Introducción a los Números Algebraicos
Lista 4 - entrega 10/5

47. Sea $K = \mathbb{Q}(\sqrt{-3}, \sqrt{-7})$, con grupo de Galois $G = \{1, \rho, \sigma, \tau\}$ donde los cuerpos fijos de ρ,σ,τ son, respectivamente, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$ y $\mathbb{Q}(\sqrt{21})$.
    (a) Determinar los grupos de inercia I_3, I_5, I_7.
    (b) Determinar los grupos de descomposición D_3, D_5, D_7.

48. (2p.) Supongamos que $K/\mathbb{Q}$ es una extensión cíclica (normal con grupo de Galois cíclico) de grado q^m, donde q es un primo. Sea $K_1/\mathbb{Q}$ la única subextensión de grado q. Mostrar que si p es un primo racional, ramificado en K_1, entonces p es totalmente ramificado en K. (Sugerencia: considerar el grupo de inercia I_p).

49. (2p.) Si $K/\mathbb{Q}$ es normal, sea $\mathrm{Desc}(K)$ el conjunto de primos racionales que descomponen totalmente en K. Mostrar que $\mathrm{Desc}(K) \subseteq \mathrm{Desc}(K')$ sii $K' \subseteq K$.

50. Sea K/k una extensión de cuerpos de grado 3, donde $K = k[\alpha]$ con $\mathrm{Irr}_k(\alpha) = F(X)$.
    (a) Mostrar que si $F(X) = (X - \alpha)(X^2 + bX + c)$, entonces $\Delta(F) = (b^2 - 4c)(\alpha^2 + b\alpha + c)^2$.
    (b) Mostrar que la clausura normal de K es $K[\sqrt{\Delta}]$.
    (c) Concluir que K/k es Galois sii $\Delta \in \mathbb{Q}^2$.

51. Sea $K/\mathbb{Q}$ una extensión normal de grado 3, con grupo de Galois G cíclico de orden 3.
    (a) Determinar la forma de la descomposición de p primo racional (no ramificado) en K según el orden del símbolo de Artin $\left(\frac{K/\mathbb{Q}}{p}\right)$.
    (b) Determinar la densidad de primos racionales que son inertes en K y la densidad de primos racionales que descomponen totalmente en K.
    (c) Sea $F(X) = X^3 - 3X + 1$, de discriminante $\Delta = 81 \in \mathbb{Q}^2$. Verificar experimentalmente el resultado en este caso calculando la cantidad de primos menores que 1000 que son inertes en el cuerpo de raíces de F, y la cantidad que descomponen.

52. Sea $K/\mathbb{Q}$ una extensión de grado 3 que *no* sea normal, con discriminante $\Delta \notin \mathbb{Q}^2$.
    (a) Determinar la forma de la descomposición de p primo racional (no ramificado) en la clausura normal $K[\sqrt{\Delta}]$ según el orden del símbolo de Artin $\left(\frac{K/\mathbb{Q}}{p}\right)$.
    (b) Determinar la forma de la descomposición de p primo racional en K según la descomposición en $K[\sqrt{\Delta}]$.
    (c) Determinar la densidad de primos racionales según la forma de su descomposición en K. Comparar con el resultado del ejercicio 34.

53. Sea $F(X) \in \mathbb{Z}[X]$ un polinomio mónico de grado 4 cuyo cuerpo de raíces tiene grado 24 sobre $\mathbb{Q}$.

   (a) ¿Cuál es la densidad del conjunto de primos p tales que $F(X)$ es producto de polinomios lineales módulo p?

   (b) ¿Cuál es la densidad del conjunto de primos p tales que $F(X)$ tiene por lo menos una raíz módulo p?

54. (Teoría de grupos) Considerar S_5 como el grupo de permutaciones de los elementos de $\mathbb{F}_5 = \mathbb{Z}/5$. Sea C_5 el subgrupo de *translaciones*, i.e. permutaciones de la forma $x \mapsto x + b$ con $b \in \mathbb{F}_5$. Sea N_5 el normalizador de C_5 en N_5, es decir $N_5 = \left\{\sigma \in S_5 \,:\, \sigma C_5 \sigma^{-1} = C_5\right\}$.

   (a) Mostrar que N_5 es el grupo de permutaciones de la forma $x \mapsto ax + b$ con $b \in \mathbb{F}_5$, $a \in \mathbb{F}_5^{\times}$.

   (b) Sea D_5 el grupo de permutaciones de la forma $x \mapsto \pm x + b$ con $b \in \mathbb{F}_5$. Mostrar que los únicos subgrupos de S_5 que contienen C_5 son S_5, A_5, N_5, D_5, y C_5, de ordenes 120, 60, 20, 10, y 5 respectivamente.

   (c) Describir las inclusiones entre esos cinco subgrupos.

55. (2p.) Sea $F(X) \in \mathbb{Z}[X]$ un polinomio mónico irreducible de grado 5. Sea K su cuerpo de raíces, y $G = \mathrm{Gal}(K/\mathbb{Q})$. Mostrar que G es isomorfo a uno de los cinco subgrupos de S_5 mencionados en el ejercicio anterior, y de hecho es *igual* a uno de esos subgrupos como un grupo de permutaciones de las raíces de $F(X)$ en K, si las raíces se identifican convenientemente con los elementos de $\mathbb{F}_5$.

56. (3p.) Sea $F(X) \in \mathbb{Z}[X]$ un polinomio mónico irreducible de grado 5. Para cada uno de los cinco posibles grupos de Galois, calcular la densidad del conjunto $P(F, i)$ de primos racionales p tales que F tiene exactamente i raíces módulo p. Hacer una tabla con los resultados.

57. (2p.) Se consideran los polinomios quínticos $A(X) = X^5 - X^3 - 2X^2 - 2X - 1$, $B(X) = X^5 - X + 3$, $C(X) = X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$, $D(X) = X^5 - 5$, $E(X) = X^5 + 10X^3 - 10X^2 + 35X - 18$. Todos son irreducibles, y sus discriminantes son $\Delta_A = 47^2$, $\Delta_B = 252869$ (primo), $\Delta_C = 11^4$, $\Delta_D = 5^9$, $\Delta_E = 2^6 \cdot 5^8 \cdot 11^2$.

   La tabla siguiente muestra para cada uno de los polinomios, la cantidad de primos p entre los primeros 1000 según el número de raíces del polinomio módulo p.

raíces	0	1	2	3	5
A	399	510	0	1	90
B	366	386	174	68	6
C	799	1	0	0	200
D	201	755	0	0	44
E	410	251	326	0	13

   Con esta información, hacer una conjetura sobre los grupos de Galois de cada uno de los polinomios.