Álgebra II
Segundo Cuatrimestre — 2009

Práctica 4: Anillos - ejemplos

1. *Anillo opuesto.*

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

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

Mostrar 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 $A \ncong A^{\mathrm{op}}$.

2. *Anillos de matrices.*

(a) Sea A un anillo y sea $n \in \mathbb{N}$. 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 otra vez A un anillo y 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 $k \in \mathbb{N}$ tal que $f(n, m) = 0$ si $m > k$; de manera similar, decimos que $f \in M_\infty(A)$ tiene *columnas finitas* si para cada $m \in \mathbb{N}$, existe $k \in \mathbb{N}$ tal que $f(n, m) = 0$ si $n > k$.

Sean $M_\infty^f(A)$ y $M_\infty^c(A)$ los subconjuntos de $M_\infty(A)$ de las 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 con el producto "usual" de matrices, $M_\infty^f(A)$, $M_\infty^c(A)$ y $M_\infty^{fc}(A)$ son anillos.

3. *Anillos de funciones.*

(a) Sea A un anillo y X un conjunto no vacío. Sea X^A el conjunto de todas las funciones $X \to A$. Definimos operaciones $+, \cdot : A \times A \to A$ poniendo

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

y

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

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

(b) Sea $n \in \mathbb{N}$, $k \in \mathbb{N}_0$ y sea $C^k(\mathbb{R}^n) \subset (\mathbb{R}^n)^{\mathbb{R}}$ el conjunto de todas las funciones $f : \mathbb{R}^n \to \mathbb{R}$ continuas y derivables k veces. Muestre que se trata de un subanillo.

4. *Anillos de polinomios.* Sea A un anillo y sea

$$S = \{f : \mathbb{N}_0 \to A : \text{existe } X \subset \mathbb{N}_0 \text{ finito tal que } f|_{\mathbb{N}_0 \setminus X} \equiv 0\}.$$

Definimos operaciones $+, \cdot : S \times S \to S$ poniendo, 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 es una variable. Si $f \in S$ y $X \subset \mathbb{N}_0$ es finito y tal que $f|_{\mathbb{N}_0 \setminus X} \equiv 0$, podemos representar a f por la suma finita formal

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

Es fácil ver que usando esta notación las operaciones de S se corresponden con las operaciones usuales de polinomios. Por eso, llamamos a S el *anillo de polinomios con coeficientes en* A y lo notamos $A[X]$.

5. *Anillos de series formales.*

(a) Sea A un anillo y sea $S = \{f : \mathbb{N}_0 \to A\}$ el conjunto de todas las funciones de $\mathbb{N}_0$ a A. Definimos operaciones $+, \cdot : S \times S \to S$ poniendo, para cada $f, g \in S$ y cada $n \in \mathbb{N}_0$,

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

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

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

$$f = \sum_{n \in \mathbb{N}0} f(n)X^n.$$

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

(b) 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.

6. *Series de Dirichlet.* Sea A un anillo y sea $S = \{f : \mathbb{N} \to A\}$ el conjunto de todas las funciones de $\mathbb{N}$ a A. Definimos operaciones $+, \cdot : S \times S \to S$ poniendo, para cada $f, g \in S$ y cada $n \in \mathbb{N}$,

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

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

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

$$f = \sum_{n \in \mathbb{N}} \frac{f(n)}{n^s}.$$

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

7. *Anillo de grupo.*

(a) Sea G un grupo, sea A un anillo y sea $A[G]$ el conjunto de todas las funciones de $f : G \to A$ tales que

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

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

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

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

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

(c) Si $g \in G$, sea $\hat{g} : G \to k$ la función tal que

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

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

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

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

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

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

8. *Álgebra de cuaterniones.* 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

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

(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.

9. *Algebras de caminos.*

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

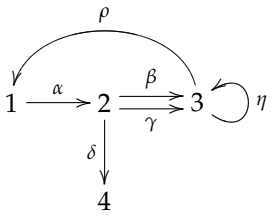
— Q_0 y Q_1 son conjuntos. Los elementos de Q_0 son los *vértices* de Q y los de Q_1 las *flechas*.

— 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 est'an 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:



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 $\cdot : kQ \times kQ \to kQ$ de manera 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 : 

(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.

10. *(a)* Sea 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) Sea 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 todo otro subanillo de A con esta propiedad contiene a $B[X]$.

(c) Tomemos $A = \mathbb{C}$, $B = \mathbb{Z}$. Describa explícitamente $B[\sqrt{2}]$, $B[\sqrt[3]{5}]$ y $B[\omega]$ si ω es una raíz primitiva p-ésima de la unidad y p un número primo. Describa $B[i]$ y $B[\eta]$ si η es una raíz primitiva sexta de la unidad.

11. *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.

12. *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 $0 \le k \le n$, 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?

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

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

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

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

15. *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) Un anillo booleano es conmutativo.

†**16.** *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 $D \cong \mathbb{H}$.

†**17.** *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 $a_1, \ldots, a_l$ 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.