Álgebra II
Primer Cuatrimestre — 2015

Práctica 4: Anillos y álgebras

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*) $\mathcal{C}^6[0,1] = \{f : [0,1] \to \mathbb{R} \mid$ las primeras 6 derivadas de f 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.

(*f*) Dado un espacio métrico (X, d), el conjunto $\mathcal{B}(X) = \{f : X \to \mathbb{R} \mid f$ es acotada$\}$.

(*g*) El conjunto $\mathcal{O} = \{z \in \mathbb{C} \mid$ existe $p \in \mathbb{Z}[X]$ mónico tal que $p(z) = 0\}$.

2. Si A es un grupo abeliano entonces $\mathsf{End}\, A$, 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. Muestre que $B = \bigcap_{C \in \mathcal{C}} C$ es un subanillo de A.

(*b*) Sean A un anillo, $B \subset A$ un subanillo y $X \subset A$. 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 η una raíz primitiva sexta de la unidad y ω 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. Describa todos los anillos con a lo sumo 10 elementos a menos de isomorfismo.

5. *Anillos de matrices.* Sea A un anillo.

(*a*) Sea $n \in \mathbb{N}$. 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. Si $n > 1$, entonces $M_n(A)$ no es conmutativo.

(*b*) Sea $M_\infty(A) = \{f : \mathbb{N} \times \mathbb{N} \to A\}$. Decimos que un elemento $f \in M_\infty(A)$ tiene *filas finitas* si para cada $n \in \mathbb{N}$ existe $k(n) \in \mathbb{N}$ tal que $f(n, m) = 0$ si $m > k(n)$; de manera similar, decimos que $f \in M_\infty(A)$ tiene *columnas finitas* si para cada $m \in \mathbb{N}$ existe $k(m) \in \mathbb{N}$ tal que $f(n, m) = 0$ si $n > k(m)$.

Sean $M_\infty^f(A)$ y $M_\infty^c(A)$ los subconjuntos de $M_\infty(A)$ de matrices con filas finitas y con columnas finitas, respectivamente, y sea $M_\infty^{fc}(A) = M_\infty^f(A) \cap M_\infty^c(A)$. Mostrar que $M_\infty^f(A)$, $M_\infty^c(A)$ y $M_\infty^{fc}(A)$ son anillos con el producto dado por

$$f \cdot g(n, m) = \sum_{k=1}^{\infty} f(n, k) g(k, m).$$

6. *Anillos de funciones.*

(*a*) Sea A un anillo y X un conjunto no vacío. Sea A^X el conjunto de todas las funciones $X \to A$. Se definen operaciones $+, \cdot : A^X \times A^X \to A^X$ de la siguiente manera: dadas $f, g \in A^X$

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

y

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

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

(*b*) Sean $n \in \mathbb{N}$, $k \in \mathbb{N}_0$ y sea $\mathcal{C}^k(\mathbb{R}^n)$ el conjunto de todas las funciones $f : \mathbb{R}^n \to \mathbb{R}$ con derivadas parciales de orden k continuas. Muestre que se trata de un subanillo de $\mathbb{R}^{(\mathbb{R}^n)}$.

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

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

Definimos operaciones de suma y producto $+, \cdot : S \times S \to S$ 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

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

Muestre 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 $A[X]$.

8. *Anillos de series formales.* Sea A un anillo.

(*a*) Sea $S = \{f : \mathbb{N}_0 \to A\}$ el conjunto de todas las funciones de $\mathbb{N}_0$ a A. Definimos operaciones $+, \cdot : S \times S \to S$ 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

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

Muestre 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*) Pruebe 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.

9. *Series de Dirichlet.* Sea A un anillo.

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

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

y

$$(f \cdot g)(n) = \sum_{\substack{d \in \mathbb{N} \\ d|n}} f(d)g(n/d).$$

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

Si s es una variable, a un elemento $f \in S$ podemos asignarle la expresión formal

$$f = \sum_{n \geq 1} \frac{f(n)}{n^s}.$$

Las operaciones de S se corresponden entonces con las operaciones evidentes de estas series. Este es el *anillo de series de Dirichlet con coeficientes en* A.

(*b*) Sea $\zeta : \mathbb{N} \to \mathbb{Z}$ la función constantemente 1. Pruebe que ζ es inversible en el anillo de series de Dirichlet con coeficientes en $\mathbb{Z}$, y halle explícitamente su inversa, que suele denotarse por μ y se llama *función de Moebius*.

10. *Anillo de grupo.* Sean G un grupo y A un anillo.

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

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

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

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

y

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

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

(*b*) Supongamos desde ahora que $A = \Bbbk$ es un cuerpo. Muestre que $\Bbbk[G]$ es un subespacio vectorial del espacio vectorial $\Bbbk^G$ de todas las funciones $G \to \Bbbk$.

(*c*) Dado $g \in G$, sea $\hat{g} : G \to \Bbbk$ la función definida por

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

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

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

con coeficientes $\alpha_g \in \Bbbk$ casi todos nulos.

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

(*e*) Describa el centro de $\Bbbk[G]$ cuando G es finito. ¿Qué pasa cuando G es infinito?

11. *Algebras de caminos.*

(*a*) Un *carcaj* Q es una 4-upla (Q_0, Q_1, s, t) en la que:

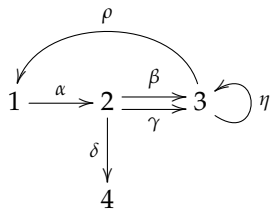
— Q_0 y Q_1 son conjuntos. Los elementos de Q_0 son los *vértices* de Q y los de Q_1 las *flechas*.

— s y t son funciones $Q_1 \to Q_0$. Si $\alpha \in Q_1$ es una flecha, decimos que $s(\alpha)$ es el *origen* de α y que $t(\alpha)$ es su final.

Por ejemplo, obtenemos un carcaj si ponemos $Q = (Q_0, Q_1, s, t)$ con $Q_0 = \{1, 2, 3, 4\}$, $Q_1 = \{\alpha, \beta, \gamma, \delta, \eta, \rho\}$ y s y t están dadas por la tabla siguiente:

	α	β	γ	δ	η	ρ
s	1	2	2	2	3	3
t	2	3	3	4	3	1

Podemos describir este carcaj más eficientemente dando el siguiente dibujo:



Fijemos un carcaj Q. Si $x, y \in Q_0$, un *camino de x a y en Q* es una secuencia finita $\kappa = (x; \alpha_1, \dots, \alpha_n; y)$ de flechas de Q tal que $s(\alpha_1) = x$, $t(\alpha_n) = y$ y para cada $i \in \{1, \dots, n-1\}$ se tiene que $t(\alpha_i) = s(\alpha_{i+1})$. El número n es la *longitud* de κ. En particular, si $x \in Q_0$, hay un camino $(x; ; x)$ de x a x de longitud 0.

Sea $P(Q)$ el conjunto de todos los caminos de Q, sea $\Bbbk$ un cuerpo y sea $\Bbbk Q$ el espacio vectorial que tiene a $P(Q)$ como base. Un elemento $u \in \Bbbk Q$ es una combinación lineal finita de caminos de Q con coeficientes en $\Bbbk$:

$$u = \sum_{\kappa \in P(Q)} a_\kappa \kappa.$$

Se define un producto asociativo bilineal $\cdot : \Bbbk Q \times \Bbbk Q \to \Bbbk Q$ de la siguiente manera: para cada par de caminos $\kappa = (x; \alpha_1, \dots, \alpha_n; y)$ y $\zeta = (z; \beta_1, \dots, \beta_m; w)$ en Q,

$$\kappa \cdot \zeta = \begin{cases} (x; \alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m; w), & \text{si } y = z; \\ 0, & \text{en caso contrario.} \end{cases}$$

Mostrar que con este producto $\Bbbk Q$ es una $\Bbbk$-álgebra si y solo si Q_0 es finito. ¿Cuál es la unidad de $\Bbbk Q$? Llamamos a $\Bbbk Q$ el *álgebra de caminos de Q sobre $\Bbbk$*.

(*b*) Sean Q y Q' como en la figura. Probar que $\Bbbk Q = \Bbbk$ y $\Bbbk Q'$ es isomorfo a $\Bbbk[X]$.

Q : • Q' : •↺

(*c*) *$\Bbbk$-álgebras libres.* Sea X un conjunto y sea Q el carcaj (Q_0, Q_1, s, t) en el que Q_0 tiene un único elemento p, $Q_1 = X$ y s, $t : Q_1 \to Q_0$ son las funciones evidentes. Escribimos $L(X)$ en vez de $\Bbbk Q$. Encuentre una base de $L(X)$ y describa el producto de esta álgebra.

(*d*) ¿Cuándo es $\Bbbk Q$ un dominio de integridad? ¿Cuándo tiene dimensión finita? ¿Cuándo es conmutativa?

(*e*) Describa el centro de $\Bbbk Q$.

(*f*) Considere el carcaj Q de n vértices de la figura:

$$1 \longrightarrow 2 \longrightarrow \quad \cdots \quad \longrightarrow n-1 \longrightarrow n$$

Muestre que $\Bbbk Q$ es isomorfo al anillo de matrices triangulares superiores de $M_n(\Bbbk)$.

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

$$p(f) = \frac{\mathrm{d}f}{\mathrm{d}X}, \qquad \text{y} \qquad q(f) = Xf.$$

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

(*a*) Pruebe que $pq - qp = 1$.

(*b*) Pruebe 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*) Describa el centro de A.

(*d*) Muestre que A no posee divisores de cero y describa el conjunto de sus unidades.

13. *El álgebra de funciones en el plano cuántico.* Sea $q \in \mathbb{C} \setminus 0$ y supongamos que q no es una raíz de la unidad. Sea $V = \{f : \mathbb{N}_0 \to \mathbb{C}\}$ el $\mathbb{C}$-espacio vectorial de todas las funciones de $\mathbb{N}_0$ en $\mathbb{C}$. Consideramos dos elementos $x, y \in \mathsf{End}_{\mathbb{C}}(V)$ definidos de la siguiente manera: si $f \in V$ y $n \in \mathbb{N}_0$, entonces $x(f), y(f) : \mathbb{N}_0 \to \mathbb{C}$ son tales que

$$\big(x(f)\big)(n) = q^n f(n),$$

e

$$\big(y(f)\big)(n) = f(n+1).$$

Sea $A_q = \mathbb{C}[x, y]$ la menor subálgebra de $\mathsf{End}_{\mathbb{C}}(V)$ que contiene a $\mathbb{C}$, a x y a y. Llamamos a A_q el *álgebra de funciones en el plano cuántico*.

(*a*) Pruebe que $yx = qxy$.

(*b*) Pruebe que A_q es una $\mathbb{C}$-álgebra de dimensión infinita, y que el conjunto $\{x^i y^j : i, j \in \mathbb{N}_0\}$ es una base.

(*c*) Describa el centro de A_q.

(*d*) Muestre que A_q no posee divisores de cero y describa el conjunto de sus unidades.

(*e*) Para cada $n \in \mathbb{N}$ definimos

$$(n)_q = \frac{q^n - 1}{q - 1},$$

y $(0)_q = 1$. Definimos además

$$(n)_q! = (1)_q (2)_q \cdots (n)_q.$$

Finalmente, si $n \in \mathbb{N}_0$ y $0 \leq k \leq n$, definimos

$$\binom{n}{k}_q = \frac{(n)_q!}{(k)_q!(n-k)_q!}.$$

Muestre que:

(i) Si $0 \leq k \leq n$, entonces

$$\binom{n}{k}_q = \binom{n}{n-k}_q.$$

(ii) Si $0 \leq k \leq n$, entonces

$$\binom{n}{k}_q = \binom{n-1}{k-1}_q + q^k \binom{n-1}{k}_q = \binom{n-1}{k}_q + q^{n-k}\binom{n-1}{k-1}_q.$$

(iii) Si $0 \leq k \leq n$, $\binom{n}{k}_q$ es un polinomio en q con coeficientes enteros.

(iv) Sean $x, y \in A_q$ los generadores del álgebra de funciones del plano cuántico. Si $n > 0$, entonces

$$(x+y)^n = \sum_{0 \leq k \leq n} \binom{n}{k}_q x^k y^{n-k}.$$

(*f*) ¿Qué pasa si q es una raíz primitiva de la unidad de orden e?

14. *Anillo opuesto.*

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

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

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

(*b*) Muestre con un ejemplo que en general $A \ncong A^{\mathrm{op}}$.

15. 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 $M_n(\mathbb{R})$.

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

Varia

17. Sean A un conjunto y $+, \cdot : A \times A \to A$ dos operaciones en A que satisfacen todos los axiomas de la definición de anillos salvo posiblemente aquel que dice que el grupo $(A, +)$ es abeliano. Muestre que $(A, +, \cdot)$ es un anillo.

18. 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*) Si $a \in A$ es un elemento inversible a izquierda y que no divide a 0 por la derecha, entonces a es inversible.

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

19. Sea A un anillo posiblemente sin unidad. Muestre que si A posee una única unidad a izquierda e, entonces A posee una unidad.

Sugerencia. Sea $a \in A$ y considere para cada $c \in A$ el elemento $(e - ae - a)c$.

20. *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.

21. *Anillos booleanos.* Un anillo A es *booleano* si todos sus elementos son idempotentes.

(*a*) Si X es un conjunto, entonces el anillo $(\mathcal{P}(X), \triangle, \cap)$ es booleano.

(*b*) Probar que un anillo booleano es conmutativo.

Morfismos, ideales y cocientes

En toda esta sección A es un anillo.

22. (*a*) Muestre que hay exactamente un morfismo de anillos $\mathbb{Z} \to A$.

(*b*) Muestre que hay a lo sumo un morfismo de anillos $\mathbb{Q} \to A$ y que puede no haber ninguno. Describa cuándo se da cada uno de estos dos casos.

23. Sea $f : \mathbb{R} \to \mathbb{R}$ un morfismo de anillos. Pruebe las siguientes afirmaciones.

(*a*) $f(\mathbb{Q}) \subset \mathbb{Q}$, y de hecho $f|_{\mathbb{Q}} = \mathsf{id}_{\mathbb{Q}}$.

(*b*) La aplicación f es estrictamente creciente.

Concluya que $f = \mathsf{id}_{\mathbb{R}}$.

24. Sea $\Bbbk$ un cuerpo. Decidir en cada caso si existe un morfismo de anillos $f : A \to B$:

(*a*) $A = \mathbb{Z}[i]$ y $B = \mathbb{R}$;

(*b*) $A = \mathbb{Z}[\sqrt{-5}]$ y $B = \mathbb{Z}[\sqrt{3}]$;

(*c*) $A = \Bbbk$ y $B = M_n(\Bbbk)$;

(*d*) $A = M_n(\Bbbk)$ y $B = \Bbbk$.

25. Sea $n \in \mathbb{N}$ compuesto. ¿Existe algún producto $\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ que haga del grupo abeliano $\mathbb{Z}_n$ un cuerpo?

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

(*a*) Muestre que $\bigcap_{I \in \mathcal{I}} I$ es un ideal a izquierda (a derecha, bilatéro) de A. Se trata del ideal más grande contenido en todos los ideales de $\mathcal{I}$.

(*b*) Muestre 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 $\mathcal{I}$.

27. Sea $I \subset A$ un ideal a izquierda. Muestre que existe un subanillo $\mathbb{I}(I) \subset A$ tal que

- $I \subset \mathbb{I}(I)$ e I es un ideal bilátero de $\mathbb{I}(I)$;
- $\mathbb{I}(I)$ es el menor subanillo de A con esa propiedad.

Llamamos a $\mathbb{I}(I)$ el *idealizador de I en A*.

28. Supongamos que A es conmutativo.

(*a*) Sean $I \subset A$ un ideal y sea

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

Muestre que $\sqrt{I}$ es un ideal de A.

(*b*) Sean I, $J \subset A$ ideales, y sea

$$(I : J) = \{a \in A : aJ \subset I\}$$

Muestre que $(I : J)$ es un ideal de A, llamado el *conductor de J en I*.

29. Supongamos que A es conmutativo.

(*a*) Sea $a \in A$ un elemento que no es inversible. Mostrar que existe un ideal maximal $\mathfrak{m} \subset A$ tal que $a \in \mathfrak{m}$.

(*b*) Sea $I \subset A$ un ideal propio. Mostrar que existe un ideal maximal $\mathfrak{m} \subset A$ tal que $I \subset \mathfrak{m}$.

30. Muestre que, al igual que las personas, los anillos conmutativos sin ideales propios no son más que un cuerpo.

31. Sean A un anillo e $I \subset A$ un ideal bilátero.

(*a*) Sea J el ideal generado por I en $A[X]$. Muestre que $A[X]/J \cong (A/I)[X]$.

(*b*) Sea $n \in \mathbb{N}$ y sea $M_n(I) \subset M_n(A)$ 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 $M_n(A)/M_n(I) \cong M_n(A/I)$.

†**32.** Sea $\Bbbk$ un cuerpo.

(*a*) Encuentre todos los ideales a izquierda de $M_n(\Bbbk)$.

(*b*) Muestre que $M_n(\Bbbk)$ es simple.

(*c*) Sean ahora A un anillo y $n \in \mathbb{N}$. Si $J \subset M_n(A)$ es un ideal bilátero, pruebe que existe un ideal bilátero $I \subset A$ tal que $J = M_n(I)$.

Sugerencia. Tomar $I = \{a \in A \mid a = M_{1,1} \text{ para alguna matriz } M \in J\}$.

33. Sea $\Bbbk$ un cuerpo. Sean G un grupo y $H \triangleleft G$ un subgrupo normal, y consideremos la proyección canónica $\pi : G \to G/H$. Muestre que π determina un morfismo sobreyectivo de anillos $\Bbbk[\pi] : \Bbbk[G] \to \Bbbk[G/H]$. Describa el núcleo de $\Bbbk[\pi]$.

Espectro de un anillo conmutativo

En esta sección A es un anillo conmutativo.

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

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

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

34. Probar las siguientes afirmaciones.

(*a*) Un ideal $\mathfrak{p} \subset A$ es primo sii $A/\mathfrak{p}$ es un dominio de integridad.

(*b*) Un ideal maximal de A es primo.

35. Determine $\mathsf{Spec}\ \mathbb{Z}$. Identificar qué ideales primos de $\mathbb{Z}$ son maximales.

36. Sea $\Bbbk$ un cuerpo. Muestre que si $\mathfrak{p} \in \mathsf{Spec}\ \Bbbk[X]$, entonces existe $f \in \mathfrak{p}$ mónico e irreducible tal que $\mathfrak{p} = (f)$. Recíprocamente, todo ideal principal generado por un polinomio mónico e irreducible es primo en $\Bbbk[X]$.

37. Probar las siguientes afirmaciones.

(*a*) Si $\mathfrak{p} \in \mathsf{Spec}\ A$ y $B \subset A$ es un subanillo, entonces $B \cap \mathfrak{p} \in \mathsf{Spec}\ B$.

(*b*) Si $I \subset A$ es un ideal, $f : A \to A/I$ es la proyección canónica y $\mathfrak{p} \in \mathsf{Spec}\ A/I$, entonces $f^{-1}(\mathfrak{p}) \in \mathsf{Spec}\ A$.

(*c*) Sea $I \subset A$ un ideal y $\mathfrak{p} \in \mathsf{Spec}\ A$ tal que $\mathfrak{p} \supset I$. Entonces $\mathfrak{p}/I \in \mathsf{Spec}\ A/I$.

38. Muestre 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 $\mathfrak{p} \in \mathsf{Spec}\ \mathbb{Z}[X]$. Muestre 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 $(p) \subset \mathfrak{p}$. Considere ahora el ideal $\mathfrak{p}/(p)$ de $\mathbb{Z}[X]/(p) \cong \mathbb{Z}_p[X]$ y use un ejercicio anterior que describe los ideales primos de este anillo.

†**39.** *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 $\mathsf{nil}(A) = \{a \in A : a \text{ es nilpotente}\}$.

(*a*) $\mathsf{nil}(A)$ es un ideal de A.

(*b*) $\mathsf{nil}(A/\mathsf{nil}(A)) = 0$.

(*c*) $\mathsf{nil}(A) = \bigcap_{\mathfrak{p} \in \mathsf{Spec}\ A} \mathfrak{p}$.

(*d*) Muestre que si $x \in \mathsf{nil}(A)$, entonces $1 + x$ es inversible.

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

Álgebras sobre cuerpos

En esta sección $\Bbbk$ es un cuerpo.

41. Sea A una $\Bbbk$-álgebra de dimensión finita.

(*a*) Probar que A es isomorfa a una subálgebra de $M_n(\Bbbk)$, con $n = \dim A$.

(*b*) Probar que si A es íntegra entonces es un cuerpo.

42. Sea $\Bbbk$ algebraicamente cerrado.

(*a*) Probar que no existen $\Bbbk$-álgebras de dimensión finita que no tengan divisores de cero.

(*b*) Describir a menos de isomorfismo todas las $\Bbbk$-álgebras de dimensión a lo sumo 3.

43. *Álgebras de cuaterniones.* Supongamos que $2 \neq 0$ en $\Bbbk$. Sean 1, i, j y k los vectores de la base canónica de $\Bbbk^4$, y sean $a, b \in \Bbbk^\times$. Mostrar que existe exactamente un producto asociativo $\Bbbk$-bilineal $\cdot : \Bbbk \times \Bbbk \to \Bbbk$ tal que 1 es el elemento unidad e

$$i^2 = a, \qquad j^2 = b, \qquad ij = -ji = k.$$

Notamos el álgebra resultante por $(a, b)_\Bbbk$. En particular $\mathbb{H} = (-1, -1)_\mathbb{R}$ es el álgebra de cuaterniones de Hamilton.

(*a*) Determinar el centro y los ideales biláteros de $(a, b)_\Bbbk$.

(*b*) Probar que para todo $c \in \Bbbk$ vale que $(a, b)_\Bbbk \cong (b, a)_\Bbbk \cong (ac^2, bc^2)_\Bbbk$.

(*c*) Probar que $(1, b)_\Bbbk \cong M_2(\Bbbk)$. Concluir que si a o b es un cuadrado en $\Bbbk$ entonces $(a, b)_\Bbbk \cong M_2(\Bbbk)$.

Sugerencia. Considere el morfismo $(1, b)_\Bbbk \to M_2(\Bbbk)$ dado por $i \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $j \mapsto \left(\begin{smallmatrix} 0 & 1 \\ b & 0 \end{smallmatrix}\right)$.

(*d*) Dado $u = \alpha + \beta i + \gamma j + \delta k \in (a, b)_\Bbbk$, se define $u^* = \alpha - \beta i - \gamma j - \delta k$. Probar que $u \mapsto u^*$ es una involución, y que $(uv)^* = v^* u^*$.

(*e*) Se define $N : u \in (a, b)_\Bbbk \mapsto uu^* \in \Bbbk$. Probar que N está bien definida, es multiplicativa, y que u es una unidad si y solo si $N(u) \neq 0$.

(*f*) Mostrar que $(a, b)_\Bbbk$ es un álgebra de división si y solo si la ecuación $ax^2 + by^2 = 1$ no tiene solución en $\Bbbk$. En particular, $(-1, -1)_\mathbb{R}$ es un álgebra de división pero $(-1, -1)_\mathbb{C}$ no.

44. *Álgebras de división reales.* El objetivo de este ejercicio es probar el siguiente teorema de Ferdinand Georg Frobenius (1849–1917, Prusia):

> **Teorema.** *Si D es una $\mathbb{R}$-álgebra de división de dimensión finita, entonces D es isomorfa a $\mathbb{R}$, a $\mathbb{C}$ o a $\mathbb{H}$.*

La conclusión del teorema vale más generalmente (y con exactamente la misma demostración) para una $\mathbb{R}$-álgebra de división arbitraria si suponemos que es *algebraica* sobre $\mathbb{R}$: esto es, si para todo elemento $d \in D$ existe $p \in \mathbb{R}[X]$ tal que $p(d) = 0$.

(*a*) Si $\dim_\mathbb{R} D = 1$ no hay nada que hacer, así que suponga que $\dim_\mathbb{R} D > 1$. Sea $a \in D \setminus \mathbb{R}$. Muestre que $\mathbb{R}[a] \subset D$ es un cuerpo y que debe ser isomorfo a $\mathbb{C}$. Concluya que existe $i \in D \setminus \mathbb{R}$ tal que $i^2 = -1$. Identifiquemos a $\mathbb{C}$ con $\mathbb{R}[i]$.

(*b*) Definamos subespacios

$$D^+ = \{d \in D : di = id\}$$

y

$$D^- = \{d \in D : di = -id\}$$

de D. Muestre que $D = D^+ \oplus D^-$.

(*c*) Claramente $\mathbb{C} \subset D^+$. Si $d \in D^+ \setminus \mathbb{C}$, muestre que $\mathbb{C}[d]$ es un cuerpo que contiene a $\mathbb{C}$. Concluya que $D^+ = \mathbb{C}$.

(*d*) Si $D^- = 0$, entonces $D = \mathbb{C}$. Supongamos desde ahora que $D^- \neq 0$. Sea $z \in D^-$ y considere la aplicación $s : d \in D^- \mapsto dz \in D^+$. Muestre que es $\mathbb{C}$-lineal e inyectiva, así que debe ser $\dim_{\mathbb{C}} D^- = 1$. Concluya que $\dim_{\mathbb{R}} D = 4$.

(*e*) Muestre que existe $j \in D^-$ tal que $j^2 = -1$. Concluya que $D \cong \mathbb{H}$.

45. *Álgebras de division finitas.* El objetivo de este ejercicio es mostrar el siguiente teorema de Joseph Henry Maclagen Wedderburn (1882–1948, Escocia):

Teorema. *Un anillo de división finito es un cuerpo.*

(*a*) Sea $\mu : \mathbb{N} \to \mathbb{Z}$ la función de Möbius, de manera que si $n = p_1^{r_1} \cdots p_k^{r_k}$ es la descomposición de n como producto de potencias de primos distintos,

$$\mu(n) = \begin{cases} 1, & \text{si } n = 1; \\ (-1)^k, & \text{si } r_1 = \cdots = r_k = 1; \\ 0, & \text{si } r_i > 1 \text{ para algún } i. \end{cases}$$

Muestre que si $n, m \in \mathbb{N}$ son coprimos, entonces $\mu(nm) = \mu(n)\mu(m)$.

(*b*) Sea $M : n \in \mathbb{N} \mapsto \sum_{d|n} \mu(d) \in \mathbb{Z}$. Muestre que si $n, m \in \mathbb{N}$ son coprimos, entonces $M(nm) = M(n)M(m)$. Muestre además que $M(1) = 1$ y que si p es primo y $r \in \mathbb{N}$, entonces $M(p^r) = 0$.

Concluya que vale la siguiente *identidad de Möbius*:

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{si } n = 1; \\ 0, & \text{en caso contrario.} \end{cases}$$

(*c*) Sea $n \in \mathbb{N}$. Sea $G_n = \{w \in \mathbb{C} : w^n = 1\}$ el conjunto de las raíces n-ésimas de la unidad y sea $G_n^* \subset G_n$ el subconjunto de G_n formado por aquellas que son primitivas. Recordemos que $X^n - 1 = \prod_{\omega \in G_n} (X - \omega)$. Definimos el polinomio $\Phi_n \in \mathbb{C}[X]$ como

$$\Phi_n = \prod_{\omega \in G_n^*} (X - \omega).$$

Muestre que $X^n - 1 = \prod_{d|n} \Phi_d(X)$ y, usando eso, que

$$\Phi_n = \prod_{d|n} (X^d - 1)^{\mu(d)}.$$

Concluya que $\Phi_n \in \mathbb{Z}[X]$.

(*d*) Muestre que si $q \in \mathbb{Z} \setminus \{1\}$ y $n, r \in \mathbb{N}$ son tales que $r \mid n$, entonces

$$\Phi_n(q) \;\Big|\; \frac{q^n - 1}{q^r - 1}.$$

(*e*) Sea D un anillo de división finito y sea F su centro. Muestre que F es un cuerpo y que D es un F-espacio vectorial de dimensión finita. Sean $q = |F|$ y $n = \dim_F D$, de manera que $|D| = q^n$ y $|D^\times| = q^n - 1$.

Supongamos que D no es conmutativo, con lo cual $n > 1$.

(*f*) Sea $a \in D$ y sea

$$\mathsf{C}(a) = \{d \in D : da = ad\}.$$

Muestre que $\mathsf{C}(a)$ es un subanillo de D que es de división y que contiene a F. Otra vez, se trata de un F-espacio vectorial. Sea $r(a) = \dim_F \mathsf{C}(A)$, con lo cual $|\mathsf{C}(a)| = q^{r(a)}$ y $|\mathsf{C}(a)^\times| = q^{r(a)} - 1$. Como $\mathsf{C}(a)^\times$ es un subgrupo de $D^\times$, se deduce que $q^{r(a)} - 1 \mid q^n - 1$. Concluya que $r(a) \mid n$.

(*g*) Muestre que si $a \in D^\times$ entonces la clase de conjugación de a en el grupo $D^\times$ tiene cardinal

$$|\mathsf{cl}(a)| = \frac{q^n - 1}{q^{r(a)} - 1}.$$

(*h*) Sean $a_1, \ldots, a_l$ representantes de las clases de conjugación no triviales de $D^\times$, y sea $r_l = r(a_l)$. Pruebe que la ecuación de clases para $D^\times$ es:

$$q^n - 1 = q - 1 + \sum_{i=1}^{l} \frac{q^n - 1}{q^{r_l} - 1},$$

y que $\Phi_n(q) \mid (q-1)$.

(*i*) En particular,

$$q - 1 \geq |\Phi_n(q)| = \prod_{\omega \in G_n^*} |q - \omega|.$$

Muestre que esto es imposible.