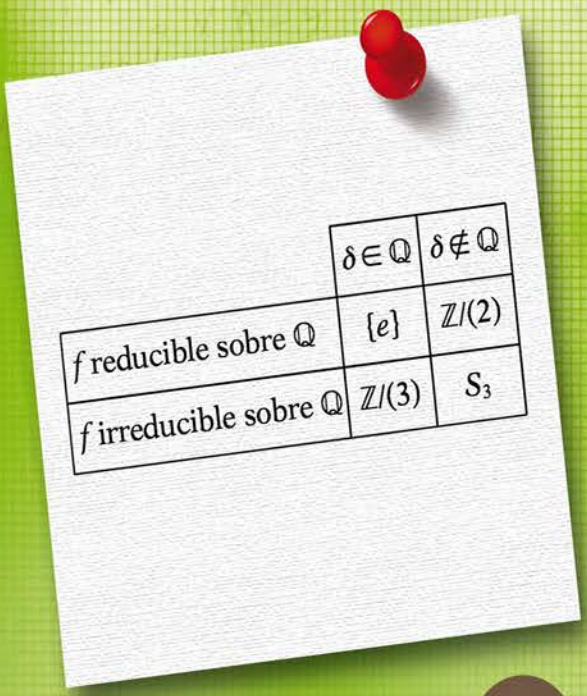
manuales matemáticas

José Manuel Gamboa
Jesús M. Ruiz

Anillos y Cuerpos

Temas Avanzados



UNED
sanz y torres

CONTENIDO

PRÓLOGO

Estos ***Temas avanzados*** de nuestro curso de ***Anillos y cuerpos*** constituyen la continuación natural del ***Curso básico,*** en el que expusimos los fundamentos de estas estructuras algebraicas. De hecho, las numeraciones de los capítulos (del VI al X) y de los ejercicios (del 54 al 109) comienzan donde terminaron las del citado ***Curso básico.***

De nuevo, el estudio de las ecuaciones polinómicas es el hilo conductor. Comenzamos en el capítulo VI con el estudio de las sumas de cuadrados en distintos anillos y cuerpos y con dos casos particulares de la más famosa de las ecuaciones polinómicas: $x^n+y^n=z^n$. En el capítulo VII se presenta la teoría de la eliminación, que es un instrumento muy útil en geometría algebraica, y nosotros emplearemos de modo esencial en el capítulo VIII dedicado a estudiar raíces de polinomios en varios ámbitos. Probamos en particular un resultado que enunciamos sin demostración en el ***Curso básico:*** cómo se determina el grupo de Galois de los polinomios de grado 4 a partir de su discriminante y su resolvente cúbica.

El capítulo IX incluye varias aplicaciones de la Teoría de Galois. La primera es explicar cuáles son los polinomios cuyas raíces se pueden expresar mediante sumas, productos y extracción de raíces de una cantidad finita de elementos del cuerpo al que pertenecen sus coeficientes. Después tratamos los llamados tres problemas clásicos de las construcciones con regla y compás: la trisección del ángulo de amplitud $\pi/3$, la cuadratura del círculo --construir un cuadrado cuya área coincida con la del círculo de radio 1-- y la duplicación del cubo – construir un cubo cuyo volumen duplique el del cubo de arista 1. Probamos que las tres construcciones son imposibles. Como última aplicación determinamos qué polígonos regulares se pueden dibujar con regla y compás.

En el capítulo X también se estudian ecuaciones polinómicas, pero difiere sustancialmente de los anteriores en los objetos y métodos empleados: los cuerpos de coeficientes son finitos.

Las citas internas, incluidas las del ***Curso Básico,*** 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. Además, citamos el texto

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

para aquellos resultados que involucran propiedades elementales de los grupos finitos.

Finalmente al completar con este segundo volumen nuestro texto de Anillos y Cuerpos, queremos agradecer a Victor Fernández-Laguna, compañero de siempre, su colaboración constante y determinante en forma y fondo.

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

Capítulo VI. NÚMEROS

En este capítulo tratamos dos cuestiones importantes de teoría de números, aunque sólo sea en su aspecto más elemental: las sumas de cuadrados de números enteros (teorema de Lagrange), y el teorema último de Fermat para exponentes $\leqslant 4$. Además de su interés en sí mismos, estos resultados son una buena ilustración de la importancia de las nociones de divisibilidad y factorialidad en anillos más generales que el de los números enteros.

§1. SUMAS DE CUADRADOS

Trataremos aquí un problema fácil de formular sobre un anillo de números como $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}$, $\mathbb{R}$ ó $\mathbb{C}$; o un anillo de restos $\mathbb{Z}/(n)$: el de la representación de sus elementos como sumas de cuadrados.

(1.1) Es conocido que todo número complejo $x = a + bi \in \mathbb{C}$ tiene raíz cuadrada, digamos $y = c + di \in \mathbb{C}$, esto es: $x = y^2$. Así, en $\mathbb{C}$ todo elemento es un cuadrado.

(1.2) El cuadrado de un número real es siempre $\geqslant 0$, y, por tanto, así lo es cualquier suma de cuadrados. Además, todo número $\geqslant 0$ (en particular, toda suma de cuadrados) tiene raíz cuadrada real. En consecuencia, en $\mathbb{R}$ todo elemento $\geqslant 0$ es suma de cuadrados, de hecho, es un cuadrado, y recíprocamente.

(1.3) En $\mathbb{Z}[i]$ tenemos la siguiente identidad: sean $x_k = a_k + b_k \cdot i \in \mathbb{Z}[i]$, $k = 1, \ldots, s$:

$$\sum_{k=1}^{s} x_k^2 = \sum_{k=1}^{s} (a_k^2 - b_k^2) + 2i \sum_{k=1}^{s} a_k b_k.$$

Si $x = a + bi \in \mathbb{Z}[i]$ es suma de cuadrados, resulta que las ecuaciones

$$a = \sum_{k=1}^{s} (a_k^2 - b_k^2)$$

(*)

$$b = 2 \sum_{k=1}^{s} a_k b_k$$

tienen solución en $\mathbb{Z}$. En particular, $2|b$, y obtenemos una condición necesaria.

Capítulo VII. ELIMINACIÓN

En este capítulo se presenta la teoría clásica de la eliminación. Para ello es necesario introducir los polinomios simétricos y establecer sus propiedades. Esto se hace en la primera sección: teorema fundamental de los polinomios simétricos, teorema del grado, fórmulas de Newton... Se aplica todo ello en la sección 2 para definir resultante y discriminante, y para probar sus propiedades básicas. Se incluyen también los cálculos explícitos para grados bajos o para polinomios especiales. Al final de esta sección segunda se introduce la noción de multiplicidad.

§1. POLINOMIOS SIMÉTRICOS

Sean A un dominio de integridad, y $X_1, \ldots, X_n$ ($n \geqslant 2$) indeterminadas. Denotaremos por $\mathrm{S} = \mathrm{S}_n$ el grupo simétrico de las permutaciones de $\{1, \ldots, n\}$.

(1.1) Acción de S sobre $A[X_1, \ldots, X_n]$.

Dada $\sigma \in S$, definimos un isomorfismo.

$$\phi_\sigma : A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_n]$$

mediante la sustitución:

$$X_1 = X_{\sigma(1)}, \ldots, X_n = X_{\sigma(n)},$$

es decir:

$$\phi_\sigma(f) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$$

(véase III.1.5.3; que ϕ_σ es isomorfismo es consecuencia de la misma definición de polinomios, puesto que según señalamos en III.1.3.1 el nombre de las indeterminadas es irrelevante).

De esta manera, S actúa sobre $A[X_1, \ldots, X_n]$ ([G] cap. 3) y define un subanillo de invariantes, que denotaremos

$$A[X_1, \ldots, X_n]^S.$$

Con precisión, $A[X_1, \ldots, X_n]^S$ consiste en los polinomios f tales que:

$$f(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$$

para toda permutación σ; en otras palabras, f no varía aunque permutemos arbitrariamente sus variables (ejercicio: compruébese que $A[X_1, \ldots, X_n]^S$ es efectivamente un subanillo).

Capítulo VIII. RAÍCES DE POLINOMIOS

En este capítulo se incluyen los resultados básicos sobre raíces de polinomios con coeficientes reales o complejos. La sección 1 contiene el teorema de d'Alambert-Gauss, y un estudio elemental de las raíces primitivas de la unidad. En la sección 2 se obtienen los teoremas de Sturm y de Budan-Fourier, para la determinación del número de raíces reales de un polinomio con coeficientes reales, contadas sin o con multiplicidad. Finalmente, en la tercera sección, se resuelven por radicales las ecuaciones de grado $\leqslant 4$.

§1. RAÍCES COMPLEJAS

El objetivo principal de esta sección es probar el teorema fundamental del Álgebra:

Proposición 1.1 (d'Alambert-Gauss).—Todo polinomio de grado mayor o igual que 1 con coeficientes complejos tiene alguna raíz compleja (i.e. en $\mathbb{C}$).

La demostración de 1.1 se basará en las construcciones generales sobre polinomios del capítulo III. Sin embargo, es imprescindible utilizar la completitud para el orden de los números reales. Más exactamente la siguiente consecuencia de esa propiedad.

Proposición 1.2 (Bolzano).—Sean $a < b$ números reales y $f\colon [a, b] \to \mathbb{R}$ una función continua tal que $f(a)f(b) < 0$. Entonces existe $c \in [a, b]$ tal que $f(c) = 0$.

Demostración.—Supondremos $f(a) < 0$ (el otro caso es análogo). Sea

$$M = \{t \in [a, b] : f(t) < 0\} \subset \mathbb{R}.$$

Se trata de un conjunto acotado (por a y b) y no vacío; por tanto, por la completitud de $\mathbb{R}$ existe

$$c = \sup M \in [a, b].$$

Afirmamos que $f(c) = 0$.

En efecto, en primer lugar, por la definición de supremo, existe una sucesión de números reales $c_n \in M$, $n \geqslant 1$, tal que

$$c = \lim_{n\to\infty} c_n.$$

Pero $c_n \in M$ significa $f(c_n) < 0$, luego por ser f continua:

$$(*) \qquad f(c) = \lim_{n\to\infty} f(c_n) \leqslant 0.$$

Capítulo IX. APLICACIONES DE LA TEORÍA DE GALOIS

Se deducen en este capítulo varias consecuencias importantes de los resultados obtenidos en el anterior. Tal vez sea el teorema de Abel-Galois (sección 1) la más destacada: las raíces de un polinomio con coeficientes en un cuerpo de característica cero dado se expresan mediante radicales de elementos de dicho cuerpo si y sólo si el grupo de Galois del polinomio es resoluble. En la sección 2 se completa el estudio, ya iniciado en el capítulo V, de los polinomios ciclotómicos, demostrándose su irreducibilidad sobre los números racionales. Por fin en la sección 3 y última, se prueba la irresolubilidad mediante regla y compás de tres problemas clásicos: la cuadratura del círculo, la duplicación del cubo y la trisección del ángulo. Además, se describen los polígonos regulares que se pueden construir con regla y compás.

§1. CÁLCULO DE RAÍCES POR RADICALES (II)

En toda la sección los cuerpos que aparecen tienen característica cero.

Para formular con precisión el problema que nos interesa necesitamos las nociones siguientes:

Definición 1.1.—*a*) Una *torre radical sobre K* es una colección finita de cuerpos

$$K = K_0 \subset K_1 \subset \ldots \subset K_n$$

de modo que K_i/K_{i-1} es la extensión de descomposición de

$$f_i(T) = T^{\ell_i} - a_i \in K_{i-1}[T]$$

para ciertos $\ell_i > 0$, $a_i \in K_{i-1}^*$ $(i = 1, \ldots, n)$.

Esta torre radical es *de Galois* si K_n/K es una extensión de Galois.

b) Se dice que la extensión L/K es *radical* si existe una torre radical sobre K

$$K = K_0 \subset K_1 \subset \ldots \subset K_n$$

tal que $L \subset K_n$.

(1.2) **Observaciones y ejemplos.**—(1) Es inmediato a partir de la definición que toda subextensión de una extensión radical es radical.

(2) También es claro que dada una extensión E/K, un elemento $a \in E$ se escribe utilizando sumas, restas, multiplicaciones, divisiones y extracciones de raíces a partir de elementos de K si y sólo si la extensión $K(a)/K$ es radical.

(3) Tomemos por ejemplo $K = \mathbb{Q}$, $a = \sqrt[3]{2 + \sqrt{2}}$.

Entonces $a^3 = 2 + \sqrt{2} = a_2$, y si $a_1 = 2$, consideramos:

Capítulo X. CUERPOS FINITOS

En este último capítulo se consideran los mismos problemas que en los anteriores, pero variando el contexto. Mientras anteriormente siempre se suponía la característica nula, aquí, por ser cuerpos finitos, la característica es necesariamente positiva. Las diferencias resultantes son notables: toda extensión finita de cuerpos finitos es una extensión de descomposición, y el orden de su grupo de automorfismos coincide con el grado de la extensión. Por otro lado, se estudia la existencia de raíces de una ecuación cuadrática: ley de reciprocidad cuadrática y teorema de Chevalley-Waring.

§1. ESTRUCTURA DE LOS CUERPOS FINITOS

Definición 1.1.—Sea A un anillo *no necesariamente conmutativo*. Diremos que es un *cuerpo* si existe un elemento $1_A \in A$ tal que

$$a \cdot 1_A = 1_A \cdot a = a \quad \text{para cada} \quad a \in A$$

y si para todo $x \in A^*$ existe $x^{-1} \in A^*$, que cumple

$$xx^{-1} = x^{-1}x = 1_A.$$

Nuestro primer objetivo en esta sección será probar que los cuerpos finitos son, necesariamente, conmutativos.

(1.2) **Característica de un cuerpo finito.**—Sea A un cuerpo finito y consideremos la aplicación

$$\phi : \mathbb{Z}^+ \to A : n \mapsto 1_A + \overset{n)}{\ldots} + 1_A,$$

donde $\mathbb{Z}^+$ es el conjunto de los enteros positivos..

Dicha aplicación no es inyectiva, por ser A finito, luego existen m y n distintos tales que $\phi(m) = \phi(n)$. Si $m > n$ resulta que $k = m - n \in \mathbb{Z}^+$ y $\phi(k) = \phi(m) - \phi(n) = 0_A$.

Si p es el menor k cumpliendo esta propiedad, necesariamente es primo.

En efecto, en caso contrario tendríamos

$$p = q \cdot r, \quad 1 < q, \ r < p$$

y también

$$0 = \phi(p) = \phi(q \cdot r) = \phi(q) \cdot \phi(r).$$

El elemento $\phi(q)$ es distinto de cero, pues $q < p$, luego

ÍNDICE

A

B

C

GLOSARIO