Práctica 1: Anillos, cuerpos, polinomios

1 Probar que todo subcuerpo de $\mathbb{C}$ es infinito.

2 Sea A un anillo conmutativo. Probar que las siguientes afirmaciones son equivalentes:

(i) A es un cuerpo;

(ii) todo morfismo de anillos $f : A \to B$ es inyectivo.

3 Sean B un anillo conmutativo, A un subanillo de B y b un elemento de B. Se define $A[b]$ como el menor subanillo de B que contiene a A y a b.

(*a*) Probar que $A[b] = \left\{ \sum_{i=0}^{n} a_i \cdot b^i \;\middle|\; n \in \mathbb{N}_0,\ a_i \in A \text{ para todo } i \right\}$.

(*b*) Observar que $A[b]$ es la imagen del morfismo de anillos $\mathrm{ev}_b : A[X] \to B$ que manda X a b y actúa como la identidad sobre los elementos de A. Deducir que $A[b] \cong A[X]/\ker \mathrm{ev}_b$. En particular, si no existe ningún polinomio no nulo en $A[X]$ que anule a b, entonces $A[b] \cong A[X]$.

(*c*) Probar que si existe N tal que b^{N+1} es una combinación lineal con coeficientes en A del conjunto $\{1, b, b^2, \ldots, b^N\}$, entonces $A[b] = \left\{ \sum_{i=0}^{N} a_i \cdot b^i \;\middle|\; a_i \in A \text{ para todo } i \right\}$.

4 Probar que $\mathbb{Q}[i]$, $\mathbb{Q}\left[\sqrt{3}\right]$ y $\mathbb{Q}\left[\sqrt[3]{2}\right]$ son cuerpos.

5 En cada uno de los siguientes casos, caracterizar todos los morfismos de anillos de A en B:

(*a*) $A = \mathbb{C}$, $B = \mathbb{R}$

(*b*) $A = \mathbb{R}$, $B = \mathbb{R}$

(*c*) $A = \mathbb{Q}$, $B = \mathbb{Z}/p\mathbb{Z}$

(*d*) $A = \mathbb{Q}$, B un cuerpo cualquiera

(*e*) $A = \mathbb{Q}[i]$, $B = \mathbb{Q}[i]$

(*f*) $A = \mathbb{Q}\left[\sqrt{2}\right]$, $B = \mathbb{Q}\left[\sqrt{3}\right]$

6 (*a*) Sea D un dominio íntegro finito. Probar que D es un cuerpo.

(*b*) 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 conmutativo. Supongamos que existen un cuerpo K y un morfismo de anillos inyectivo $i : A \hookrightarrow K$. Probar que entonces A es un dominio íntegro.

8 Sea A un dominio íntegro. El objetivo de este ejercicio es construir $i : A \hookrightarrow K$ como en el ejercicio anterior.

(*a*) En el conjunto $X = \{(a, b) \in A \times A : b \neq 0\}$ se considera la relación $\sim$ definida por

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

Verificar que $\sim$ es relación de equivalencia.

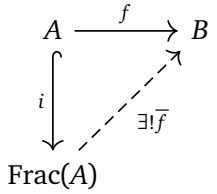
(*b*) Sea $K = X/\sim$ (es decir, el conjunto de clases de equivalencia). Denotamos $\frac{a}{b}$ a la clase de equivalencia de (a, b). Verificar que las operaciones

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} \qquad \text{y} \qquad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

están bien definidas (no dependen de los representantes elegidos) y le dan a K una estructura de cuerpo. Este cuerpo se llama el *cuerpo de fracciones* de A y se denota Frac(A).

(*c*) Verificar que $i : A \to \text{Frac}(A)$ definido por $i(a) = \frac{a}{1}$ es un morfismo de anillos inyectivo (lo cual nos permite pensar a A como subconjunto de K).

(*d*) Probar que Frac(A) es "el menor cuerpo que contiene a A", en el sentido dado por la siguiente propiedad universal: si $f : A \to B$ es un morfismo de anillos tal que para todo $a \neq 0$ vale que $f(a) \in \mathscr{U}(B)$, entonces existe un único morfismo $\overline{f} : \text{Frac}(A) \to B$ que hace conmutar el siguiente diagrama:



9 Caracterizar el cuerpo de fracciones de los siguientes dominios íntegros:

(*a*) K (un cuerpo) (*b*) $\mathbb{Z}$ (*c*) $\mathbb{Z}[i]$

10 Sea K un cuerpo. Se definen en $K \times K$ las siguientes operaciones:

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

(*a*) Probar que $(K \times K, +, \cdot)$ es un anillo.

(*b*) Probar que $(a, b) \in K \times K$ es inversible si y sólo si $a^2 + b^2 \neq 0$.

(*c*) Probar que si p es primo, las operaciones anteriores hacen de $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ un cuerpo si y sólo si $p \equiv 3 \pmod 4$.

11 (*a*) Sean K un cuerpo y sea $f \in K[X]$. Probar que $K[X]/\langle f \rangle$ es un cuerpo si y sólo si f es irreducible.

(*b*) Construir un cuerpo de 9 elementos.

(*c*) Probar que $\mathbb{R}[X]/\langle X^2 + 1 \rangle \cong \mathbb{C}$.

12 **(Teorema de la raíz racional de Gauss)** Sean A un DFU, K el cuerpo de fracciones de A y $f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in A[X]$. Probar que si $\frac{p}{q} \in K$ es raíz de f, con p, q coprimos, entonces $p \mid a_0$ y $q \mid a_n$. Deducir que si $a_n \in \mathscr{U}(A)$ (por ejemplo, si f es mónico) entonces todas las raíces en K del polinomio f están en A.

13 Hallar **todos** los valores de $m \in \mathbb{Z}$ para los cuales los siguientes polinomios son irreducibles en $\mathbb{Q}[X]$.

(*a*) $X^3 - m$ (*b*) $X^3 + mX^2 + 7X + 1$

14 Probar que los siguientes polinomios son irreducibles en $\mathbb{Q}[X]$:

(*a*) $X^3 + X^2 + 2X + m$, con m un entero impar.

(*b*) $X^3 - X + m$, con m un entero no divisible por 3.

15 Sea $K = \mathbb{Q}[i]$. Probar que si $m \in \mathbb{Z}$ no es un cubo perfecto, entonces el polinomio $X^3 - m$ es irreducible en $K[X]$.

16 Sean K un cuerpo y $a \in K$. Probar que el polinomio $X^4 - a$ es reducible en $K[X]$ si y sólo si ocurre alguna de las siguientes dos cosas:

- existe $b \in K$ tal que $a = b^2$,
- existe $c \in K$ tal que $a = -4c^4$.

La factorización que se obtiene en el segundo caso se conoce como la *identidad de Sophie Germain*.

17 Sean K un cuerpo, $f \in K[X]$ y $a \in K$ una raíz de f. Probar que a es raíz múltiple de f si y sólo si es raíz de su derivado.

18 Probar que si $f \in \mathbb{Q}[X]$ es irreducible, entonces f no tiene raíces múltiples en $\mathbb{C}$.

19 Sean $A \subsetneq B$ dos anillos conmutativos con A dominio íntegro, y sea f un polinomio con coeficientes en A.

(*a*) Mostrar con ejemplos que si f es irreducible en $A[X]$ entonces puede pasar que sea también irreducible en $B[X]$ o que deje de serlo.

(*b*) Probar que si A es un cuerpo y f es irreducible en $B[X]$, entonces también es irreducible en $A[X]$.

(*c*) Mostrar que el enunciado de (*b*) es técnicamente incorrecto si A no es un cuerpo, aunque por motivos poco interesantes. ¿Qué es lo que sí se puede concluir sobre f en $A[X]$ con esas hipótesis? ¿Qué hipótesis se puede agregar sobre f para que sí sea cierto el enunciado de (*b*)?

20 Sea A un DFU. Un polinomio $f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in A[X]$ se dice *primitivo* si no existe ningún primo $p \in A$ que divida a todos los a_i, es decir, si el máximo común divisor de los coeficientes de f es 1. Dados $f, g \in A[X]$, probar que el producto $f \cdot g$ es primitivo si y sólo si f y g lo son.

21 Dado un cuerpo K, dos polinomios $f, g \in K[X]$ son *asociados* si existe $\alpha \in K$ no nulo tal que $f = \alpha \cdot g$. Notar que dos polinomios asociados tienen necesariamente el mismo grado.

Sean A un DFU y K su cuerpo de fracciones.

(*d*) Probar que todo polinomio no nulo de $K[X]$ es asociado de algún polinomio primitivo de $A[X]$, es decir: dado $g \neq 0$ en $K[X]$, existen $\alpha \in K$ y $g_1 \in A[X]$ primitivo tales que $g = \alpha \cdot g_1$.

(*e*) Sean $f \in A[X]$ primitivo y $\lambda \in K$. Probar que $\lambda \cdot f \in A[X]$ si y sólo si $\lambda \in A$.

(*f*) Sea $f \in A[X]$. Probar que si $f = f_1 \cdot \ldots \cdot f_r$, con cada $f_i \in K[X]$, entonces existen $\widetilde{f_1}, \ldots, \widetilde{f_r} \in A[X]$, con f_i y $\widetilde{f_i}$ asociados para cada i, tales que $f = \widetilde{f_1} \cdot \ldots \cdot \widetilde{f_r}$.

(*g*) Deducir que si $f \in A[X]$ no es constante y no se puede escribir como producto de dos polinomios de grado positivo en $A[X]$ entonces f es irreducible en $K[X]$.

Lo probado en este ejercicio da una demostración del siguiente resultado clásico.

(Lema de Gauss) Sean A un DFU, K su cuerpo de fracciones y $f \in A[X]$ un polinomio no constante. Son equivalentes:

(i) f es irreducible en $A[X]$;

(ii) f es primitivo y es irreducible en $K[X]$.

22 Probar que los siguientes polinomios son irreducibles en $\mathbb{Q}[X]$:

(*a*) $X^4 + 1$ (*b*) $X^4 + 3X^2 - 4X - 2$ (*c*) $X^5 + 8X^3 - 11X^2 + 1$

23 Sean A un DFU, K su cuerpo de fracciones y $p \in A$ un primo. La proyección al cociente $A \twoheadrightarrow A/pA$ induce naturalmente un morfismo de anillos $\pi : A[X] \to (A/pA)[X]$, dado por reducir cada coeficiente módulo p. Sea $f \in A[X]$ no constante tal que su coeficiente principal no es divisible por p, es decir tal que f y $\pi(f)$ tienen el mismo grado.

(*a*) Probar que si $\pi(f)$ es irreducible en $(A/pA)[X]$, entonces f es irreducible en $K[X]$.

Supongamos ahora que A es un DIP, luego A/pA es un cuerpo (pues en un DIP todo ideal primo es maximal) y entonces $(A/pA)[X]$ es euclídeo y en particular DFU.

(*b*) Probar que si $\pi(f)$ tiene r factores irreducibles en su factorización en $(A/pA)[X]$, entonces f no puede tener más de r factores irreducibles en su factorización en $K[X]$.

(*c*) Probar que si todos los factores irreducibles de $\pi(f)$ en $(A/pA)[X]$ tienen grado al menos d, entonces también todos los factores irreducibles de f en $K[X]$ tienen grado al menos d.

(*d*) Probar que si todos los factores irreducibles de $\pi(f)$ en $(A/pA)[X]$ tienen grado divisible por m, entonces también todos los factores irreducibles de f en $K[X]$ tienen grado divisible por m.

24 Determinar todos los polinomios irreducibles de grados 2, 3, 4 y 5 con coeficientes en $\mathbb{Z}/2\mathbb{Z}$.

25 Sea K un cuerpo finito de q elementos. Probar que en $K[X]$ hay $\dfrac{q^2 - q}{2}$ polinomios mónicos irreducibles de grado 2.

26 Probar que el polinomio $X^5 + 6X^4 + 5X^2 - 2X + 105$ es irreducible en $\mathbb{Q}[X]$.

27 Factorizar el polinomio $f = X^6 - 72$ en $(\mathbb{Z}/5\mathbb{Z})[X]$ y en $(\mathbb{Z}/7\mathbb{Z})[X]$. Deducir que f es irreducible en $\mathbb{Q}[X]$.

28 **(Criterio de irreducibilidad de Eisenstein)** Sean A un DFU, K su cuerpo de fracciones y $f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in A[X]$ no constante. Supongamos que existe un primo $p \in A$ tal que:

- $p \nmid a_n$,
- $p \mid a_i$ para todo $i < n$,
- $p^2 \nmid a_0$.

Probar que f es irreducible en $K[X]$.

29 Probar que si $p \in \mathbb{Z}$ es un número primo, entonces para todo $n \in \mathbb{N}$ el polinomio $X^n - p$ es irreducible en $\mathbb{Q}[X]$. ¿Vale la recíproca?

30 Sean A un anillo conmutativo y $c \in A$. Consideramos el morfismo de anillos $\theta : A[X] \to A[X]$ tal que $\theta|_A = id_A$ y $\theta(X) = X + c$. Probar que θ es un automorfismo. Deducir que un polinomio $f \in A[X]$ es irreducible si y sólo si $\theta(f)$ lo es.

31 Consideremos el polinomio $f = X^5 + 5X^4 + 10X^3 + 13X^2 + 5X - 5 \in \mathbb{Z}[X]$. Observar que no se puede aplicar el criterio de Eisenstein de forma directa para probar que f es irreducible.

(*a*) Para $c = -1$, calcular $\theta(f)$ y deducir que f es irreducible en $\mathbb{Q}[X]$.

(*b*) ¿Pueden probar la irreducibilidad de f de alguna otra manera?

32 Probar que los siguientes polinomios son irreducibles en $\mathbb{Q}[X]$:

(*a*) $X^4 + 4X + 1$

(*b*) $X^{p-1} + X^{p-2} + \ldots + X + 1$, donde p es un número primo.

Sugerencia. Para (*b*), notar que ese polinomio es igual a $\dfrac{X^p - 1}{X - 1}$.

33 ¿Es cierto que si $f \in \mathbb{Z}[X]$ es un polinomio mónico irreducible, entonces necesariamente existe algún primo p tal que $\pi(f)$ es irreducible en $(\mathbb{Z}/p\mathbb{Z})[X]$?

Equivalentemente, ¿existe algún polinomio mónico irreducible en $\mathbb{Z}[X]$ que sea reducible módulo p para todo primo p?

Sugerencia. Una posible respuesta está contenida en los ejercicios de esta guía, pero no se preocupen si no sale. Más adelante tendremos más y mejores herramientas para atacar este problema.