Álgebra II

Primer cuatrimestre - 2026

Práctica 5

Anillos – Segunda parte: álgebra conmutativa

Convención. En esta práctica la palabra anillo significará anillo conmutativo.

Ideales primos y maximales

1.1. Sean I y J ideales de un anillo A.

(I) Pruebe que $IJ = \{a_1b_1 + \cdots + a_nb_n : a_i \in I, b_i \in J, n \in \mathbb{N}\}$ es un ideal.

(II) Pruebe que $IJ \subseteq I \cap J$.

(III) Pruebe que si $I + J = A$, entonces $IJ = I \cap J$.

1.2. Sean $I_1, \ldots, I_n$ ideales de un anillo A y sea $\mathfrak{p} \subset A$ un ideal primo tal que $\bigcap_{i=1}^{n} I_i \subseteq \mathfrak{p}$.

(I) Pruebe que existe $1 \leqslant i \leqslant n$ tal que $I_i \subseteq \mathfrak{p}$.

(II) Pruebe que si $\mathfrak{p} = \bigcap_{i=1}^{n} I_i$, entonces $\mathfrak{p} = I_i$ para algún $1 \leqslant i \leqslant n$.

1.3. Sean $m, n \in \mathbb{N}$. Exprese a los siguientes ideales de $\mathbb{Z}$ como ideales principales:

$$\langle m, n\rangle, \qquad \langle m\rangle + \langle n\rangle, \qquad \langle m\rangle \cap \langle n\rangle, \qquad \langle m\rangle\langle n\rangle.$$

1.4. Sea I un ideal de un anillo A. Pruebe que

$$\sqrt{I} = \{a \in A : \text{existe } r \in \mathbb{N} \text{ tal que } a^r \in I\}$$

es un ideal de A, que denominamos el *radical* de I.

1.5. Sea $m \in \mathbb{Z}$. Exprese a $\sqrt{\langle m\rangle}$ como ideal principal.

1.6. Sea A un anillo. Pruebe que:

(I) un ideal $\mathfrak{p} \subseteq A$ es primo si y solo si $A/\mathfrak{p}$ es un dominio íntegro;

(II) un ideal $\mathfrak{m} \subseteq A$ es maximal si y solo si $A/\mathfrak{m}$ es un cuerpo;

(III) un ideal maximal es primo.

1.7. Pruebe que si $f\colon A \to B$ es un morfismo de anillos, entonces para todo ideal primo $\mathfrak{p}$ de B se tiene que $f^{-1}(\mathfrak{p})$ es un ideal primo de A. ¿Es cierto esto si reemplazamos la palabra primo por maximal?

Dominios principales y de factorización única

Convención. Denotaremos por Spec A al conjunto de todos los ideales primos de un anillo A.

2.1. Pruebe que si A es un DIP, entonces todo ideal primo no nulo de A es maximal.

2.2. Pruebe que $\mathfrak{m} = \langle 3, Y^4 - X, Y^{12} - X^3 + Y - 1\rangle$ es un ideal maximal de $\mathbb{Z}[X, Y]$.

2.3. Sea k un cuerpo. Pruebe que si $\mathfrak{p} \in \operatorname{Spec} k[X]$, entonces existe $f \in \mathfrak{p}$ mónico e irreducible tal que $\mathfrak{p} = \langle f\rangle$. Recíprocamente, todo ideal principal generado por un polinomio mónico e irreducible es un ideal primo de $k[X]$.

2.4. Sea A un anillo y $\mathfrak{p} \in \operatorname{Spec} A$. Pruebe que:

(I) Si $B \subseteq A$ es un subanillo, entonces $B \cap \mathfrak{p} \in \operatorname{Spec} B$.

(II) Si $I \subseteq A$ es un ideal y $\pi : A \to A/I$ es la proyección canónica, dado $\mathfrak{q} \in \operatorname{Spec} A/I$, se tiene $\pi^{-1}(\mathfrak{q}) \in \operatorname{Spec} A$.

(III) Si $I \subseteq A$ es un ideal tal que $\mathfrak{p} \supseteq I$, entonces $\mathfrak{p}/I \in \operatorname{Spec} A/I$.

2.5. Pruebe que si $\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[X]$ y $\mathfrak{p} \cap \mathbb{Z} \neq (0)$, entonces existe un número primo $p \in \mathbb{N}$ tal que o bien $\mathfrak{p} = \langle p\rangle$ o bien existe un polinomio $f \in \mathbb{Z}[X]$ mónico e irreducible sobre $\mathbb{F}_p$ tal que $\mathfrak{p} = \langle p, f\rangle$. Deduzca cómo son todos los elementos de $\operatorname{Spec} \mathbb{Z}[X]$.

2.6 (Nilradical)**.** Sea A un anillo. Un elemento $a \in A$ es *nilpotente* si existe $n \in \mathbb{N}$ tal que $a^n = 0$. El *nilradical de* A es el conjunto $\operatorname{Nil}(A) = \sqrt{0} = \{a \in A : a \text{ es nilpotente}\}$. Pruebe que

(I) $\operatorname{Nil}(A)$ es un ideal de A;

(II) $\operatorname{Nil}(A/\operatorname{Nil}(A)) = 0$;

(III) $\operatorname{Nil}(A) = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$;

(IV) si $x \in \operatorname{Nil}(A)$, entonces $1 + x$ es inversible.

2.7 (Radical de Jacobson)**.** Sea A un anillo. El *radical de Jacobson de* A es la intersección $J(A)$ de todos los ideales maximales de A. Pruebe que $x \in J(A)$ si y solo si para cada $y \in A$ se tiene que $1 - xy \in A^\times$.

2.8. Pruebe que el ideal $\langle 2, X\rangle \subseteq \mathbb{Z}[X]$ no es principal.

2.9 (Máximo común divisor)**.** Sea A un anillo. Un *máximo común divisor* de dos elementos $a, b \in A$ es un elemento $d \in A$ que cumple la siguiente propiedad:

$$c \mid d \qquad \Longleftrightarrow \qquad c \mid a \quad \text{y} \quad c \mid b.$$

Pruebe que:

(I) si el máximo común divisor de dos elementos existe, entonces es único salvo asociados;

(II) en un DFU, todo par de elementos tiene un máximo común divisor;

(III) en un DIP, el máximo común divisor entre dos elementos es una combinación lineal de los mismos;

(IV) el ítem anterior no es cierto si reemplazamos la palabra DIP por DFU;

(V) en el anillo $\mathbb{Z}[\sqrt{-3}]$, los elementos 4 y $2 + 2\sqrt{-3}$ no tienen un máximo común divisor.

2.10. Pruebe que el ideal $\langle 2, 1+\sqrt{-5}\rangle \subseteq \mathbb{Z}[\sqrt{-5}]$ no es principal.

2.11. Pruebe que 2, 3, $1+\sqrt{-5}$ y $1-\sqrt{-5}$ son irreducibles en $\mathbb{Z}[\sqrt{-5}]$, no asociados entre sí. Observando que $6 = 2\cdot 3 = (1+\sqrt{-5})\cdot(1-\sqrt{-5})$, concluya que $\mathbb{Z}[\sqrt{-5}]$ no es un DFU.

2.12 (Primos Gaussianos)**.** El objetivo de este ejercicio es caracterizar los primos (irreducibles) de $\mathbb{Z}[i]$.

(I) Pruebe que un primo impar $p \in \mathbb{Z}$ es congruente a 1 módulo 4 si y solo si la ecuación

$$x^2 \equiv -1 \pmod{p}$$

tiene solución.

(II) Sea $x \in \mathbb{Z}$. Pruebe que si $a+ib \in \mathbb{Z}[i]$ es un divisor de x, entonces $a-ib$ también lo es.

(III) Pruebe que $a+ib$ con $b \neq 0$ es un elemento irreducible de $\mathbb{Z}[i]$ si y solo si a^2+b^2 es un primo de $\mathbb{Z}$ *no* congruente a 3 módulo 4.

(IV) Pruebe que un entero $p \in \mathbb{Z}$ es un elemento irreducible de $\mathbb{Z}[i]$ si y solo si es un primo de $\mathbb{Z}$ congruente a 3 módulo 4.

2.13 (Lema de Gauss)**.** Sea A un DFU. El *contenido* de un polinomio

$$f = a_0 + a_1X + \cdots + a_nX^n \in A[X]$$

es algún máximo común divisor de sus coeficientes (observe que es único salvo asociados). Decimos que f es *primitivo* si su contenido es una unidad. Pruebe que:

(I) un polinomio $f = a\cdot X + b$ de grado 1 es irreducible si y solo si es primitivo;

(II) el polinomio $XZ + XY + 1 \in \mathbb{Q}[X, Y, Z]$ es irreducible;

(III) todo polinomio $g \in A[X]$ puede escribirse como $a\cdot f$ con $a \in A$ el contenido de g y f un polinomio primitivo.

(IV) un polinomio $f \in A[X]$ es primitivo si y solo si para cada elemento irreducible $p \in A$ se tiene que f no pertenece al núcleo del morfismo canónico $A[X] \to (A/(p))[X]$.

(V) si $f, g \in A[X]$ son dos polinomios primitivos, entonces $f\cdot g$ es primitivo.

(VI) el contenido de un producto es el producto de los contenidos de sus factores.

2.14. Sean $f, g \in \mathbb{Z}[X]$ dos polinomios primitivos y $h \in \mathbb{Q}[X]$. Pruebe que si $f = h\cdot g$ entonces $h \in \mathbb{Z}[X]$.