EXAMEN FINAL DE ÁLGEBRA II,
3^o MATEMÁTICAS

Sábado, 4 de junio de 2005

---

1. (2 puntos) Sea A el anillo $\mathbb{Z}[\sqrt{3}]$.

a. Demuestra que $A \simeq \mathbb{Z}[x]/\langle x^2-3\rangle$.

Consideramos la función $\phi : \mathbb{Z}[x] \to A$ con $\phi(p(x)) = p(\sqrt{3})$. Claramente ϕ es un homomorfismo de anillos ya que:
• $\phi(p(x)+q(x)) = p(\sqrt{3}) + q(\sqrt{3}) = \phi(p(x)) + \phi(q(x))$;
• $\phi(p(x)q(x)) = p(\sqrt{3})q(\sqrt{3}) = \phi(p(x))\phi(q(x))$;
• $\phi(1) = 1$.
Además ϕ es sobreyectiva: dado $a+b\sqrt{3} \in A$, basta observar que $\phi(a+bx) = a+b\sqrt{3}$. Por lo tanto, por el Primer Teorema de Isomorfía para anillos, $\phi : \mathbb{Z}[x]/\mathrm{Ker}\phi \simeq A$. Para concluir basta probar que $\mathrm{Ker}\phi = \langle x^2-3\rangle$. Claramente $\langle x^2-3\rangle \subset \mathrm{Ker}(\phi)$. Probemos ahora la otra inclusión. Sea $p(x) \in \mathrm{Ker}(\phi)$. Entonces $p(x) = q(x)(x^2-3) + r(x)$, con $\deg(r(x)) \leq 1$, ó $r(x) = 0$ (esto se puede hacer aunque $\mathbb{Z}$ no sea un cuerpo, dado que x^2-3 es mónico). Como $p(\sqrt{3}) = 0$ entonces $r(\sqrt{3}) = 0$ lo cual sólo es posible si $r(x) = 0$. Por lo tanto $p(x) \in \langle x^2-3\rangle$.

b. ¿Cuántos ideales maximales tiene $A/\langle 3\rangle$.

Por el apartado (a), $A/\langle 3\rangle \simeq \mathbb{Z}[x]/\langle x^2-3, x^2\rangle \simeq \mathbb{F}_3[x]/\langle x^2\rangle$. Los ideales de $\mathbb{F}_3[x]/\langle x^2\rangle$ son precisamente las imágenes en el cociente de los ideales de $\mathbb{F}_3[x]$ que contienen a $\langle x^2\rangle$. Como $\mathbb{F}_3$ es un cuerpo, todos los ideales de $\mathbb{F}_3[x]$ son principales, y por lo tanto los únicos que contienen a $\langle x^2\rangle$ son los generados por los divisores de x^2. Como consecuencia, los ideales de $\mathbb{F}_3[x]/\langle x^2\rangle$ son: $\langle\overline{x^2}\rangle = \langle\overline{0}\rangle$; $\langle\overline{x}\rangle$ y $\langle\overline{1}\rangle$, así que hay un único maximal, que es $\langle\overline{x}\rangle$. Por el isomorfismo descrito en (a) este ideal se corresponde con el único maximal de $A/\langle 3\rangle$, que es por tanto $\langle\overline{\sqrt{3}}\rangle$.

---

2. (3 puntos) Decide razonadamente el grado de las siguientes extensiones:

a. $\mathbb{Q}(\sqrt[7]{2} + 2\sqrt[7]{4} + 3\sqrt[7]{8})/\mathbb{Q}$.

Observamos en primer lugar que $\mathbb{Q}(\sqrt[7]{2}+2\sqrt[7]{4}+3\sqrt[7]{8}) \subset \mathbb{Q}(\sqrt[7]{2})$, y que $[\mathbb{Q}(\sqrt[7]{2}) : \mathbb{Q}] = 7$, ya que el polinomio mínimo de $\sqrt[7]{2}$ sobre $\mathbb{Q}$ es x^7-2 (irreducible por el Criterio de Eisenstein con $p=2$). Por lo tanto $[\mathbb{Q}(\sqrt[7]{2}+2\sqrt[7]{4}+3\sqrt[7]{8}) : \mathbb{Q}] = 1$ ó 7. Si fuese 1, $\sqrt[7]{2}+2\sqrt[7]{4}+3\sqrt[7]{8} \in \mathbb{Q}$, lo cual no es posible ya que 1, $\sqrt[7]{2}$, $\sqrt[7]{4}$ y $3\sqrt[7]{8}$ son linealmente independientes sobre $\mathbb{Q}$. Por lo tanto el grado pedido es 7.

b. $\mathbb{Q}(\sqrt[5]{5}, e^{\frac{2\pi i}{5}})/\mathbb{Q}$.

Sea $n = [\mathbb{Q}(\sqrt[5]{5}, e^{\frac{2\pi i}{5}}) : \mathbb{Q}]$. Por un lado, $[\mathbb{Q}(\sqrt[5]{5}) : \mathbb{Q}] = 5$, ya que el polinomio mínimo de $\sqrt[5]{5}$ sobre $\mathbb{Q}$ es $x^5 - 5$ (irreducible por el Criterio de Eisenstein con $p = 5$). Como consecuencia $5|n$. Por otro, $[\mathbb{Q}(e^{\frac{2\pi i}{5}}) : \mathbb{Q}] = 4$ ya que el polinomio mínimo de $e^{\frac{2\pi i}{5}}$ sobre $\mathbb{Q}$ es $x^4 + x^3 + x^2 + x + 1$ (polinomio ciclotómico), por lo que $4|n$. Como 5 y 4 son coprimos, necesariamente $20|n$, pero como $[\mathbb{Q}(\sqrt[5]{5}, e^{\frac{2\pi i}{5}}) : \mathbb{Q}(\sqrt[5]{5})][\mathbb{Q}(\sqrt[5]{5} : \mathbb{Q}] \leq 4 \times 5 = 20$, el grado pedido es 20.

c. $L/\mathbb{F}_2$, con L el cuerpo de descomposición de $x^3 + x^2 + x + 1$.

Como $x^3 + x^2 + x + 1 = (x + 1)^3$, el grado es 1.

d. $\mathbb{Q}(\sqrt[6]{2}, i)/\mathbb{Q}(\sqrt[3]{2})$.

Por un lado $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$ ya que el polinomio mínimo de $\sqrt[6]{2}$ sobre $\mathbb{Q}$ es $x^6 - 2$ (irreducible por Eisenstein con $p = 2$). Como además $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ dado que el polinomio mínimo de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ es $x^3 - 2$ (irreducible por Eisenstein con $p = 2$), se tiene que $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 2$.

Por otro lado, $[\mathbb{Q}(i, \sqrt[6]{2}) : \mathbb{Q}(\sqrt[6]{2})] = 2$ puesto que $\mathbb{Q}(\sqrt[6]{2}) \subset \mathbb{R}$ y las raíces de $x^2 + 1$ son imaginarias, lo que significa que $x^2 + 1$ es irreducible sobre $\mathbb{Q}(\sqrt[6]{2})$. Como consecuencia, $[\mathbb{Q}(\sqrt[6]{2}, i) : \mathbb{Q}(\sqrt[3]{2})] = [\mathbb{Q}(\sqrt[6]{2}, i) : \mathbb{Q}(\sqrt[6]{2})][\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 4$.

---

3. (2 puntos) Decide si cada uno de los siguientes enunciados es **verdadero** o **falso**. Justifica tus respuestas.

a. $\mathbb{F}_{32}$ es una extensión de $\mathbb{F}_8$.

FALSO: Si $\mathbb{F}_8 \subset \mathbb{F}_{32}$, entonces $3 = [\mathbb{F}_8 : \mathbb{F}_2]$ dividiría a $[\mathbb{F}_{32} : \mathbb{F}_2] = 5$, lo cual es imposible.

b. La extensión $\mathbb{Q}(x)/\mathbb{Q}(x^2)$ es normal.

VERDADERO: Como la extensión es finita (ya que x es algebraico sobre $\mathbb{Q}(x^2)$ al ser raíz de $T^2 - x^2 \in \mathbb{Q}(x^2)[T]$), es suficiente probar que $\mathbb{Q}(x)$ es el cuerpo de descomposición de algún polinomio con coeficientes en $\mathbb{Q}(x^2)$, pero esto es inmediato, dado que es el cuerpo más pequeño que contiene las dos raíces de $T^2 - x^2$, que son $x, -x$.

c. Una extensión de grado primo es simple.

VERDADERO: Sea L/K una extensión de grado primo p, y sea $\alpha \in L$ con $\alpha \notin K$. Entonces $[K(\alpha) : K]$ divide a p y es mayor que 1, por lo que necesariamente $[K(\alpha) : K] = p$ y como consecuencia $K(\alpha) = L$.

d. Sea L/K una extensión Galois con grupo de Galois isomorfo a D_4. Entonces hay exactamente dos extensiones intermedias de grado 4 sobre K.

FALSO: En D_4 hay al menos tres subgrupos de orden 2 (basta considerar las simetrías del cuadrado con vértices consecutivos 1, 2, 3, 4: las permutaciones $(12)(34), (13)(24)$ y (23) son elementos distintos de D_4 con orden 2). Por el Teorema Fundamental de la Teoría de Galois estos subgrupos se corresponden con tres subcuerpos intermedios distintos con grado $8/2 = 4$ sobre K.

---

4. (3 puntos) Sea $L = \mathbb{Q}(e^{\frac{2\pi i}{5}})$. Responde razonadamente a las siguientes preguntas:

a. Calcula $\mathcal{G}(L/\mathbb{Q})$.

En primer lugar observamos que la extensión $L/\mathbb{Q}$ es Galois ya que:
- Es finita porque $e^{\frac{2\pi i}{5}}$ es algebraico sobre $\mathbb{Q}$, al ser raí de $x^5 - 1$.
- Es normal porque $e^{\frac{2\pi i}{5}}$ y sus potencias son todas las raíces de $x^5 - 1$, por lo que L es el cuerpo de descomposición de este polinomio sobre $\mathbb{Q}$.
- Es separable porque $\mathbb{Q}$ tiene característica cero.

Por lo tanto $|\mathcal{G}(L/\mathbb{Q})| = [L/\mathbb{Q}]$, y este último grado es 4 (ver justificación en el ejercicio 2 (b)). Como consecuencia, $\mathcal{G}(L/\mathbb{Q}) \simeq \mathbb{Z}_4$ ó $\mathbb{Z}_2 \times \mathbb{Z}_2$, que son los únicos grupos de orden 4 salvo isomorfismos.

Sea $\xi = e^{\frac{2\pi i}{5}}$. Para cada $i = 1, \ldots, 4$, existe $\gamma_i \in \mathcal{G}(L/\mathbb{Q})$ tal que $\gamma_i(\xi) = \xi^i$. Como todos estos automorfismos son distintos, se tiene que necesariamente $\mathcal{G}(L/\mathbb{Q}) = \{\gamma_1, \ldots, \gamma_4\}$. Para finalizar, basta observar que el elemento γ_2 tiene orden 4, ya que $\gamma_2(\xi) = \xi^2$, $\gamma_2^2(\xi) = \xi^4$, $\gamma_2^3(\xi) = \xi^8 = \xi^3$, y $\gamma_2^4(\xi) = \xi^6 = \xi$. Por lo tanto $\mathcal{G}(L/\mathbb{Q}) \simeq \mathbb{Z}_4$.

b. Calcula el número de subcuerpos intermedios.

Como $\mathbb{Z}_4$ sólo tiene un subgrupo propio, por el Teorema Fundamental de la Teoría de Galois la extensión tiene un único subcuerpo intermedio, que necesarimente tendrá grado 2 sobre $\mathbb{Q}$.

c. Describe todas las extensiones intermedias que sean normales sobre $\mathbb{Q}$.

Por lo visto en (b) sólo hay una extensión intermedia, que además es normal ya que $\mathbb{Z}_4$ es abeliano y por tanto todos subgrupos son normales. Sea M esta extensión intermedia. Entonces, por el Teorema Fundamental de la Teor´ía de Galois M coincide con el cuerpo fijo por el único subgrupo de orden 2 de $\mathcal{G}(L/\mathbb{Q})$, que es $\langle\gamma_4\rangle$.

Para describir M, fijamos una base de $L/\mathbb{Q} : \{1, \xi, \xi^2, \xi^3\}$, y sea $\lambda_0 + \lambda_1\xi + \lambda_2\xi^2 + \lambda_3\xi^3$, con $\lambda_i \in \mathbb{Q}$, un elemento genérico de L. Este elemento se queda fijo por γ_4 si y sólo si:

$$\lambda_0 + \lambda_1\xi + \lambda_2\xi^2 + \lambda_3\xi^3 = \gamma_4(\lambda_0 + \lambda_1\xi + \lambda_2\xi^2 + \lambda_3\xi^3) = \lambda_0 + \lambda_1\xi^4 + \lambda_2\xi^3 + \lambda_3\xi^2 =$$
$$= \lambda_0 + \lambda_1(-\xi^3 - \xi^2 - \xi - 1) + \lambda_2\xi^3 + \lambda_3\xi^2.$$

Por lo tanto: $\lambda_1 = 0$, $\lambda_3 = \lambda_2$ y $M = \mathbb{Q}(\xi^2 + \xi^3) = \mathbb{Q}(\cos\frac{2\pi}{5})$.

d. Describe $\mathcal{G}(L/\mathbb{Q}(\cos\frac{2\pi}{5}))$ y $\mathcal{G}(\mathbb{Q}(\cos\frac{2\pi}{5})/\mathbb{Q})$.

Por el Teorema Fundamental de la Teoría de Galois, $\mathcal{G}(L/\mathbb{Q}(\cos\frac{2\pi}{5}))$ es un subgrupo de $\mathcal{G}(L/\mathbb{Q})$ que tiene orden 2 (ver apartado (c)) y consta de aquellos elementos de $\mathcal{G}(L/\mathbb{Q})$ que fijan $\mathbb{Q}(\cos\frac{2\pi}{5})$). Por lo visto en (c) este grupo es $\langle\gamma_4\rangle$, que es isomorfo a $\mathbb{Z}_2$.

De nuevo, por el Teorema Fundamental de la Teoría de Galois, $\mathcal{G}(\mathbb{Q}(\cos\frac{2\pi}{5})/\mathbb{Q})$ es isomorfo al cociente $\mathcal{G}(L/\mathbb{Q})/\mathcal{G}(L/\mathbb{Q}(\cos\frac{2\pi}{5}))$, que tiene orden 2, y por lo tanto es isomorfo a $\mathbb{Z}_2$. Además es fácil observar que este grupo coincide con el generado por $\gamma_2 \bmod \langle\gamma_4\rangle$, y que $\gamma_2(\cos\frac{2\pi}{5}) = 1/2\gamma_2(\xi + \xi^4) = 1/2(\xi^2 + \xi^3) = -\cos\frac{2\pi}{5}$.