PRÁCTICO 6

Factorización.

(1) Probar las siguientes afirmaciones.
  (a) $\mathbb{Z}$ es un dominio de ideales principales.
  (b) Si R es un anillo de ideales principales y $f : R \to S$ es un homomorfismo de anillos suryectivo, entonces S es un anillo de ideales principales.
  (c) $\mathbb{Z}_n$ es anillo de ideales principales, para todo $n \geq 2$.

(2) Sea $R := \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$. Probar las siguientes afirmaciones.
  (a) R es subanillo de $\mathbb{R}$.
  (b) La función $N : R \to \mathbb{Z}$ dada por $N(a + b\sqrt{10}) := a^2 - 10b^2$ satisface $N(uv) = N(u)N(v)$, para todo $u, v \in R$.
  (c) $N(u) = 0$ si y sólo si $u = 0$.
  (d) u es una unidad en R si y sólo si $N(u) = \pm 1$.
  (e) 2, 3, $4 + \sqrt{10}$ y $4 - \sqrt{10}$ son elementos irreducibles de R.
  (f) 2, 3, $4 + \sqrt{10}$ y $4 - \sqrt{10}$ no son elementos primos de R.

(3) Probar que en un DIP las nociones de ideal primo e ideal maximal son equivalentes.

(4) Si R es un DFU, $a, b \in R$ son coprimos y $a \mid bc$, entonces $a \mid c$.

(5) Sea (R, φ) anillo euclidiano. Probar que a es unidad en R si y sólo si $\varphi(a) = \varphi(1)$.

(6) Consideremos el anillo de *enteros Gaussianos* $\mathbb{Z}[i]$.
  (a) Probar que es dominio euclidiano con $\varphi(a + bi) = a^2 + b^2$.
  (b) Determinar las unidades.
  (c) Calcular el máximo común divisor de $11 + 7i$ y $18 - i$ en $\mathbb{Z}[i]$.

(7) Dar ejemplos de:
  (a) Anillos de ideales principales con 1 que no son anillos euclídeos.
  (b) Dominios de factorización única que no son dominios de ideales principales.

(8) Sea R el dominio euclídeo de enteros de Gauss $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$.
  (a) Dividir $4 + 5i$ por $2 + 3i$ de dos maneras distintas.
  (b) ¿De cuántas maneras distintas se puede hacer la división del item anterior?
  (c) Dividir $a + bi$ por la unidad i. ¿Se puede hacer de dos maneras distintas?
  (d) Diseñar un algoritmo para dividir dos enteros de Gauss cualesquiera.

Anillos de polinomios.

(9) Describir los siguientes anillos.
  (i) $\mathbb{Z}[x]/(2, x)$.
  (ii) $\mathbb{Z}[x]/(2x)$.
  (iii) $\mathbb{Z}[i]/(i)$.
  (iv) $\mathbb{Z}[i]/(1 + i)$.

(10) Sean R anillo conmutativo con 1 y $p = \sum_{j=0}^{n} a_j x^j$ un polinomio en $R[x]$. Probar las siguientes afirmaciones:
  (a) p es divisor de cero si y sólo si existe $0 \neq b \in R$ tal que $ba_n = ba_{n-1} = \cdots = ba_0 = 0$.
  (b) p es unidad si y sólo si a_0 es unidad y $a_1, \ldots, a_n$ son nilpotentes.

(11) Sea K cuerpo. Probar que (x) es un ideal maximal en $K[x]$.

(12) Sea D un dominio íntegro.
  (a) Si D tiene un elemento irreducible c, entonces $I = (c, x)$ no es un ideal principal de $D[x]$.
  (b) Mostrar que $\mathbb{Z}[x]$ no es un dominio de ideales principales.

(c) Sean K un cuerpo y $n \in \mathbb{Z}$, con $n \geq 2$. Probar que $K[x_1, \ldots, x_n]$ no es un dominio de ideales principales. (Ayuda: mostrar que x_1 es irreducible en $K[x_1, \ldots, x_{n-1}]$).

(13) Sea R un anillo y denotemos por $R[[x]]$ al conjunto de todas las sucesiones de elementos de R, $(a_0, a_1, \ldots)$. Probar las siguientes afirmaciones:

(a) $R[[x]]$ es un anillo con la adición y la multiplicación definidas por:

$$\begin{aligned}(a_0, a_1, \ldots) + (b_0, b_1, \ldots) &= (a_0 + b_0, a_1 + b_1, \ldots),\\ (a_0, a_1, \ldots)\,(b_0, b_1, \ldots) &= (c_0, c_1, \ldots),\end{aligned}$$

donde $c_n = \sum_{i=0}^{n} a_i b_{n-i} = \sum_{k+j=n} a_k b_j$.

(b) El anillo de polinomios $R[x]$ es un subanillo de $R[[x]]$.

(c) Si R tiene la propiedad P, donde P es ser conmutativo, tener 1, no tener divisores de cero o ser dominio íntegro, entonces $R[[x]]$ también tiene la propiedad P.

Al anillo $R[[x]]$ se lo llama el anillo *de series formales sobre* R y al elemento $(a_0, a_1, \ldots) \in R[[x]]$ se lo denota por la serie formal $\sum_{i=0}^{\infty} a_i x^i$.

(14) Probar las siguientes afirmaciones:

(a) $x + 1$ es una unidad en $\mathbb{Z}[[x]]$, pero no es una unidad en $\mathbb{Z}[x]$.

(b) $x^2 + 3x + 2$ es irreducible en $\mathbb{Z}[[x]]$, pero no en $\mathbb{Z}[x]$.

(15) Sea K cuerpo y sea $p \in K[x]$. Probar que $K[x]/(p)$ es cuerpo si y sólo si p es irreducible. ¿Sigue valiendo esta afirmación si asumimos que K es anillo conmutativo con 1?

(16) Dado $m \in \mathbb{N}$, consideremos el anillo de polinomios con coeficientes en $\mathbb{Z}_m$, $\mathbb{Z}_m[x]$ y sea $f(x) \in \mathbb{Z}_m[x]$ de grado n.

(a) Probar que si $m = p$ es un primo, entonces la ecuación $f(x) = 0$ tiene a lo sumo n soluciones distintas.

(b) Calcular las soluciones de $2x^2 - 2x = 0$ y de $x^2 + x + 2 = 0$ para los casos $m = 3$ y $m = 4$.

(c) Sea $m = p_1^{\ell_1} \ldots p_r^{\ell_r}$ la factorización de m. Probar que la ecuación $f(x) = 0$ tiene solución en $\mathbb{Z}_m$ si y sólo si $f(x) = 0$ tiene solución en $\mathbb{Z}_{p_i^{\ell_i}}$ para todo $i = 1 \ldots r$.

(d) Resolver la ecuación $3x^2 + 2x + 3 = 0$ en $\mathbb{Z}_{30}$.

Ejercicios adicionales

(17) Sean R un anillo y S un subanillo. Decir si las siguientes afirmaciones son verdaderas o falsas.

(a) Si R es DFU, S es DFU.

(b) Si S es DFU, R es DFU.

(18) Sea R un dominio de factorización única (DFU), $d \in R$, $d \neq 0$. Probar que existe sólo un número finito de ideales principales distintos que contienen al ideal (d).

(19) (Algoritmo euclidiano). Sea (R, φ) un dominio euclidiano. Sean $a, b \in R$, con $b \neq 0$. Consideremos el siguiente algoritmo.

$$\begin{array}{rcccc} a = q_0 b + r_1 & \text{con} & r_1 = 0 & \text{ó} & \varphi(r_1) < \varphi(b); \\ b = q_1 r_1 + r_2 & \text{con} & r_2 = 0 & \text{ó} & \varphi(r_2) < \varphi(r_1); \\ \vdots & & & & \\ r_k = q_{k+1} r_{k+1} + r_{k+2} & \text{con} & r_{k+2} = 0 & \text{ó} & \varphi(r_{k+2}) < \varphi(r_{k+1}); \\ \vdots & & & & \end{array}$$

Sea $r_0 = b$ y sea n el mínimo entero tal que $r_{n+1} = 0$ (un tal n existe pues $(\varphi(r_k))_k$ forma una sucesión estrictamente decreciente de enteros no negativos). Probar que r_n es el máximo común divisor de a y b.

(20) Sean D un dominio íntegro y c_j, $d_j \in D$, $0 \leq j \leq n$, con $c_0, \ldots, c_n$ distintos entre sí. Probar que existe a lo sumo un polinomio $f \in D[x]$, con $\mathrm{gr}(f) \leq n$, tal que $f(c_j) = d_j$, $0 \leq j \leq n$.

(21) Sea R un anillo con identidad y sea $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$.
  (a) f es una unidad en $R[[x]]$ si y sólo si su término constante a_0 es una unidad en R.
  (b) si a_0 es irreducible en R, entonces f es irreducible en $R[[x]]$.

(22) Sea $R = M_2(\mathbb{Z})$. Probar que, para todo $A \in R$, $(x + A)(x - A) = x^2 - A^2$ en $R[x]$.

(23) Sea R un anillo cualquiera y sean $f, g, h \in R[x]$ tales que $f = gh$. ¿Se puede asegurar que $f(r) = g(r)h(r)$, para todo $r \in R$?