

Práctica 1

Nota: En esta práctica los anillos son conmutativos y tienen unidad $1 \neq 0$. Los morfismos de anillos respetan la unidad.

1. Sea A un anillo. Probar que:
 - (a) A tiene ideales maximales y todo ideal propio de A está contenido en un ideal maximal.
 - (b) \mathfrak{p} es un ideal primo de A si y sólo si A/\mathfrak{p} es un dominio íntegro.
 - (c) A es un cuerpo si y sólo si tiene exactamente dos ideales.
 - (d) \mathfrak{m} es un ideal maximal de A si y sólo si A/\mathfrak{m} es un cuerpo.
2. Probar que:
 - (a) Si K es un cuerpo y $f : K \rightarrow B$ es un morfismo de anillos, entonces f es inyectivo.
 - (b) Si A es un anillo tal que todo morfismo de anillos $f : A \rightarrow B$ es inyectivo, entonces A es un cuerpo.
3. Probar que si D es un dominio íntegro finito entonces D es un cuerpo.
4. Dado $b \in \mathbb{C}$ se define $\mathbb{Q}[b] = \{\sum_{i=0}^n a_i b^i \in \mathbb{C} : a_i \in \mathbb{Q}, n \in \mathbb{N}\}$. Probar que $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[i]$ y $\mathbb{Q}[\sqrt[3]{2}]$ son cuerpos.
5. Caracterizar los siguientes conjuntos:
 - (a) $\{f : \mathbb{C} \rightarrow \mathbb{R}, f \text{ morfismo de cuerpos}\}$.
 - (b) $\{f : \mathbb{Q} \rightarrow \mathbb{F}_p, f \text{ morfismo de cuerpos}\}$, p primo.
 - (c) $\{f : \mathbb{Q} \rightarrow K, f \text{ morfismo de cuerpos}\}$, K cuerpo fijo.
 - (d) $\{f : \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{2}], f \text{ morfismo de cuerpos}\}$.
 - (e) $\{f : \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{3}], f \text{ morfismo de cuerpos}\}$.
 - (f) $\{f : \mathbb{Q}[\sqrt[3]{2}] \rightarrow \mathbb{Q}[\sqrt[3]{2}], f \text{ morfismo de cuerpos}\}$.
 - (g) $\{f : \mathbb{C} \rightarrow \mathbb{C}, f \text{ morfismo de cuerpos tal que } f(a) = a \forall a \in \mathbb{R}\}$.
 - (h) $\{f : \mathbb{R} \rightarrow \mathbb{R}, f \text{ morfismo de cuerpos}\}$.
6. Sean K un cuerpo y A una K -álgebra de dimensión finita. Probar que si A es un dominio íntegro, entonces es un cuerpo.
7. Sea A un anillo. Notamos $\mathcal{U}(A)$ al conjunto de los elementos de A que tienen inverso multiplicativo.
 - (a) Probar que $(\mathcal{U}(A), \cdot)$ es un grupo, llamado el *grupo de unidades* de A .
 - (b) Caracterizar el grupo de unidades de los siguientes anillos: \mathbb{Z} , K (K cuerpo), $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-5}]$, $A[X]$ (A dominio íntegro) y $\mathbb{Z}/n\mathbb{Z}$.

8. Probar que si A es un dominio íntegro entonces $A[X]$ también lo es. Deducir que en ese caso $A[X_1, \dots, X_n]$ es dominio íntegro. ¿Qué pasa con $A[X_i : i \in I]$ donde I es un conjunto cualquiera?

9. Sea A un dominio íntegro. Consideramos en el conjunto $A \times (A - \{0\})$ la relación

$$(a, b) \sim (c, d) \iff ad = bc.$$

- (a) Probar que \sim es una relación de equivalencia.
 (b) Probar que $K = A \times (A - \{0\}) / \sim$ es un cuerpo con las siguientes operaciones:

$$\begin{aligned}(a, b) + (c, d) &= (ad + cb, bd) \\ (a, b) \cdot (c, d) &= (ac, bd).\end{aligned}$$

Decimos que K es el *cuerpo de cocientes* de A .

- (c) Probar que $f : A \rightarrow K$ definida por $f(a) = (a, 1)$ es un monomorfismo de anillos.
 (d) Sea D un anillo. Probar que son equivalentes:
 (i) D es un dominio íntegro.
 (ii) Existe $f : D \rightarrow K$ monomorfismo de anillos para algún cuerpo K .
10. Caracterizar el cuerpo de cocientes de los siguientes dominios íntegros: \mathbb{Z} , $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $A[X]$ (A dominio íntegro) y K (K cuerpo).
11. Sea A un dominio íntegro y sea $P \in A[X]$. Definimos $e_P : A[X] \rightarrow A[X]$ en la forma $e_P(Q) = Q(P(X))$. Probar que:
- (a) e_P es un morfismo de anillos, llamado *especialización en P* .
 (b) Todo morfismo de anillos de $A[X]$ en $A[X]$ que vale la identidad sobre A es una especialización en algún P .
 (c) Si una especialización e_P es un automorfismo de $A[X]$ entonces su inversa también es una especialización.
 (d) e_{cX+b} es un automorfismo de anillos si y sólo si $c \in \mathcal{U}(A)$.
 (e) Si f es un automorfismo de $A[X]$ tal que $f(a) = a \forall a \in A$, entonces f es de la forma e_{cX+b} para algún $c \in \mathcal{U}(A)$.
12. Sea A un dominio íntegro y sea $a \in A$. Probar que:
- (a) Si a es primo, entonces a es irreducible.
 (b) Si A es DFU (dominio de factorización única), a irreducible implica a primo.
 (c) En $\mathbb{Z}[\sqrt{-5}]$ los elementos $3, 7, 4 + \sqrt{-5}, 4 - \sqrt{-5}, 1 + 2\sqrt{-5}$ y $1 - 2\sqrt{-5}$ son irreducibles pero no primos. Concluir que $\mathbb{Z}[\sqrt{-5}]$ no es DFU.
 (d) Si A es DIP (dominio de ideales principales) entonces A es DFU, pero no vale la recíproca.
13. Un dominio íntegro A se dice *euclideo* si está provisto de un algoritmo de división, es decir, si existe $N : A - \{0\} \rightarrow \mathbb{N} \cup \{0\}$ que satisface las dos condiciones siguientes:

- $\forall a, b \in A - \{0\}$, si $a \mid b$ entonces $N(a) \leq N(b)$.
- $\forall a, b \in A - \{0\}$ existen $q, r \in A$ tales que $a = bq + r$ con $r = 0$ o $N(r) < N(b)$.

Probar que:

- \mathbb{Z} , $\mathbb{Z}[i]$, K y $K[X]$ (K cuerpo) son euclidianos.
 - Si A es euclidiano, entonces A es DIP.
- Sea $p \in \mathbb{Z}$ primo. Probar que son equivalentes:
 - $x^2 + 1$ es irreducible en $\mathbb{F}_p[X]$.
 - -1 no es un cuadrado en \mathbb{F}_p .
 - $p \equiv 3$ módulo 4.
 - p no es suma de dos cuadrados en \mathbb{Z} .
 - p es irreducible en $\mathbb{Z}[i]$.
 - Sea K un cuerpo y sea $f \in K[X]$. Probar que $K[X]/(f)$ es un cuerpo si y sólo si f es irreducible.
 - Construir un cuerpo de 9 elementos.
 - Probar que $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$.
 - Sean $p \in \mathbb{N}$ primo, $\pi : \mathbb{Z} \rightarrow \mathbb{F}_p$ el único morfismo de anillos, y $\bar{\pi} : \mathbb{Z}[X] \rightarrow \mathbb{F}_p[X]$ el morfismo de anillos inducido por π definido como $\bar{\pi}(\sum a_i X^i) = \sum \pi(a_i) X^i$. Sea $f \in \mathbb{Z}[X]$ tal que $\bar{\pi}(f) \neq 0$ y $\text{gr } \bar{\pi}(f) = \text{gr } f$. Probar que si $\bar{\pi}(f)$ es irreducible en $\mathbb{F}_p[X]$ entonces f no se factoriza en $\mathbb{Z}[X]$ como producto de polinomios de grado positivo.
 - Sea A un DFU y sea K su cuerpo de cocientes. Probar que si $f \in A[X]$ es un polinomio irreducible de grado > 0 entonces, visto como polinomio con coeficientes en K , también es irreducible. ¿Vale la recíproca?
 - Probar que si A es DFU entonces $A[X]$ también lo es. Deducir que en ese caso $A[X_1, \dots, X_n]$ también es DFU.
 - Criterio de irreducibilidad de Eisenstein.* Sea A un DFU y sea K su cuerpo de cocientes. Sea $f = \sum_{i=0}^n a_i X^i \in A[X]$, con $n > 0$. Probar que si existe un primo $p \in A$ que verifica: $p \nmid a_n$, $p \mid a_i$ ($\forall 0 \leq i \leq n-1$) y $p^2 \nmid a_0$, entonces f es irreducible en $K[X]$.
 - Teorema de Gauss.* Sea A un DFU y sea K su cuerpo de cocientes. Sea $f = \sum_{i=0}^n a_i X^i \in A[X]$ con $a_0 \neq 0$. Demostrar que si p y q son elementos no nulos de A , coprimos entre sí, tales que $\frac{p}{q} \in K$ es raíz de f , entonces $p \mid a_0$ y $q \mid a_n$ en A .
 - Sea $p \in \mathbb{Z}$ primo. Probar que:
 - $(X+1)^p - 1$ es divisible por X y $\frac{(X+1)^p - 1}{X}$ es irreducible en $\mathbb{Q}[X]$.
 - $1 + X + X^2 + \dots + X^{p-1}$ es irreducible en $\mathbb{Q}[X]$.
 - $X^n - p$ es irreducible en $\mathbb{Q}[X] \forall n \in \mathbb{N}$.

22. Sea K un cuerpo. Sea $f \in K[X]$ y sea $a \in K$ una raíz de f . Probar que a es raíz múltiple de f si y sólo si es raíz de su derivado.
23. Probar que si $f \in \mathbb{Q}[X]$ es irreducible, entonces f no tiene raíces múltiples en \mathbb{C} .
24. (a) Probar que $\sum_{i=0}^n X^i$ no tiene raíces múltiples en \mathbb{C} .
 (b) Probar que $\sum_{i=0}^n \frac{X^i}{i!}$ no tiene raíces múltiples en \mathbb{C} .
25. Determinar todos los polinomios de grado 2, 3, 4 y 5 irreducibles en $\mathbb{F}_2[X]$.
26. Sean $a, b \in \mathbb{Z}$.
 (a) Probar que $X^3 + aX^2 + bX + 1$ es reducible en $\mathbb{Z}[X]$ si y sólo si $a = b$ o $a + b = -2$.
 (b) Determinar condiciones necesarias y suficientes para que $X^3 + aX^2 + bX - 1$ sea reducible en $\mathbb{Z}[X]$. Lo mismo para $X^3 + b$.
27. Sea K un cuerpo y sea $a \in K$. Probar que $X^4 - a$ es reducible en $K[X]$ si y sólo si $a = b^2$ para algún $b \in K$ o $a = -4c^4$ para algún $c \in K$.
28. Factorizar $X^5 + X^4 + X^2 + X + 2$ en $\mathbb{Q}[X]$.
29. Analizar la reducibilidad de:
 (a) $2X^5 + 18X^3 + 30X^2 - 24$; $X^4 + 4X^2 + 10$; $X^3 - X^2 + 7X + 2$ en $\mathbb{Q}[X]$ y en $\mathbb{Z}[X]$.
 (b) $X^4 - 4$; $X^3 + X^2 + X + 1$; $X^4 + X^3 + 1$; $X^5 + 6X^4 + 5X^2 - 2X + 9$ en $\mathbb{Z}[X]$.
 (c) $(X + a)^4 + 1$ en $\mathbb{Q}[X]$ ($a \in \mathbb{Q}$).
 (d) $X^2 + Y^2 + 1$ en $\mathbb{Q}[X, Y]$.
30. Sea K un cuerpo finito de q elementos. ¿Cuántos polinomios irreducibles mónicos de grado 2 hay en $K[X]$? ¿Y de grado 3?