ÁLGEBRA **Problemas propuestos** **25-5-2004**

Apellidos **Nombre**

Ejercicio 1.– Sea $f(X) = 2X^5 - 10X + 5 \in \mathbb{Q}[X]$.

1. Pruebe que $f(X)$ es irreducible en $\mathbb{Q}[X]$ y que tiene 5 raíces distintas.
2. Deduzca que G_f es isomorfo a un subgrupo de S_5.
3. Pruebe que 5 divide a $|G_f|$.
4. El teorema de Cauchy para grupos dice: si G es un grupo finito y p es un primo que divide a $|G|$, entonces G tiene un elemento de orden p. Con este resultado, pruebe que G_f tiene un elemento que se corresponde con un ciclo de orden 5 en S_5.
5. Compruebe que $f(-2) < 0, f(-1) > 0, f(1) < 0, f(2) > 0$, y deduzca que $f(X)$ tiene exactamente 3 raíces reales.
6. Pruebe que el automorfismo definido por la conjugación está en G_f.
7. Deduzca que $G_f \simeq S_5$. ¿Es $f(X)$ resoluble por radicales?

Ejercicio 2.– Calcule el grupo de Galois de $X^4 - 5$ sobre $\mathbb{Q}[i]$.

Ejercicio 3.– (2) Sea $\mathbb{F}_2 = \mathbb{Z}/\mathbb{Z}2$ el cuerpo finito con dos elementos. Sea α raíz de $X^2 + X + 1$ sobre $\mathbb{F}_2$ y $K_1 = \mathbb{F}_2[\alpha]$. Sea $g(X) = X^2 + \alpha X + 1 \in K_1[X]$.

1. ¿Cuántos elementos tiene K_1? Expréselos en función de α.
2. Pruebe que $g(X)$ es irreducible sobre $K_1[X]$.
3. Sea β raíz de $g(X)$ y $K_2 = K_1[\beta]$. ¿Cuántos elementos tiene K_2? Calcule $[K_2 : \mathbb{F}_2]$.
4. Sea $\varphi : K_2 \to K_2$ definida por $\varphi(x) = x^2$. Pruebe que $\varphi \in \mathrm{Gal}(K_2|\mathbb{F}_2)$, y que el orden de φ es 4. Deduzca que $\mathrm{Gal}(K_2|\mathbb{F}_2) = \langle\varphi\rangle$.
5. Sea $\gamma = \alpha\beta$. Pruebe que γ no permanece invariante por ningún elemento de $\mathrm{Gal}(K_2|\mathbb{F}_2)$ distinto de la identidad. Concluya que $K_2 = \mathbb{F}_2[\gamma]$.

Ejercicio 4.– (2) Sea K un cuerpo finito,car$(K) \neq 2$, y θ un generador del grupo multiplicativo K^*.

1. Sea $b \in K^*$ y $k \in \mathbb{N}$ tal que $\theta^k = b$. Pruebe que b es un cuadrado en K si y solamente si k es par.
2. Pruebe que si $a_1, a_2 \in K$ no son cuadrados entonces $a_1 a_2$ es un cuadrado en K.
3. Sea $a \in K$ no cuadrado y consideremos $K_1 = K[\sqrt{a}]$. Calcule el número de elementos de K_1.
4. Sea $b \in K$. Pruebe que existe $b_1 \in K_1$ tal que $b_1^2 = b$.
5. Pruebe que si $d_1, d_2 \in K$ no son cuadrados entonces $[K[\sqrt{d_1}, \sqrt{d_2}] : K] = 2$.
6. Pruebe que el cuerpo de descomposición de $f(X) = X^4 - 10X^2 + 1$ sobre $\mathbb{Q}$ es igual a $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Demuestre que para cualquier primo p, $f(X)$ es reducible sobre $\mathbb{F}_p[X]$.

Ejercicio 5.– Construya cuerpos de descomposición de los polinomios $X^3 + 2X + 1$ y $X^3 + X^2 + X + 2$ sobre $\mathbb{Z}/3\mathbb{Z}$. Determine si son isomorfos y, en tal caso, calcule un isomorfismo.

Ejercicio 6.– Sea $L|k$ una extensión de cuerpos finitos, con $[L : k] = n$, y $f(X) \in k[X]$ un polinomio irreducible que tiene una raíz $a \in L$. Sea Φ generador del grupo $\mathrm{Gal}(L|k)$ y

$$g(X) = (X - a)(X - \Phi(a)) \cdots (X - \Phi^{n-1}(a)) \in L[X].$$

1. Pruebe que
$$g(X) = X^n - a_1 X^{n-1} + \ldots + (-1)^n a_n,$$
donde $a_i = S_i(a, \Phi(a), \ldots, \Phi^{n-1}(a))$, y S_i las funciones simétricas elementales (ejercicio 107 de la relación).

2. Deduzca que $\Phi(a_i) = a_i$ para todo $i = 1, \ldots, n$.

3. A partir de lo anterior, concluya que $g(X) \in k[X]$ y que $f(X)$ factoriza en $L[X]$ en factores lineales.

Ejercicio 7.– Construya un cuerpo finito de 16 elementos y calcule un generador del grupo multiplicativo. ¿Cuántos generadores hay?

Ejercicio 8.– Pruebe que $2, 3$ o 6 es un cuadrado en $\mathbb{Z}/\mathbb{Z}p$ para todo primo p. Concluya que el polinomio $(x^2 - 2)(x^2 - 3)(x^2 - 6)$ tiene una raíz en $\mathbb{Z}/\mathbb{Z}p$ para todo primo p pero no tiene raíces en $\mathbb{Z}$.

Ejercicio 9.– Sea $k = \mathbb{Z}/\mathbb{Z}p$ y $a \in k, a \neq 0$. El cuerpo de descomposición del polinomio $f(x) = x^p - x - a$ sobre k es $k[\alpha]$, donde α es una raíz de $f(x)$ (ejercicio 2, 12 Mayo). Pruebe explícitamente que el grupo de Galois de $k[\alpha]$ sobre k es cíclico.