# 1. Introducción

Para el lector moderno es difícil seguir la famosa memoria de Galois (escrita alrededor de 1830) porque el lenguaje del álgebra no estaba desarrollado y porque los razonamientos de Galois no son del todo claros.

La propia definición del grupo de Galois de un polinomio $P$ ya parece tener poco que ver con la actual. A cambio, de alguna manera es más elemental pues no se necesitan grandes conocimientos teóricos de álgebra. A continuación describimos la definición original con una notación más moderna y algunas explicaciones. Si se quiere, para fijar ideas, se puede suponer $P \in \mathbb{Q}[x]$, aunque no es necesario y en cualquier extensión algebraica suya, e incluso con más generalidad, todo funcionaría igual.

1 Galois supone que $P$ no tiene raíces repetidas (notando que esto ocurre siempre que sea irreducible). Si $r_1, r_2, \ldots, r_n$ con $n = \partial P$ son las raíces (en $\mathbb{C}$, hoy en día pensaríamos en el cuerpo de descomposición), Galois "prueba" que existe una combinación lineal $\alpha = \lambda_1 r_1 + \cdots + \lambda_n r_n$ con $\lambda_j \in \mathbb{Z}$ tal que cada raíz se expresa racionalmente en función de $\alpha$. En lenguaje moderno, si el cuerpo base es $\mathbb{Q}$, para alguna elección de los $\lambda_j$, el cuerpo de descomposición es $\mathbb{Q}(\alpha)$.

2 Galois considera lo que hoy llamaríamos el polinomio mínimo de $\alpha$. Sean $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$ sus raíces (de nuevo en $\mathbb{C}$ o en el cuerpo de descomposición). Por el apartado anterior, existen funciones racionales sobre el cuerpo base $f_1, f_2, \ldots, f_n$ tales que $r_j = f_j(\alpha_1)$. Galois dice que por un resultado de Abel, $f_j(\alpha_k)$ es también raíz de $P$ cualesquiera que sean $1 \leq j \leq n$ y $1 \leq k \leq m$.

3 Finalmente, dentro de la demostración de un teorema (el antecesor de lo que hoy llamamos teorema fundamental de la teoría de Galois), considera la aplicación $(r_1, r_2, \ldots, r_n) \mapsto \big(f_1(\alpha_k), f_2(\alpha_k), \ldots, f_n(\alpha_k)\big)$. Para cada $1 \leq k \leq m$ se obtiene una permutación de las raíces. Estas permutaciones forman el GRUPO DE GALOIS.

# 2. Enunciados

**1)** Lee con atención los tres pasos descritos anteriormente y comprueba que con la definición original, el grupo de Galois de $P = x^4 - 7x^2 + 10 \in \mathbb{Q}[x]$ es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, concretamente dado por las permutaciones $(\sqrt{2}, \sqrt{5}) \mapsto (\pm\sqrt{2}, \pm\sqrt{5})$. Escribe explícitamente las funciones $f_j$ y las raíces $\alpha_j$ explicando cómo las has obtenido.

Para los siguientes ejercicios puedes utilizar lo que sabes de teoría de Galois "moderna".

**2)** [opcional] Explica por qué se cumple el resultado de Abel mencionado en $\boxed{2}$ y por qué las aplicaciones $(r_1, r_2, \ldots, r_n) \mapsto \big(f_1(\alpha_k), f_2(\alpha_k), \ldots, f_n(\alpha_k)\big)$ de $\boxed{3}$ son permutaciones. ¿Son todas distintas?

**3)** [opcional] Sigue las indicaciones del ejercicio 109 en la p.75 de *¡Qué bonita es la teoría de Galois!* y demuestra $\boxed{1}$.

**4)** [opcional] Demuestra que para cualquier polinomio $P \in \mathbb{Q}[x]$ sin raíces repetidas la definición original del grupo de Galois coincide con la actual.

# 3. Evaluación

La máxima calificación por hacer sólo el primer ejercicio es un 7.5. Si se hace además uno de los problemas opcionales puede aumentar hasta un 9, y hasta 10 si se hacen dos de ellos.