ESTRUCTURAS ALGEBRAICAS **Soluciones examen final de Enero 31-01-2002**

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 $h(X) = (X^2 - \eta X + r)(X^2 + p - \eta)$.

Solución del Ejercicio 1.-

• Apartado 1.- Aplicar el criterio de Eisenstein para $p = 2$.

• Apartado 2.-

$g(x) = x^3 - 6x^2 - 8x + 48 = (x-6)(x^2-8)$ es la resolvente cúbica de $f(x)$ y sus raíces son $\eta = 6$, $\eta_1 = 2\sqrt{2}$ y $\eta_2 = -2\sqrt{2}$ luego su cuerpo de descomposición sobre $\mathbb{Q}$ es $K' = \mathbb{Q}[\sqrt{2}]$. Como sólo una de las raíces pertenece a $\mathbb{Q}$, G será isomorfo a un subgrupo cíclico de orden 4 o a uno de orden 8 de S_4. Las raíces de $h(x) = (x^2 - 6x + 2)x^2$ son 0 y $3 \pm \sqrt{7} \notin K'$ por tanto G es isomorfo a un subgrupo de orden 8 de S_4.

Veamos a cuál de ellos: $K = \mathbb{Q}[\alpha_1, \alpha_2]$.

Sabemos que $[\mathbb{Q}[\alpha_1] : \mathbb{Q}] = 4$ por tanto $[K : \mathbb{Q}[\alpha_1]] = 2$; así, podemos considerar $\mathrm{Gal}(K : \mathbb{Q}[\alpha_1]) = \{1, \sigma\}$ y como $\mathbb{Q} \subset \mathbb{Q}[\alpha_1]$, $\sigma \in G$. Además $\sigma(\alpha_1) = \alpha_1$ luego $\sigma(\alpha_3) = \alpha_3$ y al ser $\sigma \neq 1$, $\sigma(\alpha_2) = \alpha_4$ y $\sigma(\alpha_4) = \alpha_2$; por tanto: $(24) \in G$; entonces:

$$G \simeq \{1,\ (13),\ (24),\ (12)(34),\ (13)(24),\ (14)(23),\ (1234),\ (1432)\}$$

Los subgrupos no triviales de G son los siguientes:
$H_1 = \{1, (13)\}$; $H_2 = \{1, (24)\}$; $H_3 = \{1, (14)(23)\}$; $H_4 = \{1, (13)(24)\}$; $H_5 = \{1, (12)(34)\}$; $H_36 = V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$; $H_7 = \{1, (13)(24), (1234), (1432)\}$; $H_8 = \{1, (13), (24), (13)(24)\}$.
Notaremos $K_i = F(H_i),\ i = 1, \ldots, 8$.

Cálculo de K_36

$K_6 = F(G \cap V_4) = \mathbb{Q}[\sqrt{2}]$.

Cálculo de K_1

$\alpha_2 \in K_1$ y $[\mathbb{Q}[\alpha_2] : \mathbb{Q}] = 4$ ya que el polinomio mínimo de α_2 es $f(x)$. Por tanto:

$$\underbrace{\overbrace{\mathbb{Q} \overset{4}{\subset} \mathbb{Q}[\alpha_2] \subset K_1}^{4} \overset{2}{\subset} K}_{8} \Rightarrow K_1 = \mathbb{Q}[\alpha_2]$$

Cálculo de K_2

De forma análoga al caso anterior se obtiene que $K_2 = \mathbb{Q}[\alpha_1]$.

Cálculo de K_5

Sea $\alpha = \alpha_1 + \alpha_2 = \sqrt{-3+\sqrt{7}} + \sqrt{-3-\sqrt{7}} \in K_5$. α es raíz del polinomio $x^4 + 12x^2 + 28$ que es irreducible sobre $\mathbb{Q}$, luego es su polinomio mínimo sobre $\mathbb{Q}$; así:

$$\underbrace{\overbrace{\mathbb{Q} \overset{4}{\subset} \mathbb{Q}[\alpha_1 + \alpha_2] \subset K_5}^{4} \overset{2}{\subset} K}_{8} \Rightarrow K_5 = \mathbb{Q}[\alpha_1 + \alpha_2]$$

Cálculo de K_3

Razonando como en el caso anterior se tiene que $K_3 = \mathbb{Q}[\alpha_1 + \alpha_4]$.

Cálculo de K_8

$\sqrt{7} = 3 + \alpha_1.\alpha_3 \in K_8$, luego $\mathbb{Q}[\sqrt{67}] \subset K_8$, además $[\mathbb{Q}[\sqrt{7}] : \mathbb{Q}] = 2 = [K_8 : \mathbb{Q}]$; así $K_8 = \mathbb{Q}[\sqrt{7}]$.

Cálculo de K_4

$H_4 \subset H_8 \Rightarrow K_8 \subset K_4 \Rightarrow \sqrt{67} \in K_4$.

$H_4 \subset H_6 \Rightarrow K_6 \subset K_4 \Rightarrow \sqrt{2} \in K_4$.

Por tanto $\mathbb{Q}[\sqrt{2}, \sqrt{7}] \subset K_4$; además $[\mathbb{Q}[\sqrt{2}, \sqrt{7}] : \mathbb{Q}] = 4 = [K_4 : \mathbb{Q}]$ luego $K_4 = \mathbb{Q}[\sqrt{2}, \sqrt{7}]$.

Cálculo de K_7

Basta probar que $\mathbb{Q}[\sqrt{14}]$ es una extensión de grado 2 sobre $\mathbb{Q}$ distinta de las extensiones $\mathbb{Q}[\sqrt{2}]$ y $\mathbb{Q}[\sqrt{7}]$. Como $\mathbb{Q} \subset \mathbb{Q}[\sqrt{14}] \subset K$, $\mathbb{Q}[\sqrt{14}]$ es el cuerpo fijo de un subgrupo de orden 4, luego $K_7 = \mathbb{Q}[\sqrt{14}]$.

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.

Solución del Ejercicio 2.- `Falta`

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 $N \otimes_B (B \otimes_A M) \cong N \otimes_A M$. 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.

Solución del Ejercicio 3.-

1. (a) Hemos de probar que $I[X]$ es un subgrupo aditivo de $A[X]$ y que si $f \in A[X]$ y $g \in I[X]$ entonces $fg \in I[X]$.
   Obviamente el polinomio nulo de $A[X]$ está en $I[X]$, pues I es un ideal de A y por tanto contiene al $0 \in A$.
   Si $g = g_0 + g_1X + g_2X^2 + \cdots, g' = g'_0 + g'_1X + g'_2X^2 + \cdots \in I[X]$, entonces $g_i, g'_i \in I$ para todo i, y como I es un ideal de A entonces

$g_i - g'_i \in I$ para todo i, de donde $g - g' = (g_0 - g'_0) + (g_1 - g'_1)X + (g_2 - g'_2)X^2 + \cdots \in I[X]$.

Así pues ya sabemos que $I[X]$ es un subgrupo aditivo de A.

Si $f = f_0 + f_1X + f_2X^2 + \cdots \in A[X]$, $g = g_0 + g_1X + g_2X^2 + \cdots \in I[X]$, entonces $f_i \in A, g_i \in I$ y

$$fg = (f_0g_0) + (f_0g_1 + f_1g_0)X + (f_0g_2 + f_1g_1 + f_2g_0)X^2 + \cdots,$$

pero $f_0g_0 \in I$, $f_0g_1, f_1g_0 \in I$ $f_2g_0, f_1g_1, f_0g_2 \in I$, y en general $f_ig_j \in I$ porque I es ideal de A, de donde se deduce que los coeficientes de fg están todos en I y por tanto $fg \in I[X]$.

Veamos ahora que $I[X] = I^e$.

Si $f = f_0 + f_1X + f_2X^2 + \cdots \in I[X]$, entonces $f_i \in I$ y por tanto f es suma de productos de elementos de $A[X]$ (los X^i) por elementos de I (los f_i), de donde $f \in I^e$. Así pues, $I[X] \subset I^e$.

Sea ahora un elemento $f \in I^e$, i.e. $f = \sum a_if_i$ donde los $a_i \in I$ y los $f_i \in A[X]$. Es claro que cada a_if_i será un polinomio cuyos coeficientes tienen como factor a a_i y por tanto estarán en I, de donde $a_if_i \in I[X]$, y como $I[X]$ es un grupo aditivo (de hecho es un ideal), entonces $f = \sum a_if_i \in I[X]$ y $I^e \subset I[X]$.

(b) Siempre se tiene $I \subset I^{ec}$. Sea ahora $a \in I^{ec}$. Por el apartado anterior, $I^e = I[X]$ y por tanto $a \in I^{ec} = I[X]^c$, es decir que $a = i(a) = a + 0X + 0X^2 + \cdots \in I[X]$, de donde $a \in I$.

(c) Supongamos que $I[X]$ es primo. Por los dos apartados anteriores, $I = I^{ec} = I[X]^c$, y como el contraido de cualquier ideal primo es primo deducimos que I es primo.

Supongamos ahora que I es primo. Para probar que $I[X]$ es primo hemos de probar que si $f = \sum f_iX^i, g = \sum g_iX^i \in A[X]$ tales que $fg \in I[X]$, entonces o bien f o bien g pertenecen a $I[X]$. Supongamos que $f \notin I[X]$, i.e. que no todos los coeficientes f_i pertenecen a I. Sea f_N el primer coeficiente de f que no pertenece a I :

$$f_0, \ldots, f_{N-1} \in I, f_N \notin I.$$

El coeficiente de X^N de fg es $f_0g_N + \cdots + f_{N-1}g_1 + f_Ng_0$, que ha de pertenecer a I (pues $fg \in I[X]$). Como $f_0, \ldots, f_{N-1} \in I$ deducimos que $f_Ng_0 \in I$ y como I es primo y $f_N \notin I$, entonces $g_0 \in I$.

El coeficiente de X^{N+1} de fg es $f_0g_{N+1} + \cdots + f_Ng_1 + f_{N+1}g_0$, que también pertenece a I. Como ya sabemos que $g_0 \in I$ y $f_0, \ldots, f_{N-1} \in I$ deducimos que $f_Ng_1 \in$ y como I es primo y $f_N \notin I$, entonces $g_1 \in I$.

Así sucesivamente vamos probando (por inducción) que $g_0, g_1, g_2, \ldots$ pertenecen a I y por tanto $g \in I[X]$.

2. (a) Primeramente hemos de definir una operación

$$(b, \xi) \in B \times (N \otimes_A M) \mapsto b \cdot \xi \in N \otimes_A M$$

que cada vez que ξ sea de la forma $n \otimes m$, se tenga $b \cdot (n \otimes m) = (bn) \otimes m$ (ATENCIÓN: no todos los elementos $\xi \in N \otimes_A M$ son de esa forma; son siempre sumas de tales elementos).

Notemos por $g : N \times M \to N \otimes_A M$ la aplicación bilineal canónica (por notación: $n \otimes m = g(n, m)$).

Sea $b \in B$ un elemento, fijo por el momento. Consideremos la aplicación

$$\mu_b : (n, m) \in N \times M \mapsto \mu_b(n, m) = g(bn, m) \in N \otimes_A M.$$

Se comprueba sin mayor problema que μ_b es A-bilineal, y por tanto, por la propiedad universal del producto tensorial, existe una única aplicación A-lineal $\nu_b : N \otimes_A M \to N \otimes_A M$ tal que $\nu_b \circ g = \mu_b$.

Ahora ya podemos definir la operación: Para cada $b \in B$ y cada $\xi \in N \otimes_A M$, $b \cdot \xi := \nu_b(\xi)$. Veamos que esta operación define una estructura de B-módulo en $N \otimes_A M$.

Claramente se tiene

$$b \cdot (\xi_1 + \xi_2) = \nu_b(\xi_1 + \xi_2) = \nu_b(\xi_1) + \nu_b(\xi_2) = b \cdot \xi_1 + b \cdot \xi_2.$$

Ahora hemos de probar que $(b_1 + b_2) \cdot \xi = b_1 \cdot \xi + b_2 \cdot \xi$, o dicho de otra forma, que $\nu_{b_1+b_2} = \nu_{b_1} + \nu_{b_2}$. Pero

$$\nu_{b_1} + \nu_{b_2} : N \otimes_A M \to N \otimes_A M$$

es una aplicación lineal tal que $(\nu_{b_1} + \nu_{b_2}) \circ g = \nu_{b_1} \circ g + \nu_{b_2} \circ g = \mu_{b_1} + \mu_{b_2}$. Ahora bien, se tiene fácilmente (debería comprobarse) que $\mu_{b_1} + \mu_{b_2} = \mu_{b_1+b_2}$ y por tanto $(\nu_{b_1} + \nu_{b_2}) \circ g = \mu_{b_1+b_2}$, y por la unicidad de $\nu_{b_1+b_2}$ deducimos $\nu_{b_1+b_2} = \nu_{b_1} + \nu_{b_2}$.

También hemos de probar que $1 \cdot \xi = \xi$, pero esto es consecuencia de que $\mu_1 = g$ y por tanto ν_1 es la identidad (unicidad en la propiedad universal del producto tensorial).

Por último hemos de probar que $b_1 \cdot (b_2 \cdot \xi) = (b_1 b_2) \cdot \xi$, o lo que es lo mismo, que $\nu_{b_1 b2} = \nu_{b_1} \circ \nu_{b_2}$. Pero esto es consecuencia de la igualdad $\nu_{b_1} \circ \mu_{b_2} = \mu_{b_1 b_2}$ y de nuevo de la unicidad en la propiedad universal del producto tensorial.

(b) `Falta`

3. Supongamos que N es un sumando directo de M: $M = N \oplus P$. Para cada $m \in M$, existen unos únicos $n \in N, p \in P$ tales que $m = n + p$. Definimos

$$\pi : m \in M \to \pi(m) = n \in N.$$

Se comprueba fácilmente que π es un homomorfismo y es claro que $\pi(x) = x$ si $x \in N$, pues en tal caso la descomposición única de x es $x = x + 0$, $x \in N, 0 \in P$.

Supongamos $\pi : M \to N$ es un homomorfismo tal que $\pi(x) = x$ para cada $x \in N$.

Para cada $m \in M$ se tiene $m = \pi(m) + (m - \pi(m))$, pero $\pi(m) \in N$ y $\pi(m-\pi(m)) = \pi(m)-\pi(\pi(m)) = \pi(m)-\pi(m) = 0$, de donde $m-\pi(m) \in \ker \pi$. Así pues $M = N + \ker \pi$.

Se comprueba fácilmente que $N \cap \ker \pi = 0$ y por tanto la suma anteror es directa.

4. Sea A un anillo local y M su único ideal maximal. Sea $x \in A$ un idempotente, i.e. $x^2 = x$, o lo que es lo mismo, $x(x-1) = 0$. Hay dos posibilidades, o bien $x \notin M$ o bien $x \in M$.

   Si $x \notin M$ entonces x es una unidad (M es el único ideal maximal) y por tanto de $x(x-1) = 0$ deducimos que $x - 1 = 0$, i.e. $x = 1$.

   Si $x \in M$, entonces $x - 1 \notin M$ y por tanto es una unidad, de donde $x = 0$.