Algebra III (Doble grado Informática-Matemáticas)

Ejercicios 2ª Evaluación (Temas 3,4).

Ejercicio 1. *Sea* $f = x^4 - 5x^2 + 5 \in \mathbb{Q}[x]$ *(que es irreducible).*

(1) *Probar que* $\mathbb{Q}(f) = \mathbb{Q}\left(\sqrt{\frac{5+\sqrt{5}}{2}}\right)$ *(Indicación: Calcular las raíces de* f *y analizar los resultados de multiplicarlas entre sí).*

(2) *Describir los elementos del grupo* $G(f/\mathbb{Q})$*, calcular sus ordenes, y probar que este grupo es cíclico mostrando un generador del mismo.*

(3) *Describir el retículo de subgrupos de* $G(f/\mathbb{Q})$ *y, usando la conexión de Galois, el correpondiente retículo de subcuerpos de* $\mathbb{Q}(f)$*.*

Ejercicio 2. *Sea* $z = z_9$*.*

(1) *Determinar el polinomio* $Irr(z, \mathbb{Q})$ *y mostrar una base de la extensión* $\mathbb{Q}(z)/\mathbb{Q}$*.*

(2) *Describir el grupo* $G(\mathbb{Q}(z)/\mathbb{Q})$ *y calcular el orden de sus elementos ¿Qué tipo de grupo es?. Describir el retículo de subgrupos de* $G(\mathbb{Q}(z)/\mathbb{Q})$*.*

(3) *Describir* z^3 *en la forma* $a + bi$*, con* $a, b \in \mathbb{R}$*, y probar también que* $z + \overline{z}$ *es raíz del polinomio* $x^3 - 3x + 1$*. Usar esa información para describir el retículo de subcuerpos de* $\mathbb{Q}(z)$*. ¿Qué subcuerpo es* $\mathbb{Q}(z) \cap \mathbb{R}$*?*

② $z = z_9$

1) $Irr(z, \mathbb{Q}) = \Phi_9$,

$x^9 - 1 = \Phi_1 \cdot \Phi_3 \cdot \Phi_9$, sabemos que $\Phi_1 = x-1$, $\Phi_3 = x^2+x+1$

Luego $\Phi_9 = \dfrac{x^9-1}{(x-1)(x^2+x+1)} = x^6 + x^3 + 1 = Irr(z, \mathbb{Q})$

Es de grado 6, luego $[\mathbb{Q}(z):\mathbb{Q}] = 6$ y una base es:

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

2) Por teoría sabemos que

$G(\mathbb{Q}(z)/\mathbb{Q}) \cong \mathbb{Z}_9^\times = \{1, 2, 4, 5, 7, 8\}$

Y sus componentes son las 6 $\mathbb{Q}$-inmersiones cuya imagen del generador es:

	σ_1	σ_2	σ_4	σ_5	σ_7	σ_8
$z \mapsto$	z	z^2	z^4	z^5	z^7	z^8

Orden?

* $ord(\sigma_1) = 1$, $\sigma_1(z) = z$
* $\sigma_2^2(z) = \sigma_2(z^2) = z^4 = \sigma_4(z)$

$\sigma_2^3(z) = \sigma_2(z^4) = z^8 = \sigma_8(z)$

$\sigma_2^4(z) = \sigma_2(z^8) = z^7 = \sigma_7(z)$

$\sigma_2^5(z) = \sigma_2(z^7) = z^5 = \sigma_5(z)$

$\sigma_2^6(z) = \sigma_2(z^5) = z = \sigma_1$

$ord(\sigma_2) = 6$

Y además $G = \langle\sigma_2\rangle$

$\Rightarrow G$ es un grupo cíclico

* $\left.\begin{array}{l} \sigma_4^2 = (\sigma_2^2)^2 = \sigma_2^4 = \sigma_7 \\ \sigma_4^3 = (\sigma_2^2)^3 = \sigma_2^6 = \sigma_1 \end{array}\right\} ord(\sigma_4) = 3$

* $\left.\begin{array}{l} \sigma_5^2 = (\sigma_2^5)^2 = \sigma_2^{10} = \sigma_7 \\ \sigma_5^3 = (\sigma_2^5)^3 = \sigma_2^{15} = \sigma_2^3 = \sigma_8 \\ \sigma_5^4 = (\sigma_2^5)^4 = \sigma_2^{20} = \sigma_2^2 = \sigma_4 \\ \sigma_5^5 = (\sigma_2^5)^5 = \sigma_2^{25} = \sigma_2 \\ \sigma_5^6 = (\sigma_2^5)^6 = \sigma_2^{30} = \sigma_1 \end{array}\right\} ord(\sigma_5) = 6$

* $\sigma_7^2 = (\sigma_2^4)^2 = \sigma_2^8 = \sigma_2^2 = \sigma_4$
  $\sigma_7^3 = (\sigma_2^4)^3 = \sigma_2^{12} = \sigma_1$ $\Big\}$ $\operatorname{ord}(\sigma_7) = 3$

* $\sigma_8^2 = (\sigma_2^3)^2 = \sigma_2^6 = \sigma_1$ $\}$ $\operatorname{ord}(\sigma_8) = 2$

Retículo de subgrupos: Los subgrupos propios de un grupo cíclico son subgrupos cíclicos de orden divisor del orden del grupo, por tanto:

$$\begin{tikzcd}
 & G(\mathbb{Q}(z)/\mathbb{Q}) & \\
\langle\sigma_7\rangle = \langle\sigma_4\rangle \arrow[ur, "2"] & & \langle\sigma_8\rangle \arrow[ul, "3"'] \\
 & \{\sigma_1\} \arrow[ul, "3"] \arrow[ur, "2"'] &
\end{tikzcd}$$

(3) $z^3 = e^{i\frac{2\pi\cdot 3}{9}} = e^{i\frac{6\pi}{9}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$; $z^3 + \bar{z}^3 = -1$ $(*)$
$z\bar{z} = 1$ $(**)$

$$(z+\bar{z})^3 - 3(z+\bar{z}) + 1 = z^3 + \bar{z}^3 + 3z^2\bar{z} + 3z\bar{z}^2 - 3z - 3\bar{z} + 1 =$$

$$= \underbrace{z^3 + \bar{z}^3 + 1}_{=0\ (*)} + \underbrace{3z}_{(**)} + \underbrace{3\bar{z}}_{(**)} - 3z - 3\bar{z} = 0$$

En efecto, $z+\bar{z}$ es raíz de $x^3 - 3x + 1$

Por conexión de Galois, necesariamente:

$\mathbb{Q}(z)^{G(\mathbb{Q}(z)/\mathbb{Q})} = \mathbb{Q}$ y $\mathbb{Q}(z)^{\{\sigma_1\}} = \mathbb{Q}(z)$

Además, como $[G(\mathbb{Q}(z)/\mathbb{Q}) : \langle\sigma_4\rangle] = 2$, necesariamente

$[\mathbb{Q}(z)^{\langle\sigma_4\rangle} : \mathbb{Q}] = 2$

Como $[G(\mathbb{Q}(z)/\mathbb{Q}) : \langle\sigma_8\rangle] = 3$, necesariamente

$[\mathbb{Q}(z)^{\langle\sigma_8\rangle} : \mathbb{Q}] = 3$

$$
\begin{tikzcd}
 & \mathbb{Q} \arrow[dl, "2"'] \arrow[dr, "3"] & \\
\mathbb{Q}(z)^{\langle\sigma_4\rangle} \arrow[dr, "3"'] & & \mathbb{Q}(z)^{\langle\sigma_8\rangle} \arrow[dl, "2"] \\
 & \mathbb{Q}(z) &
\end{tikzcd}
$$

$\mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(z^3) \leq \mathbb{Q}(z)^{\langle\sigma_4\rangle}$ pues $\sigma_4(z^3) = \sigma_4(z)^3 = z^{12} = z^3 \Rightarrow \mathbb{Q}(z)^{\langle\sigma_4\rangle} = \mathbb{Q}(i\sqrt{3})$

(5) Observamos que $z^6 = z^{-1} = \bar{z}$, el conjugado de z. Por tanto $\sigma_6 : z \mapsto z^6$ es justamente la restricción del automorfismo de conjugación compleja $a + bi \mapsto a - bi$.

(6) Es claro entonces que el número $z + \bar{z}$ queda fijo por σ_6. Entonces $\cos\frac{2\pi}{7} = \frac{1}{2}(z + \bar{z}) \in \mathbb{Q}(z)^{\sigma_6}$. Como la extensión $\mathbb{Q}(z)^{\sigma_6}/\mathbb{Q}$ es de grado 3, y $\mathbb{Q}(\cos\frac{2\pi}{7})/\mathbb{Q}$ es también de grado tres (ver Ejercicio 7), concluimos que

$$\mathbb{Q}(z)^{\sigma_6} = \mathbb{Q}(\cos(2\pi/7))\,.$$

(6)

$$
\begin{tikzcd}
 & \mathbb{Q} \arrow[dl, "2"'] \arrow[r, "3"] & \mathbb{Q}(\cos(2\pi/7)) \arrow[dl, "2"] \\
\mathbb{Q}(i\sqrt{7}) \arrow[r, "3"'] & \mathbb{Q}(z_7) &
\end{tikzcd}
$$

$\Rightarrow \mathbb{Q}(\frac{1}{2}(z+\bar{z})) = \mathbb{Q}(\cos(\frac{2\pi}{9})) \leq \mathbb{Q}(z)^{\langle\sigma_8\rangle}$

$\underbrace{\mathbb{Q} \overset{3}{\leq} \mathbb{Q}(\cos(\tfrac{2\pi}{9})) \overset{=}{\underset{1}{\leq}} \mathbb{Q}(z)^{\langle\sigma_8\rangle}}_{3}$

$Irr(z+\bar{z}, \mathbb{Q}) = x^3 - 3x + 1$

$\mathbb{Q}(z) \cap \mathbb{R} = \mathbb{Q}(\cos(\frac{2\pi}{9}))$

Ejercicio 7. *Sea $n > 2$ y $z = z_n$ la raíz n-ésima primitiva de la unidad.*

(1) *Observando que $(z + \bar{z}) = 2\cos\frac{2\pi}{n}$, probar que z y $\bar{z}$ son las raíces del polinomio $x^2 - 2\cos\frac{2\pi}{n}x + 1 \in \mathbb{R}[x]$.*

(2) *Argumentar que $\mathbb{Q}(\cos\frac{2\pi}{n}) \leq \mathbb{Q}(z)$, pero $\mathbb{Q}(\cos\frac{2\pi}{n}) \neq \mathbb{Q}(z)$.*

(3) *Probar que $Irr(z, \mathbb{Q}(\cos\frac{2\pi}{n})) = x^2 - 2\cos\frac{2\pi}{n}x + 1$ y que $[\mathbb{Q}(z) : \mathbb{Q}(\cos\frac{2\pi}{n})] = 2$.*

(4) *Probar que $[\mathbb{Q}(\cos\frac{2\pi}{n}) : \mathbb{Q}] = \varphi(n)/2$ y que el polinomio $Irr(\cos\frac{2\pi}{n}, \mathbb{Q})$ es de grado $\varphi(n)/2$.*

Indicación de solución: (1) Puesto que $z^{-1} = \bar{z}$, tenemos las igualdades $z\bar{z} = 1$ y $z + \bar{z} = 2\cos(\frac{2\pi}{n})$, de donde el z y $\bar{z}$ son las raíces raíz del polinomio $x^2 - 2\cos(\frac{2\pi}{n})x + 1$.

(2) $\cos(\frac{2\pi}{n}) = \frac{1}{2}(z + \bar{z}) = \frac{1}{2}(z + z^{n-1}) \in \mathbb{Q}(z)$. Los cuerpos son distintos pues $\mathbb{Q}(\cos\frac{2\pi}{n}) \leq \mathbb{R}$ y $z \notin \mathbb{R}$ al ser $n \geq 3$.

(4) Se deduce de los apartados anteriores, teniendo en cuenta la torre

$$\mathbb{Q} \leq \mathbb{Q}(\cos(2\pi/n)) \leq \mathbb{Q}(z).$$