Examen parcial de Álgebra II

Viernes, 26 de marzo de 2004

SOLUCIONES

Solución del problema 1. (a) Observamos en primer lugar que la aplicación ϕ evalúa cada polinomio en 1, es decir, si $p(x) \in \mathbb{Z}[x]$, entonces $\phi(p(x)) = p(1)$. Esta función es un homomorfismo de anillos si para todo par de polinomios $p(x), q(x) \in \mathbb{Z}[x]$, se tiene que:

(i) $\phi(p(x) + q(x)) = \phi(p(x)) + \phi(q(x))$.

(ii) $\phi(p(x)q(x)) = \phi(p(x))\phi(q(x))$.

iii) $\phi(1) = 1$.

Sean $p(x), q(x) \in \mathbb{Z}[x]$. Entonces

$$\phi(p(x) + q(x)) = \phi((p + q)(x)) = (p + q)(1) = p(1) + q(1) = \phi(p(x)) + \phi(q(x)),$$

lo que prueba (i), y

$$\phi(p(x)q(x)) = \phi((pq)(x)) = (pq)(1) = p(1)q(1) = \phi(p(x))\phi(q(x)),$$

lo que prueba (ii). La condición (iii) se cumple de manera trivial (aquellos que no hayan incluido la condición (iii) en la definición de homomorfismo, no han sido penalizados por ello).

Además ϕ es sobreyectivo, dado que si $n \in \mathbb{Z}$, entonces basta tomar el polinomio constante $p(x) = n$ como su preimagen.

(b) Por definición

$$\ker \phi = \{p(x) \in \mathbb{Z}[x] : \phi(p(x)) = 0\},$$

es decir,

$$\ker \phi = \{p(x) \in \mathbb{Z}[x] : p(1) = 0\},$$

y de hecho, $\ker \phi = \langle x - 1\rangle$. Para probar esta afirmación en primer lugar observamos que obviamente $\langle x - 1\rangle \subset \ker \phi$. Para probar la otra inclusión, notamos que como $x - 1$ es un polinomio mónico, todo polinomio $p(x) \in \mathbb{Z}[x]$ se puede escribir como

$$p(x) = q(x)(x - 1) + r(x) \tag{1}$$

para ciertos $q(x), r(x) \in \mathbb{Z}[x]$, con $r(x) = 0$, o $\deg(r(x)) < 1$. Si $p(x) \in \ker \phi$, entonces $p(1) = 0$, y por lo tanto $r(1) = 0$. Esto prueba que en (1), necesariamente $r(x) = 0$, y por lo tanto $p(x) \in \langle x - 1\rangle$.

Errores más comunes. El apartado (a) se puede hacer probando directamente que, dados dos polinomios genéricos

$$p(x) = a_0 + a_1x + \ldots + a_nx^n, q(x) = b_0 + b_1x + \ldots + b_mx^m \in \mathbb{Z}[x],$$

$\phi(p(x)+q(x)) = \phi(p(x))+\phi(q(x))$, y $\phi(p(x)q(x)) = \phi(p(x))\phi(q(x))$. En tal caso **NO** se puede suponer que los dos polinomios tienen el mismo grado.

Solución del problema 2. (a) El ideal I es maximal si siempre que un ideal J contiene a I, se tiene que o bien $I = J$ o bien $J = \mathbb{Z} \oplus \mathbb{Z}$. Supongamos que J contiene a I, pero que $I \neq J$. Entonces existe un elemento $(a, b) \in J$ tal que $(a, b) \notin I$ (es decir a es impar). Pero si este es el caso, el elemento $(a, b) - (a - 1, b - 1) = (1, 1) \in J$ ya que $(a - 1, b - 1)$ está en I y por tanto en J. Como consecuencia

$$\mathbb{Z} \oplus \mathbb{Z} = \langle(1, 1)\rangle = J,$$

luego I es maximal.

(b) Dos elementos $(a, b), (c, d) \in \mathbb{Z} \oplus \mathbb{Z}$ representan la misma clase en $\mathbb{Z} \oplus \mathbb{Z}/I$, si su diferencia $(a, b) - (c, d) = (a - c, b - d)$ está en I. Por lo tanto

$$(a, b) = (c, d) \bmod I \Leftrightarrow \begin{cases} a \equiv b \bmod 2; \text{ y} \\ c - d \in \mathbb{Z}. \end{cases}$$

Por lo tanto

$$\mathbb{Z} \oplus \mathbb{Z}/I = \{\overline{(0, 0)}, \overline{(1, 0)}\} \simeq \mathbb{Z}_2.$$

Obsérvese que esto además prueba que I es maximal ya que $\mathbb{Z}_2$ es un cuerpo.

Errores más comunes. El anillo $\mathbb{Z} \oplus \mathbb{Z}$ **NO** es igual a $\langle(1, 0)\rangle$.

Solución del problema 3. El polinomio $x^2 + 3$ es irreducible sobre $\mathbb{Z}$ (por ejemplo, por el Criterio de Eisenstein con $p = 3$). Por otro lado, $\overline{x^2 + 3} = \overline{x}^2 \in \mathbb{Z}_3[x]$ es reducible sobre $\mathbb{Z}_3$.

Errores más comunes. Sea $p(x) = a_0+a_1x+\ldots+a_nx^n \in \mathbb{Z}$. El Criterio de Eisenstein se aplica cuando existe un primo p que divide a $a_0, \ldots, a_{n-1}$, que no divide a a_n, y cuyo cuadrado no divide a a_0. La condición de que a_0 es divisible por p es necesaria para aplicar el criterio correctamente.

Solución del problema 4. a) A es un cuerpo si y sólo si (x^2+x+1) es un ideal maximal en $\mathbb{Z}_2[x]$, y como $\mathbb{Z}_2[x]$ es un dominio de ideales principales esto ocurre si y sólo si x^2+x+1 es irreducible en $\mathbb{Z}_2[x]$. Si no fuera irreducible, $x^2+x+1=(x-\alpha)(x-\beta)$, entonces tendría raíces en $\mathbb{Z}_2$, lo cual no es cierto porque $0^2+0+1\neq 0$, $1^2+1+1\neq 0$.

b) $x^2+x+1=(x+1)x+1$, y de aquí $1=x^2+x+1+(x+1)x$ (en $\mathbb{Z}_2, 1=-1$). Por tanto en A, $\overline{1}=\overline{x+1}\cdot\overline{x}$ y se sigue que $\overline{x}$ es el inverso buscado.

Errores más comunes. El polinomio ciclotómico es irreducible en $\mathbb{Q}[x]$ pero eso no implica que lo sea en todo $\mathbb{Z}_p[x]$. Por ejemplo, x^2+x+1 no es irreducible en $\mathbb{Z}_3[x]$.

Solución del problema 5.

Evidentemente $\alpha^2\in K(\alpha)$ y se tienen el esquema indicado, donde $a\cdot b=5$. Esto implica $a=1$, $b=5$ o $a=5$, $b=1$. El primer caso implica $[K(\alpha^2):K]=5$, como queremos probar, y el segundo lleva a una contradicción, porque $[K(\alpha^2):K]=1\Rightarrow\alpha^2\in K\Rightarrow x^2-\alpha^2\in K[x]$ y tiene a α como raíz $\Rightarrow[K(\alpha):K]\leq 2$, lo que contradice el enunciado.

$$\begin{array}{c} K(\alpha) \\ |\,a \\ K(\alpha^2) \\ |\,b \\ K \end{array}$$

Errores más comunes. No tiene sentido en general hablar de $K(\alpha^2)/K(\alpha)$ y de su grado. La inclusión natural es $K(\alpha)\supset K(\alpha^2)$ y la contraria no tiene por qué ser cierta, de modo que en general $K(\alpha^2)$ no extiende a $K(\alpha)$. Por ejemplo, si $\alpha=\sqrt{2}$, se tiene $\mathbb{Q}(\alpha)\not\subset\mathbb{Q}(\alpha^2)=\mathbb{Q}$.

Solución del problema 6. Sea $\alpha=\sqrt{1+\sqrt{3}}$. Entonces $\alpha^2-1=\sqrt{3}\Rightarrow\alpha^4-2\alpha^2+1=3\Rightarrow\alpha$ es raíz de $P=x^4-2x^2-2\in\mathbb{Q}[x]$. Este polinomio es mónico e irreducible por el criterio de Eisenstein con $p=2$, por tanto P es el polinomio mínimo de α y se tiene $[\mathbb{Q}(\alpha):\mathbb{Q}]=\partial P=4$.

Errores más comunes. Emplear $[\mathbb{Q}(\alpha):\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}]$ no es erróneo pero lleva a cálculos más complicados, ya que no es en absoluto evidente que $[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{3})]=2$.
