ESTRUCTURAS ALGEBRAICAS **Examen final** **31-01-2002**

Apellidos **Nombre**

Ejercicio 1.- (4 puntos) Consideremos el polinomio $f(X) = X^4 + 6X^2 + 2 \in \mathbb{Q}[X]$, cuyas raíces son:

$$\alpha_1 = \sqrt{-3+\sqrt{7}} \quad \alpha_2 = \sqrt{-3-\sqrt{7}}$$
$$\alpha_3 = -\sqrt{-3+\sqrt{7}} \quad \alpha_4 = -\sqrt{-3-\sqrt{7}}.$$

Se pide:

1. Probar que $f(X)$ es irreducible.
2. Establecer la correspondencia de Galois para $f(X)$.
3. Sea K el cuerpo de descomposición de $f(X)$ sobre $\mathbb{Q}$. Dar explícitamente una torre de extensiones por radicales entre $\mathbb{Q}$ y K.

Nota.- Por si fuera necesario, se recuerda que si $p(X) = X^4 + pX^2 + qX + r$, la resolvente cúbica es $g(X) = X^3 - pX^2 - 4rX - q^2 + 4pr$ y que si $g(X)$ tiene una única raíz $\eta \in \mathbb{Q}$ es útil el polinomio auxiliar $h(X) = (X^2 - \eta X + r)(X^2 + p - \eta)$.

Ejercicio 2.- (3 puntos) Se pide:

1. Demostrar que $x^3 - x + 2$ es irreducible en $\mathbb{F}_3[x]$. Construir un cuerpo de descomposición de $x^3 - x + 2$ sobre $\mathbb{F}_3[x]$.
2. Sea p un número primo y m un entero positivo tal que p no divide a m. Sea ε una raíz primitiva m-ésima de la unidad sobre $\mathbb{F}_p$. Demostrar que $[\mathbb{F}_p[\varepsilon] : \mathbb{F}_p] = d$ donde d es el orden de $\overline{p}$ en el grupo multiplicativo U_m de las unidades de $\mathbb{Z}/\mathbb{Z}m$. (**Ayuda:** Recordar que el grupo de Galois de la extensión está generado por el automorfismo de Frobenius).

   Deducir que Φ_m es irreducible sobre $\mathbb{F}_p$ si y sólo si $U_m = \langle \overline{p} \rangle$.
3. Sea p un número primo. Consideremos las extensiones

   $$\mathbb{F}_p \subset J \subset K \subset L$$

   donde $J = \mathbb{F}_p(\alpha)$ con α trascendente sobre $\mathbb{F}_p$, $K = J(\beta)$ con β trascendente sobre J y L es un cuerpo de descomposición de $(x^p - \alpha)(x^p - \beta)$ sobre K.

   Probar que $\lambda^p \in K$ para todo $\lambda \in L$. Demostrar que $[L : K] = p^2$ y que dicha extensión no es simple.

Ejercicio 3.- (3 puntos) Se pide:

1. Dado un anillo A, consideremos el anillo de polinomios $A[X]$ y la inclusión $i : A \to A[X]$, que es un homomorfismo de anillos. Probar que para cada ideal $I \subset A$:
   (a) El conjunto $I[X]$ de los polinomios con coeficientes en I es un ideal de $A[X]$, y además $I[X] = I^e$.
   (b) Se tiene $I = I^{ec}$.
   (c) I es primo si y sólo si $I[X]$ es primo.
2. Sea B un anillo y $A \subset B$ un subanillo. Es claro que todo B-módulo puede ser considerado también como A-módulo. Sea M un A-módulo y N un B-módulo. Probar que
   (a) Sobre el A-módulo $N \otimes_A M$ podemos definir una estructura de B-módulo de manera que $b \cdot (n \otimes m) = (bn) \otimes m$ para $b \in B$, $m \in M$, $n \in N$.
   (b) Probar que existe un isomorfismo natural de B-módulos $N \otimes_B (B \otimes_A M) \simeq N \otimes_A M$. Concluir que si N es un B-módulo plano y B es plano considerado como A-módulo, entonces N también es plano considerado como A-módulo.
3. Sea M un A-módulo y $N \subset M$ un submódulo. Probar que N es un sumando directo de M, i.e. que exista otro submódulo $P \subset M$ tal que $M = N \oplus P$, si y sólo si existe un homomorfismo $\pi : M \to N$ tal que $\pi(x) = x$ para todo $x \in N$.
4. Probar que en un anillo local, los únicos idempotentes (i.e. $x = x^2$) son 0 y 1.