Práctica 4: Grupos de Galois

$\boxed{1}$ Repasar o buscar cómo se clasifican todos los grupos finitos de orden menor que 12.

Nota. Un recurso que puede ser útil tener a mano en esta guía es el sitio

`https://groupprops.subwiki.org/`

$\boxed{2}$ En cada uno de los siguientes casos, calcular el grupo de Galois de E/K, donde E es un cuerpo de descomposición sobre K del polinomio $f \in K[X]$ dado:

(*a*) $f = X^2 - 3, \quad K = \mathbb{Q}$

(*b*) $f = (X^2 - 5)(X^2 - 7), \quad K = \mathbb{Q}$

(*c*) $f = X^4 - 2, \quad K = \mathbb{Q}(i)$

(*d*) $f = X^3 - 2, \quad K = \mathbb{Q}$

$\boxed{3}$ Sean K un cuerpo, $f \in K[X]$ un polinomio irreducible y separable de grado n y E un cuerpo de descomposición de f sobre K.

(*a*) Probar que $\mathrm{Gal}(E/K)$ es isomorfo a un subgrupo de S_n.

Sugerencia. Un elemento de $\mathrm{Gal}(E/K)$ queda determinado por su valor en las raíces de f.

(*b*) Deducir que $[E:K]$ es un divisor de $n!$.

$\boxed{4}$ Para cada una de las extensiones E/K del ejercicio $\boxed{2}$, hallar todas sus subextensiones, indicando cuáles son normales.

$\boxed{5}$ En cada uno de los siguientes casos, calcular el grupo de Galois de $E/\mathbb{Q}$ y determinar todas sus subextensiones de grado 2.

(*a*) $E = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$

(*b*) $E =$ cuerpo de descomposición de $X^4 - 2X^2 - 1$ sobre $\mathbb{Q}$.

$\boxed{6}$ Sea E un cuerpo de descomposición del polinomio $X^6 - 4X^3 + 1$ sobre $\mathbb{Q}$.

(*a*) Calcular $\mathrm{Gal}(E/\mathbb{Q})$.

(*b*) Calcular la cantidad de subextensiones de grado 6 de $E/\mathbb{Q}$.

(*c*) Determinar todas las subextensiones de grado 4 de $E/\mathbb{Q}$.

Sugerencia. En la guía anterior ya calcularon $[E:\mathbb{Q}]$.

$\boxed{7}$ **(Sylow, el regreso)** Sea E/K una extensión de Galois de grado $n = p^m \cdot s$, con $p \nmid s$.

(*a*) Probar que para todo k con $0 \le k < m$ existe una subextensión de E/K de grado $p^k \cdot s$.

(*b*) Probar que la cantidad de subextensiones de grado s de E/K es congruente a 1 módulo p y divide a s.

(*c*) Probar que si F_1/K y F_2/K son dos subextensiones de grado s, entonces son isomorfas. Deducir que una subextensión de grado s es normal si y sólo si es la única subextensión de ese grado.

8 Sea E/K una extensión de Galois de grado $2n$. Probar que la cantidad de subextensiones normales de grado n es igual a la cantidad de elementos de orden 2 en el centro de G.

Nota. El *centro* de un grupo G, que se denota $Z(G)$, es el conjunto de los elementos que conmutan con todos los elementos de G.

9 Sea $E = \mathbb{Q}\big(\sqrt[3]{2}, \sqrt{3}, i\big)$.

(a) Probar que $E/\mathbb{Q}$ es una extensión de Galois.

(b) Determinar todas las subextensiones de grado 2, 3 y 4 de $E/\mathbb{Q}$.

(c) ¿Existe alguna subextensión $F/\mathbb{Q}$ tal que $\mathrm{Gal}(E/F) \cong \mathbb{Z}_4$?

10 Sea K un cuerpo cuya característica no es 2 y sea E/K una extensión de Galois tal que $\mathrm{Gal}(E/K) = (\mathbb{Z}_2)^n$. Probar que existen $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$ tales que $\alpha_i^2 \in K$ para todo i y $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

11 Sean K un cuerpo cuya característica no es 2, $f = X^4 + bX^2 + c$ un polinomio irreducible en $K[X]$, y E un cuerpo de descomposición de f sobre K.

(a) Probar que si c es un cuadrado en K, entonces $\mathrm{Gal}(E/K) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) Probar que si $c(b^2 - 4c)$ es un cuadrado en K, entonces $\mathrm{Gal}(E/K) \cong \mathbb{Z}_4$.

12 Sea K un cuerpo cuya característica no es 2 y sea E/K una extensión de Galois tal que $\mathrm{Gal}(E/K) \cong \mathbb{Z}_4$. Probar que existen $a, b \in K$ con $b \notin K^2$ tales que E es un cuerpo de descomposición del polinomio $(X^2 - a)^2 - b$ sobre K.

13 (a) Probar que $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$.

(b) ¿Existe algún $n \in \mathbb{N}$ tal que $\sqrt[3]{2} \in \mathbb{Q}(\xi_n)$?

14 (a) Probar que $\mathbb{Q}(\xi_5)/\mathbb{Q}$ tiene una **única** subextensión $F/\mathbb{Q}$ de grado 2.

(b) Hallar el único $d \in \mathbb{Z}$ libre de cuadrados tal que $F = \mathbb{Q}(\sqrt{d})$.

15 Sean $p > 2$ primo y E un cuerpo de descomposición del polinomio $X^p - 2$ sobre $\mathbb{Q}$.

(a) Probar que $\mathrm{Gal}(E/\mathbb{Q}) \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z}/p\mathbb{Z},\ a \neq 0 \right\}$.

(b) Probar que E no contiene ninguna raíz p^2-ésima primitiva de la unidad.

16 Sea $E/\mathbb{Q}$ una extensión de Galois tal que $E \not\subseteq \mathbb{R}$. Probar que $[E : E \cap \mathbb{R}] = 2$.

17 Sean K un cuerpo, $f \in K[X]$ un polinomio separable de grado n y E un cuerpo de descomposición de f sobre K. Supongamos que $\mathrm{Gal}(E/K) \cong S_n$.

(a) Probar que f es irreducible en $K[X]$.

(b) Probar que si $\alpha \in \overline{K}$ es una raíz de f, entonces $K(\alpha)/K$ no tiene subextensiones propias.

18 Sean $p > 2$ un número primo y $f \in \mathbb{Q}[X]$ un polinomio irreducible de grado p que tiene exactamente dos raíces no reales. Sea E un cuerpo de descomposición de f sobre $\mathbb{Q}$. Probar que $\mathrm{Gal}(E/\mathbb{Q}) \cong S_p$.

Sugerencia. En S_p, si σ es un p-ciclo y τ es una trasposición, entonces $\langle \sigma, \tau \rangle = S_p$.

19 Probar que los elementos $\sigma = (12345)$ y $\tau = (12)(34)$ generan el grupo A_5.

Sugerencia. Encontrar un elemento de orden 3 en $\langle \sigma, \tau \rangle$ y usar que A_5 es *simple*, es decir no tiene subgrupos normales no triviales.

20 Sea $f \in \mathbb{Q}[X]$ un polinomio irreducible de grado 5 que tiene exactamente una raíz real, sean $\alpha, \overline{\alpha}, \beta, \overline{\beta}$ las otras raíces de f. Sea E un cuerpo de descomposición de f sobre $\mathbb{Q}$. Supongamos que existe un elemento $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ de orden 5 tal que $\sigma(\alpha) = \overline{\alpha}$ y $\sigma(\beta) = \overline{\beta}$. Probar que $\mathrm{Gal}(E/\mathbb{Q})$ es isomorfo a A_5 o a S_5.

21 Sea E un cuerpo de descomposición del polinomio $X^{12} - 3$ sobre $\mathbb{Q}$.

(a) Determinar todas las subextensiones de grado 8 de $E/\mathbb{Q}$.

(b) Determinar todas las subextensiones de grado 3 de $E/\mathbb{Q}$.

(c) Probar que $\mathrm{Gal}(E/\mathbb{Q})$ no es isomorfo a D_{12} ni a S_4.

Nota. Este puede ser muy cuentoso. Pueden no hacerlo si no les divierte, o pueden usarlo como excusa para investigar cómo hacer estas cuentas en la computadora.

22 Sea $E = \mathbb{C}(X)$. Consideremos los automorfismos f y g de E definidos por $g(X) = X^{-1}$ y $f(X) = \xi X$, donde ξ es una raíz n-ésima primitiva de la unidad. Probar que:

(a) $f^n = g^2 = \mathrm{id}_E$ y $fg = gf^{-1}$.

(b) El subgrupo H generado por f y g es isomorfo a D_n.

(c) $E^H = \mathbb{C}(X^n + X^{-n})$.

23 Sea $E = \mathbb{Z}/7\mathbb{Z}(X)$ y sea $\sigma \in \mathrm{Aut}(E)$ definido por $\sigma(X) = 2X$. Si H es el subgrupo de $\mathrm{Aut}(E)$ generado por σ, calcular E^H.