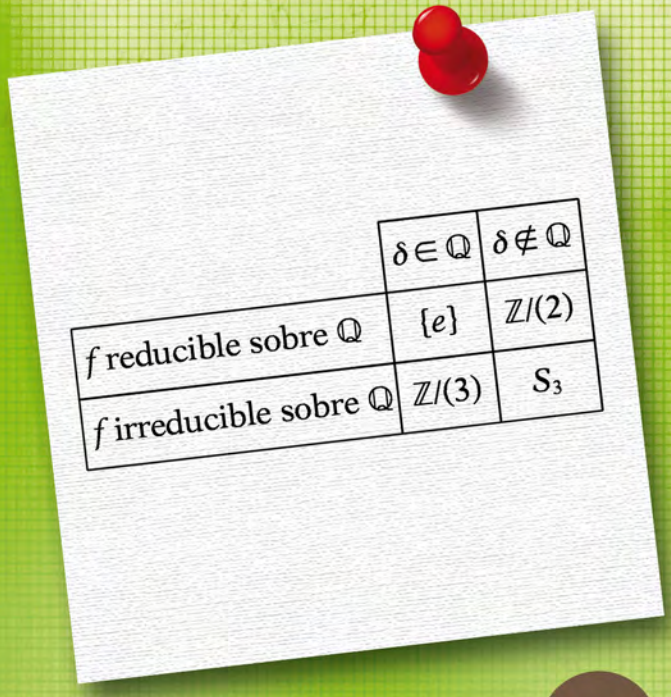
manuales matemáticas π

José Manuel Gamboa
Jesús M. Ruiz

Anillos y Cuerpos

Curso Básico



UNED
sanz y torres

Anillos y Cuerpos

Curso Básico

José Manuel Gamboa
Jesús M. Ruiz

UNED

sanz y torres

ANILLOS Y CUERPOS. CURSO BÁSICO

© EDITORIAL SANZ Y TORRES, S. L.
Vereda de los Barros, 17
Pol. Ind. Ventorro del Cano – 28925 Alcorcón (Madrid)
☏ 902 400 416 – 91 323 71 10
www.sanzytorres.com
libreria@sanzytorres.com
www.editorialsanzytorres.com
editorial@sanzytorres.com

ISBN: 978-84-
Depósito legal: M-

Portada:

Impresión y encuadernación:

Contenido

Prólogo

Los actuales planes de estudio de las Facultades de Matemáticas en las universidades europeas difieren notablemente de los que estaban en vigor hace veinte años, lo que exige una adecuación de los textos empleados en la impartición de los cursos. Una característica fundamental del cambio producido es el notable aumento de la opcionalidad en el diseño del itinerario que el alumno elige para completar sus estudios de Grado. Esto exige un replanteamiento del contenido de las asignaturas; cuanto mayor sea su número menos se podrá profundizar en cada una. Los docentes nos hemos visto así obligados a exponer el contenido de textos clásicos de modo no lineal, eligiendo aquello cuyo conocimiento nos parece esencial para todo el alumnado y reservando la materia que consideramos más avanzada para cursos posteriores o trabajos de fin de grado.

Es por ello que hemos decidido presentar una teoría de *Anillos y Cuerpos* en dos textos: un *Curso básico* en el que exponemos los fundamentos de estas estructuras algebraicas, y un segundo texto de *Temas avanzados*, que se apoya en el anterior y recoge aspectos más elaborados de las mismas. Ambos textos comparten el mismo hilo conductor: las ecuaciones polinómicas, que de hecho constituyeron el objeto de estudio del Álgebra hasta comienzos del siglo XIX.

Aún siendo un curso elemental, el primero de estos libros profundiza en el comportamiento de la divisibilidad y la factorización en distintas clases de anillos y en cómo se traducen estos resultados al tratar algunas ecuaciones diofánticas. Ese es el contenido del primer capítulo, mientras que en el segundo se presentan los polinomios, esencialmente en una variable, y algunos criterios de irreducibilidad, noción crucial en diversas áreas del quehacer matemático.

En el tercer capítulo se inicia el estudio de los cuerpos o, con más precisión, de las extensiones de cuerpos. Buena parte se consagra a introducir los nuevos conceptos apoyándonos en multitud de ejemplos, pero también se demuestran resultados fundamentales pero no triviales, como el teorema de Lüroth y el del elemento primitivo.

El cuarto capítulo se consagra a exponer los fundamentos de la teoría de Galois, considerada como una de las piezas más bellas y perfectas de las ma-

temáticas. Hemos optado por tratarla, únicamente, para extensiones finitas de característica cero, pues creemos que lo que perdemos en generalidad lo ganamos, con creces, en transparencia.

El quinto capítulo incluye dos nociones esencialmente no finitas: la de cierre algebraico y la de número real trascendente.

Las citas internas del texto se hacen por el número del resultado de que se trate, precedido del capítulo en el que esté, si es distinto del que contiene la cita. Aunque el libro es esencialmente autocontenido, en el Capítulo IV se requieren ciertos resultados de grupos finitos que aparecen en el texto

[G] E. Bujalance, J.J. Etayo, J.M. Gamboa: *Teoría elemental de grupos*. Madrid: UNED 2018.

Una de las múltiples aplicaciones de la teoría de Galois, y cuya presentación hemos pospuesto al libro que recoge los temas avanzados, es la irresolubilidad mediante radicales de la inmensa mayoría de las ecuaciones polinómicas de grado 5. Los matemáticos de la escuela italiana del siglo XVI obtuvieron fórmulas para las raíces de estas ecuaciones si el grado de estas es menor o igual que 4, pero se estrellaron al intentar abordar la quíntica. Hubieron de pasar tres siglos hasta que, independientemente, Abel y Galois demostraran que sus antecesores no eran torpes, sino insensatos: las fórmulas que buscaban ni existen ni existirán.

Para disfrutar de éste y de otros resultados notables, como el estudio de algunos casos particulares del denominado último teorema de Fermat, la teoría de la eliminación y sus fascinantes aplicaciones de naturaleza geométrica, o la ley de reciprocidad cuadrática de Gauss, emplazamos al lector más entusiasta a embarcarse en el estudio del texto que recoge los temas avanzados y que constituye el complemento natural de éste.

Madrid, Majadahonda *José Manuel Gamboa, Jesús M. Ruiz*

CAPÍTULO

I

Anillos

Dedicamos este capítulo al estudio de las propiedades generales de los anillos, en especial a las cuestiones de divisibilidad, abstracción de las propiedades conocidas de los números enteros. En la primera sección se introducen las nociones básicas: anillo, ideal, anillo cociente, homomorfismo... En la sección 2 se trata de la divisibilidad y de las propiedades de factorización en dominios de integridad. Finalmente, en la sección 3 y última de este capítulo se estudian las congruencias de números enteros, o si se prefiere decir así, los cocientes del anillo de los números enteros.

Definición 2.14.—Sean $x, y \in A^*$. Se dice que $z \in A$ es:

(1) Un *máximo común divisor* (mcd) de x, y si z divide tanto a x como a y, y es múltiplo de cualquier otro divisor de ambos.

(2) Un *mínimo común múltiplo* (mcm) de x, y si z es múltiplo de x y de y, y divide a cualquier otro múltiplo de ambos.

(2.15) **Observaciones.**—(1) Si z, z' son dos mcd de x, y, entonces $z|z'$ y $z'|z$, luego los dos elementos difieren en una unidad, o si se quiere: $(z) = (z')$ (2.2 y 2.3). En este sentido hay unicidad del mcd y se escribe tanto $z = \text{mcd}\,(x, y)$ como $z' = \text{mcd}\,(x, y)$. La misma observación sirve para el mcm.

(2) Se puede expresar 2.14.1 mediante las operaciones con ideales descritas en 1.19 como sigue:

$$(x) + (y) \subset (z) \subset \bigcap \{I : I \supset (x) + (y) \text{ e } I \text{ es principal}\}.$$

(3) La descripción del mcm mediante ideales es: z es el mcm de x, y si y sólo si $(x) \cap (y) = (z)$.

En efecto, si z es el mcm, $z \in (x)$ y $z \in (y)$, luego se tiene el contenido $(x) \cap (y) \supset (z)$. Pero si $t \in (x) \cap (y)$, entonces t es múltiplo de x y de y, luego $z|t$ y $t \in (z)$. Esto da la igualdad.

Recíprocamente, si $(x) \cap (y) = (z)$, entonces $x|z$, $y|z$, y si t es otro múltiplo común, entonces $t \in (x) \cap (y) = (z)$ y $z|t$.

(4) En general, el mcd puede no existir, como se verá más adelante. Esto está relacionado con las propiedades de los elementos irreducibles de A. Véase 2.20 y 2.25.6.

Lema 2.16.—Sean $x, y \in A^*$, y supongamos que tienen un mcm z. Entonces $t = xy/z \in A$ y es un mcd de x, y.

Demostración.—Por definición de mcm, z divide a xy, luego ciertamente t es un elemento de A bien definido. Por otra parte, $x|z$ e $y|z$, luego $z = ax$, $z = by$, con $a, b \in A$.

Se tiene $zx = byx = btz$, y como A es dominio $x = bt$ y $t|x$. Análogamente, $t|y$. Por otra parte, si u es un divisor común de x e y, será $x = cu$, $y = du$, con $c, d \in A$. Observamos que

$$xy/u = (x/u)y = cy, \quad xy/u = (y/u)x = dx,$$

luego xy/u es múltiplo común de x e y, con lo que z divide a xy/u, y en consecuencia, u divide a $xy/z = t$. Esto prueba que t es múltiplo de cualquier divisor común u de x e y.

El recíproco del lema anterior debe establecerse con una modificación, que conduce al siguiente enunciado.

CAPÍTULO

II

Polinomios

En este capítulo se desarrolla un estudio sistemático de los anillos de polinomios en una y varias variables. En la primera sección se definen y estudian las nociones básicas: evaluación y funciones polinomiales, sustitución, grado, derivadas... En la sección 2 se trata de la división de polinomios. En primer lugar se describe el algoritmo de división cuando el anillo de coeficientes es un dominio de integridad arbitrario. A continuación se caracterizan los anillos de polinomios que son dominios euclídeos, y la sección concluye con la demostración del teorema de Gauss que determina qué anillos de polinomios son dominios de factorización única. La tercera sección del capítulo está dedicada al problema de la factorización efectiva de polinomios cuando el anillo de coeficientes es suficientemente tratable. Se describe el método de factorización de Kronecker, así como diversos criterios para decidir si un polinomio es irreducible o no (criterio de Eisenstein, criterio del módulo finito...).

(1.5.4) *Los ideales* (X_i), $i = 1, \ldots, n$.

Otro ejemplo importante de evaluación es el siguiente: tómese

$$B = A[X_1, \ldots, X_n],$$
$$x_1 = X_1, \ldots, x_{i-1} = X_{i-1},$$
$$x_i = 0, x_{i+1} = X_{i+1}, \ldots, x_n = X_n.$$

Entonces:

$$A[x_1, \ldots, x_n] = A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$$
$$I = X_i B = (X_i) \subset A[X_1, \ldots, X_n].$$

En efecto, lo primero es inmediato, y en cuanto a lo segundo, obsérvese que en $f = \sum a_v X_1^{v_1} \ldots X_n^{v_n}$ al evaluar en los $x_1, \ldots, x_n$ elegidos desaparecen exactamente los sumandos que tienen X_i, y los demás no se alteran. Así, $ev(f) = 0$ equivale a que X_i esté en todos los sumandos, luego a que $X_i | f$.

En consecuencia tenemos el isomorfismo

$$A[X_1, \ldots, X_n]/(X_i) \simeq A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n].$$

(1.6) **Funciones polinomiales.**—Sean A un anillo conmutativo unitario, $X_1, \ldots, X_n$ indeterminadas, y f un polinomio de $A[X_1, \ldots, X_n]$. Sea B un anillo conmutativo y unitario que contenga A como subanillo. Definimos una aplicación asociada a f como sigue:

$$F: B \overset{(n}{\times \cdots \times} B \to B: (x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n).$$

(recuérdese la definición de $f(x_1, \ldots, x_n)$ en 1.5). Una aplicación tal como F, definida a través de un polinomio se llama *función polinomial,* y debe distinguirse siempre del polinomio que la define.

En efecto, veamos que polinomios distintos pueden proporcionar la misma función polinomial. Tómese $A = B = \mathbb{Z}/(p)$, p un primo positivo. Consideramos el anillo de polinomios en una indeterminada, que ahora denotamos T. Entonces los *polinomios*

$$f = T^p, \quad g = T \in \mathbb{Z}/(p)[T]$$

son distintos, pero las funciones polinomiales asociadas

$$F: \mathbb{Z}/(p) \to \mathbb{Z}/(p): x \to x^p, \quad G: \mathbb{Z}/(p) \to \mathbb{Z}/(p): x \to x$$

son idénticas. Ciertamente, hay que ver

$$F(x) = G(x)$$

CAPÍTULO

III

Extensiones de cuerpos

En este capítulo se analiza de modo sistemático la noción de extensión, que aparece de modo natural en el estudio de las raíces de polinomios. La sección primera contiene las nociones y propiedades básicas en las que se profundizará después: grado de una extensión, extensiones finitas, extensiones finitamente generadas, dependencia e independencia algebraica... La sección 2 está dedicada a las extensiones simples algebraicas y las simples transcendentes. Se prueba en ella el teorema de Luröth. En la sección 3, que trata de las extensiones finitamente generadas, se introduce el grado de transcendencia, y se demuestra el teorema del elemento primitivo para cuerpos de característica cero.

$$K[X_1]/I \simeq K[a_1] \subset E.$$

Como E es cuerpo no tiene divisores de cero, luego tampoco los tiene $K[X_1]/I$, e I es un ideal primo $\neq \{0\}$. Como el anillo $K[X_1]$ es un *DIP* (II.2.6) todo ideal primo no nulo, y en particular I, es maximal (I.2.24.4), con lo que $K[X_1]/I$ es cuerpo. En virtud del isomorfismo anterior también lo es $K[a_1]$, y concluimos

$$K[a_1] = K(a_1)$$

(recuérdese el ejemplo 1.12.5).

(5) En $K(T)$, T indeterminada, los elementos $a_1 = T$, $a_2 = T^2$, son algebraicamente dependientes: tómese $f = X_1^2 - X_2$ y queda

$$f(a_1, a_2) = a_1^2 - a_2 = T^2 - T^2 = 0.$$

(1.15) **Existencia de números transcendentes.**—Uno de los problemas más interesantes sobre números es la búsqueda de números reales o complejos que sean *transcendentes sobre* $\mathbb{Q}$. Encontrar ejemplos concretos es sumamente difícil, y algo diremos al respecto en V.2. Paradójicamente, no es difícil dar una prueba no constructiva de que existe una *infinidad no numerable* de ellos. Presentamos aquí esa prueba, debida a Cantor

Sea L el conjunto de todos los números reales algebraicos sobre $\mathbb{Q}$. Para cada $\alpha \in L$ podemos elegir un polinomio no nulo $f_\alpha \in \mathbb{Q}[T]$ de modo que α sea raíz de f_α. Esto proporciona una aplicación

$$\Phi : L \to \mathbb{Q}[T]^* : \alpha \mapsto f_\alpha,$$

y se tiene

$$(*) \qquad L = \bigcup_{f \neq 0} \Phi^{-1}(f).$$

Ahora obsérvese que cada conjunto $\Phi^{-1}(f)$ es finito, pues el número de raíces de f está acotado por su grado (II.2.3). Pero además $\mathbb{Q}[T]$ es numerable (véase la prueba de 1.12.4), con lo que la igualdad (*) describe L como unión numerable de conjuntos finitos. Así, L es numerable.

En fin, $\mathbb{R}$ no es numerable, luego $\mathbb{R} \setminus L$ tampoco puede serlo.

Evidentemente, la misma prueba sirve con $\mathbb{C}$ en lugar de $\mathbb{R}$, y se obtiene el teorema de Cantor:

«El conjunto de números complejos algebraicos sobre $\mathbb{Q}$ es numerable».

CAPÍTULO

IV

Teoría de Galois

Este capítulo trata de los grupos de automorfismos de las extensiones de cuerpos de característica cero. Se estudia principalmente el caso de las extensiones finitas, aunque en la sección 1 se incluya el cálculo del grupo de automorfismos de una extensión simple transcendente. Además de eso, en dicha sección se acota el orden del grupo de automorfismos de una extensión finita mediante el grado de la extensión. En la sección 2 se analizan las extensiones en que esos orden y grado coinciden, o sea, las extensiones de Galois, y se demuestra el teorema fundamental de la teoría: las subextensiones se corresponden biyectivamente con los subgrupos, y las subextensiones de Galois con los subgrupos normales. En la sección 3 se establece la equivalencia de las nociones de extensión de Galois y extensión de descomposición, esencial para decidir la resolubilidad de polinomios mediante radicales. Finalmente se introduce el grupo de Galois de un polinomio y se describe para grado $\leqslant 4$.

	g reducible sobre $\mathbb{Q}$		g irreducible sobre $\mathbb{Q}$	
	$\delta \in \mathbb{Q}$	$\delta \notin \mathbb{Q}$	$\delta \in \mathbb{Q}$	$\delta \notin \mathbb{Q}$
f reducible sobre $\mathbb{Q}(\delta)$	—	$\mathbb{Z}/(4)$	—	—
f irreducible sobre $\mathbb{Q}(\delta)$	$\mathbb{Z}/(2) \times \mathbb{Z}/(2)$	D_4	A_4	S_4

(D_4 representa al grupo diedral de orden 8, A_4 al grupo alternado de orden 12 y S_4 al grupo simétrico de orden 24).

Para construir polinomios $T^4 + bT^2 - cT + d$ cuyos grupos de Galois sean los de la tabla anterior es bueno saber que para este polinomio también tenemos una igualdad mágica:

$$\Delta = \delta^2 = 256d^3 - 128d^2 + 144bc^2d + 16b^2d - 4b^3c^2 - 27c^4.$$

(3.10) **Observación.**—La proposición anterior no trata el caso de los polinomios de grado 4 *reducibles* en $\mathbb{Q}[T]$. La razón es que los subcasos se multiplican y la tabla se complica grandemente, mientras que la naturaleza del problema es muy sencilla. En efecto, sea $f \in \mathbb{Q}[T]$, reducible de grado 4.

Si f tiene alguna raíz racional α, entonces $h = f/(T - \alpha) \in \mathbb{Q}[T]$, y evidentemente $\mathbb{Q}_f = \mathbb{Q}_h$, con lo que los grupos de Galois de f y h coinciden. Como h tiene grado 3, se aplica 3.8 y hemos acabado.

Si f no tiene raíces racionales, entonces $f = h \cdot k$, $h, k \in \mathbb{Q}[T]$ irreducibles de grado 2. Sean α, α' (resp. β, β') las raíces de h (resp. de k). Sabemos que

$$\alpha' \in \mathbb{Q}(\alpha), \quad \beta' \in \mathbb{Q}(\beta),$$

luego $\mathbb{Q}_f = \mathbb{Q}(\alpha, \beta)$ y tenemos la cadena

$$\mathbb{Q}_f = \mathbb{Q}(\alpha)(\beta) \supset \mathbb{Q}(\alpha) \supset \mathbb{Q},$$

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \quad ; \quad [\mathbb{Q}_f : \mathbb{Q}(\alpha)] = 1 \text{ ó } 2 \text{ (según } \beta \in \mathbb{Q}(\alpha) \text{ ó } \beta \notin \mathbb{Q}(\alpha)).$$

Por tanto, orden $G(\mathbb{Q}_f : \mathbb{Q}) = [\mathbb{Q}_f : \mathbb{Q}] = 2$ ó 4. En el primer caso es claro que $G(\mathbb{Q}_f : \mathbb{Q}) \simeq \mathbb{Z}/(2)$. En el segundo es fácil ver que $G(\mathbb{Q}_f : \mathbb{Q}) \simeq \mathbb{Z}/(2) \times \mathbb{Z}/(2)$ (ejercicio).

(3.11) **Ejemplos.**—Para justificar completamente las tablas 3.8 y 3.9 es preciso exhibir ejemplos de todas las posibilidades que aparecen. Haremos eso ahora.

(1) El grupo de Galois de $f = T^3 - T$ es $\{e\}$. En efecto:

$$\Delta = -4(-1)^3 = 4 \text{ y } \delta = 2 \in \mathbb{Q},$$

CAPÍTULO

V

Extensiones infinitas

Este capítulo se dedica a dos cuestiones que, contrariamente a todos los demás temas tratados en el libro, son de carácter esencialmente infinitista: la construcción del cierre algebraico de un cuerpo dado (sección 1) y la transcendencia de ciertos números reales (sección 2). El carácter no finito viene dado en el primer caso por la naturaleza de los argumentos utilizados: lema de Zorn, cadenas infinitas de subextensiones... En cuanto al segundo, radica en el uso que se hace de las nociones de límite y de integral, propias del Análisis más que del Álgebra.

$$f = P(\alpha, E_1) \in E_1[T].$$

Este es un polinomio mónico irreducible. Ahora bien, por ser E algebraicamente cerrado, todo polinomio de $E[T]$ se descompone en producto de factores lineales. Como $E[T]$ es isomorfo a $E_1[T]$ (vía Φ), el anillo $E_1[T]$ tendrá esta misma propiedad, que aplicamos al polinomio anterior f. Pero f es irreducible, luego no tiene divisores propios, y la única posibilidad es que él mismo sea lineal. Como es mónico, necesariamente $f = T - a \in E_1[T]$. Finalmente, $0 = f(\alpha) = \alpha - a$ y así $\alpha = a \in E_1$.

(1.13) **Observaciones.**—Sean K un cuerpo y E su cierre algebraico.

(1) Toda extensión algebraica de K es subextensión de E.

En efecto, sea L/K algebraica. Aplicamos 1.11 con $L' = E$ y obtenemos un homomorfismo ϕ: $L/K \to E/K$. Como se trata de cuerpos ϕ: $L \to \phi(L)$ es isomorfismo, luego $L/K \simeq \phi(L)/K$ y esta última es una subextensión de E/K.

(2) E es subextensión de toda extensión algebraicamente cerrada de K.

Ciertamente, sea L'/K algebraicamente cerrada. Por 1.11 con $L = E$, tenemos ϕ: $E/K \to L'/K$. Como antes $E/K \simeq \phi(E)/K$, y la última es una subextensión de L'/K.

(3) Supóngase que se tiene *a priori* una extensión algebraicamente cerrada L'/K. Entonces el cierre algebraico de K en L' es un cuerpo algebraicamente cerrado (1.8.2) y, por tanto, es el cierre algebraico de K. Sin embargo la dificultad estriba precisamente en disponer de tal extensión L' y a eso se debe el desarrollo de esta sección desde 1.9 hasta el final.

§2. NÚMEROS TRANSCENDENTES

Según sabemos, el cuerpo $\mathbb{Q}_0$ de los números algebraicos es numerable, por lo que existe una infinidad no numerable de números transcendentes sobre $\mathbb{Q}$ (cf. 1.8.3 y III.1.15). Sin embargo, a pesar de esta abundancia, es muy difícil decidir si un número dado es transcendente o no. Aquí lo haremos con detalle para el número e.

(2.1) **Transcendencia del número *e*.**

La demostración que sigue se debe a Hermite (1873). Para desarrollarla se precisan algunas propiedades especiales de la siguiente familia de polinomios. Sea r un entero positivo. Para cada entero primo positivo p consideramos el polinomio

$$h_p = \frac{1}{(p-1)!} T^{p-1}(T-1)^p \dots (T-r)^p \in \mathbb{Q}[T]. \tag{2.1.1}$$

Soluciones de los ejercicios

Ejercicio 1. (*a*) Dados $x, y \in (I\colon J)$, $a \in A$ y $z \in J$ se verifica:

$$(x+y)z = xz + yz \in I \quad ; \quad (ax)z = a(xz) \in I.$$

Esto prueba que $(I\colon J)$ es un ideal de A.

Si $x, y \in \sqrt{I}$ y $a \in A$, existen $n, m > 0$ tales que

$$x^n \in I, \quad y^m \in I.$$

Por tanto, si $n + m = k$,

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

Para probar que $x + y \in \sqrt{I}$ es suficiente comprobar que

$$x^j y^{k-j} \in I, \quad j = 0, \ldots, k.$$

Esto es obvio, pues al ser $j + (k - j) = k = n + m$,

$$\text{o bien} \quad j \geqslant n, \quad \text{y entonces} \quad x^j = x^{j-n} \cdot x^n \in I,$$
$$\text{o bien} \quad k - j \geqslant m, \quad \text{y por ello} \quad y^{k-j} = y^{k-j-m} \cdot y^m \in I.$$

En ambos casos, $x^j y^{k-j} \in I$.

Además, $(ax)^n = a^n x^n \in I$, luego $ax \in \sqrt{I}$, con lo que $\sqrt{I}$ es un ideal.

(*b*) Por hipótesis, existen $n > 0$ tal que $x^n = 0$ y $v = u^{-1} \in A$. Pongamos

$$y = v - v^2 x + v^3 x^2 - \ldots + (-1)^{n-1} v^n x^{n-1}.$$

Entonces

Índice

A

B

C