Práctica 4: Grupos de Galois

- Un **polinomio** $f \in K[X]$ es separable si no tiene raíces múltiples, es decir si no existe $\alpha \in \overline{K}$ tal que $(X-\alpha)^2 \mid f$.
- Un **elemento** $\alpha \in \overline{K}$ es separable sobre K si $m(\alpha, K)$ es un polinomio separable.
- Una **extensión** algebraica E/K es separable si todo elemento de E es separable sobre K.

1 Sea K un cuerpo cualquiera. Verificar que la función $\partial : K[X] \to K[X]$ dada por $\partial(f) = f'$ cumple las propiedades usuales de la derivada, que son ser K-lineal y la regla del producto $\partial(f \cdot g) = \partial(f) \cdot g + f \cdot \partial(g)$.

2 ¿Es cierto en cualquier cuerpo que $f' = 0$ sólo cuando f es constante?

3 Probar que $\alpha \in \overline{K}$ es raíz múltiple de f si y sólo si es raíz de f y de su polinomio derivado f'. Deducir que f es separable si y sólo si es coprimo con f'.

4 Sea $f \in K[X]$ un polinomio **irreducible**. Probar que f es separable si y sólo si $f' \neq 0$.

5 Sea K un cuerpo de **característica cero**. Probar que toda extensión algebraica E/K es separable.

6 Sea $\tau : K \to L$ un morfismo de cuerpos. Recordemos que τ induce naturalmente un morfismo de anillos de $K[X]$ en $L[X]$ que consiste en aplicar τ a cada coeficiente.

Sea $f \in K[X]$ un polinomio separable. Probar que $\tau(f)$ también es separable.

Sugerencia. Sería más fácil si pudiéramos aplicar τ al polinomio factorizado linealmente, ¿no? ¿Podemos?

7 Sea E/K una extensión separable finitamente generada. Probar que la cantidad de morfismos de extensiones $\sigma : E/K \to \overline{K}/K$ es exactamente $[E : K]$.

Sugerencia. Revisar el ejercicio 6 de la práctica 3 y hacer inducción.

Una extensión E/K es una *extensión de Galois* si es normal y separable. Dada una tal extensión, se define su *grupo de Galois* como

$$\mathrm{Gal}(E/K) := \{\sigma : E/K \to E/K \text{ automorfismo de extensiones}\}.$$

Recordar de la guía anterior que para extensiones algebraicas vale que $\mathrm{Aut}(E/K) = \mathrm{End}(E/K)$, y que si la extensión es normal entonces $\mathrm{End}(E/K) = \mathrm{Hom}(E/K, \overline{K}/K)$. Con esto y el ejercicio 7 se deduce que en una extensión de Galois finita el orden del grupo de Galois coincide con el grado de la extensión:

$$\boxed{|\mathrm{Gal}(E/K)| = [E : K]}.$$

8 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/`

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

10 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 $n!$.

Los dos ejercicios que siguen apuntan a probar el ***Teorema Fundamental de la Teoría de Galois***.

11 Sean E un cuerpo y G un subgrupo finito de $\mathrm{Aut}(E)$. Definimos

$$E^G := \{\alpha \in E \mid \sigma(\alpha) = \alpha \text{ para todo } \sigma \in G\}.$$

(*a*) Verificar que E^G es un subcuerpo de E, que se llama el *cuerpo fijo* de G.

(*b*) Dado $\alpha \in E$, la *órbita* de α por G es el conjunto $\mathcal{O}_G(\alpha) = \{\sigma(\alpha) \mid \sigma \in G\}$.[1] Sean $\beta_1, \beta_2, \ldots, \beta_r$ los elementos de la órbita de α. (Notar que podría pasar que $r < |G|$.) Consideramos el polinomio $f = (X-\beta_1)(X-\beta_2)\ldots(X-\beta_r)$. Probar que los coeficientes de f están en E^G.

(*c*) Deducir que E/E^G es una extensión de Galois. Observar que $G \subseteq \mathrm{Gal}(E/E^G)$.

12 En la situación del ejercicio anterior, sea $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ y sean $\alpha_1, \alpha_2, \ldots, \alpha_m$ elementos distintos de E, con $m > n$. Consideramos la matriz

$$A = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_m) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_m) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_m) \end{pmatrix} \in E^{n\times m}.$$

(*a*) Probar que para todo j entre 1 y n, $\sigma_j(A)$ (la matriz que se obtiene al aplicar σ_j a todas las entradas de A) tiene las mismas filas que A, posiblemente en otro orden.

(*b*) Probar que existen soluciones no triviales del sistema de ecuaciones $Ax = 0$.

Dentro de todas estas soluciones tomamos una que tenga la máxima cantidad posible de ceros, llamémosla $y = (y_1, y_2, \ldots, y_m)$. Sin pérdida de generalidad podemos suponer que $y_1 \neq 0$ (si no, sólo hay que renombrar los α_i, que es como permutar columnas de A). Más aún, multiplicando por una constante podemos suponer que $y_1 = 1$.

(*c*) Probar que para todo j entre 1 y n, el vector $\sigma_j(y) = (\sigma_j(y_1), \sigma_j(y_2), \ldots, \sigma_j(y_m))$ también es solución del mismo sistema de ecuaciones.

(*d*) Supongamos que existe algún i tal que $y_i \notin E^G$, es decir que existe j tal que $\sigma_j(y_i) \neq y_i$. Mostrar que entonces hay una solución no trivial del sistema que tiene más ceros que y, lo cual es un absurdo. Por lo tanto todas las coordenadas de y están en E^G.

(*e*) Recordando que uno de los elementos de G es la identidad, concluir que $\alpha_1, \alpha_2, \ldots, \alpha_m$ son linealmente dependientes sobre E^G.

(*f*) Deducir que $[E : E^G] \leq |G|$, y por lo tanto, $\mathrm{Gal}(E/E^G) = G$.

[1] Esto se corresponde con lo visto en Álgebra II sobre acciones de grupos: aquí G actúa en E vía $\sigma \cdot \alpha := \sigma(\alpha)$.

13 **(Teorema de Galois)** Sea E/K una extensión de Galois finita. Consideramos los conjuntos

$$\mathbb{I} = \{\text{subextensiones de } E/K\}, \qquad \mathbb{S} = \{\text{subgrupos de } \mathrm{Gal}(E/K)\}.$$

Podemos definir una función $\alpha : \mathbb{I} \to \mathbb{S}$ que a cada subextensión F/K le asigna $\mathrm{Gal}(E/F)$, y también una función $\beta : \mathbb{S} \to \mathbb{I}$ que a cada subgrupo H le asigna la subextensión E^H/K.

(*a*) Probar que α y β *invierten el orden* dado por la inclusión en $\mathbb{I}$ y en $\mathbb{S}$ respectivamente. Es decir, $F_1 \subseteq F_2 \Rightarrow \alpha(F_1) \supseteq \alpha(F_2)$, y análogamente para β.

(*b*) Probar que α y β son inversas, es decir:

- para toda subextensión F/K vale que $E^{\mathrm{Gal}(E/F)} = F$;
- para todo subgrupo H vale que $\mathrm{Gal}(E/E^H) = H$.

De modo que tenemos una biyección entre $\mathbb{I}$ y $\mathbb{S}$.[2]

(*c*) Probar que en esta biyección, para cada d, las **subextensiones de grado** d de E/K se corresponden con los **subgrupos de índice** d de $\mathrm{Gal}(E/K)$.

(*d*) Probar que en esta biyección, las **subextensiones normales** de E/K se corresponden con los **subgrupos normales** de $\mathrm{Gal}(E/K)$.

14 Para cada una de las extensiones E/K del ejercicio **9**, hallar todas sus subextensiones, indicando cuáles son normales.

15 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 $\mathbb{Q}$.

16 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 $[E : \mathbb{Q}]$.

17 **(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 $0 \leq k < m$ 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.

18 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.

[2] Más precisamente, tenemos un isomorfismo de posets entre $(\mathbb{I}, \subseteq)$ y $(\mathbb{S}, \subseteq)^{op}$.

19 Sean E/K una extensión de Galois finita y F/K una subextensión normal (notar que entonces F/K también es de Galois). Probar que $\mathrm{Gal}(F/K) \cong \mathrm{Gal}(E/K)/\mathrm{Gal}(E/F)$.

20 Sea L/K una extensión de Galois y sean E/K y F/K dos subextensiones finitas, con E/K normal.[3]

(*a*) Probar que $\mathrm{Gal}(EF/F) \cong \mathrm{Gal}(E/E \cap F)$.

Sugerencia. Es fácil definir un morfismo inyectivo $\Phi : \mathrm{Gal}(EF/F) \to \mathrm{Gal}(E/E \cap F)$. Para probar que $\mathrm{Im}(\Phi) = \mathrm{Gal}(E/E \cap F)$, basta probar que los correspondientes cuerpos fijos son iguales.

(*b*) Deducir que $[EF : F]$ **divide** a $[E : K]$, y si $E \cap F = K$ entonces esos grados son iguales.

(*c*) Mostrar que las afirmaciones de (*b*) son falsas si E/K no es normal, aún si EF/K lo es.

Sugerencia. Considerar subextensiones de $\mathbb{Q}(\sqrt[3]{2}, \xi_3)/\mathbb{Q}$.

21 Sean E/K y F/K dos extensiones finitas tales que EF/K es una extensión de Galois, $E \cap F = K$ y E/K es normal.

(*a*) Probar que $\mathrm{Gal}(EF/K)$ es producto semidirecto de $\mathrm{Gal}(EF/E)$ y $\mathrm{Gal}(EF/F)$.

(*b*) Probar que si F/K también es normal, entonces $\mathrm{Gal}(EF/K) \cong \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$.

22 Sea $E = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}, i\right)$.

(*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 $\mathrm{Gal}(E/F) \cong \mathbb{Z}_4$?

23 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 $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

24 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 $\mathrm{Gal}(E/K) \cong \mathbb{Z}_4$.

25 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.

Una extensión de cuerpos E/K se dice *abeliana* (respectivamente, *cíclica*) si es de Galois y $\mathrm{Gal}(E/K)$ es un grupo abeliano (respectivamente, cíclico).

26 (*a*) Probar que toda subextensión de una extensión abeliana también es abeliana.

(*b*) Probar que toda subextensión de una extensión cíclica también es cíclica.

27 Sea E/K una extensión cíclica de grado n. Probar que para cada divisor d de n, hay exactamente una subextensión de grado d.

[3] Recordar que esto último implica que EF/F también es normal. Ver ejercicio 9, práctica 3.

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

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

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

(*b*) Calcular el polinomio minimal de $\xi_5 + \xi_5^{-1}$ sobre $\mathbb{Q}$.

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

30 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.

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

32 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 $\langle \sigma, \tau \rangle = S_p$.

33 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.

34 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.

35 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.

36 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.