Teoría de álgebras
Segundo cuatrimestre — 2010

Práctica 1: Álgebras

Construcciones

1. *Álgebra opuesta.*

(a) Sea A una k-álgebra. Sea $*: A \times A \to A$ la operación definida por

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

Muestre que $(A, +, *)$ es una k-álgebra. Se trata del *álgebra opuesta de A*, que escribimos habitualmente A^{op}.

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

2. Si A y B son k-álgebras, el *producto cartesiano* $A \times B$ es el álgebra que como k-espacio vectorial coincide con la suma directa $A \oplus B$ y en la que el producto está dado por

$$(a, b) \cdot (a', b') = (aa', bb')$$

cualesquiera sean a, $a' \in A$ y b, $b' \in B$.

3. Si A es una k-álgebra, el *centro* de A es

$$Z(A) = \{z \in A : \text{para todo } a \in A \text{ es } az = za\}.$$

Muestre que $Z(A)$ es una subálgebra de A.

Álgebras de matrices

4. Sea A una k-álgebra y sea $n \in \mathbb{N}$. El conjunto de matrices $M_n(A)$ con coeficientes en A es una k-álgebra con respecto a las operaciones usuales de suma y producto de matrices. Si $n > 1$, entonces $M_n(A)$ no es conmutativa.

5. Si A es una k-álgebra y $n \in \mathbb{N}$, determine el centro de $M_n(A)$.

6. Determine todos los ideales biláteros de $M_n(k)$.

7. Si A es una k-álgebra y m, $n \in \mathbb{N}$, entonces hay un isomorfismo de k-álgebras $M_n(M_m(A)) \cong M_{nm}(A)$.

8. Sea A una k-álgebra y sea $M_\infty(A)$ el conjunto de todas las "matrices infinitas" $(a_{ij})_{i,j\in\mathbb{N}}$ con coeficientes en A.

Decimos que una matriz $a = (a_{ij})_{i,j\in\mathbb{N}} \in M_\infty(A)$ tiene *filas finitas* si para cada $n \in \mathbb{N}$, existe $k \in \mathbb{N}$ tal que $a_{n,m} = 0$ si $m > k$; de manera similar, decimos que a tiene *columnas finitas* si para cada $m \in \mathbb{N}$, existe $k \in \mathbb{N}$ tal que $a_{n,m} = 0$ si $n > k$.

Sean $M_\infty^{\mathrm{f}}(A)$ y $M_\infty^{\mathrm{c}}(A)$ los subconjuntos de $M_\infty(A)$ de las matrices con filas finitas y con columnas finitas, respectivamente, y sea

$$M_\infty^{\mathrm{fc}}(A) = M_\infty^{\mathrm{f}}(A) \cap M_\infty^{\mathrm{c}}(A).$$

Con el producto “usual” de matrices, $M_\infty^{\mathrm{f}}(A)$, $M_\infty^{\mathrm{c}}(A)$ y $M_\infty^{\mathrm{fc}}(A)$ son k-álgebras.

Álgebras de grupo

9. Sea G un grupo y sea A una k-álgebra. Sea AG el A-módulo izquierdo libre generado por el conjunto G, de manera que G es una base de AG. Muestre que existe exactamente una estructura de k-álgebra en AG para la cual se tiene que

$$ag \cdot bh = (ab)(gh)$$

cualesquiera sean a, $b \in A$ y g, $h \in G$. Llamamos a AG el *álgebra de grupo* de G con coeficientes en A.

10. Sean C_2 y C_3 grupos cíclicos de 2 y 3 elementos, respectivamente. Muestre que hay isomorfismos $\mathbb{C}C_2 \cong \mathbb{C} \times \mathbb{C}$ y $\mathbb{C}C_3 \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C}$ de $\mathbb{C}$-álgebras, y $\mathbb{R}C_2 \cong \mathbb{R} \times \mathbb{R}$ de $\mathbb{R}$-álgebras. Describa además la $\mathbb{R}$-álgebra $\mathbb{R}C_3$.

11. Si G es un grupo y k un cuerpo, describa el centro de la k-álgebra kG.

12. Si G es solamente un *monoide*, esto es, está dotado de un producto $G \times G \to G$ que es asociativo y que posee un elemento neutro, la construcción del ejercicio **9** también produce un álgebra, que en ese caso llamamos el *álgebra de monoide* de G.

13. Sea k un cuerpo.

(a) Si $G = (\mathbb{N}_0, +)$ es el monoide del conjunto de los números enteros no negativos con la operación dada por la suma, existe un isomorfismo de k-álgebras $kG \cong k[X]$.

(b) Si G es un grupo cíclico infinito, hay un isomorfismo $kG \cong k[X^{\pm 1}]$. Aquí $k[X^{\pm 1}]$ es la k-álgebra de los *polinomios de Laurent* con coeficientes en k.

Productos cruzados

14. Sea A una k-álgebra y sea G un grupo. Sea $\mathrm{Aut}_k(A)$ el grupo de automorfismos de A en tanto k-álgebra y supongamos que $\phi : G \to \mathrm{Aut}_k(A)$ es un homomorfismo de grupos. Sea $A * G$ el A-módulo a izquierda con base en el conjunto G, de manera que un elemento de $A * G$ es una combinación lineal formal finita $\sum_{g\in G} a_g G$ de elementos de G con coeficientes en A.

Es claro que $A * G$ es un k-espacio vectorial de manera evidente. Muestre que $A * G$ posee una única estructura de k-álgebra para la cual se tiene que

$$ag \cdot bh = \underbrace{a\phi(g)(b)}_{\in A}\underbrace{gh}_{\in G}$$

para cada a, $b \in A$ y cada g, $h \in G$. Llamamos al álgebra $A * G$ el *producto cruzado* de A por G (con respecto a la acción ϕ)

15. Si el morfismo $\phi : G \to \mathsf{Aut}_k(A)$ es trivial, entonces $A * G$ es isomorfa, en tanto k-álgebra, al álgebra de grupo AG.

16. Determine el centro de $A * G$.

17. Sea C_2 un grupo cíclico de órden 2 y sea $\sigma \in C_2$ el elemento no trivial. Consideremos a $\mathbb{C}$ como una $\mathbb{R}$-álgebra y sea $\phi : C_2 \to \mathsf{Aut}_{\mathbb{R}}(\mathbb{C})$ el morfismo tal que $\phi(\sigma)$ es la conjugación compleja. Muestre que $\mathbb{C} * C_2 \cong \mathsf{End}_{\mathbb{R}}(\mathbb{C})$ como $\mathbb{R}$-álgebras.

Sugerencia. Muestre que hay un isomorfismo $f : \mathbb{C} * C_2 \to \mathsf{End}_R R(\mathbb{C})$ tal que para cada $z \in \mathbb{C} \subseteq \mathbb{C} * C_2$ la aplicación $f(z) : \mathbb{C} \to \mathbb{C}$ es la multiplicación por z, y $f(\sigma) : \mathbb{C} \to \mathbb{C}$ es una conjugación.

Álgebras de convolución

18. *Álgebras de funciones.* Sea A una k-álgebra y sea X un conjunto no vacío. Sea X^A el k-espacio vectorial de todas las funciones $X \to A$ y consideremos el producto $\cdot : A \times A \to A$ dado por

$$(f \cdot g)(x) = f(x)g(x), \qquad \forall x \in X$$

para cada $f, g \in A^X$. Muestre que X^A es una k-álgebra.

19. *Álgebras de series formales.* Sea A una k-álgebra y sea S el conjunto de todas las sucesiones $(a_n)_{n\geq 0}$ de elementos de A. El conjunto S es de manera natural un k-espacio vectorial y podemos definir un producto $\cdot : S \times S \to S$ de manera que para cada $a = (a_n)_{n\geq 0}$, $b = (b_n)_{n\geq 0} \in S$ el producto $c = a \cdot b$ es la sucesión $c = (c_n)_{n\geq 0}$ con

$$c_n = \sum_{\substack{k,l\geq 0\\ k+l=n}} a_k b_l.$$

Muestre que S es una k-álgebra.

Si introducimos una variable X, podemos representar cada sucesión $a = (a_n)_{n\geq 0}$ por una serie formal

$$\sum_{n\geq 0} a_n X^n.$$

Usando esta notación, las definiciones de la suma y el producto de S imitan formalmente a las correspondientes operaciones con las series. Esto hace que llamemos a S el *álgebra de series formales de potencias con coeficientes en A*. La notación usual para este álgebra es $A[[X]]$.

20. *Series de Dirichlet.* Sea A una k-álgebra y sea S el conjunto de todas las sucesiones $a = (a_n)_{n\geq 1}$ de elementos de A. El conjunto S es de manera evidente un k-espacio vectorial. Definimos un producto $\cdot : S \times S \to S$ poniendo, para cada $a = (a_n)_{n\geq 0}$, $b = (b_n)_{n\geq 0} \in S$ el producto $c = a \cdot b$ es la sucesión $c = (c_n)_{n\geq 0}$ con

$$c_n = \sum_{\substack{d\in\mathbb{N}\\ d|n}} a_d b_{n/d}.$$

Muestre que S es una k-álgebra.

Si s es una variable, a un elemento $(a_n)_{n\geq 1} \in S$ podemos asignarle la expresion formal

$$\sum_{n\in\mathbb{N}} \frac{a_n}{n^s}.$$

Las operaciones de S se corresponden entonces con las operaciones evidentes de estas series.

21. Sea M un monoide y supongamos que M es *localmente finito*, de manera que para cada $m \in M$ el conjunto $\{(a,b) \in M \times M : ab = m\}$ es finito.

Sea A una k-álgebra y sea $A[M]$ el conjunto de todas las funciones $M \to A$, con su estructura usual de k-espacio vectorial. Definimos un producto $\star : M \times M \to M$ de manera que

$$(f \star g)(m) = \sum_{\substack{a,b\in M\\ ab=m}} f(a)g(b)$$

cada vez que f, $g \in A[M]$ y $m \in M$; notemos que esta expresión tiene sentido precisamente porque M es localmente finito.

(a) Muestre que $A[M]$ es una k-álgebra, a la que llamamos el *álgebra de convolución* de M con valores en A.

(b) Muestre que las álgebras de series formales como en **19** y las álgebras de series de Dirichlet del ejercicio **20** pueden obtenerse como álgebras de convolución de monoides apropiados.

Álgebras de cuaterniones

22. Sea k un cuerpo y sea $\mathbb{H} = k^4$. Sean 1, i, j y k los vectores de la base canónica de $\mathbb{H}$. Mostrar que existe exactamente un producto asociativo k-bilineal $\cdot : \mathbb{H} \times \mathbb{H} \to \mathbb{H}$ tal que 1 es el elemento unidad y

$$\begin{aligned} &i^2 = j^2 = k^2 = 1, \\ &ij = -ji = k, \qquad jk = -kj = i, \qquad ki = -ik = j. \end{aligned}$$

Si queremos poner en evidencia el cuerpo k, escribimos $\mathbb{H}(k)$.

(a) Muestre que con este producto $\mathbb{H}$ es una k-álgebra.

(b) Muestre que $\mathbb{H}(k)$ es conmutativa sii k tiene característica 2.

(c) Determine el centro de $\mathbb{H}$.

(d) Si $u = \alpha 1 + \beta i + \gamma j + \delta k$, sea $\bar{u} = \alpha 1 - \beta i - \gamma j - \delta k$. Muestre que esto define un anti-automorfismo de k-álgebras $\iota : u \in \mathbb{H} \mapsto \bar{u} \in \mathbb{H}$; esto es, muestre que ι es un isomorfismo de k-espacios vectoriales tal que

$$\overline{uv} = \bar{v}\,\bar{u}.$$

(e) Muestre que existe una función $N : \mathbb{H} \to k$ tal que

$$u\bar{u} = N(u)1, \qquad \forall u \in \mathbb{H}.$$

Además, si $u, v \in \mathbb{H}$, entonces $N(uv) = N(u)N(v)$.

(f) Muestre que si $u \in \mathbb{H}$ es tal que $N(u) \neq 0$, entonces u es inversible en $\mathbb{H}$.

(g) Muestre que $\mathbb{H}(\mathbb{R})$ es un álgebra de división pero que $\mathbb{H}(\mathbb{C})$ no lo es.

Álgebras de caminos

23. (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, tenemos un carcaj si ponemos $Q = (Q_0, Q_1, s, t)$ con vértices $Q_0 = \{1, 2, 3, 4\}$, flechas $Q_1 = \{\alpha, \beta, \gamma, \delta, \eta, \rho\}$ y s y t están dados 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:

$$\begin{tikzcd}
1 \arrow[r, "\alpha"] & 2 \arrow[r, shift left, "\beta"] \arrow[r, shift right, "\gamma"'] \arrow[d, "\delta"'] & 3 \arrow[ll, bend right, "\rho"'] \arrow[loop right, "\eta"] \\
& 4 &
\end{tikzcd}$$

Fijemos un carcaj Q. Si $x, y \in Q_0$, un *camino de x a y en Q* es una secuencia finita $\gamma = (x; \alpha_1, \ldots, \alpha_n; y)$ de flechas de Q tal que $s(\alpha_1) = x$, $t(\alpha_n) = y$ y para cada $i \in \{1, \ldots, n-1\}$ se tiene que $t(\alpha_i) = s(\alpha_{i+1})$. El número n es la *longitud* de γ. 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 k un cuerpo y sea kQ el espacio vectorial que tiene a $P(Q)$ como base. Un elemento $u \in kQ$ es una combinación lineal finita de caminos de Q con coeficientes en k:

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

Muestre que hay exactamente una forma de definir un producto asociativo

$$\cdot : kQ \times kQ \to kQ$$

tal que para cada par de caminos $\gamma = (x; \alpha_1, \ldots, \alpha_n; y)$ y $\eta = (z; \beta_1, \ldots, \beta_m; w)$ en Q, es

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

Mostrar que, con este producto, kQ es una k-álgebra. ¿Cuál es la unidad de esta álgebra? Llamamos a kQ la *k-álgebra de caminos de Q*.

(b) Si Q tiene un solo vértice y ninguna flecha, entonces $kQ = k$

(c) Si Q tiene un solo vertice y una única flecha, entonces kQ es isomorfo a $k[X]$, el anillo de polinomios en una variable con coeficientes en k.

$$Q: \qquad \bullet \circlearrowleft$$

(d) *k-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 kQ. Describa una base de $L(X)$ y su multiplicación

(e) ¿Cuándo es kQ un dominio de integridad? ¿Cuándo tiene dimensión finita? ¿Cuándo es conmutativa?

(f) Describa el centro de kQ.

Dos ejemplos de dimensión infinita

24. *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

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

y 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) A es una $\mathbb{C}$-álgebra de dimensión infinita.

(b) En A es $pq - qp = 1$.

(c) El conjunto $\{p^i q^j : i, j \in \mathbb{N}_0\}$ es una base de A como $\mathbb{C}$-espacio vectorial.

(d) Describa el centro de A.

(e) Muestre que A no posee divisores de cero.

(f) Describa el conjunto de unidades de A.

25. *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

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

y

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

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

(a) En A_q vale que $yx = qxy$.

(b) El conjunto $\{x^i y^j : i, j \in \mathbb{N}_0\}$ es una base de A_q.

(c) Se tiene que $\mathsf{Z}(A_q) = \mathbb{C}$.

(d) Muestre que no hay en A_q divisores de cero.

(e) Describa el conjunto de unidades de A_q.

†(f) Para cada $n \in \mathbb{N}$ definimos

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

Ponemos, además, $(0)_q! = 1$ y si $n \in \mathbb{N}$,

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

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

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

Muestre que:

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

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

(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

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

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

Álgebras de Boole

26. Si X un conjunto y escribimos $\mathscr{P}(X)$ al conjunto de partes de X y $\triangle$ a la operación de diferencia simétrica, entonces $(\mathscr{P}(X), \triangle, \cap)$ es un anillo.

27. Un anillo A es *booleano* si todos sus elementos son idempotentes.

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

(b) Un anillo booleano es conmutativo.

28. Si A es un anillo booleano, existe exactamente una forma de hacer de A una $\mathbb{Z}_2$-álgebra.

Dos teoremas clásicos

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

> **Teorema.** *Sea D una $\mathbb{R}$-álgebra de división tal que $\dim_{\mathbb{R}} D < \infty$. 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 $\mathbb{C}$. En particular, 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 $s : d \in D^- \mapsto dx \in D^+$. 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 $D \cong \mathbb{H}$.

30. Describa todas las $\mathbb{Q}$-álgebras de división de dimensión 2.

†**31.** *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,
$$\mu(n) = \begin{cases} 1, & \text{si } n = 1; \\ (-1)^k, & \text{si } p_1 = \cdots = p_k = 1; \\ 0, & \text{si } r_i > 1 \text{ para algún } i. \end{cases}$$
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 $\Omega_n = \{w \in \mathbb{C} : w^n = 1\}$ el conjunto de las raíces n-ésimas de la unidad y sea $\Omega_n^* \subset \Omega_n$ el subconjunto de Ω_n formado por aquellas que son primitivas. Recordemos que $X^n - 1 = \prod_{\omega \in \Omega_n}(X - \omega)$. Definimos un polinomio $\Phi_n \in \mathbb{C}[X]$ poniendo

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

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. Debe ser entonces $n > 1$.

(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 $r(a) = \dim_F \mathsf{C}(A)$; es entonces $|\mathsf{C}(a)| = q^{r(a)}$ y $|\mathsf{C}(a)^\times| = q^{r(a)} - 1$. Como $\mathsf{C}(a)^\times$ es un subgrupo de $D^\times$, debe ser $q^{r(a)} - 1 \mid q^n - 1$. Concluya que $r(a) \mid n$.

(g) Si $a \in D^\times$, entonces la clase $\mathsf{cl}(a)$ de conjugación de a en el grupo $D^\times$ tiene cardinal

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

(h) Sean $a_1, \dots, a_l$ representantes de las clases de conjugación no triviales de $D^\times$. Entonces la ecuación de clases para $D^\times$ es:

$$q^n - 1 = q - 1 + \sum_{i=1}^{l} \frac{q^n - 1}{q^{r(a)} - 1}.$$

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

(i) En particular,

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

Muestre que esto es imposible.

32. Si k es un cuerpo algebraicamente cerrado, entonces no existen k-álgebras de dimensión finita que no tengan divisores de cero.

33. Sea k un cuerpo algebraicamente cerrado. Describa, a menos de isomorfismo, todas las k-álgebras de dimensión a lo sumo 3.