Relación de problemas

Tema 3: Teoría de Galois.

Ejercicio 3.1. Encontrar el polinomio mínimo de los números complejos $\alpha = \frac{\sqrt{5}+1}{2}$ y $\beta = \frac{\sqrt{5}(i-1)}{2}$.

Ejercicio 3.2. Calcular $\left[\mathbb{Q}(\sqrt{1+\sqrt{3}}) : \mathbb{Q}\right]$.

Ejercicio 3.3. Sean L y K subcuerpos de $\mathbb{C}$ con $K \subset L$. Probar que si $[L : K]$ es primo, entonces para todo elemento $\alpha \in L \setminus K$ se verifica que $L = K(\alpha)$.

Ejercicio 3.4. Sea $\alpha \in \mathbb{C}$ un elemento algebraico. Demostrar que si el grado de α es impar, entonces $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\alpha)$.

Ejercicio 3.5. Sean α, β números algebraicos tales que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = m$ y $[\mathbb{Q}(\beta) : \mathbb{Q}] = n$. Demostrar que

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = n \iff [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)] = m,$$

y que estas condiciones se cumplen si m y n son primos entre sí, en cuyo caso $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = mn$. Dar un ejemplo en el que se verifique la condición sin que m y n sean primos entre sí.

Ejercicio 3.6. Sea $m, n \in \mathbb{Z}$. Probar que $\mathbb{Q}\left(\sqrt{m} + \sqrt{n}\right) = \mathbb{Q}(\sqrt{m}, \sqrt{n})$. Si $m \neq n$ entonces se tiene que $\mathbb{Q}\left(\sqrt{m} - \sqrt{n}\right) = \mathbb{Q}(\sqrt{m}, \sqrt{n})$.

Ejercicio 3.7. Dar una base de $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}\right)$ como espacio vectorial sobre $\mathbb{Q}$. Expresar en dicha base $1/\left(\sqrt{2} + \sqrt{3} + \sqrt{5}\right)$.

Ejercicio 3.8. Sean m y n enteros. Dar una condición necesaria y suficiente para que $\mathbb{Q}\left(\sqrt{m}\right)$ y $\mathbb{Q}\left(\sqrt{n}\right)$ sean isomorfos como espacios vectoriales. Idem como cuerpos.

Ejercicio 3.9. Sea m un entero. Calcular el grupo de automorfismos (como anillo) del cuerpo $\mathbb{Q}\left(\sqrt{m}\right)$ y dar la expresión matricial de cada uno de ellos en función de una base.

Ejercicio 3.10. Sea $\alpha \in \mathbb{C}$ algebraico. Para cada $\beta \in \mathbb{Q}[\alpha]$, definimos $F(\beta) = \alpha\beta$. Probar que F es un endomorfismo de $\mathbb{Q}[\alpha]$ como $\mathbb{Q}$-espacio vectorial. Hallar el polinomio característico $\det(\lambda\ \mathrm{id} - F)$ de F.

Ejercicio 3.11. Sea $\alpha \in \mathbb{C}$ una raíz del polinomio $X^3 + 2X^2 + 3X - 2$. Se pide:

1. Hallar $[\mathbb{Q}[\alpha] : \mathbb{Q}]$.
2. Encontrar el polinomio mínimo de $1 + \alpha$ sobre $\mathbb{Q}$.

3. Calcular el inverso de $1-\alpha^2$ como combinación lineal de elementos de una base de $\mathbb{Q}[\alpha]$.

Ejercicio 3.12. Sean los números complejos $\alpha = \sqrt{1+\sqrt{2}}$ y $\beta = \sqrt{1-\sqrt{2}}$. Se pide:

1. Hallar el polinomio mínimo $f(X)$ de β sobre $\mathbb{Q}$, y el valor de $[\mathbb{Q}[\beta] : \mathbb{Q}]$.
2. Probar que el polinomio mínimo de α sobre $\mathbb{Q}$ es también $f(X)$.
3. Hallar $[\mathbb{Q}[\alpha, \beta] : \mathbb{Q}]$.

Ejercicio 3.13. Consideremos la siguiente extensión de cuerpos: $\mathbb{Q} \subset K = \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}]$. Se pide:

1. Calcular el grado de la extensión $[K : \mathbb{Q}]$.
2. Probar que $\alpha = \sqrt{2} + \sqrt[3]{2}$ es elemento *primitivo*, esto es, que $K = \mathbb{Q}[\alpha]$.
3. Dar la lista de todos los subcuerpos L verificando $\mathbb{Q} \subset L \subset K$ con $[L : \mathbb{Q}] = 2$.

Ejercicio 3.14.

1. Si sabemos que el polinomio $X^4 + 4$ es producto de dos polinomios irreducibles de $\mathbb{Q}[X]$, ¿qué grado tienen estos polinomios? Calcular dichos factores irreducibles.
2. Si α es el número complejo $\sqrt{2i}$ determinar $[\mathbb{Q}[\alpha] : \mathbb{Q}]$.
3. Razonar si alguna de las siguientes igualdades es cierta:
   a) $\mathbb{Q}(\alpha) = \mathbb{Q}(i)$.
   b) $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2})$.

Ejercicio 3.15. Sea $\beta \in \mathbb{C}$ una raíz del polinomio $F(X) = X^3 - 3X + 1$ y $K = \mathbb{Q}(\beta)$.

1. Calcular el grado de la extensión $[K : \mathbb{Q}]$.
2. Sea $m : K \to K$ la aplicación $\mathbb{Q}$-lineal definida por $m(c) = (1+\beta^2)c$ para cada $c \in K$. Calcular la matriz de m respecto de alguna $\mathbb{Q}$-base de K, así como su polinomio característico.

Ejercicio 3.16. Sea $\mathbb{K}$ un cuerpo y $a \in \mathbb{K}$ un elemento tal que $f(X) = X^n - a$ es un polinomio irreducible. Si m es un divisor de n y α es una raíz de $f(X)$ en alguna extensión de $\mathbb{K}$, calcular el polinomio mínimo de α^m sobre $\mathbb{K}$.

Ejercicio 3.17. Sea $a = \tan\frac{2\pi}{5}, c = \sec\frac{2\pi}{5}$.

1. Calcular el polinomio mínimo de a sobre $\mathbb{Q}$.
2. Calcular el polinomio mínimo de c sobre $\mathbb{Q}$.
3. Expresar $\cos\frac{2\pi}{5}$ mediante radicales.

Ejercicio 3.18. Sea $\alpha = \frac{2k\pi}{7}$. Comprobar que $\cos 4\alpha - \cos 3\alpha = 0$ y deducir el polinomio mínimo de $\cos\alpha$ sobre $\mathbb{Q}$.

Ejercicio 3.19. Sea p un número primo y $a \in \mathbb{Z}/p\mathbb{Z}$. Sea α una raíz del polinomio $f(X) = X^p - X - a$. Expresar las raíces de $f(X)$ en función de α y encontrar un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Z}/p\mathbb{Z}$.

Ejercicio 3.20. Construir cuerpos de descomposición de los polinomios $X^3 + 2X + 1$ y $X^3 + X^2 + X + 2$ sobre $\mathbb{Z}/3\mathbb{Z}$. Determinar si son isomorfos y, en tal caso, calcular un isomorfismo.

Ejercicio 3.21. Sea $f(X) \in \mathbb{Q}[X]$ un polinomio irreducible de grado n, y $\mathbb{K}$ un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$. Demostrar que $[\mathbb{K} : \mathbb{Q}]$ divide a $n!$.

Ejercicio 3.22. Calcular $\mathbb{K}$ un cuerpo de descomposición de $X^5 - 2$ sobre $\mathbb{Q}$. Determinar $[\mathbb{K} : \mathbb{Q}]$.

Ejercicio 3.23. Sea $\mathbb{Q} \subset \mathbb{K}$ una extensión de cuerpos tal que $[\mathbb{K} : \mathbb{Q}] = 2$. Probar que existe $d \in \mathbb{Z}$ libre de cuadrados tal que $\mathbb{K} = \mathbb{Q}[\sqrt{d}]$.

Ejercicio 3.24. Sea $\mathbb{Q}[\alpha]$ una extensión de $\mathbb{Q}$, donde α es raíz del polinomio $X^3 + 2X^2 + 3X - 2$.

1. Probar que el grado de la extensión es 3.
2. Calcular el polinomio mínimo de $1 + \alpha$ y $1 + \alpha + \alpha^2$ sobre $\mathbb{Q}$.
3. Expresar $\frac{1}{1+5\alpha-7\alpha^2}$ como combinación lineal de los elementos de una base de la extensión.

Ejercicio 3.25. Sea $\mathbb{K}$ una extensión finita de k de grado n y tomemos un elemento $y \in \mathbb{K}$. Probar que el grado del polinomio mínimo de y sobre k es un divisor de n. En particular, si n es primo y el elemento $y \notin k$, entonces el grado del polinomio mínimo de y sobre k es n. Deducir que $\mathbb{K} = k[y]$.

Ejercicio 3.26. Sean α, β números algebraicos sobre $\mathbb{Q}$, de grados respectivos m y n. Probar que $[\mathbb{Q}[\alpha + \beta] : \mathbb{Q}] \leq mn$. Dar un ejemplo en el que se verifique la igualdad.

Ejercicio 3.27. Encontrar el polinomio mínimo del número complejo $\alpha = \frac{\sqrt{2}+1}{2}$ y calcular $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Ejercicio 3.28.

1. Encontrar el polinomio mínimo del número complejo $\beta = \frac{\sqrt{2}(i-1)}{2}$.
2. Averiguar si $\mathbb{Q}(i) \subset \mathbb{Q}(\beta)$ y, en caso afirmativo, hallar el grado de la extensión.
3. Hallar $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}]$.
4. Averiguar si $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\beta)$.

Ejercicio 3.29. Sea α un elemento algebraico sobre k, $f(X) \in k[X]$ su polinomio mínimo sobre k. Expresar el inverso de α como polinomio en α con coeficientes en k.

Ejercicio 3.30. Sea $\alpha \in \mathbb{C}$ una raíz de $X^3 + 3X + 1 = 0$.

1. Hallar $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.
2. Encontrar el polinomio mínimo de $\alpha^2 + 1$.
3. Expresar el inverso del número anterior como polinomio en α con coeficientes racionales.

Ejercicio 3.31.
1. Demostrar que $X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$ es irreducible sobre $\mathbb{Q}$.
2. Si $\alpha = e^{2\pi i/5} \in \mathbb{C}$, hallar $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.
3. Hallar el polinomio mínimo de $\cos \frac{2\pi}{5} = \frac{\alpha+\alpha^4}{2}$ sobre $\mathbb{Q}$.
4. Hallar un entero d tal que $\mathbb{Q}(\cos \frac{2\pi}{5}) = \mathbb{Q}(\sqrt{d})$.

Ejercicio 3.32.
1. Demostrar que $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$ es irreducible sobre $\mathbb{Q}$.
2. Si $\alpha = e^{2\pi i/7} \in \mathbb{C}$, hallar $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.
3. Hallar el polinomio mínimo de $\cos \frac{2\pi}{7} = \frac{\alpha+\alpha^6}{2}$ sobre $\mathbb{Q}$.

Ejercicio 3.33. Supongamos que tenemos las extensiones de cuerpos $k \subset \mathbb{L} \subset \mathbb{L}[\alpha]$, y que $[k[\alpha] : k]$ y $[\mathbb{L} : k]$ son primos entre sí. Probar que el polinomio mínimo de α sobre $\mathbb{L}$ tiene sus coeficientes en k.

Ejercicio 3.34. Calcular un cuerpo de descomposición de $X^p - 2 \in \mathbb{Q}[X]$, p primo, y su grado sobre $\mathbb{Q}$.

Ejercicio 3.35. Calcular un cuerpo de descomposición sobre $\mathbb{Q}$ de los siguientes polinomios:

1. $X^2 - p$, con $p > 0$ y primo.
2. $X^4 - 8X^2 + 15$.
3. $X^4 + 1$.

Ejercicio 3.36. Sea k un cuerpo, $a \in k$ y p, q enteros positivos y primos entre sí.

1. Probar que z es raíz de $X^{pq} - a$ si y sólo si z^q es raíz de $X^p - a$.
2. Si $X^p - a, X^q - a$ son polinomios irreducibles sobre k, entonces $[k[z^p] : k] = q$ y $[k[z^q] : k] = p$.
3. $X^{pq} - a$ es irreducible sobre k si y sólo si $X^p - a$ y $X^q - a$ son irreducibles sobre k.

Ejercicio 3.37. Sea $a \in \mathbb{Q}$ un número racional que no sea el cubo de ningún número racional.

1. ¿Cuál es el grado de un cuerpo de descomposición del polinomio $X^3 - a$ sobre $\mathbb{Q}$?
2. Si z_1, z_2, z_3 son las raíces de $X^3 - a$ en $\mathbb{C}$, ¿son iguales $\mathbb{Q}[z_1], \mathbb{Q}[z_2], \mathbb{Q}[z_3]$?

Ejercicio 3.38. Sea $\mathbb{K}$ una extensión de k, con $[\mathbb{K} : k] = p$, y $g(X) \in k[X]$ un polinomio irreducible de grado q, primo con p. Probar que $g(X)$ es irreducible sobre $\mathbb{K}[X]$.

Ejercicio 3.39. Sea $K|k$ una extensión y $\alpha \in K$. Probar que α es algebraico sobre k si y solamente si la extensión $k(\alpha)|k$ es finita.

Ejercicio 3.40. Sea $\alpha = \sqrt[3]{2}$

1. Calcular $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ y escriba una base de $\mathbb{Q}(\alpha)$ como $\mathbb{Q}$-espacio vectorial.
2. Escribir la expresión en la misma del elemento $1/\sqrt[3]{2}$
3. Calcular el polinomio mínimo de $\alpha^2 - 1$ sobre $\mathbb{Q}$.
4. Expresar el inverso del número anterior como polinomio en α con coeficientes racionales.
5. Calcular los automorfismos del cuerpo K que dejan fijo a $\mathbb{Q}$.

Ejercicio 3.41. Sea $p \in \mathbb{Z}$ un número primo, y $\zeta = \exp(2\pi i/p)$ raíz p-ésima de la unidad. Probar que un cuerpo de descomposición del polinomio $X^p - 1$ sobre $\mathbb{Q}$ es $\mathbb{Q}[\zeta]$, y que $[\mathbb{Q}[\zeta] : \mathbb{Q}] = p - 1$.

Ejercicio 3.42. Sea $p \in \mathbb{Z}$ un número primo, y $\zeta = \exp(2\pi i/p)$ raíz p-ésima de la unidad. Probar que un cuerpo de descomposición del polinomio $X^p - 2$ sobre $\mathbb{Q}$ es $K = \mathbb{Q}[\sqrt[p]{2}, \zeta]$, y que $[K : \mathbb{Q}] = p(p-1)$.

Ejercicio 3.43. Sea $\rho = \exp(2\pi i/3) = \frac{-1+\sqrt{3}i}{2}$ raíz cúbica de la unidad, y consideremos el cuerpo $K = \mathbb{Q}[\sqrt[3]{2}, \rho]$. Sea σ el automorfismo de K definido por

$$\sigma(\sqrt[3]{2}) = \rho\sqrt[3]{2}, \sigma(\rho) = \rho.$$

Probar que el conjunto de elementos de K que quedan fijos por la acción de σ es $\mathbb{Q}[\rho]$.

Ejercicio 3.44. Sea $\omega = \exp(2\pi i/7)$ y $\alpha = \omega + \omega^{-1}$.

1. Probar que ω es raíz del polinomio cuadrático $X^2 - \alpha X + 1$ sobre $\mathbb{Q}[\alpha]$.
2. A partir del polinomio mínimo de ω sobre $\mathbb{Q}$, calcular el polinomio mínimo de α sobre $\mathbb{Q}$.

Ejercicio 3.45. Calcular un elemento primitivo de un cuerpo de descomposición del polinomio $X^5 - 2$ sobre $\mathbb{Q}$.

Ejercicio 3.46. Sea $\mathbb{K} = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Probar que $\mathbb{K}$ es de Galois. Calcular $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, sus subgrupos y sus cuerpos fijos correspondientes.

Ejercicio 3.47. Sea $f(X) \in \mathbb{Q}[X]$ un polinomio irreducible de grado 3, Δ su discriminante y fijemos $\delta = \sqrt{\Delta}$ una raíz cuadrada. Sea $\mathbb{L}$ un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$. Probar que

- Si $\delta \in \mathbb{Q}$ entonces $\mathrm{Gal}(\mathbb{L}|\mathbb{Q}) = A_3$.
- Si $\delta \notin \mathbb{Q}$ entonces $\mathrm{Gal}(\mathbb{L}|\mathbb{Q}) = S_3$.

Ejercicio 3.48. Calcular el grupo de Galois de las siguientes ecuaciones:

- $X^3 - 2 = 0$.
- $X^3 + X^2 + X + 1 = 0$.
- $X^3 - 3X + 4 = 0$.

Ejercicio 3.49. Sea $f(X) = X^4 + 1$, $\alpha = \sqrt{2}$.

1. Probar que $\mathbb{L} = \mathbb{Q}[\alpha, i]$ es un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$.
2. Calcular $[\mathbb{L} : \mathbb{Q}]$.
3. Probar que $\mathrm{Gal}(\mathbb{L}|\mathbb{Q})$ es isomorfo a $C_2 \times C_2$, donde C_2 es el grupo cíclico de 2 elementos.
4. A partir de los subgrupos de $\mathrm{Gal}(\mathbb{L}|\mathbb{Q})$ determinar los cuerpos intermedios $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{L}$.

Ejercicio 3.50. Consideremos las extensiones de cuerpos

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{K} \subset \mathbb{K}[\beta] = \mathbb{L}$$

donde

$$\beta^2 = \frac{1}{\sqrt{2}}\sqrt{3}(\sqrt{2}+1)(\sqrt{3}+1) \in \mathbb{K}.$$

1. Probar que las siguientes ecuaciones definen dos automorfismos ϕ_1, ϕ_2 de $\mathbb{L}$:

$$\phi_1(r) = r, \text{ para todo } r \in \mathbb{Q}, \phi_1(\sqrt{2}) = -\sqrt{2}, \phi_1(\sqrt{3}) = \sqrt{3}, \phi_1(\beta) = \tfrac{1}{1+\sqrt{2}}\beta$$
$$\phi_2(r) = r, \text{ para todo } r \in \mathbb{Q}, \phi_1(\sqrt{2}) = \sqrt{2}, \phi_1(\sqrt{3}) = -\sqrt{3}, \phi_2(\beta) = \beta\tfrac{\sqrt{2}}{\sqrt{3}+1}.$$

2. Probar que el grupo de automorfismos de $\mathbb{L}$ que deja invariante cada elemento de $\mathbb{Q}$ es isomorfo al grupo de los cuaterniones de orden 8

$$Q_8 = \langle x, y | x^2 = y^2, xyx = y, y^4 = 1 \rangle.$$

3. Probar que los subgrupos de Q_8 son 1, Q_8 y los grupos cíclicos generados por x^2, x, y y xy (sus órdenes respectivos son $2, 4, 4, 4$).
4. Mediante la aplicación del teorema fundamental de la teoría de Galois, calcular todos los cuerpos intermedios $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{L}$.

Ejercicio 3.51. Sea $f(X) = X^4 - 2$, $\alpha = \sqrt[4]{2}$.

1. Probar que $\mathbb{L} = \mathbb{Q}[\alpha, i]$ es un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$.
2. Calcular $[\mathbb{L} : \mathbb{Q}]$ y deducir que el grupo de Galois $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ tiene orden 8.
3. Consideremos los automorfismos de $\mathbb{L}$ definidos por

$$\sigma(r) = r \text{ para todo } r \in \mathbb{Q}, \sigma(\alpha) = \alpha i, \sigma(i) = i,$$
$$\tau(r) = r \text{ para todo } r \in \mathbb{Q}, \tau(\alpha) = \alpha, \tau(i) = -i.$$

   Probar que $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) = \langle \sigma, \tau \rangle$.
4. Demostrar que $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ es isomorfo a D_8, el grupo diédrico de 8 elementos, definido por $\langle x, y | x^4 = 1, y^2 = 1, xy = yx^3 \rangle$.
5. Calcular todos los subgrupos de D_8 (hay 10 en total).
6. Calcular todos los cuerpos intermedios $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{L}$.

Ejercicio 3.52. Sea $f(X) = X^3 - 7 \in \mathbb{Q}[X]$. Calcular $\mathbb{K}$ un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$ y los cuerpos intermedios $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{K}$. ¿Cuáles son cuerpos de descomposición?

Ejercicio 3.53. Se sabe que $f(X) = X^4 + X^3 + X^2 + X + 1 = \frac{X^5-1}{X-1}$ es un polinomio irreducible sobre $\mathbb{Q}$. Sean $\alpha = \cos\frac{2\pi}{5} + i \sin\frac{2\pi}{5} \in \mathbb{C}$, $K = \mathbb{Q}(\alpha)$ y G_f el grupo de Galois de f sobre $\mathbb{Q}$.

1. Deducir que $\{\alpha, \alpha^2, \alpha^3, \alpha^4\}$ son todas las raíces de f. Averigüe si K es un cuerpo de descomposición de f sobre $\mathbb{Q}$.
2. Calcular $|G_f|$.
3. Si $\sigma_j \in G_f$ viene dado por $\sigma_j(\alpha) = \alpha^j$, con $j = 1, 2, 3, 4$, deducir si $G_f = \langle \sigma_j \rangle$ para algún valor de j.
4. Numerando las raíces de f por $x_j = \alpha^j$, con $j = 1, 2, 3, 4$, identifique G_f con un subgrupo de S_4. Razonar si la conjugación en $\mathbb{C}$ define algún elemento de G_f.
5. Hallar todos los subgrupos de G_f.
6. Hallar todos los cuerpos intermedios entre $\mathbb{Q}$ y K. Deducir si $\mathbb{Q}(\cos\frac{2\pi}{5})$ y $\mathbb{Q}(\cos\frac{\pi}{5})$ son algunos de estos cuerpos. Hallar un valor $d \in \mathbb{Z}$, si existe, tal que $\mathbb{Q}(\cos\frac{2\pi}{5}) = \mathbb{Q}(\sqrt{d})$.

Ejercicio 3.54. Sea $f(X) = X^8 - 1 \in \mathbb{Q}[X]$ y α una raíz octava primitiva de la unidad, por ejemplo $\alpha = \frac{1}{2}(1+i)\sqrt{2}$. Sea K un cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$ y G el grupo de Galois de $f(X)$ sobre $\mathbb{Q}$.

1. Demostrar que $K = \mathbb{Q}[\alpha]$.
2. Hallar $[K : \mathbb{Q}]$.
3. Sea $\sigma \in G$. Probar que $\sigma(\alpha) = \alpha^k$ si y solamente si k es impar. Verifique si $\sigma^2 = id$.
4. Si llamamos $x_k = \alpha^k, k = 1, \ldots, 8$ a las raíces de $f(X)$, expresar G como subgrupo de S_8.

5. Hallar todos los subgrupos de G.

6. Razonar cuáles de los siguientes cuerpos son intermedios entre $\mathbb{Q}$ y K y justifique si hay alguno más:

$$\text{(a) } \mathbb{Q}[i], \quad \text{(b) } \mathbb{Q}[\sqrt{2}], \quad \text{(c) } \mathbb{Q}[\sqrt{-2}], \quad \text{(d) } \mathbb{Q}[\alpha^2], \text{(e) } \mathbb{Q}[\alpha+\alpha^2], \quad \text{(f) } \mathbb{Q}[\sqrt{3}]$$

Ejercicio 3.55. Sean $f(X) = X^6 + 1 \in \mathbb{Q}[X]$, $\omega \in \mathbb{C}$ una raíz de $X^2 + X + 1$, $K \subset \mathbb{C}$ un cuerpo de descomposición de f sobre $\mathbb{Q}$ y $G = \mathrm{Gal}(K|\mathbb{Q})$.

1. Demostrar que $K = \mathbb{Q}(\omega, i)$. Para ello demostrar primero que $x_1 = i$, $x_2 = -i$, $x_3 = i\omega$, $x_4 = -i\omega$, $x_5 = i\omega^2$, $x_6 = -i\omega^2$ son todas las raíces de f.

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

3. Con la notación del apartado 1), expresar G como subgrupo de S_6.

4. Hallar todos los subgrupos de G.

5. Razonar cuáles de los siguientes cuerpos son intermedios entre $\mathbb{Q}$ y K, y justificar si hay alguno más:

$$(a) \quad \mathbb{Q}(i) \quad (b) \quad \mathbb{Q}(\sqrt{2}) \quad (c) \quad \mathbb{Q}(\sqrt{3}) \quad (d) \quad \mathbb{Q}(\sqrt{-3}) \quad (e) \quad \mathbb{Q}(\omega) \quad (f) \quad \mathbb{Q}(i\omega)$$

Ejercicio 3.56. Sea $f(X) = 2X^5 - 10X + 5 \in \mathbb{Q}[X]$.

1. Probar que $f(X)$ es irreducible en $\mathbb{Q}[X]$ y que tiene 5 raíces distintas.

2. Deducir que G_f es isomorfo a un subgrupo de S_5.

3. Probar que 5 divide a $|G_f|$.

4. El teorema de Cauchy para grupos dice: si G es un grupo finito y p es un primo que divide a $|G|$, entonces G tiene un elemento de orden p. Con este resultado, probar que G_f tiene un elemento que se corresponde con un ciclo de orden 5 en S_5.

5. Comprobar que $f(-2) < 0, f(-1) > 0, f(1) < 0, f(2) > 0$, y deducir que $f(X)$ tiene exactamente 3 raíces reales.

6. Probar que el automorfismo definido por la conjugación está en G_f.

7. Deducir que $G_f \simeq S_5$. ¿Es $f(X)$ resoluble por radicales?

Ejercicio 3.57. Calcular el grupo de Galois de $X^4 - 5$ sobre $\mathbb{Q}[i]$.