

---

# ÁLGEBRA II

## Primer Cuatrimestre — 2019

### Práctica 3: Anillos

---

#### Ejemplos y construcciones

1. Probar que los siguientes conjuntos son anillos con las operaciones indicadas. Decidir en cada caso si son conmutativos, íntegros, de división, cuerpos, etc.

- (a)  $M_8(\mathbb{R})$  con el producto y la suma de matrices.
- (b)  $\mathbb{Z}_{12}[X]$  con el producto usual de polinomios.
- (c)  $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$  donde  $d \in \mathbb{Z}$  es libre de cuadrados, con la suma y el producto de números complejos.
- (d)  $\mathcal{C}^6(0, 1) = \{f : (0, 1) \rightarrow \mathbb{R} \mid \text{las primeras 6 derivadas de } f \text{ existen y son continuas}\}$ , con la suma y el producto usual de funciones.
- (e)  $A = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$ , con el producto y la suma de matrices.

2. Si  $A$  es un grupo abeliano entonces  $\text{End } A$ , el conjunto de endomorfismos de grupo de  $A$ , es un anillo con la suma habitual de funciones y la composición como producto. Encontrar descripciones explícitas para este anillo cuando  $A$  es  $\mathbb{Z}^n$  o  $\mathbb{Z}_n$ .

3. (a) Sean  $A$  un anillo y  $\mathcal{C}$  una familia de subanillos de  $A$ . Mostrar que  $B = \bigcap_{C \in \mathcal{C}} C$  es un subanillo de  $A$ .

(b) Sean  $A$  un anillo,  $B \subseteq A$  un subanillo y  $X \subseteq A$ . Mostrar que existe un subanillo  $B[X]$  de  $A$  que contiene a  $X$  y a  $B$  y tal que cualquier otro subanillo de  $A$  que contiene a  $B$  y a  $X$  contiene a  $B[X]$ .

(c) Sea  $\eta$  una raíz primitiva sexta de la unidad y  $\omega$  una raíz primitiva  $p$ -ésima de la unidad, donde  $p$  es algún número primo. Describir explícitamente  $\mathbb{Z}[\sqrt{2}]$ ,  $\mathbb{Z}[\sqrt[3]{5}]$ ,  $\mathbb{Z}[i]$ ,  $\mathbb{Z}[\eta]$ ,  $\mathbb{Z}[\sqrt{6}, \sqrt{p}]$  y  $\mathbb{Z}[\omega]$  como subanillos de  $\mathbb{C}$ .

4. *Anillos de matrices.* Sean  $A$  un anillo y  $n \in \mathbb{N}$ . Probar que el conjunto de matrices  $M_n(A)$  con coeficientes en  $A$  es un anillo con respecto a las operaciones usuales de suma y producto de matrices. Probar que si  $n > 1$ , entonces  $M_n(A)$  no es conmutativo.

5. *Anillos de funciones.* Sean  $A$  un anillo y  $X$  un conjunto no vacío. Sea  $A^X$  el conjunto de todas las funciones  $X \rightarrow A$ . Definimos operaciones  $+, \cdot : A^X \times A^X \rightarrow A^X$  de la siguiente manera: dadas  $f, g \in A^X$

$$(f + g)(x) = f(x) + g(x) \quad \text{para todo } x \in X,$$

y

$$(f \cdot g)(x) = f(x)g(x) \quad \text{para todo } x \in X.$$

Mostrar que  $(A^X, +, \cdot)$  es un anillo. ¿Cuándo es conmutativo?

6. *Anillos de polinomios.* Sea  $A$  un anillo, y sea

$$S = \{f : \mathbb{N}_0 \rightarrow A \mid \text{existe un conjunto finito } T \subset \mathbb{N}_0 \text{ tal que } f|_{T^c} \equiv 0\}.$$

Definimos operaciones de suma y producto  $+, \cdot : S \times S \rightarrow S$  de la siguiente manera: para cada  $f, g \in S$  y cada  $n \in \mathbb{N}_0$ ,

$$(f + g)(n) = f(n) + g(n)$$

y

$$(f \cdot g)(n) = \sum_{\substack{k,l \geq 0 \\ k+l=n}} f(k)g(l).$$

Mostrar que estas operaciones están bien definidas y que  $(S, +, \cdot)$  es un anillo.

Sea  $X$  una variable formal. Si  $f \in S$  y  $T \subset \mathbb{N}$  es tal que  $f|_{T^c} \equiv 0$ , podemos representar a  $f$  por la suma finita formal

$$\sum_{n \in T} f(n)X^n.$$

Con esta notación, las operaciones de  $S$  imitan formalmente las correspondientes operaciones entre polinomios. Llamamos a  $S$  el *anillo de polinomios con coeficientes en  $A$*  y lo notamos  $A[X]$ .

7. *Anillos de series formales.* Sea  $A$  un anillo.

(a) Sea  $S = \{f : \mathbb{N}_0 \rightarrow A\}$  el conjunto de todas las funciones de  $\mathbb{N}_0$  a  $A$ . Definimos operaciones  $+, \cdot : S \times S \rightarrow S$  de la siguiente manera: para cada  $f, g \in S$  y cada  $n \in \mathbb{N}_0$ ,

$$(f + g)(n) = f(n) + g(n)$$

y

$$(f \cdot g)(n) = \sum_{\substack{k,l \geq 0 \\ k+l=n}} f(k)g(l).$$

Mostrar que  $(S, +, \cdot)$  es un anillo.

Sea  $X$  una variable formal. Podemos representar a una función  $f \in S$  por una serie

$$f = \sum_{n=0}^{\infty} f(n)X^n.$$

Usando esta notación, las definiciones de la suma y el producto de  $S$  imitan formalmente a las correspondientes operaciones con las series. Llamamos a  $S$  el *anillo de series formales de potencias con coeficientes en  $A$* , y lo notamos  $A[[X]]$ .

(b) Probar que la función representada por la serie  $1 - X$  es inversible en  $A[[X]]$ .

(c) Tomamos ahora  $A = \mathbb{R}$  y sea  $\mathbb{R}\{\{X\}\} \subset \mathbb{R}[[X]]$  el subconjunto de las series formales que tienen radio de convergencia positivo. Mostrar que se trata de un subanillo.

8. *Anillo de grupo.* Sean  $G$  un grupo y  $A$  un anillo.

(a) Sea  $A[G]$  el conjunto de todas las funciones  $f : G \rightarrow A$  tales que

$$|\{g \in G : f(g) \neq 0\}| < \infty.$$

Definimos operaciones  $+, \cdot : A[G] \times A[G] \rightarrow A[G]$  de la siguiente manera: para cada  $s, t \in A[G]$  y cada  $g \in G$ ,

$$(s + t)(g) = s(g) + t(g)$$

y

$$(s \cdot t)(g) = \sum_{h \in G} s(gh^{-1})t(h).$$

Mostrar que  $(A[G], +, \cdot)$  es un anillo.

(b) Supongamos desde ahora que  $A = \mathbb{k}$  es un cuerpo. Mostrar que  $\mathbb{k}[G]$  es un subespacio vectorial del espacio vectorial  $\mathbb{k}^G$  de todas las funciones  $G \rightarrow \mathbb{k}$ .

(c) Dado  $g \in G$ , sea  $\hat{g} : G \rightarrow \mathbb{k}$  la función definida por

$$\hat{g}(h) = \begin{cases} 1, & \text{si } g = h; \\ 0, & \text{en caso contrario.} \end{cases}$$

Mostrar que  $\{\hat{g} : g \in G\}$  es una base de  $\mathbb{k}[G]$ . En particular, todo elemento  $f \in \mathbb{k}[G]$  puede escribirse como

$$f = \sum_{g \in G} \alpha_g \hat{g}$$

con coeficientes  $\alpha_g \in \mathbb{k}$  casi todos nulos.

(d) Mostrar que si  $g, h \in G$ , entonces  $\hat{g} \cdot \hat{h} = \widehat{gh}$ .

†(e) Describir el centro de  $\mathbb{k}[G]$  cuando  $G$  es finito. ¿Qué pasa cuando  $G$  es infinito?

†9. *El álgebra de Weyl.* Sea  $\text{End}_{\mathbb{C}}(\mathbb{C}[X])$  el anillo de endomorfismos de  $\mathbb{C}[X]$  considerado como  $\mathbb{C}$ -espacio vectorial. Sean  $p, q \in \text{End}_{\mathbb{C}}(\mathbb{C}[X])$  definidos de la siguiente manera: si  $f \in \mathbb{C}[X]$ , entonces

$$p(f) = \frac{df}{dX}, \quad \text{y} \quad q(f) = Xf.$$

Sea  $A = \mathbb{C}[p, q]$  el menor subanillo de  $\text{End}_{\mathbb{C}}(\mathbb{C}[X])$  que contiene a  $\mathbb{C}$ , a  $p$  y a  $q$ . Llamamos a  $A$  el *álgebra de Weyl*.

(a) Probar que  $pq - qp = 1$ .

(b) Probar que  $A$  es una  $\mathbb{C}$ -álgebra de dimensión infinita sobre  $\mathbb{C}$ , y que  $\{p^i q^j : i, j \in \mathbb{N}_0\}$  es una base.

(c) Describir el centro de  $A$ .

(d) Mostrar que  $A$  no posee divisores de cero y describir el conjunto de sus unidades.

10. *Anillo opuesto.*

(a) Sea  $A$  un anillo. Sea  $*$  :  $A \times A \rightarrow A$  la operación definida por

$$a * b = ba, \quad \forall a, b \in A.$$

Probar que  $(A, +, *)$  es un anillo. Se trata del *anillo opuesto de  $A$* , que escribimos habitualmente  $A^{\text{op}}$ .

(b) Mostrar con un ejemplo que en general  $A \not\cong A^{\text{op}}$ .

11. Un cuadrado mágico es una matriz cuadrada con entradas enteras, tal que la suma de los elementos de cualquier fila o columna es igual a la suma de los elementos de cualquier otra fila o columna. Probar que para cada  $n \in \mathbb{N}$  los cuadrados mágicos de tamaño  $n$  forman un subanillo de  $M_n(\mathbb{R})$ .

12. Sea  $X$  un conjunto. Mostrar que  $(\mathcal{P}(X), \Delta, \cap)$  es un anillo. Aquí  $\Delta$  es la operación diferencia simétrica.

13. Sea  $A$  un anillo. Probar las siguientes afirmaciones.

(a) Si cada elemento de  $A$  tiene inverso a izquierda entonces  $A$  es un anillo de división.

(b) Sea  $a \in A$ . Si existe  $n \in \mathbb{N}$  tal que  $a^n$  es inversible, entonces  $a$  es inversible.

14. *Idempotentes.* Sea  $A$  un anillo. Un elemento  $e \in A$  es *idempotente* si  $e^2 = e$ . Probar las siguientes afirmaciones.

(a) Si  $e \in A$  es idempotente, el subconjunto  $eAe$  con las operaciones de  $A$  restringidas es un anillo. Se trata de un subanillo de  $A$  si y solo si  $e = 1$ .

(b) Si  $e \in A$  es idempotente, entonces  $1 - e$  también lo es.

(c) Sea  $G$  un grupo finito y sea  $\mathbb{k}$  un cuerpo en el que  $|G| \neq 0$ . Probar que

$$e = \frac{1}{|G|} \sum_{g \in G} g$$

es un idempotente en  $\mathbb{k}[G]$ .

<sup>†</sup>15. *Anillos booleanos.* Un anillo  $A$  es *booleano* si todos sus elementos son idempotentes.

- (a) Probar que si  $X$  es un conjunto, entonces el anillo  $(\mathcal{P}(X), \Delta, \cap)$  es booleano.
- (b) Probar que un anillo booleano es conmutativo.

### Morfismos, ideales y cocientes

En toda esta sección  $A$  y  $B$  son anillos. Denotamos  $\text{Hom}(A, B)$  al conjunto de morfismos de anillos  $A \rightarrow B$ .

- 16. (a) Mostrar que hay exactamente un morfismo de anillos  $\mathbb{Z} \rightarrow A$ .
- (b) Mostrar que hay a lo sumo un morfismo de anillos  $\mathbb{Q} \rightarrow A$  y que puede no haber ninguno.

17. Sea  $f : \mathbb{R} \rightarrow \mathbb{R}$  un morfismo de anillos. Probar las siguientes afirmaciones.

- (a)  $f(\mathbb{Q}) \subseteq \mathbb{Q}$ , y de hecho  $f|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$ .
- (b) La aplicación  $f$  es estrictamente creciente.

Concluir que  $f = \text{id}_{\mathbb{R}}$ .

18. Sea  $\mathbb{k}$  un cuerpo. Decidir en cada caso si existe un morfismo de anillos  $f : A \rightarrow B$ :

- (a)  $A = \mathbb{Z}[i]$  y  $B = \mathbb{R}$ ;
- (b)  $A = \mathbb{Z}[\sqrt{-5}]$  y  $B = \mathbb{Z}[\sqrt{3}]$ ;
- (c)  $A = \mathbb{k}$  y  $B = M_n(\mathbb{k})$ ;
- (d)  $A = M_n(\mathbb{k})$  y  $B = \mathbb{k}$ .

19. Sea  $A$  un anillo. El *grupo de unidades de  $A$*  es el conjunto

$$\mathcal{U}(A) = \{a \in A \mid a \text{ es inversible}\}$$

con la multiplicación de  $A$ .

- (a) Probar que  $\mathcal{U}(A)$  es un grupo.
- (b) Hallar las unidades de  $\mathbb{Z}$  y  $\mathbb{Z}[\sqrt{2}]$ .
- (c) Probar que  $\mathcal{U}(A[X]) = \mathcal{U}(A)$ .
- (d) Sea  $G$  un grupo. Probar que  $1 \cdot G \subseteq \mathcal{U}(\mathbb{Z}[G])$  pero que no vale la igualdad.

20. Probar que si  $G$  es un grupo, la aplicación

$$\begin{aligned} \text{Hom}(\mathbb{Z}[G], A) &\rightarrow \text{Hom}_{\text{Grp}}(G, \mathcal{U}(A)) \\ f &\mapsto f|_G \end{aligned}$$

es una biyección.

21. Sea  $\mathcal{I}$  una familia de ideales a izquierda (a derecha, biláteros) de  $A$ .

- (a) Mostrar que  $\bigcap_{I \in \mathcal{I}} I$  es un ideal a izquierda (a derecha, bilátero) de  $A$ . Se trata del ideal más grande contenido en todos los ideales de  $\mathcal{I}$ .
- (b) Mostrar que  $\sum_{I \in \mathcal{I}} I$  es un ideal a izquierda (a derecha, bilátero) de  $A$ . Se trata del ideal más chico que contiene a todos los ideales de  $\mathcal{I}$ .

22. Sea  $I \subseteq A$  un ideal bilátero. Sea  $J$  el ideal generado por  $I$  en  $A[X]$ . Mostrar que  $A[X]/J \cong (A/I)[X]$ .

23. Ideales biláteros de  $M_n(A)$ .

- (a) Sean  $I \subseteq A$  un ideal bilátero y  $n \in \mathbb{N}$ . Sea  $M_n(I) \subseteq M_n(A)$  el subconjunto de las matrices de  $M_n(A)$  que tienen todos sus coeficientes en  $I$ . Mostrar que  $M_n(I)$  es un ideal bilátero de  $M_n(A)$  y que  $M_n(A)/M_n(I) \cong M_n(A/I)$ .
- (b) Probar que si  $J \subseteq M_n(A)$  es un ideal bilátero, entonces existe un ideal bilátero  $I \subseteq A$  tal que  $J = M_n(I)$ .
- Sugerencia.* Tomar  $I = \{a \in A \mid a = M_{1,1} \text{ para alguna matriz } M \in J\}$ .
- (c) Probar que si  $\mathbb{k}$  es un cuerpo, entonces  $M_n(\mathbb{k})$  es simple —es decir que los únicos ideales biláteros de  $M_n(\mathbb{k})$  son  $0$  y  $M_n(\mathbb{k})$ .

24. Ideales a izquierda de  $M_n(\mathbb{k})$ . Sea  $\mathbb{k}$  un cuerpo.

- (a) Sean  $V \subseteq \mathbb{k}^n$  un subespacio vectorial e  $I_V$  el subconjunto de  $M_n(\mathbb{k})$  formado por todas las matrices cuyas filas pertenecen a  $V$ . Probar que  $I_V$  es un ideal a izquierda de  $M_n(\mathbb{k})$ .
- (b) Probar que todo ideal a izquierda de  $M_n(\mathbb{k})$  es de la forma  $I_V$  para algún subespacio  $V \subseteq \mathbb{k}^n$ .
- Sugerencia.* Llamar  $V$  al conjunto formado por las todas filas de todas las matrices del ideal y probar que es un subespacio.

25. Probar que  $Z(M_n(A)) = Z(A) \cdot \text{id}$ .

26. Sea  $\mathbb{k}$  un cuerpo. Sean  $G$  un grupo y  $H \trianglelefteq G$  un subgrupo normal, y consideremos la proyección canónica  $\pi : G \rightarrow G/H$ . Mostrar que  $\pi$  determina un morfismo sobreyectivo de anillos  $\mathbb{k}[\pi] : \mathbb{k}[G] \rightarrow \mathbb{k}[G/H]$ . Describir el núcleo de  $\mathbb{k}[\pi]$ .

## Anillos conmutativos

En esta sección  $A$  es un anillo conmutativo.

27. Mostrar que  $A$  es un cuerpo sii los únicos ideales de  $A$  son  $0$  y  $A$ .

28. (a) Sea  $a \in A$  un elemento que no es inversible. Mostrar que existe un ideal maximal  $\mathfrak{m} \subseteq A$  tal que  $a \in \mathfrak{m}$ .
- (b) Sea  $I \subsetneq A$ . Mostrar que existe un ideal maximal  $\mathfrak{m} \subseteq A$  tal que  $I \subseteq \mathfrak{m}$ .

**Definición.** Decimos que un ideal  $\mathfrak{p} \subsetneq A$  es primo si

$$ab \in \mathfrak{p} \implies a \in \mathfrak{p} \vee b \in \mathfrak{p}.$$

Notamos por  $\text{Spec } A$  al conjunto de todos los ideales primos de  $A$ .

29. Probar las siguientes afirmaciones.

- (a) Un ideal  $\mathfrak{p} \subsetneq A$  es primo sii  $A/\mathfrak{p}$  es un dominio de integridad.
- (b) Un ideal maximal de  $A$  es primo.

30. Determinar  $\text{Spec } \mathbb{Z}$ . Identificar qué ideales primos de  $\mathbb{Z}$  son maximales.

31. Sea  $\mathbb{k}$  un cuerpo. Mostrar que si  $\mathfrak{p} \in \text{Spec } \mathbb{k}[X]$ , entonces existe un único  $f \in \mathfrak{p}$  mónico e irreducible tal que  $\mathfrak{p} = (f)$ . Recíprocamente, probar que todo ideal principal generado por un polinomio mónico e irreducible es primo en  $\mathbb{k}[X]$ .

32. (a) Sea  $f : A \rightarrow B$  un morfismo de anillos. Probar que si  $\mathfrak{p} \in \text{Spec } B$ , entonces  $f^{-1}(\mathfrak{p}) \in \text{Spec } A$ . En particular, si  $A \subseteq B$  es un subanillo y  $\mathfrak{p} \in \text{Spec } B$ , entonces  $\mathfrak{p} \cap A \in \text{Spec } A$ .
- (b) Sea  $I \subseteq A$  un ideal. Probar que la correspondencia entre ideales de  $A$  que contienen a  $I$  e ideales de  $A/I$  se restringe a una correspondencia entre los ideales primos de  $A$  que contienen a  $I$  y los ideales primos de  $A/I$ .

33. Mostrar que todo ideal primo no nulo de  $\mathbb{Z}[X]$  es de alguna de las siguientes formas:

- (a)  $(p)$ , con  $p \in \mathbb{N}$  primo;

- (b)  $(f)$ , con  $f \in \mathbb{Z}[X]$  un polinomio mónico irreducible;
- (c)  $(p, f)$ , con  $p$  primo y  $f$  irreducible en  $\mathbb{Z}_p[X]$ .

*Sugerencia.* Sea  $\mathfrak{p} \in \text{Spec } \mathbb{Z}[X]$ . Mostrar que si  $\mathfrak{p} \cap \mathbb{Z} \neq \{0\}$  entonces es un ideal principal de  $\mathbb{Z}$  generado por un número primo  $p$ , así que en particular  $(p) \subseteq \mathfrak{p}$ . Considerar ahora el ideal  $\mathfrak{p}/(p)$  de  $\mathbb{Z}[X]/(p) \cong \mathbb{Z}_p[X]$  y usar un ejercicio anterior que describe los ideales primos de este anillo.

**34. Nilradical.** 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  $\text{nil}(A) = \{a \in A : a \text{ es nilpotente}\}$ . Probar las siguientes afirmaciones:

- (a)  $\text{nil}(A)$  es un ideal de  $A$ ;
- (b)  $\text{nil}(A/\text{nil}(A)) = 0$ ;
- (c)  $\text{nil}(A) = \bigcap_{\mathfrak{p} \in \text{Spec } A} \mathfrak{p}$ ;
- (d) si  $x \in \text{nil}(A)$ , entonces  $1 + x$  es inversible.

**35. Radical de Jacobson.** El *radical de Jacobson* de  $A$  es la intersección de todos los ideales maximales de  $A$ , y se nota  $J(A)$ . Mostrar que  $x \in J(A)$  sii para cada  $y \in A$  se tiene que  $1 - xy$  es inversible.