Grupos de Galois

En esta guía, si p es un número primo y $f = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$, entonces $\bar{f} = \bar{a}_n X^n + \cdots + \bar{a}_1 X + \bar{a}_0$ donde $\bar{a} \equiv a \mod p$.

Ejercicio 1. En este ejercicio se da un método para construir una extensión de Galois $E/\mathbb{Q}$ tal que $\mathrm{Gal}(E/\mathbb{Q}) = \mathbb{S}_n$.

(*a*) Sea $n > 3 \in \mathbb{N}$. Encontrar $f_1, f_2, f_3 \in \mathbb{Z}[X]$. tales que
  (*i*) $\mathrm{gr}\, f_1 = n$ y $\bar{f}_1 \in \mathbb{Z}_2[X]$ es irreducible.
  (*ii*) $\mathrm{gr}\, f_2 = n$ y $\bar{f}_2 \in \mathbb{Z}_3[X]$ se factoriza como $\bar{f}_2 = gh$ con $\mathrm{gr}\, g = n - 1$.
  (*iii*) $\mathrm{gr}\, f_3 = n$ y $\bar{f}_3 \in \mathbb{Z}_5[X]$ se factoriza como $\bar{f}_3 = gh$ o $\bar{f}_3 = gh_1h_2$ con g irreducible y cuadrático en $\mathbb{Z}_5[X]$ y h, h_1, h_2 polinomios irreducibles de grado impar en $\mathbb{Z}_5[X]$.

(*b*) Sea $f = -15f_1 + 10f_2 + 6f_3$. Probar que $f \equiv f_1 \mod 2$, $f \equiv f_2 \mod 3$ y $f \equiv f_3 \mod 5$.

(*c*) Probar que el grupo de Galois G de f es transitivo.
Ayuda: $\bar{f}$ es irreducible en $\mathbb{Z}_2[X]$.

(*d*) Probar que G contiene un ciclo de la forma $\zeta = (i_1 i_2 \dots i_{n-1})$ y un elemento $\sigma\tau$ donde σ es una trasposición y τ un producto de ciclos de orden impar. Por lo tanto, $\sigma \in G$ y $(i_k i_n) \in G$ para algún $1 \leq k \leq n-1$.

(*e*) Probar que $G = \mathbb{S}_n$.