Álgebra II
Segundo Cuatrimestre — 2008
Ejercicios adicionales de Anillos

1. Definiciones

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

1.2. *(a)* Si A es un anillo en el que cada elemento tiene un inverso a izquierda, entonces A es un anillo de divisiï¿½n.

(b) Sea A un anillo y $a \in A$ un elemento que es 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.

1.3. Sea A un anillo posiblemente sin unidad. Muestre que si A posee una ï¿½nica unidad a izquierda e, entonces A posee una unidad.

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

1.4. Describa, a menos de isomorfismo, todos los anillos con a lo sumo 10 elementos.

1.5. Sea k un cuerpo algebraicamente cerrado. Entonces no existen k-ï¿½lgebras de dimensiï¿½n finita que no tengan divisores de cero.

1.6. Sea k un cuerpo algebraicamente cerrado. Describa, a menos de isomorfismo, todas las k-ï¿½lgebras de dimensiï¿½n a lo sumo 3.

1.7. *Álgebras 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 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 $\gamma = (x; \alpha_1, \dots, \alpha_n; y)$ 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 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 $\cdot : kQ \times kQ \to kQ$ de manera que para cada par de caminos $\gamma = (x; \alpha_1, \dots, \alpha_n; y)$ y $\eta = (z; \beta_1, \dots, \beta_m; w)$ en Q, es

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

Mostrar que, con este producto, 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.

1.8. *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, $y \in \operatorname{End}_{\mathbb{C}}(V)$ 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 $\operatorname{End}_C C(V)$ 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?

†**1.9.** *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 $D \cong \mathbb{H}$.

†**1.10.** *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 Moebius, 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 Moebius*:

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

(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.