \xi^8 \to \xi^4 \to \xi^2 \to \xi$ 6

$j=7$ $\xi \to \xi^7 \to \xi^4 \to \xi$ 6

$j=8$ $\xi \to \xi^8 \to \xi$ 6

$\varphi_{4,j}$ $\eta \to \eta^4 \to \eta^2 \to \eta$

$j=1$ $\xi \to \xi$ 3

$j=2$ $\xi \to \xi^2 \to \xi^4 \to \xi^8 \to \xi^7 \to \xi^5 \to \xi$ 6

$j=4$ $\xi \to \xi^4 \to \xi^7 \to \xi$ 3

$j=5$ $\xi \to \xi^5 \to \xi^7 \to \xi^8 \to \xi^4 \to \xi^2 \to \xi$ 6

$j=7$ $\xi \to \xi^7 \to \xi^4 \to \xi$ 3

$j=8$ $\xi \to \xi^8 \to \xi$ 6

$\varphi_{5,j}$ $\eta \to \eta^5 \to \eta^4 \to \eta^6 \to \eta^2 \to \eta^3 \to \eta$

$j=1$ $\xi \to \xi$ 6

$j=2$ $\xi \to \xi^2 \to \xi^4 \to \xi^8 \to \xi^7 \to \xi^5 \to \xi$ 6

$j=4$ $\xi \to \xi^4 \to \xi^7 \to \xi$ 6

$j=5$ $\xi \to \xi^5 \to \xi^7 \to \xi^8 \to \xi^4 \to \xi^2 \to \xi$ 6

$j=7$ $\xi \to \xi^7 \to \xi^4 \to \xi$ 6

$j=8$ $\xi \to \xi^8 \to \xi$ 6

$\varphi_{6,j}$ $\eta \to \eta^6 \to \eta$.

$j=1$ $\xi \to \xi$ 2

$j=2$ $\xi \to \xi^2 \to \xi^4 \to \xi^8 \to \xi^7 \to \xi^5 \to \xi$ 6

$j=4$ $\xi \to \xi^4 \to \xi^7 \to \xi$ 6

$j=5$ $\xi \to \xi^5 \to \xi^7 \to \xi^8 \to \xi^4 \to \xi^2 \to \xi$ 6.

$j=7$ $\xi \to \xi^7 \to \xi^4 \to \xi$ 6

$j=8$ $\xi \to \xi^8 \to \xi$ 2

Contando elementos llegamos a que hay:

- Un elemento de orden 1
- Tres elementos de orden 2
- Ocho elementos de orden 3
- 24 elementos de orden 6.

Se podía haber simplificado mucho y no habría necesidad de escribirlos todos (razonando directamente sobre $\mathbb{Z}_6 \times \mathbb{Z}_6$) pero así ya los tenemos todos bien identificados y ordenados.

(6) El número de subgrupos de orden 2 es igual al número de elementos de orden 2 ya que cada elemento de orden 2 genera un subgrupo formado por él mismo y la identidad. Por tanto hay exactamente 3 subgrupos de orden 2.

El número de subgrupos de orden 3 es la mitad del número de elementos de orden 3 ya que cada elemento de orden 3 genera un subgrupo formado por él mismo, la identidad y su inverso, que también tiene orden 3. Por tanto, hay exactamente 4 subgrupos de orden 3.

De orden 6, en principio puede haber de dos tipos ($\mathbb{Z}_6$ y $D_3$) pero como $\mathbb{Z}_6 \times \mathbb{Z}_6$ es abeliano todos sus subgrupos lo tienen que ser y sólo puede haber de tipo $\mathbb{Z}_6$. Como $\mathbb{Z}_6$ tiene exactamente 2 elementos de orden 6 ($1+6\mathbb{Z}$ y $5+6\mathbb{Z}$), el número de subgrupos de orden 6 será igual al número de elementos de orden 6 entre dos, ya que cada elemento de orden 6 genera uno, pero ese subgrupo contiene a su inverso, que también tiene orden 6. Por tanto hay exactamente 12 subgrupos de orden 6, todos ellos de tipo $\mathbb{Z}_6$.

7) Los <u>subgrupos de orden 4</u> son de tipo $\mathbb{Z}_4$ o $\mathbb{Z}_2\times\mathbb{Z}_2$. No puede haber ningún subgrupo de tipo $\mathbb{Z}_4$ porque en $\mathbb{Z}_6\times\mathbb{Z}_6$ no hay elementos de orden 4, y de tipo $\mathbb{Z}_2\times\mathbb{Z}_2$ hay como mucho uno porque hemos visto que $\mathbb{Z}_6\times\mathbb{Z}_6$ solo tiene tres elementos de orden 2 (los mismos que $\mathbb{Z}_2\times\mathbb{Z}_2$). Existe un subgrupo de tipo $\mathbb{Z}_2\times\mathbb{Z}_2$ que es $\langle(3,0),(0,3)\rangle=\{(0,0),(3,0),(0,3),(3,3)\}$ ya que $(3,0)$ y $(0,3)$ conmutan. Por tanto hay exactamente un subgrupo de orden 4 y es isomorfo a $\mathbb{Z}_2\times\mathbb{Z}_2$.

Los <u>subgrupos de orden 9</u> son de tipo $\mathbb{Z}_9$ o $\mathbb{Z}_3\times\mathbb{Z}_3$ pero como no tenemos elementos de orden 9 solo puede haber de tipo $\mathbb{Z}_3\times\mathbb{Z}_3$. Además hay como mucho uno porque $\mathbb{Z}_3\times\mathbb{Z}_3$ tiene un elemento de orden 1 y 8 de orden 3 y nosotros solo tenemos un elemento de orden 1 y 8 de orden 3. Además existe y es $\langle(2,0),(0,2)\rangle=\{(0,0),(2,0),(4,0),(0,2),(2,2),(4,2),(0,4),(2,4),(4,4)\}$. Por tanto hay exactamente un subgrupo de orden 9 y es isomorfo a $\mathbb{Z}_3\times\mathbb{Z}_3$.

Los <u>subgrupos de orden 12</u> (tienen que ser abelianos porque $\mathbb{Z}_6\times\mathbb{Z}_6$ lo es), pueden ser de tipo $\mathbb{Z}_{12}$ o de tipo $\mathbb{Z}_6\times\mathbb{Z}_2$. Del primer tipo no hay ninguno porque no tenemos elementos de orden 4 y del segundo veamos que hay 4. Estos están generados por un elemento de orden 6 y un elemento de orden 2 y el elemento de orden 6 al cubo no es el de orden 2. Por tanto tienen que estar los tres elementos de orden 2 en todos y basta coger los generadores de orden 6. Son

$\langle(1,0),(0,3)\rangle$

$\langle(0,1),(3,0)\rangle$

$\langle(1,1),(0,3)\rangle$ y estos son todos.

$\langle(1,2),(0,3)\rangle$

18

Por último de orden 18 y abelianos hay de tipo $\mathbb{Z}_{18}$ o $\mathbb{Z}_3\times\mathbb{Z}_6$, pero del primer tipo no pueden ser porque no tenemos elementos de orden 9 y veamos cuántos hay del segundo tipo. Están generados por un elemento de orden 3 y otro de orden 6 cuyo cuadrado no es el de orden 3. Son:

$$<(1,0),(0,2)>, <(0,1),(2,0)>, <(1,1),(2,0)>.$$

y no puede haber más.

8) Por el Teorema fundamental de la teoría de Galois, como la extensión $L|\mathbb{Q}$ es de Galois existe una biyección entre los subgrupos de $G(L:\mathbb{Q})$ de orden $d$ y las subextensiones de $L|\mathbb{Q}$ de grado $\frac{[L:\mathbb{Q}]}{d}=\frac{36}{d}$.

Como hemos probado que hay un único subgrupo de orden 4 $(H_4)$, hay una única subextensión de grado $\frac{36}{4}=9$ que es $Fix(H_4)|\mathbb{Q}$

Como hemos probado que hay un único subgrupo de orden 9 $(H_9)$, hay una única subextensión de grado $\frac{36}{9}=4$ que es $Fix(H_9)|\mathbb{Q}$.

El subgrupo de orden 4 ~~está~~ formado por los 3 elementos de orden 2 que son $\varphi_{18}:\begin{matrix}\eta\to\eta\\ \xi\to\xi^8\end{matrix}$ $\varphi_{68}:\begin{matrix}\eta\to\eta^6\\ \xi\to\xi^8\end{matrix}$ $\varphi_{61}:\begin{matrix}\eta\to\eta^6\\ \xi\to\xi\end{matrix}$. $\Rightarrow \eta+\eta^6$ y $\xi+\xi^8$ quedan fijos por los automorfismos. Hay que probar que $\mathbb{Q}(\eta+\eta^6,\xi+\xi^8)$ tiene grado 9. Sabemos que $\mathbb{Q}(\eta+\eta^6)=\mathbb{Q}(\eta+\eta^{-1})$ tiene grado 3 porque 7 es primo y tenemos el diagrama $6\left[\begin{matrix}\mathbb{Q}(\eta)\\ 2|\\ \mathbb{Q}(\eta+\eta^{-1})\\ 3|\\ \mathbb{Q}\end{matrix}\right.$. También se cumple lo mismo para

$\underset{\overset{\shortparallel}{2\cos\frac{2\pi}{9}}}{}$ $\xi+\xi^8=\xi+\xi^{-1}\in\mathbb{R}$ porque $(t-\xi)(t-\xi^{-1})=t^2-t(\xi+\xi^{-1})+1\in\mathbb{Q}(\xi+\xi^{-1})[t]$ $\overset{\mathbb{R}}{\cup}$ y $\mathbb{Q}(\xi)\subset\mathbb{C}\setminus\mathbb{R}\Rightarrow[\mathbb{Q}(\xi):\mathbb{Q}(\xi+\xi^{-1})]$ es $\leq 2$ y mayor que $1\Rightarrow$ es 2.

$\Rightarrow$ Las extensiones $\mathbb{Q}(\eta+\eta^{-1})|\mathbb{Q}$ y $\mathbb{Q}(\xi+\xi^{-1})|\mathbb{Q}$ tienen grado 3.

Por otro lado hemos visto en algún ejercicio de clase (También está en el Apéndice F del libro) que $\mathbb{Q}(\eta+\eta^2+\eta^4)|\mathbb{Q}$ tiene grado 2 y $\mathbb{Q}(\xi^3)=\mathbb{Q}(e^{\frac{2\pi i}{3}})$ también tiene grado $2=\varphi(3)$.

Además, tanto $\eta+\eta^2+\eta^4$ como $\xi^3$ quedan fijos por todos los automorfismos de orden 3, es decir, todos los automorfismos de $H_9$.

Por tanto para probar que $\mathbb{Q}(\xi^3,\eta+\eta^2+\eta^4)=\mathrm{Fix}(H_9)$ basta ver que la extensión tiene grado 4.

A falta de demostrar que $\underbrace{[\mathbb{Q}(\eta+\eta^{-1},\xi+\xi^{-1}):\mathbb{Q}]=9 \text{ y } [\mathbb{Q}(\xi^3,\eta+\eta^2+\eta^4):\mathbb{Q}]}_{\text{Ver en "Cosas que quedaban por justificar" 1) y 6)}}$ $\overset{\shortparallel}{4}$

ya tenemos que $\mathrm{Fix}(H_9)=\mathbb{Q}(\xi^3,\eta+\eta^2+\eta^4)$ y

$\mathrm{Fix}(H_4)=\mathbb{Q}(\eta+\eta^{-1},\xi+\xi^{-1})$.

9) Nuevamente, por el Teorema fundamental de la teoría de Galois, el número de subextensiones de grado 2 es igual al número de subgrupos de orden $\frac{36}{2}=18$, que ya hemos visto que era 3.

Ya hemos visto en el apartado anterior que $\mathbb{Q}(\eta+\eta^2+\eta^4)|\mathbb{Q}$ y $\mathbb{Q}(\xi^3)=\mathbb{Q}(e^{\frac{2\pi i}{3}})$ tienen grado 2 y nos falta encontrar la tercera. La que falta por encontrar es, probablemente,

$\mathbb{Q}(\xi^3\cdot(\eta+\eta^2+\eta^4))$

10) Dos de las subextensiones de grado 3 tienen como generadores a $\{\eta+\eta^{-1}\}$ y a $\{\xi+\xi^{-1}\}$ según hemos visto en el apartado 8), es decir $[\mathbb{Q}(\eta+\eta^{-1}):\mathbb{Q}] = 3 = [\mathbb{Q}(\xi+\xi^{-1}):\mathbb{Q}]$. Falta justificar que son distintas. (Justificado en "Cosas que quedan por justificar" 5))

Dos de las subextenciones de grado 6 tienen como generadores a $\{\xi\}$ y $\{\eta\}$. Son distintas porque $\mathbb{Q}(\xi,\eta)=L$ que tiene grado 36.

Por tanto $[\mathbb{Q}(\xi):\mathbb{Q}] = 6 = [\mathbb{Q}(\eta):\mathbb{Q}]$.

De las subextensiones de grado 12 tenemos que dos conjuntos de generadores son: $\{\xi, \eta+\eta^2+\eta^4\}$ y $\{\eta, \xi^3\}$.

Falta justificar que $\mathbb{Q}(\xi,\eta+\eta^2+\eta^4) \neq \mathbb{Q}(\eta,\xi^3)$ y que de hecho tienen grado 12. (Se justifica al final en "Cosas que quedan por justificar" 2) y 3))

De las subextenciones de grado 18 tenemos que dos conjuntos de generadores son $\{\xi, \eta+\eta^{-1}\}$ y $\{\eta, \xi+\xi^{-1}\}$.

Falta justificar que son distintas y tienen grado 18. Se justifica en "Cosas que quedan por justificar" 4) y 7)

4) Ofrecemos como torre cíclica

$$\{id\} \triangleleft \mathbb{Z}_6 \triangleleft \mathbb{Z}_6\times\mathbb{Z}_6$$ donde cada factor es cíclico

ya que $\mathbb{Z}_6$ lo es y $\mathbb{Z}_6 \cong \frac{\mathbb{Z}_6\times\mathbb{Z}_6}{\mathbb{Z}_6}$.

Una torre de resolución es:

$$\mathbb{Q} \underset{\eta^7=1}{\subset} \mathbb{Q}(\eta) \underset{\xi^9=1}{\subset} \mathbb{Q}(\eta,\xi) = L$$

# Cosas que quedaban por justificar

1) $[\mathbb{Q}(\eta+\eta^2+\eta^4, \xi^3):\mathbb{Q}]=4$, es decir, $\mathbb{Q}(\eta+\eta^2+\eta^4)\neq\mathbb{Q}(\xi^3)$ porque ya hemos justificado que ambas tienen grado 2.
Si fueran iguales $\mathbb{Q}(\xi^3)$ sería una subextensión de $\mathbb{Q}(\eta)$ y $e^{\frac{2\pi i}{3}}\in\mathbb{Q}(e^{\frac{2\pi i}{7}})$. Podríamos entonces generar $e^{\frac{2\pi i}{21}}$ por un argumento de identidad de Bezut similar al usado en el apartado 1 y entonces $\mathbb{Q}(e^{\frac{2\pi i}{7}})=\mathbb{Q}(e^{\frac{2\pi i}{21}})$.
Pero $[\mathbb{Q}(e^{\frac{2\pi i}{21}}):\mathbb{Q}]=\varphi(21)=2\cdot 6=12\neq 6$.

2) $\mathbb{Q}(\xi,\eta+\eta^2+\eta^4)\neq\mathbb{Q}(\eta,\xi^3)$. ¡Si fueran iguales tendríamos que $\xi$ y $\eta$ están, por lo que la extensión sería $\mathbb{Q}(\xi,\eta)$ que tiene grado 36 y esto no puede ser porque vamos a ver que tienen grado 12 ambas.

3) $[\mathbb{Q}(\xi,\eta+\eta^2+\eta^4):\mathbb{Q}]=12=[\mathbb{Q}(\eta,\xi^3):\mathbb{Q}]$.

La segunda igualdad es clara por lo que hemos visto en 1) de "Cosas sin demostrar". Para la primera igualdad construimos el siguiente diagrama:

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\xi) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\xi+\xi^{-1}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\xi^3) \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Se tiene que cumplir que $\mathbb{Q}(\xi)=\mathbb{Q}(\xi^3,\xi+\xi^{-1})$ por los grados que tienen las extensiones ya que $\mathrm{mcd}(2,3)=1$.
Por tanto $\mathbb{Q}(\xi,\eta+\eta^2+\eta^4)=\mathbb{Q}(\xi^3,\xi+\xi^{-1},\eta+\eta^2+\eta^4)$ y tenemos el diagrama:

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\xi^3,\xi+\xi^{-1},\eta+\eta^2+\eta^4) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "12"] & \\
\mathbb{Q}(\xi^3,\eta+\eta^2+\eta^4) \arrow[dr, dash, "4"'] & & \mathbb{Q}(\xi+\xi^{-1}) \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

que demuestra la igualdad por ser 4 y 3 coprimos y por lo probado en 1 de "Cosas por justificar"

4) $\mathbb{Q}(\xi, \eta+\eta^{-1}) \neq \mathbb{Q}(\eta, \xi+\xi^{-1})$. Es claro porque si fueran iguales tendríamos a $\xi$ y $\eta$ y el orden de la extensión sería 36 y en ambos casos es menor o igual que $6 \cdot 3 = 18$.

5) $\mathbb{Q}(\eta+\eta^{-1}) \neq \mathbb{Q}(\xi+\xi^{-1})$. Si fueran iguales tendríamos el diagrama:

$$\begin{tikzcd}
 & \mathbb{Q}(\xi,\eta) \arrow[dl, dash] \arrow[dr, dash] \arrow[d, dash, "\leq 4"] & \\
\mathbb{Q}(\eta) \arrow[dr, dash, "2"'] & {} & \mathbb{Q}(\xi) \arrow[dl, dash, "2"] \\
 & \mathbb{Q}(\eta+\eta^{-1}) = \mathbb{Q}(\xi+\xi^{-1}) \arrow[d, dash, "3"] & \\
 & \mathbb{Q} &
\end{tikzcd} \quad \leq 12$$

y no puede ser porque la extensión tiene grado 36.

6) $[\mathbb{Q}(\eta+\eta^{-1}, \xi+\xi^{-1}) : \mathbb{Q}] = 9$

Sabemos que es 3, 6 y 9 pero 3 no es porque no son iguales. Argumentando igual que antes, si tuviera grado 6 tendríamos

$$\begin{tikzcd}
 & \mathbb{Q}(\eta,\xi) \arrow[dl, dash] \arrow[dr, dash] \arrow[d, dash, "\leq 4"] & \\
\mathbb{Q}(\xi+\xi^{-1},\eta) \arrow[dr, dash, "2"'] & {} & \mathbb{Q}(\eta+\eta^{-1},\xi) \arrow[dl, dash, "2"] \\
 & \mathbb{Q}(\xi+\xi^{-1},\eta+\eta^{-1}) \arrow[d, dash, "6"] & \\
 & \mathbb{Q} &
\end{tikzcd} \quad \leq 24.$$

y llegamos nuevamente a contradicción porque tiene grado 36.

7) $[\mathbb{Q}(\xi,\eta+\eta^{-1}) : \mathbb{Q}] = 18 = [\mathbb{Q}(\eta, \xi+\xi^{-1})]$

Argumentando de forma similar a en 3).

$$\begin{tikzcd}
 & \mathbb{Q}(\xi,\eta+\eta^{-1}) = \mathbb{Q}(\xi^3, \xi+\xi^{-1}, \eta+\eta^{-1}) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "18"] & \\
\mathbb{Q}(\xi^3) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\xi+\xi^{-1}, \eta+\eta^{-1}) \arrow[dl, dash, "9"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$mcd(2,9) = 1$

$$\begin{tikzcd}
 & \mathbb{Q}(\eta, \xi+\xi^{-1}) = \mathbb{Q}(\eta+\eta^{-1}, \eta+\eta^{2}+\eta^{4}, \xi+\xi^{-1}) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "18"] & \\
\mathbb{Q}(\eta+\eta^{-1}, \xi+\xi^{-1}) \arrow[dr, dash, "9"'] & & \mathbb{Q}(\eta+\eta^{2}+\eta^{4}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$mcd(2,9) = 1$