EXAMEN FINAL DE ÁLGEBRA II, 3^o MATEMÁTICAS

Viernes, 10 de septiembre de 2004

Apellidos:______________________________ **Nombre:**____________________

D.N.I.:____ **Grupo:**________________

Nota: Escribe un problema en cada hoja, y justifica todas tus respuestas.

---

1. (2 puntos) Sea I el ideal $\langle 1+3i, 3+4i\rangle$ de $\mathbb{Z}[i]$.

a. Probar que I es principal.

b. Dar un ejemplo de un ideal en $\mathbb{Z}[i]$ que no sea maximal.

---

2. (2 puntos) Sea β un cero de x^5+2x+6.

a. Probar que $\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2} \notin \mathbb{Q}(\beta)$.

b. Probar que $\mathbb{Q}(\beta) = \mathbb{Q}(\beta^3)$.

---

3. (3 puntos) Decidir justificadamante si cada uno de los siguientes enunciados es **verdadero** o **falso**:

a. Si L es el cuerpo de descomposición de un polinomio $P \in \mathbb{Q}[x]$ y $\mathcal{G}(L/\mathbb{Q}) \simeq S_5 \times \mathbb{Z}_5$, entonces P **no** es soluble por radicales.

b. El anillo $\mathbb{Q}[x]/\langle x^3+x^2+1\rangle$ es un dominio de integridad.

c. Los cuerpos $\mathbb{F}_3[x]/\langle x^3+2x^2+x+1\rangle$ y $\mathbb{F}_2[x]/\langle x^3+x^2+2x+1\rangle$ son isomorfos.

d. Si $p(x)$ es un polinomio irreducible de grado 3 sobre $\mathbb{F}_3$, y $L/\mathbb{F}_3$ es su cuerpo de descomposición, entonces $[L:\mathbb{F}_3] = 3$ ó 6.

---

4. (3 puntos) Sea $L = \mathbb{Q}(\xi)$, con $\xi = e^{\frac{2\pi i}{7}}$.

a. Explicar por qué $L/\mathbb{Q}$ es Galois.

b. Si $M = \mathbb{Q}(\xi^2+\xi^5, \xi^3+\xi^4)$, hallar $\mathcal{G}(L/M)$, y utilizar este resultado para calcular $[M:\mathbb{Q}]$.

Álgebra II
Soluciones septiembre 2004

$\boxed{\textbf{Solución problema 1.}}$ **a)** I principal $\Leftrightarrow I = (\alpha)$. Quizá multiplicando por una de las unidades ± 1, $\pm i$, podemos suponer que $\alpha = a + bi$ con a y b enteros no negativos.

$$\begin{array}{lllll} 1+3i \in (\alpha) & \Rightarrow & \alpha\beta = 1+3i \Rightarrow & \text{(tomando normas)} & a^2+b^2|1^2+3^2 = 10 \\ 3+4i \in (\alpha) & \Rightarrow & \alpha\gamma = 3+4i \Rightarrow & \text{''} & a^2+b^2|3^2+4^2 = 25 \end{array}$$

Las únicas posibilidades son por tanto $a^2 + b^2 = 5 = \text{mcd}(10, 25)$ y $a^2 + b^2 = 1$; lo que conduce a $\alpha = 2 + i, 1 + 2i, 1, i$. Como $(1 + 3i)/(2 + i) = 1 + i \in \mathbb{Z}[i]$ y $(3 + 4i)/(2 + i) = 2 + i \in \mathbb{Z}[i]$, se tiene $I \subset \langle 2 + i\rangle$. La otra inclusión se sigue de $(3 + 4i) - (1 + 3i) = 2 + i$, lo que asegura $I = \langle 2 + i\rangle$.

b) Por ejemplo $I = \langle 4\rangle$ ya que

$$\{0\} \neq I \subset \langle 2\rangle \subset \mathbb{Z}[i]$$

y evidentemente $\langle 2\rangle \neq \mathbb{Z}[i]$, porque $1 \neq 2n + 2mi$, e $I \neq \langle 2\rangle$, porque $2 \neq 4n + 4mi$.

Errores más comunes: a) $1 + 3i, 3 + 4i \in \langle 2 + i\rangle$ no asegura sin argumentos adicionales que $I = \langle 2 + i\rangle$.

b) $\langle 2 + 2i\rangle \neq \{n + mi \ : \ 2|n, \ 2|m\}$.

$\boxed{\textbf{Solución problema 2.}}$ El polinomio $P = x^5 + 2x + 6$ es irreducible sobre $\mathbb{Q}$ por el criterio de Eisenstein con $p = 2$, de lo que se deduce que $[\mathbb{Q}(\beta) : \mathbb{Q}] = 5$.

a) Si $\sqrt[k]{2} \in \mathbb{Q}(\beta)$ con $k = 2, 3$, ó 4, entonces $\mathbb{Q}(\sqrt[k]{2}) \subset \mathbb{Q}(\beta)$ y $[\mathbb{Q}(\sqrt[k]{2}) : \mathbb{Q}]$ divide a 5. Pero esto es una contradicción ya que el polinomio mínimo de $\sqrt[k]{2}$ es $x^k - 2$ (irreducible por Eisenstein), lo que implica $[\mathbb{Q}(\sqrt[k]{2}) : \mathbb{Q}] = k$ y $k \not| 5$.

b) La inclusión $\mathbb{Q}(\beta^3) \subset \mathbb{Q}(\beta)$ implica que $n = [\mathbb{Q}(\beta^3) : \mathbb{Q}]$ divide a 5, como antes. De hecho

$$n \cdot [\mathbb{Q}(\beta) : \mathbb{Q}(\beta^3)] = 5.$$

Si $n = 5$ entonces $[\mathbb{Q}(\beta) : \mathbb{Q}(\beta^3)] = 1 \Rightarrow \mathbb{Q}(\beta) = \mathbb{Q}(\beta^3)$. Y si $n = 1$, entonces $[\mathbb{Q}(\beta^3) : \mathbb{Q}] \Rightarrow \beta^3 \in \mathbb{Q}$, con lo cual β sería raíz del polinomio $x^3 - \beta^3 \in \mathbb{Q}[x]$, lo que contradice $[\mathbb{Q}(\beta) : \mathbb{Q}] = 5$.

Errores más comunes: a) $\alpha \in \mathbb{Q}(\beta) \not\Rightarrow \alpha$ es raíz del polinomio mínimo de β.

b) $\beta^3 \in \mathbb{Q} \not\Rightarrow \beta \in \mathbb{Q}$. Considérese por ejemplo el caso $\beta = \sqrt[3]{2}$.

$\boxed{\textbf{Solución problema 3.}}$ (a) VERDADERO. P es soluble por radicales si y sólo si su grupo de Galois es soluble. $S_5 \times \mathbb{Z}_5$ no es soluble, porque contiene el subgrupo $S_5 \times \{0\} \simeq S_5$ que no es soluble.

(b) VERDADERO. $\mathbb{Q}[x]/\langle x^3 + x^2 + 1\rangle$ es un dominio de integridad si y sólo si el ideal $\langle x^3 + x^2 + 1\rangle$ es primo, lo cual sucede si y sólo si $x^3 + x^2 + 1$ es irreducible. El polinomio $x^3 + x^2 + 1$ es irreducible sobre $\mathbb{Z}_2$, porque no tiene raíces sobre este cuerpo, por lo tanto es irreducible sobre $\mathbb{Z}$ y como consecuencia lo es sobre $\mathbb{Q}$.

(c) FALSO. $\mathbb{F}_3[x]/\langle x^3+2x^2+x+1\rangle$ tiene característica 3 y $\mathbb{F}_2[x]/\langle x^3+x^2+2x+1\rangle$ tiene característica 2, y dos cuerpos con características distintas no pueden ser isomorfos. También se puede argumentar observando que el cardinal de $\mathbb{F}_3[x]/\langle x^3+2x^2+x+1\rangle$ es 27 mientras que el de $\mathbb{F}_2[x]/\langle x^3+x^2+2x+1\rangle$ es 8.

(d) FALSO. Si $p(x)$ es un polinomio irreducible sobre $\mathbb{F}_3$ entonces $\mathbb{F}_3/\langle p(x)\rangle \simeq \mathbb{F}_9$ contiene al menos una de sus raíces. Pero $\mathbb{F}_9$ es una extensión normal de $\mathbb{F}_3$, al ser el cuerpo de descomposición de x^9-x, por lo tanto si contiene una raíz de $p(x)$ las tiene que contener todas. En consecuencia $L \simeq \mathbb{F}_9$, y $[L:\mathbb{F}_3]$ sólo puede ser 3.

$\boxed{\textbf{Solución del problema 4.}}$ (a) Hay que comprobar que L es una extensión normal, finita y separable de $\mathbb{Q}$. Es **normal** porque es el cuerpo de descomposición de x^7-1 sobre $\mathbb{Q}$: sus raíces son ξ^i, $i=1,\ldots,7$ y $\mathbb{Q}(\xi)$ es el menor cuerpo que las contiene. Es **finita** porque $\mathbb{Q}(\xi)\simeq \mathbb{Q}[x]/\langle x^6+x^5+x^4+x^3+x^2+x+1\rangle$ que tiene grado 6 sobre $\mathbb{Q}$. Es **separable** porque $\mathbb{Q}$ tiene característica 0, y cualquier extensión de un cuerpo de característica 0 es separable.

(b) $\mathcal{G}(L/M)$ es isomorfo a $\mathbb{Z}_7^*$. Si denotamos por σ_i al automorfismo de L con $\sigma_i(\xi)=\xi^i$ para $i=1,\ldots,6$, entonces $\mathcal{G}(L/M)=\{\sigma_1,\ldots,\sigma_6\}=\langle\sigma_3\rangle$, y sus dos únicos subgrupos propios son $\langle\sigma_3^2\rangle$ y $\langle\sigma_3^3\rangle$.

$\mathcal{G}(L/M)$ es el subgrupo de $\mathcal{G}(L/\mathbb{Q})$ formado por los elementos que fijan M. Por un lado, $\sigma_3^2(\xi^2+\xi^5)=\xi^5+\xi^2$, y $\sigma_3^2(\xi^3+\xi^4)=\xi^4+\xi^3$, por lo que $\langle\sigma_3^2\rangle \subseteqq \mathcal{G}(L/M)$. Para demostrar la igualdad es suficiente observar que $M\neq\mathbb{Q}$ porque $M\neq\sigma_3^3(M)$ (éste último contiene números complejos con parte imaginaria no nula, mientras que $M\subset\mathbb{R}$).

Dado que $|\mathcal{G}(L/M)|=|\langle\sigma_3^2\rangle|=2$, se tiene que $[L:M]=2$ y por lo tanto $[M:\mathbb{Q}]=3$.