

Ecuaciones Algebraicas. Curso 2006/7. Hoja de problemas 1.

1. Demostrar que si $f : A \rightarrow B$ es un homomorfismo suprayectivo de anillos y todos los ideales del anillo A son principales entonces todos los ideales de B son principales. Calcular todos los ideales de \mathbb{Z}_{12} y \mathbb{Z}_{16} .
2. Sea $a \in \mathbb{R}$. ¿Qué se deduce al aplicar el Primer Teorema de Isomorfía al homomorfismo $\mathbb{R}[X] \rightarrow \mathbb{R}$, dado por $P(X) \mapsto P(a)$? ¿Y qué se deduce al aplicarlo al homomorfismo $\mathbb{R}[X] \rightarrow \mathbb{C}$, dado por $P(X) \mapsto P(i)$?
3. Sea $f : A \rightarrow B$ un homomorfismo de anillos. Demostrar que:
 - (a) Si p es un ideal primo de B , entonces $f^{-1}(p)$ es un ideal primo de A .
 - (b) Si m es un ideal maximal de B y f es suprayectiva, entonces $f^{-1}(m)$ es un ideal maximal de A . Dar un ejemplo que muestre la necesidad de suponer que f sea suprayectiva.
 - (c) Concluir que las biyecciones del Teorema de la Correspondencia llevan ideales maximales (respectivamente primos) de A que contienen a I a ideales maximales (respectivamente primos) de A/I , y viceversa.
4. Demostrar que las siguientes condiciones son equivalentes para un anillo A .
 - (a) A es un cuerpo.
 - (b) Los únicos ideales de A son 0 y A .
 - (c) Todo homomorfismo de anillos $A \rightarrow B$ es inyectivo.
5. Sea $m \in \mathbb{Z}$. Decimos que m es *libre de cuadrados* si p^2 no divide a m para ningún número primo p (en particular 1 es libre de cuadrados). Demostrar:
 - (a) Si m no es un cuadrado en \mathbb{Z} , entonces tampoco es un cuadrado en \mathbb{Q} .
 - (b) Existe un $d \in \mathbb{Z}$ libre de cuadrados tal que $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{d}]$. ¿Ocurre lo mismo si cambiamos \mathbb{Q} por \mathbb{Z} ?
 - (c) $\mathbb{Q}(\sqrt{m})$ es un cuerpo, es decir, todos sus elementos no nulos son invertibles.
6. Demostrar que la característica de un dominio es 0 ó un número primo.
7. Sea A un anillo cuya característica es un número primo p . Demostrar que la aplicación $x \mapsto x^{p^n}$ es un endomorfismo de A para todo $n \in \mathbb{N}$.
8. Demostrar que, si K es un cuerpo finito con un subcuerpo F , entonces el cardinal de K es una potencia del cardinal de F . Deducir que:
 - (a) El cardinal de cualquier cuerpo finito es una potencia de un número primo. (Indicación: Considerar el subanillo primo de K .)
 - (b) Si K es un cuerpo finito con un subcuerpo F , entonces existen un número primo p y enteros positivos n y m tales que $n \mid m$, $|F| = p^n$ y $|K| = p^m$.
9. Sea A un anillo. Demostrar que A es un dominio si y sólo si el anillo de polinomios $A[X]$ es un dominio.
10. Sea D un dominio y sea Q su cuerpo de fracciones. Demostrar que:

- (a) Si D' es un subanillo de D con cuerpo de fracciones Q' , entonces Q contiene un subcuerpo isomorfo a Q' .
- (b) Si A es un subanillo de Q que contiene a D , entonces Q es un cuerpo de cocientes de A .
11. Sean D un DFU y P un conjunto de representantes de los irreducibles de D por la relación de equivalencia “ser asociados”, es decir P está formado por irreducibles de D y cada elemento irreducible p de D es asociado de un único elemento de P .
- (a) Demostrar que cada elemento a de D se puede escribir de forma única como $a = u \prod_{p \in P} p^{\alpha_p}$, donde u es una unidad de D , cada $\alpha_p \geq 0$ y $\alpha_p = 0$ para casi todo $p \in P$. Llamaremos a esto “la” factorización de a en irreducibles de P .
- (b) Demostrar que si
- $$a = u \prod_{p \in P} p^{\alpha_p} \quad \text{y} \quad b = v \prod_{p \in P} p^{\beta_p}$$
- son las factorizaciones de a y b en irreducibles de P entonces $a \mid b$ precisamente si $\alpha_p \leq \beta_p$, para todo $p \in P$.
- (c) El número de divisores de un elemento no nulo a de D es finito, salvo asociados. Es decir, existe un conjunto finito F tal que todos los divisores de a son asociados de un elemento de F .
- (d) Obtener una fórmula para calcular el número de divisores de a , salvo asociados, en términos de una factorización de a .
- (e) Dar ejemplos de conjuntos P como los del ejercicio para \mathbb{Z} y $K[X]$ donde K es un cuerpo.
12. Sea D un dominio y sean $S \subseteq D$ y $d \in D$. Decimos que d es un máximo común divisor de S en D si para todo $x \in D$ se verifica que $x \mid s$ en D para todo $s \in S$ si y sólo si $x \mid d$ en D . De forma análoga se define mínimo común múltiplo de S en D . Demostrar:
- (a) Si D es un DFU, entonces todo subconjunto finito de D un máximo común divisor y un mínimo común múltiplo en D .
- (b) Si D es un DIP y $d, m \in D$, entonces d es máximo común divisor de S en D si y sólo si $(d) = (S)$ y m es mínimo común múltiplo de S en D si y sólo si $(m) = \bigcap_{s \in S} (s)$.
13. Un *dominio euclídeo* es un dominio que admite una función euclídea. Una *función euclídea* en un dominio D es una aplicación $\delta : D \setminus \{0\} \rightarrow \mathbb{N}$ que cumple las siguientes condiciones:
- (DE1) Si $a, b \in D \setminus \{0\}$ verifican $a \mid b$ entonces $\delta(a) \leq \delta(b)$.
- (DE2) Dados $a, b \in D$ con $b \neq 0$, existen $q, r \in D$ tales que $a = bq + r$ y o bien $r = 0$ o bien $\delta(r) < \delta(b)$.
- (a) Demostrar que los siguientes anillos son dominios euclídeos: \mathbb{Z} , $\mathbb{Z}[i]$, $K[X]$, donde K es un cuerpo. (Indicación: Considerar el valor absoluto en \mathbb{Z} y $\mathbb{Z}[i]$ y el grado en $K[X]$.)
- (b) Demostrar que si δ es una función euclídea en D y $a \in D$, entonces:
- $$a \in D^* \Leftrightarrow \delta(a) = \delta(1) \Leftrightarrow \delta(a) \leq \delta(x), \forall x \in D \setminus \{0\}.$$
- (c) Calcular las unidades de $\mathbb{Z}[i]$.
- (d) Demostrar que todo dominio euclídeo es un DIP.