Teoría Algebraica de Números - Práctica 2

2do. Cuatrimestre 2020

Cuerpos finitos y extensiones de Galois

(1) Para los siguientes polinomios en $\mathbb{Q}[x]$ hallar el grupo de Galois de su cuerpo de descomposición:

$$\text{i)} X^3 - 2 \qquad \text{ii)} (X^2-2)(X^2-3)$$
$$\text{iii)} X^4 - 2 \qquad \text{iv)} (X^4+1)(X^2+5)$$

(2) Dado el primo 11, encontrar un polinomio irreducible de grado 3 en $\mathbb{F}_{11}[x]$.

(3) Sea p un número primo.
- Calcular el número de polinomios mónicos irreducibles de grado 2 en $\mathbb{F}_p[x]$.
- ¿Cuál es la probabilidad de que un polinomio de grado 2 mónico en $\mathbb{F}_p[x]$ sea irreducible? (esperaban esta respuesta?).

(4) Como vimos en la teórica, el grupo multiplicativo de un cuerpo finito es cíclico.
- Probar (se puede usar computadora) que el número 2 genera al cuerpo finito de 101 elementos.
- El ítem anterior dice que todo elemento de $\mathbb{F}_{101}$ no nulo es una potencia de 2. Encontrar al entero a entre 1 y 100 tal que $2^a = 3$ (en $\mathbb{F}_{101}$). Este problema se llama el problema del *logaritmo discreto*. Es un problema computacionalmente difícil de resolver (no se conocen al momento algoritmos eficientes).

(5) Sea K un cuerpo, y L_1, L_2 extensiones finitas K.
   (a) Probar que existe un cuerpo M que es una extensión finita de K tal que tal que $L_1 \subset M$ y $L_2 \subset M$ (pensar que quiere decir estas contenciones).
   (b) Probar existe una mínima tal extensión, o sea que existe M extensión finita de K tal que si N es una extensión que contiene a L_1 y a L_2 entonces M está contenido en N. Deducir que M es único. A tal cuerpo lo denotamos por $L_1 \cdot L_2$.

(6) En las hipótesis del ejercicio anterior, supongamos que L_1 y L_2 son extensiones de Galois de K.
   (a) Probar que entonces $L_1 \cdot L_2$ es una extensión de Galois de K.
   (b) Por el ítem anterior tenemos una función
   $$\psi : \mathrm{Gal}(L_1 \cdot L_2/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K),$$
   dada por $\psi(\sigma) = (\sigma|_{L_1}, \sigma|_{L_2})$ (restringir el morfismo a cada cuerpo). Probar que ψ es un morfismo inyectivo.
   (c) ($\star$) Probar que si F, L son extensiones finitas de K ambas contenidas en un cuerpo M tales que F/K es Galois, probar que $F \cdot L/L$ es Galois y además
   $$\mathrm{Gal}(F \cdot L) \simeq \mathrm{Gal}(F/F \cap L),$$
   por la función restricción. Deducir que $[F \cdot L : L] = [F : F \cap L]$.
   (d) Probar que $[L_1 \cdot L_2 : K] = \frac{[L_1:K][L_2:K]}{[L_1 \cap L_2:K]}$.
   (e) Deducir que la función del segundo ítem es suryectiva si y sólo si $L_1 \cap L_2 = K$.

(7) Usar el ítem anterior para encontrar una extensión de $\mathbb{Q}$ con grupo de Galois: $\mathbb{Z}/6$, $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ y $S_3 \times \mathbb{Z}/2$.