Universidad de la Aepública
Facultad de Ciencias
Centro de Matemática

Álgebra I
Segundo semestre 2005

Práctico 5

1. Sea $A = \{f : \mathbb{Z}^+ \to \mathbb{Z} : \; f \text{ es función}\}$. Se definen $+, * : A \times A \to A$ mediante

$$(f+g)(n) = f(n) + g(n), \quad (f*g)(n) = \sum_{xy=n} f(x)\, g(y), \quad \forall f, g \in A, \; n \in \mathbb{Z}^+.$$

a) Probar que $(A, +, *)$ es un anillo conmutativo con elemento unidad $\delta : \mathbb{Z}^+ \to \mathbb{Z}$ definido por $\delta(n) = 1$ si $n = 1$ y $\delta(n) = 0$ si $n \neq 1$.

b) Una función $f \in A$ se dice *multiplicativa* si verifica $f(mn) = f(m)\, f(n)$, $\forall m, n \in \mathbb{Z}^+$ tales que $\operatorname{mcd}(m, n) = 1$. Probar que si $f, g \in A$ son multiplicativas, entonces $f * g$ es multiplicativa.

c) Se define la *función de Möbius* $\mu : \mathbb{Z}^+ \to \mathbb{Z}$ mediante:

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si el cuadrado de un primo divide a } n, \\ (-1)^k & \text{si } n \text{ es el producto de } k \text{ primos diferentes.} \end{cases}$$

1) Probar que μ es multiplicativa.

2) Probar que $\forall n \in \mathbb{Z}^+$ es $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \neq 1 \end{cases}$.
Sugerencia: sea $\varphi_1 \in A$ la función constante 1; observar que la igualdad que se quiere probar equivale a $\mu * \varphi_1 = \delta$ y basta con probar esta última para potencias de primos.

3) Si ϕ es la función de Euler, probar la *fórmula de inversión*:

$$\phi(n) = \sum_{d|n} \mu(n/d) d, \quad \forall n \in \mathbb{Z}^+.$$

2. *a*) Probar que $D = \left\{a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in \mathbb{Z}[X] : \; a_1 = 0\right\}$ es un dominio que no es un dominio factorial.

b) Probar que $\mathbb{Z}[X]$ es un dominio factorial que no es un dominio de ideales principales.

3. Sea $D = \{a + b\sqrt{10} : a, b \in \mathbb{Z}\} \subset \mathbb{R}$. Probar que:

a) Si definimos $* : D \to D$ mediante $\left(a + b\sqrt{10}\right)^* = a - b\sqrt{10}$, se verifica que $\forall u, v \in D$ es $(uv)^* = u^* v^*$ y que $u^* = u$ si y solo si $u \in \mathbb{Z}$.

b) La función $N : D \to \mathbb{Z}$ definida por $N(u) = u\, u^*$, verifica $N(uv) = N(u)N(v)$ para todo $u, v \in D$, y $N(u) = 0$ si y solo si $u = 0$.

c) Un elemento $u \in D$ es invertible si y solo si $N(u) = \pm 1$.

d) Los elementos $2, \; 3, \; 4 + \sqrt{10}$ y $4 - \sqrt{10}$ son irreducibles en D.
Sugerencia: observar que las ecuaciones $x^2 = 2$ y $x^2 = 3$ no tienen solución en $\mathbb{Z}_5$.

e) Los elementos $2, \; 3, \; 4 + \sqrt{10}$ y $4 - \sqrt{10}$ no son primos en R.
Sugerencia: observar que $3 \cdot 2 = \left(4 + \sqrt{10}\right)\left(4 - \sqrt{10}\right)$.

4. Sea D un dominio de ideales principales.

   a) Sea P un ideal propio de D. Probar que existen ideales maximales $P_1, \dots, P_r$ de D tales que $P = P_1 \cdots P_r$ y que esta descomposición es única a menos del orden de los factores.

   b) Un ideal P de D se dice *primario* si verifica $ab \in P$ y $a \notin P$, entonces $\exists n \in \mathbb{Z}^+$ tal que $b^n \in P$. Probar que un ideal P es primario si y solo si $P = \{0\}$ o existen $n \in \mathbb{Z}^+$ y $p \in D$ irreducible tales que $P = \langle p^n \rangle$.

   c) Si $P_1, \dots, P_n$ son ideales primarios con $P_i = \langle p_i^{m_i} \rangle$, $\forall i = 1, \dots, n$, siendo $p_1, \dots, p_n$ elementos irreducibles no asociados, entonces $P_1 \cdots P_n = P_1 \cap \cdots \cap P_n$.

   d) Sea P un ideal propio de D. Probar que existen ideales primarios $P_1, \dots, P_n$ de D tales que $P = P_1 \cap \cdots \cap P_n$ y que esta descomposición es única a menos del orden de los factores.

5. Un dominio D se dice *euclídeo* si existe una función $\delta : D \setminus \{0\} \to \mathbb{N}$ que verifica:

   - Para todo $a, b \in D \setminus \{0\}$ es $\delta(a) \leq \delta(ab)$.
   - Si $a, b \in D$ con $b \neq 0$, entonces existen $q, r \in D$ tales que $a = bq + r$, con $r = 0$ o $r \neq 0$ y $\delta(r) < \delta(b)$.

   a) Probar que $\mathbb{Z}$ y $K[X]$ son dominios euclídeos (K cuerpo).

   b) Probar que todo dominio euclídeo es un dominio de ideales principales.

   c) Probar que si D es un dominio euclídeo, entonces $\delta(a) \geq \delta(1)$, $\forall a \in D \setminus \{0\}$ y $a \in D \setminus \{0\}$ es invertible si y solo si $\delta(a) = \delta(1)$.

6. *Algoritmo de Euclides*. Sean a_1, a_2 elementos no nulos de un dominio euclídeo D.
   Se definen a_i y q_i por recurrencia por $a_1 = q_1 a_2 + a_3$, $a_i = q_i a_{i+1} + a_{i+2}$, donde $\delta(a_{i+2}) < \delta(a_{i+1})$, $\forall i = 1, 2, \dots$.

   a) Probar que existe n tal que $a_n \neq 0$ y $a_{n+1} = 0$, y que $a_n = \operatorname{mcd}(a_1, a_2)$.

   b) Utilizar la construcción de la parte anterior para expresar $\operatorname{mcd}(a_1, a_2)$ en la forma $xa_1 + ya_2$, con $x, y \in D$.

   c) Utilizar el algoritmo de Euclides para encontrar el máximo común divisor de $x^3 + x^2 + x - 3$ y $x^4 - x^3 + 3x^2 + x - 4$ en $\mathbb{Q}[x]$.

7. *a*) Sean $m, n \in \mathbb{Z}$, $n > 0$. Probar que existen $q, r \in \mathbb{Z}$ tales que $m = qn + r$ y $|r| \leq n/2$.

   b) Sean $a, b, c \in \mathbb{Z}$, $c > 0$. Probar que existen $r, q \in \mathbb{C}$ tales que $a + bi = qc + r$ y $|r|^2 < c^2$.
   Sugerencia: aplicar la parte anterior con a y b en lugar de m.

   c) Probar que los enteros de Gauss $\mathbb{Z}[i]$ son un dominio euclídeo definiendo $\delta(z) = z\overline{z} = |z|^2$, $z \in \mathbb{Z}[i] \subset \mathbb{C}$.
   Sugerencia: dados $y = a + bi$ y $x = c + di \in \mathbb{Z}[i]$, $x \neq 0$, hay que probar que existen $q, r \in \mathbb{Z}[i]$ tales que $y = qx + r$ con $r = 0$ o $r \neq 0$ y $\delta(r) < \delta(x)$. Si $x \in \mathbb{Z}^+$, es la parte anterior. En el caso general, probar que existen $q, r_0 \in \mathbb{Z}[i]$ tales que $y\overline{x} = qx\overline{x} + r_0$ y $r_0 = 0$ o $r_0 \neq 0$ y $\delta(r_0) < \delta(x\overline{x})$; luego tomar $r = y - qx$.

   d) Hallar los elementos invertibles de $\mathbb{Z}[i]$.