

# Algebra III

## Práctica 1 - Anillos y Cuerpos

2do cuatrimestre 2015

**Nota:** En esta materia, anillo significa anillo conmutativo con  $1 \neq 0$  y todo morfismo de anillo  $f : A \rightarrow B$  manda el  $1_A$  en el  $1_B$ .

**Ejercicio 1.** Sea  $A$  un anillo. Probar que:

1.  $A$  tiene ideales maximales y todo ideal propio  $I$  está contenido en un ideal maximal.
2.  $P$  es ideal primo si y sólo si  $A/P$  es dominio íntegro.
3.  $A$  es cuerpo si y sólo si tiene exactamente dos ideales.
4.  $M$  es ideal maximal si y sólo si  $A/M$  es cuerpo.

**Ejercicio 2.** Probar que:

1. Si  $K$  es cuerpo y  $f : K \rightarrow B$  es morfismo de anillos, entonces  $f$  es inyectivo.
2. Si  $A$  es anillo tal que todo morfismo de anillos  $f : A \rightarrow B$  es inyectivo, entonces  $A$  es cuerpo.

**Ejercicio 3.** Sea  $D$  un dominio íntegro finito. Probar que  $D$  es un cuerpo.

**Ejercicio 4.** Dado  $b \in \mathbb{C}$  se define  $\mathbb{Q}[b] = \{\sum_{i=0}^n a_i b^i / a_i \in \mathbb{Q}\}$ . Probar que  $\mathbb{Q}[\sqrt{2}]$ ,  $\mathbb{Q}[\sqrt{3}]$ ,  $\mathbb{Q}[i]$  y  $\mathbb{Q}[\sqrt[3]{2}]$  son cuerpos.

**Ejercicio 5.** Sea  $K$  un cuerpo y sea  $A$  una  $K$ -álgebra de dimensión finita. Probar que si  $A$  es un dominio íntegro, entonces es un cuerpo.

**Ejercicio 6.** Determinar el grupo de unidades  $\mathcal{U}(A)$  de los siguientes anillos  $A$ :

$$\mathbb{Z}, K \text{ (cuerpo)}, \mathbb{Z}[i], \mathbb{Z}[\sqrt{-5}], D[X] \text{ con } D \text{ dominio íntegro}, \mathbb{Z}/n\mathbb{Z}.$$

**Ejercicio 7.** Caracterizar los siguientes conjuntos:

1.  $\{f : \mathbb{R} \rightarrow \mathbb{C}, f \text{ isomorfismo de cuerpos}\}$ .
2.  $\{f : \mathbb{C} \rightarrow \mathbb{R}, f \text{ morfismo de cuerpos}\}$ .
3.  $\{f : \mathbb{Q} \rightarrow \mathbb{Z}/p\mathbb{Z}, f \text{ morfismo de cuerpos}\}, p \text{ primo}$ .
4.  $\{f : \mathbb{Q} \rightarrow \mathbb{K}, f \text{ morfismo de cuerpos}\}, \mathbb{K} \text{ cuerpo fijo}$ .
5.  $\{f : \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{3}], f \text{ morfismo de cuerpos}\}$ .
6.  $\{f : \mathbb{C} \rightarrow \mathbb{C}, f \text{ morfismo de cuerpos tal que } f(a) = a \forall a \in \mathbb{R}\}$ .
7.  $\{f : \mathbb{Q}[i] \rightarrow \mathbb{Q}[i], f \text{ morfismo de cuerpos}\}$ .
8.  $\{f : \mathbb{Q}[i] \rightarrow \mathbb{Q}[i], f \text{ isomorfismo de cuerpos}\}$ .
9.  $\{f : \mathbb{Q}[i] \rightarrow \mathbb{R}, f \text{ morfismo de cuerpos}\}$ .
10.  $\{f : \mathbb{R} \rightarrow \mathbb{R}, f \text{ morfismo de cuerpos}\}$ .

**Ejercicio 8.** Sea  $A$  un dominio íntegro y sea  $K$  su cuerpo de cocientes.

1. Probar que  $f : A \rightarrow K$  dada por  $a \mapsto \frac{a}{1}$  es un monomorfismo de anillos.
2. Sea  $D$  un anillo. Probar que son equivalentes:
  - a)  $D$  es dominio íntegro.
  - b) Existe  $f : D \rightarrow K$  monomorfismo de anillos para algún cuerpo  $K$ .

**Ejercicio 9.** Caracterizar el cuerpo de cocientes de los siguientes dominios íntegros:

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

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

1. Si  $a$  es primo entonces es irreducible.
2. Si  $A$  es DFU, entonces todo irreducible es primo.
3. Dar ejemplos en  $\mathbb{Z}[\sqrt{-5}]$  de elementos que sean irreducibles pero no primos.

**Ejercicio 11.** Sea  $A$  un dominio íntegro. Probar que valen las siguientes implicaciones pero no las recíprocas:

$$A \text{ es euclideo} \implies A \text{ es principal} \implies A \text{ es DFU}.$$

**Ejercicio 12.** Probar que  $\mathbb{Z}, \mathbb{Z}[i], K$  y  $K[X]$  ( $K$  cuerpo) son anillos euclideos.

**Ejercicio 13.** Sea  $p \in \mathbb{N}$  primo. Probar que:

1.  $-1$  es un cuadrado en  $\mathbb{Z}/p\mathbb{Z}$  si y sólo si  $p = 2$  o  $p \equiv 1 \pmod{4}$ .
2.  $p$  es irreducible en  $\mathbb{Z}[i]$  si y sólo si  $p$  no es suma de dos cuadrados (en  $\mathbb{Z}$ ).
3.  $p$  es primo en  $\mathbb{Z}[i]$  si y sólo si  $p \equiv 3 \pmod{4}$ .
4.  $p$  es suma de dos cuadrados (en  $\mathbb{Z}$ ) si y sólo si  $p = 2$  o  $p \equiv 1 \pmod{4}$ .

**Ejercicio 14.** Sea  $A$  un DFU,  $K$  su cuerpo de cocientes y  $f \in A[X]$  con  $\text{gr}(f) \geq 1$ . Probar que:

1.  $A[X]$  es DFU.
2.  $f$  es irreducible (en  $A[X]$ ) si y sólo si  $f$  es irreducible en  $K[X]$  y  $\text{cont}(f) = 1$ .

**Ejercicio 15.** Sea  $K$  un cuerpo y sea  $f \in K[X]$ .

1. Probar que  $K[X]/\langle f \rangle$  es un cuerpo si y sólo si  $f$  es irreducible.
2. Construir un cuerpo de 9 elementos.
3. Probar que  $\mathbb{R}[X]/\langle X^2 + 1 \rangle \simeq \mathbb{C}$ .
4. Supongamos que  $f = \prod_{i=1}^n (X - \alpha_i)$  con los  $\alpha_i \in K$  todos distintos. Sea  $g_j := \prod_{i \neq j} (X - \alpha_i)$ ,  $1 \leq j \leq n$ . Probar que  $\{\bar{g}_1, \dots, \bar{g}_n\}$  es base de  $K[X]/\langle f \rangle$ , y para un  $h \in K[X]$ , calcular las coordenadas de  $\bar{h}$  en esa base.

**Ejercicio 16.** Sea  $p \in \mathbb{N}$  primo. Definimos  $\Phi : \mathbb{Z}[X] \rightarrow (\mathbb{Z}/p\mathbb{Z})[X]$  mediante:

$$\Phi(a_n X^n + \cdots + a_1 X + a_0) = \overline{a_n} X^n + \cdots + \overline{a_1} X + \overline{a_0}.$$

Probar que:

1.  $\Phi$  es un morfismo de anillos.
2. Para un  $f \in \mathbb{Z}[X]$  tal que  $\Phi(f) \neq 0$  y  $\text{gr}(\Phi(f)) = \text{gr}(f)$ , si  $\Phi(f)$  es irreducible en  $(\mathbb{Z}/p\mathbb{Z})[X]$ , entonces  $f$  no se factoriza en  $\mathbb{Z}[X]$  como producto de polinomios de grado positivo.

**Ejercicio 17.** *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 satisface  $p \nmid a_n$ ,  $p \mid a_i \forall 0 \leq i < n$  y  $p^2 \nmid a_0$ , entonces  $f$  es irreducible en  $K[X]$ .

**Ejercicio 18.** Sea  $p \in \mathbb{N}$  primo. Probar que:

1.  $(X+1)^p - 1$  es divisible por  $X$  y  $\frac{(X+1)^p - 1}{X} = \sum_{i=0}^{p-1} \binom{p}{i} X^{p-i-1} \in \mathbb{Z}[X]$  es irreducible.
2.  $1 + X + X^2 + \cdots + X^{p-1}$  es irreducible.
3.  $X^n - p$  es irreducible  $\forall n \in \mathbb{N}$ .

**Ejercicio 19.** Sea  $K$  un cuerpo y sea  $a \in K$ . Probar que  $X^4 - a$  es reducible en  $K[X]$  si y solo si  $a = b^2$  para algún  $b \in K$  o  $a = -4c^4$  para algún  $c \in K$ .

**Ejercicio 20.** *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  $a_0 a_n \neq 0$ . Demostrar que si  $p, q \in A$  son irreducibles coprimos tales que  $f(p/q) = 0$ , entonces  $p \mid a_0$  y  $q \mid a_n$ .

**Ejercicio 21.** Sea  $K$  un cuerpo. Sea  $f \in K[X]$  y sea  $a \in K$  una raíz de  $f$ . Probar que:

1.  $a$  es raíz múltiple de  $f$  si y sólo si  $f'(a) = 0$ .
2. Si  $K = \mathbb{C}, \mathbb{R}$  o  $\mathbb{Q}$  entonces  $\frac{f}{\text{mcd}(f, f')} \in K[X]$  tiene las mismas raíces que  $f$  pero todas simples.

**Ejercicio 22.** Probar que si  $f \in \mathbb{Q}[X]$  es irreducible, entonces no tiene raíces múltiples en  $\mathbb{C}$ .

**Ejercicio 23.** Probar que  $\sum_{i=0}^n X^i$  y  $\sum_{i=0}^n \frac{X^i}{i!}$  no tienen raíces múltiples en  $\mathbb{C}$  para todo  $n \in \mathbb{N}$ .

**Ejercicio 24.** Determinar todos los polinomios irreducibles en  $(\mathbb{Z}/2\mathbb{Z})[X]$  de grado  $< 6$ .

**Ejercicio 25.** Sea  $K$  un cuerpo finito de  $q$  elementos. ¿Cuántos polinomios irreducibles mónicos de grado 2 hay en  $K[X]$ ? ¿Y de grado 3?

**Ejercicio 26.** Sea  $f = \sum_{i=0}^n a_i X^i \in \mathbb{C}[X]$  con  $a_n \neq 0$ . Definimos  $M = 1 + |\frac{a_{n-1}}{a_n}| + \cdots + |\frac{a_0}{a_n}|$ . Probar que:

1. Si  $\alpha \in \mathbb{C}$  es raíz de  $f$ , entonces  $|\alpha| < M$ .
2. Si  $f \in \mathbb{R}[X]$ , entonces:  $f(M) > 0 \iff a_n > 0$  y  $f(-M) > 0 \iff (-1)^n a_n > 0$ .

**Ejercicio 27.** Sea  $f = \sum_{i=0}^n a_i X^i = a_n \prod_{i=1}^n (X - \alpha_i) \in \mathbb{C}[X]$  con  $a_n \neq 0$  y  $n \geq 2$ . Se define el discriminante de  $f$  mediante:

$$\Delta(f) = a_n^{2n-2} \prod_{i < j} (\alpha_i - \alpha_j)^2.$$

Probar que:

1. Si  $f = aX^2 + bX + c$ , entonces  $\Delta(f) = b^2 - 4ac$ .
2. Si  $f = X^3 + pX + q$ , entonces  $\Delta(f) = -4p^3 - 27q^2$ .
3.  $\text{Res}_X(f, f') = a_n^{n-1} \prod_{i=1}^n f'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} a_n \Delta(f)$ .

**Ejercicio 28.** Sea  $K$  un cuerpo. Para un polinomio

$$f = \sum_{|\mathbf{a}| \leq d} f_{\mathbf{a}} \mathbf{X}^{\mathbf{a}} \in K[\mathbf{X}] := K[X_1, \dots, X_n],$$

donde  $\mathbf{a} = (a_1, \dots, a_n)$ ,  $|\mathbf{a}| = a_1 + \dots + a_n$ ,  $\mathbf{X} = (X_1, \dots, X_n)$  y  $\mathbf{X}^{\mathbf{a}} = X_1^{a_1} \dots X_n^{a_n}$ , se define el grado de  $f$  como  $\text{gr}(f) = \max\{|\mathbf{a}| : f_{\mathbf{a}} \neq 0\}$ .

Probar las siguientes afirmaciones:

1.  $f + g = 0$  o  $\text{gr}(f + g) \leq \max\{\text{gr}(f), \text{gr}(g)\}$ ,  $\forall f, g \in K[\mathbf{X}]$ .
2.  $fg = 0 \implies f = 0$  o  $g = 0$ ,  $\forall f, g \in K[\mathbf{X}]$ .
3. Si  $f \neq 0$  y  $g \neq 0$  entonces  $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g)$ ,  $\forall f, g \in K[\mathbf{X}]$ .
4.  $\mathcal{U}(K[\mathbf{X}]) = K - \{0\}$ .
5.  $K[\mathbf{X}]$  es un  $K$ -espacio vectorial. Exhibir una base.
6.  $K[\mathbf{X}]_{\leq d} = \{f : f = 0 \text{ o } \text{gr}(f) \leq d\}$  es un subespacio de  $K[\mathbf{X}]$ . Calcular su dimensión.

**Ejercicio 29.** Probar que  $X^2 + Y^2 - 1$  y  $XT - YZ$  son irreducibles en  $\mathbb{Q}[X, Y]$  y  $\mathbb{Q}[X, Y, Z, T]$  respectivamente.

**Ejercicio 30.** Sea  $f \in \mathbb{C}[X_1, \dots, X_n]$  de grado  $\leq d$ . Probar que:

1. Si  $f$  se anula en  $\mathbb{Z}^n$ , entonces  $f = 0$ .
2. Lo mismo si  $f$  se anula en  $\{(x_1, \dots, x_n) \in \mathbb{Z}^n : 0 \leq x_i \leq d\}$ .

**Ejercicio 31.** Sean  $f = XY - 1$  y  $g = X^2 + Y^2 - 2$ . Calcular  $\text{Res}_X(f, g)$  y decidir si  $f$  y  $g$  tienen un factor común en  $\mathbb{Q}(Y)[X]$  y en  $\mathbb{Q}[X, Y]$ . ¿En que puntos de  $\mathbb{C}^2$  se anulan simultáneamente ambos polinomios?

**Ejercicio 32.** Sean  $f = \prod_{i=1}^n (X - \alpha_i) \in \mathbb{C}[X]$  y  $g = \prod_{j=1}^m (X - \beta_j) \in \mathbb{C}[X]$ .

- i) ¿Cuáles son las raíces del polinomio  $\text{Res}_Y(f(X - Y), g(Y)) \in \mathbb{C}[X]$ ?
- ii) ¿Y cuáles las de  $\text{Res}_Y(Y^n f(X/Y), g(Y)) \in \mathbb{C}[X]$ ?
- iii) Probar que  $a = \prod (\pm\sqrt{1} \pm \sqrt{2} \pm \sqrt{3} \pm \dots \pm \sqrt{n})$  es entero.
- iv) (*Difícil*) Probar que  $a$  de (iii) es un cuadrado perfecto para todo  $n \geq 2$ .