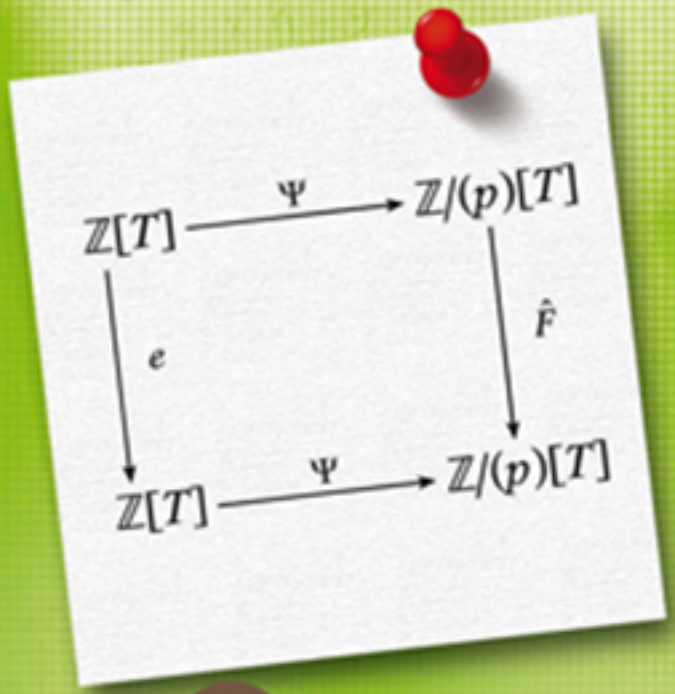
manuales matemáticas π

José Manuel Gamboa
Jesús M. Ruiz

Anillos y Cuerpos

Temas Avanzados



sanz y torres

Anillos y Cuerpos

Temas avanzados

Anillos y Cuerpos

Temas avanzados

José Manuel Gamboa
Jesús M. Ruiz

UNED

sanz y torres

ANILLOS Y CUERPOS. TEMAS AVANZADOS

© 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: 978-84-19947-78-9
ISBN (ebook): 978-84-19947-79-6
Depósito legal: M-19031-2024

Portada:
Javier Rojo Abuín

Impresión y encuadernación:
Copias Centro

En memoria de Víctor Fernández Laguna

Contenido

PRÓLOGO **XI**

CAPÍTULO VI. **NÚMEROS** **1**

§1. Sumas de cuadrados 3
§2. Teorema último de Fermat 20

Ejercicios 31

CAPÍTULO VII. **ELIMINACIÓN** **33**

§1. Polinomios simétricos 35
§2. Resultante y discriminante 50

Ejercicios 65

CAPÍTULO VIII. **RAÍCES DE POLINOMIOS** **67**

§1. Raíces complejas 69
§2. Raíces reales 83
§3. Cálculo de raíces por radicales (I) 106
§4. Resolvente cúbica y grupo de Galois 116

Ejercicios 123

CAPÍTULO IX. **APLICACIONES DE LA TEORÍA DE GALOIS** **127**

§1. Cálculo de raíces por radicales (II) 129
§2. Polinomios ciclotómicos 145
§3. Construcciones con regla y compás 154

Ejercicios 170

CAPÍTULO X. **CUERPOS FINITOS** **173**

§1. Estructura de los cuerpos finitos 175
§2. Ecuaciones polinomiales sobre cuerpos finitos 184
§3. Grupos de automorfismos de cuerpos finitos 195

Ejercicios 199

SOLUCIONES DE LOS EJERCICIOS **201**

ÍNDICE **257**

GLOSARIO **263**

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 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 polinomiales, 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 este segundo volumen de nuestro texto *Anillos y Cuerpos*, queremos recordar a Victor Fernández-Laguna, compañero de siempre, cuya colaboración hizo mejor nuestro trabajo.

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

Julio 2024

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 $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$; 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.

57. Demostrar que para todo entero $m \geqslant 0$, el número $16^m \cdot 31$ no puede escribirse como suma de menos de 16 potencias cuartas, y por tanto $16 \leqslant G(4) \leqslant g(4)$.

58. Demostrar que toda solución entera x, y, z de la ecuación $X^2 + Y^2 = Z^2$ verifica $xyz \equiv 0 \bmod 60$.

59. Obtener las soluciones enteras de la ecuación $X^2 + 4 = Y^3$.

60. ¿Tiene soluciones enteras no triviales la ecuación $X^4 + 4Y^4 = Z^2$?

61. Sea n un entero impar. Probar que si x, y, z son una solución entera no trivial de $X^{2n} + Y^{2n} = Z^{2n}$ con mcd $(n, xyz) = 1$, entonces $n \equiv 1 \bmod 8$. (Obsérvese que esto es trivial si se conoce el teorema último de Fermat, que implica $n = 1$).

CAPÍTULO

VII

Eliminación

En este capítulo se presenta la teoría clásica de 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 $S = S_n$ 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 II.1.5.3; que ϕ_σ es isomorfismo es consecuencia de la misma definición de polinomios, puesto que según señalamos en II.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).

$$C_1 : y^2 + x^2 - y - 3x = 0 \quad ; \quad C_2 : y^2 - 6xy - x^2 + 11y + 7x - 12 = 0.$$

69. ¿Para qué valores del parámetro real a tiene alguna raíz múltiple el polinomio

$$f(T) = T^4 - 4T^3 + (2-a)T^2 + 2T - 2?$$

70. Sean A un dominio y T una indeterminada. Consideramos un polinomio mónico $f \in A[T]$ y ponemos $g(T) = f(T^2) \in A[T]$. Calcular $\Delta(g)$ en función de $\Delta(f)$.

71. Sean $X_1, \ldots, X_n$ indeterminadas, A_n el grupo alternado (o de las permutaciones pares) de $\{1, \ldots, n\}$, y δ el determinante de Vandermonde:

$$\delta = \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_n \\ X_1^2 & X_2^2 & \cdots & X_n^2 \\ \vdots & \vdots & & \vdots \\ X_1^{n-1} & X_2^{n-1} & \cdots & X_n^{n-1} \end{pmatrix} \in \mathbb{Z}[X_1, \ldots, X_n].$$

(a) Probar que si $f \in \mathbb{Z}[X_1, \ldots, X_n]$ y para cada $\sigma \in S_n$ se tiene

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

donde $\varepsilon(\sigma)$ denota la signatura de σ, entonces

$$f = g\delta, \quad \text{con } g \text{ simétrico.}$$

(b) Deducir que si $f \in \mathbb{Z}[X_1, \ldots, X_n]$ y para cada $\sigma \in A_n$ se tiene

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

entonces

$$f = h + g\delta, \quad \text{con } g, h \text{ simétricos}, \quad g, h \in \mathbb{Q}[X_1, \ldots, X_n].$$

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. En la tercera sección se resuelven por radicales las ecuaciones de grado $\leqslant 4$, y en la cuarta de calculan sus grupos de Galois.

§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 II. 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: $[a, b] \to \mathbb{R}$ 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:

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

82. (a) Hallar la relación que deben cumplir los coeficientes del polinomio $g(T) = T^3 + pT^2 + qT + r$ para que una de las raíces coincida con la suma de las otras dos.
(b) Calcular las raíces de $f(T) = 36T^3 - 12T^2 - 5T + 1$

83. (a) Encontrar una condición necesaria y suficiente para que la suma de dos raíces del polinomio $f(T) = T^4 + aT^3 + bT^2 + cT + d$ coincida con la suma de las otras dos.
(b) Calcular las raíces de $f(T) = T^4 - 4T^3 + 5T^2 - 2T - 6$

84. Sean $K \subset \mathbb{R}$ un cuerpo y $f \in K[T]$ un polinomio irreducible de grado 4 que tiene, exactamente, dos raíces reales. Probar que su grupo de Galois (sobre K) es D_4 o S_4.

85. Sea $p > 5$ un número primo. Determinar el grupo de Galois de

$$f(T) = T^4 + pT + p \in \mathbb{Q}[T]$$

86. Calcular el grupo de Galois G_{f_i} de los polinomios $f_i \in \mathbb{Q}[T]$ siguientes

$$f_1(T) = T^4 + 3T^3 - 3T - 2, \quad f_2(T) = T^4 + T^2 - 2T + 1.$$

CAPÍTULO

IX

Aplicaciones de la teoría de Galois

Se deducen en este capítulo varias consecuencias importantes de los resultados obtenidos en el capítulo IV. 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 VIII, 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:

96. Sean m y n dos enteros positivos tales que todo divisor primo de m es divisor de n. Demostrar que

$$\Phi_{mn}(T) = \Phi_n(T^m).$$

97. Calcular Φ_{24}.

98. Calcular Φ_{100}.

99. Sean m y n enteros positivos y M su mínimo común múltiplo. Demostrar que si los polígonos regulares de m y de n lados son constructibles con regla y compás, también lo es el de M lados.

100. Demostrar que si n es un divisor de $2^{32} - 1$, el polígono regular de n lados es constructible con regla y compás.

101. Construir un pentágono regular.

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

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

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 $\chi(m) = \chi(n)$. Si $m > n$ resulta que $k = m - n \in \mathbb{Z}^+$ y $\chi(m) = \chi(k) + \chi(n) = 0_A$, luego $\chi(k) = 0_A$.

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

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

El elemento $\chi(r)$ es distinto de cero, pues $r < p$, luego $q = 0$, lo que es absurdo.

108. Sea K un cuerpo finito y $f(T) = T^3 + aT + b \in K[T]$ un polinomio irreducible. Demostrar que $\Delta(f) = -4a^3 - 27b^2$ tiene raíz cuadrada en K.

109. Sea K un cuerpo con k elementos y T una indeterminada.
(a) Calcular el orden del grupo $G = G(K(T):K)$.
(b) Sea L el cuerpo fijo de G. Demostrar que

$$\eta = \frac{\left(T^{q^2} - T\right)^{q+1}}{\left(T^q - T\right)^{q^2+1}}$$

es un elemento primitivo de L/K.

Soluciones de los ejercicios

Ejercicio 54. Sean a, b y c enteros tales que

$$p = a^2 + b^2 + c^2.$$

Como $2 = 1^2 + 1^2$ es suma de dos cuadrados, p es impar, luego o bien a y b son pares y c es impar, o bien los tres son impares.

En el primer caso:

$$a = 2a',\ \ b = 2b',\ \ c = 2c' - 1;\ \ p = 4(a'^2 + b'^2 + c'^2 - c') + 1,$$

y por ello $p - 1 \in (4)$. Esto implica que p es suma de dos cuadrados, contra la hipótesis. En consecuencia:

$$a = 2a' - 1,\ \ b = 2b' - 1,\ \ c = 2c' - 1,$$
$$p = 4(a'^2 - a' + b'^2 - b' + c'^2 - c') + 3.$$

Pero $x^2 - x = x(x - 1)$ es par para todo entero x y por tanto,

$$p = 8k + 3.$$

Así, el resto de la división de p entre 8 es 3.

Ejercicio 55. Supongamos que podemos escribir

(*) $$8m + 7 = x^2 + y^2 + z^2.$$

Para cada natural t se tiene:

$$t^2 = (2n-1)^2 = 4(n^2 - n) + 1 = 4n(n-1) + 1 \quad \text{si} \quad t \text{ es impar},$$
$$t^2 = (2n)^2 = 4n^2 \quad \text{si} \quad t \text{ es par}.$$

Como los enteros $n - 1$ y n son consecutivos, $n(n - 1)$ es par, luego, en el primer caso:

Índice

A

Abel, teorema de 144
Automorfismo de Frobenius 149

B

Bolzano, teorema de 69
Budan-Fourier, teorema de 99

C

Cálculo por radicales de raíces de polinomios 106, 129
Cálculo por radicales de las raíces de la ecuación cuártica 114
Cálculo por radicales de las raíces de la ecuación cúbica 110
Cardano-Viète, fórmulas de 45
Chevalley-Waring, teorema de 193
Constructibilidad con regla y compás 154
Cota de las raíces reales de un polinomio 92
Cuadrados de cuerpos finitos 184
Cuadratura del círculo 158

D

d'Alambert-Gauss, teorema de 69
Descartes, regla de 102
Diofanto 20

Glosario

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 3

$\mathbb{Z}[i]$ 3

$\mathbb{Z}/(n)$ 3

a^* 8

$M_2(\mathbb{Z}[i])$ 8

$\|\cdot\|$ 8

DFU 16

$g(k)$, $G(k)$ 19

$\mathbb{Z}[\zeta], \zeta = \frac{-1+\sqrt{3i}}{2}$ 24

$S = S_n$ 35

ϕ_σ 35

$A[X_1, ..., X_n]^S$ 35

isomorfismo ρ 36

$G = S_n \times S_m$ 42

B^G 42

isomorfismo η 43

$\Delta \in \mathbb{Z}[U_1, ..., U_n]$ 44

$R \in \mathbb{Z}[U_1, ..., U_n, V_1, ..., V_m]$ 45

$R_{n,m}$; $R^*_{n,m}$ 50

$R(f, g)$ 55

Δ_n, Δ^*_n 56, 57

$\Delta(f)$ 59

A_n 66