

ÁLGEBRA III

Práctica 1 – Segundo Cuatrimestre de 2023

Nota: En esta práctica la palabra anillo significará anillo conmutativo con unidad $1 \neq 0$, y todo morfismo de anillos $f : A \rightarrow B$ manda 1_A en 1_B . Dado $p \in \mathbb{N}$ primo, denotaremos \mathbb{F}_p al cuerpo finito $\mathbb{Z}/p\mathbb{Z}$.

Repaso de anillos, cuerpos y morfismos

Ejercicio 1. Sean A, B anillos y $f : A \rightarrow B$ un morfismo de anillos. Pruebe que:

- i) A tiene ideales maximales, y todo ideal propio está contenido en un ideal maximal.
- ii) \mathfrak{p} es un ideal primo de A si y solo si A/\mathfrak{p} es un dominio íntegro.
- iii) \mathfrak{m} es un ideal maximal de A si y solo si A/\mathfrak{m} es un cuerpo.
- iv) Si \mathfrak{p} es un ideal primo de B , entonces $f^{-1}(\mathfrak{p})$ es un ideal primo de A .
- v) Si f es sobreyectivo y \mathfrak{m} es un ideal maximal de B entonces $f^{-1}(\mathfrak{m})$ es un ideal maximal de A .
- vi) Si \mathbb{K} es un cuerpo y $f : \mathbb{K} \rightarrow B$ es un morfismo de anillos, entonces f es inyectivo.

Ejercicio 2. Pruebe que si D es un dominio íntegro finito, entonces D es un cuerpo.

Ejercicio 3. Dado $b \in \mathbb{C}$, se define $\mathbb{Q}[b] = \left\{ \sum_{i=0}^n a_i b^i / a_i \in \mathbb{Q} \right\}$. Pruebe que $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[i]$ y $\mathbb{Q}[\sqrt[3]{2}]$ son cuerpos. ¿Cómo se podría generalizar esto?

Ejercicio 4. Caracterice los siguientes conjuntos:

- i) $\{f : \mathbb{R} \rightarrow \mathbb{C} : f \text{ isomorfismo de cuerpos}\}$.
- ii) $\{f : \mathbb{C} \rightarrow \mathbb{R} : f \text{ morfismo de cuerpos}\}$.
- iii) $\{f : \mathbb{Q} \rightarrow \mathbb{F}_p : f \text{ morfismo de cuerpos}\}$, donde $p \in \mathbb{Z}$ es un primo.
- iv) $\{f : \mathbb{Q} \rightarrow \mathbb{K} : f \text{ morfismo de cuerpos}\}$, donde \mathbb{K} es un cuerpo fijo.
- v) $\{f : \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{3}] : f \text{ morfismo de cuerpos}\}$.
- vi) $\{f : \mathbb{C} \rightarrow \mathbb{C} : f \text{ morfismo de cuerpos y } f(a) = a \forall a \in \mathbb{R}\}$.
- vii) $\{f : \mathbb{Q}[i] \rightarrow \mathbb{Q}[i] : f \text{ morfismo de cuerpos}\}$.
- viii) $\{f : \mathbb{Q}[i] \rightarrow \mathbb{Q}[i] : f \text{ isomorfismo de cuerpos}\}$.
- ix) $\{f : \mathbb{Q}[i] \rightarrow \mathbb{R} : f \text{ morfismo de cuerpos}\}$.
- x) $\{f : \mathbb{R} \rightarrow \mathbb{R} : f \text{ morfismo de cuerpos}\}$.

Ejercicio 5. Sea \mathbb{K} un cuerpo y sea A una \mathbb{K} -álgebra de dimensión finita. Pruebe que si A es un dominio íntegro, entonces es un cuerpo.

Ejercicio 6. Sea A un anillo. Notamos $\mathcal{U}(A)$ al conjunto de los elementos de A que tienen inverso multiplicativo.

- i) Pruebe que $(\mathcal{U}(A), \cdot)$ es un grupo, llamado *grupo de unidades* de A .
- ii) Caracterice el grupo de unidades de los siguientes anillos:
 \mathbb{Z} , \mathbb{K} (\mathbb{K} cuerpo), $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-5}]$, $A[X]$ (A dominio íntegro), $\mathbb{Z}/n\mathbb{Z}$.

Ejercicio 7. Sea A un dominio íntegro. Consideremos en el conjunto $A \times (A - \{0\})$ la relación de equivalencia

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

Definimos en $K = A \times (A - \{0\}) / \sim$ las siguientes operaciones:

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

- i) Pruebe que $(K, +, \cdot)$ es un cuerpo, llamado el *cuerpo de fracciones* (o de cocientes) del anillo A . Se suele denotar $K = \text{Frac}(A)$.
- ii) Pruebe que $f : A \rightarrow K$ definida por $f(a) = (a, 1)$ es un monomorfismo de anillos.
- iii) Sea D un anillo. Pruebe que son equivalentes:
 - (a) D es un dominio íntegro.
 - (b) Existe $f : D \rightarrow K$ monomorfismo de anillos para algún cuerpo K .

Ejercicio 8. Caracterice el cuerpo de fracciones de los siguientes dominios íntegros:

$$\mathbb{Z}; \mathbb{Z}[i]; \mathbb{Z}[\sqrt{2}]; A[X] \text{ (} A \text{ dominio íntegro); } \mathbb{K} \text{ (} \mathbb{K} \text{ cuerpo)}.$$

Dominios de factorización única, álgebras de polinomios e irreducibilidad

Ejercicio 9. Pruebe que si A es un dominio íntegro, entonces $A[(X_i)_{i \in I}]$ es un dominio íntegro.

Ejercicio 10. Sea A un dominio íntegro y sea $a \in A$. Pruebe que:

- i) Si a es primo, entonces a es irreducible.
- ii) Si A es DFU (dominio de factorización única) y a es irreducible, entonces es primo.
- iii) En general, no vale que irreducible implica primo.
Sugerencia: $\mathbb{Z}[\sqrt{-5}]$
- iv) Si A es DFU, entonces $A[(X_i)_{i \in I}]$ es DFU.
- v) Si A es principal entonces A es DFU, pero no vale la recíproca.

Ejercicio 11. Un dominio íntegro A se dice *euclideo* si está provisto de un algoritmo de división, es decir, si existe $g : A - \{0\} \rightarrow \mathbb{N} \cup \{0\}$ que satisface las dos condiciones siguientes:

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

Pruebe que:

- i) \mathbb{Z} , $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, \mathbb{K} y $\mathbb{K}[X]$ (\mathbb{K} cuerpo) son anillos euclideos.
- ii) Si A es un anillo euclideo, entonces A es principal.

Ejercicio 12. Sea A un dominio de factorización única. Para $f \in A[X]$ se define su *contenido* $c(f)$ como el máximo común divisor de sus coeficientes. Un polinomio $f \in A[X]$ se dice *primitivo* si $c(f) = 1$. Sea K el cuerpo de fracciones de A . Pruebe que:

1. Si $p \in A$ es primo en A , también lo es en $A[X]$.
2. Si $f, g \in A[X]$ son primitivos, también lo es $fg \in A[X]$.
3. $c(fg) = c(f)c(g)$.
4. (*Lema de Gauss.*) $f \in A[X] \setminus A$ es irreducible si y sólo si es primitivo e irreducible en $K[X]$.
5. $A[X]$ es dominio de factorización única.

Ejercicio 13. Sea $p \in \mathbb{Z}$ primo. Pruebe que:

- i) -1 es un cuadrado en \mathbb{F}_p si y solo si $p = 2$ o $p \equiv 1 \pmod{4}$.
- ii) p es irreducible en $\mathbb{Z}[i]$ si y solo si p no es suma de dos cuadrados (en \mathbb{Z}).
- iii) p es suma de dos cuadrados (en \mathbb{Z}) si y solo si $p = 2$ o $p \equiv 1 \pmod{4}$.

Ejercicio 14.

- i) Sea \mathbb{K} un cuerpo y sea $f \in \mathbb{K}[X]$. Pruebe que $\mathbb{K}[X]/\langle f \rangle$ es un cuerpo si y solo si f es irreducible.
- ii) Construya un cuerpo de 9 elementos.
- iii) Pruebe que $\mathbb{R}[X]/\langle X^2 + 1 \rangle \simeq \mathbb{C}$.

Ejercicio 15. Sea A un DFU y sea K su cuerpo de fracciones. Pruebe que si $f \in A[X]$ es un polinomio irreducible de grado positivo entonces, visto como polinomio con coeficientes en K , también es irreducible. ¿Vale la recíproca? ¿Y agregando alguna hipótesis razonable?

Ejercicio 16. Sea $p \in \mathbb{N}$ primo, y sea $\Phi_p : \mathbb{Z}[X] \rightarrow \mathbb{F}_p[X]$ definida por

$$\Phi_p(a_n X^n + \cdots + a_0) = \bar{a}_n X^n + \cdots + \bar{a}_0$$

donde \bar{a}_i denota el resto de a_i módulo p .

- i) Pruebe que $\Phi_p(f) + \Phi_p(g) \equiv \Phi_p(f + g) \pmod{p}$ y $\Phi_p(f) \cdot \Phi_p(g) \equiv \Phi_p(f \cdot g) \pmod{p}$.
- ii) Sea $f \in \mathbb{Z}[X]$ tal que $\Phi_p(f) \neq 0$ y $\text{gr}(\Phi_p(f)) = \text{gr}(f)$. Pruebe que si $\Phi_p(f)$ es irreducible en $\mathbb{F}_p[X]$, entonces f no se factoriza en $\mathbb{Z}[X]$ en la forma $f = gh$ con g, h de grado mayor o igual que 1.
- iii) Pruebe que $X^4 + 1$ es irreducible en $\mathbb{Z}[X]$ pero reducible en $\mathbb{F}_p[X]$ para todo primo p .

Ejercicio 17. (*Criterio de irreducibilidad de Eisenstein.*) Sea A un DFU y sea K su cuerpo de fracciones. Sea $f = \sum_{i=0}^n a_i X^i \in A[X]$, con $n > 0$. Pruebe 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 $K[X]$.

Ejercicio 18. (*Teorema de Gauss.*) Sea A un DFU y sea K su cuerpo de fracciones. Sea $f = \sum_{i=0}^n a_i X^i \in A[X]$ con $a_0 \neq 0$. Demuestre 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 .

Ejercicio 19. Sea $p \in \mathbb{Z}$ primo. Pruebe que:

- i) $(X + 1)^p - 1$ es divisible por X y $\frac{(X + 1)^p - 1}{X}$ es irreducible en $\mathbb{Q}[X]$.
- ii) $1 + X + X^2 + \dots + X^{p-1}$ es irreducible en $\mathbb{Q}[X]$.
- iii) $X^n - p$ es irreducible en $\mathbb{Q}[X]$ para todo $n \in \mathbb{N}$.

Ejercicio 20. Sea $n > 1$ un entero. Pruebe que $X^n + 5X^{n-1} + 3$ es irreducible en $\mathbb{Z}[X]$.

Ejercicio 21.

- i) Sea \mathbb{K} un cuerpo. Sea $f \in \mathbb{K}[X]$ y sea $a \in \mathbb{K}$ una raíz de f . Pruebe que a es raíz múltiple de f y solo si es raíz de su derivado.
- ii) Pruebe que si $f \in \mathbb{Q}[X]$ es irreducible, entonces f no tiene raíces múltiples en \mathbb{C} .
- iii) Pruebe que $\sum_{i=0}^n X^i$ no tiene raíces múltiples en \mathbb{C} .
- iv) Pruebe que $\sum_{i=0}^n \frac{X^i}{i!}$ no tiene raíces múltiples en \mathbb{C} .

Ejercicio 22. Analice la reducibilidad de:

- i) $X^2 + Y^2 - 1$ en $\mathbb{Q}[X, Y]$.
- ii) $X^6 + tX^5 - t^2(t-1)X + t(t-1)$ en $\mathbb{Q}(t)[X]$.
- iii) $X^7 + 15X^3 + 5$ en $\mathbb{Z}[i][X]$.
- iv) $X^m - Y^n$ en $\mathbb{C}[X, Y]$ con $(m, n) = 1$.

Ejercicio 23. Sea $p \in \mathbb{Z}$ primo:

i) Pruebe que $P(X) = X^p - X - a \in \mathbb{F}_p[X]$ es irreducible si y sólo si $a \neq 0$.

Sugerencia: pruebe que si $Q(X)$ divide a $P(X)$, entonces $Q(X+1)$ también.

ii) Pruebe que $X^p - a \in \mathbb{Q}[X]$ es reducible si y solo si tiene alguna raíz racional.

Ejercicio 24. Pruebe que $X^n + 4 \in \mathbb{Z}[X]$ es reducible si y solo si n es múltiplo de 4.

Ejercicio 25. Sea K un cuerpo. Pruebe que $X^2 + Y^3 + Z^5 \in K[X, Y, Z]$ es irreducible.

Ejercicio 26. Sea K un cuerpo de característica coprima con $n \in \mathbb{Z}_{\geq 1}$ y $P(Y) \in K[Y]$ un polinomio libre de cuadrados de grado positivo. Pruebe que $X^n - P(Y)$ es irreducible en $K[X, Y]$.

Ejercicio 27. Factorice $f = X^5 + 3X^4 + X^2 + 2X + 1$ en $\mathbb{F}_2[X]$, $\mathbb{F}_3[X]$ y en $\mathbb{Z}[X]$.

Ejercicio 28. Pruebe que $5X^4 - 5X^2 + 1$ es irreducible en $\mathbb{Z}[X]$.

Ejercicio 29. Pruebe que $X^5 \pm 6X^4 \pm 6X^3 \pm 24X \pm 72$ es irreducible en $\mathbb{Z}[X]$ para cualquier elección de signos.

Sugerencia: considerar los primos 2 y 3.

* **Ejercicio 30.** Sean $a, b \in \mathbb{Z}$.

i) Pruebe que $X^3 + aX^2 + bX + 1$ es reducible en $\mathbb{Z}[X]$ si y sólo si $a = b$ o $a + b = -2$.

ii) Sea \mathbb{K} un cuerpo y sea $a \in \mathbb{K}$. Pruebe que $X^4 - a$ es reducible en $\mathbb{K}[X]$ si y solo si $a = b^2$ para algún $b \in \mathbb{K}$ o $a = -4c^4$ para algún $c \in \mathbb{K}$.

iii) Halle a, b, c enteros no nulos distintos dos a dos tales que

$$X(X - a)(X - b)(X - c) + 1$$

sea reducible en $\mathbb{Z}[X]$.

iv) Factorice $X^5 + X^4 + X^2 + X + 2$ en $\mathbb{Q}[X]$.

* **Ejercicio 31.** Sean a_1, a_2, \dots, a_n enteros distintos dos a dos.

i) Pruebe que $(X - a_1)(X - a_2) \cdots (X - a_n) - 1$ es irreducible en $\mathbb{Z}[X]$.

ii) Pruebe que $(X - a_1)^2(X - a_2)^2 \cdots (X - a_n)^2 + 1$ es irreducible en $\mathbb{Z}[X]$.

* **Ejercicio 32.** Pruebe que el polinomio $(X^2 + X)^{2^n} + 1$ es irreducible en $\mathbb{Z}[X]$ para todo n entero no negativo.

Sugerencia: $X^2 + X + 1$ es irreducible en $\mathbb{F}_2[X]$.

* **Ejercicio 33.** Sea $f \in \mathbb{Z}[X]$ mónico tal que $f(0) \neq 0$. Supongamos que f tiene una única raíz de valor absoluto mayor o igual que 1. Pruebe que f es irreducible en $\mathbb{Z}[X]$.