ÍNDICE TEMÁTICO

PRÓLOGO A LA TERCERA EDICIÓN 9

INTRODUCCIÓN 11

CAP. I. ANILLOS 15

§1. Generalidades 19
§2. Divisibilidad 35
§3. Congruencias 56

EJERCICIOS 67

CAP. II. NÚMEROS 69

§1. Sumas de cuadrados 73
§2. Teorema último de Fermat 90

EJERCICIOS 101

CAP. III. POLINOMIOS 103

§1. Generalidades 107
§2. División de polinomios 122
§3. Factorización 136

EJERCICIOS 151

CAP. IV. ELIMINACIÓN 153

§1. Polinomios simétricos 157
§2. Resultante y discriminante 172

EJERCICIOS 187

CAP. V. RAÍCES DE POLINOMIOS 189

§1. Raíces complejas 193
§2. Raíces reales 207
§3. Cálculo de raíces por radicales (I) 229

EJERCICIOS 239

CAP. VI. EXTENSIONES DE CUERPOS 243

§1. Generalidades 247
§2. Extensiones simples 257
§3. Extensiones finitamente generadas 269

EJERCICIOS 280

CAP. VII. EXTENSIONES INFINITAS 283

§1. Cierre algebraico 287
§2. Números transcendentes 298

EJERCICIOS 304

CAP. VIII. TEORÍA DE GALOIS 307

§1. Grupos de automorfismos 311
§2. Extensiones de Galois 319
§3. Cuerpos de descomposición 335

EJERCICIOS 355

CAP. IX. APLICACIONES 359

§1. Cálculo de raíces por radicales (II) 363
§2. Polinomios ciclotómicos 379
§3. Construcciones con regla y compás 388

EJERCICIOS 404

CAP. X. CUERPOS FINITOS 407

§1. Estructura de los cuerpos finitos 411
§2. Ecuaciones polinomiales sobre cuerpos finitos 420
§3. Grupos de automorfismos de cuerpos finitos 431

EJERCICIOS 435

APÉNDICE. SOLUCIONES DE LOS EJERCICIOS PROPUESTOS 437

ÍNDICE ANALÍTICO 535

GLOSARIO DE ABREVIATURAS Y SÍMBOLOS 545

§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: $[a, b] \to \mathbb{R}$ 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:

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

En particular, $c < b$, pues $f(b) > 0$, y para n suficientemente grande, digamos $n \geqslant n_0$ se tiene

$$c'_n = c + \frac{1}{n} < b.$$

Ahora bien, $c'_n > c$, luego $c'_n \notin M$, y por tanto, $f(c'_n) \geqslant 0$. De nuevo por ser f continua, y como $\lim_{n\to\infty} c'_n = c$, es:

(**) $$f(c) = \lim_{n\to\infty} f(c'_n) \geqslant 0.$$

De (*) y (**) resulta $f(c) = 0$.

Del anterior teorema resulta inmediatamente una propiedad de sobra conocida de los números reales:

(1.3) Todo número real positivo tiene raíz cuadrada positiva.

En efecto, si $a \in \mathbb{R}$, $a > 0$, consideramos la función continua

$$f : \mathbb{R} \to \mathbb{R} : t \mapsto t^2 - a.$$

Se tiene $f(0) = -a < 0$, y

$$f(a+1) = (a+1)^2 - a = a^2 + a + 1 > 0,$$

luego aplicando 1.2 a $f|[0, a+1]$ encontramos $c > 0$ con $f(c) = 0$, i.e. $c^2 = a$.

La observación anterior permite ya resolver en $\mathbb{C}$ cualquier ecuación de grado 2:

Lema 1.4.—Todo polinomio de segundo grado

$$f(T) = a_0T^2 + a_1T + a_2; \quad a_0 \neq 0,$$

con coeficientes complejos se factoriza en la forma:

$$f(T) = a_0(T - x_1)(T - x_2),$$

con $x_1, x_2 \in \mathbb{C}$.

Demostración.—Basta ver que f tiene alguna raíz $x_1 \in \mathbb{C}$, pues entonces

$$f = (T - x_1)g, \quad g = aT + b \in \mathbb{C}[T], \quad a \neq 0.$$

Necesariamente $a = a_0$ y poniendo $x_2 = -b/a$ queda la factorización del enunciado.

Esto dicho, supongamos que existe $z = x + yi$, $x, y \in \mathbb{R}$, con

$$z^2 = \Delta(f) = a_1^2 - 4a_0a_2 \quad \text{(cf. IV.2.14.3)}.$$

Se comprueba inmediatamente que $f\left(\frac{-a_1+z}{2a_0}\right)=0,$ luego podríamos tomar

(1.4.1) $$x_1=\frac{-a_1+z}{2a_0}.$$

Por supuesto, esto no es otra cosa que el cálculo clásico de las raíces de una ecuación de segundo grado. De lo que se trata es de justificar rigurosamente que tal solución existe siempre para coeficientes complejos.

Así, nuestro problema se reduce a buscar z. Pongamos $\Delta(f) = a + bi$, con $a, b \in \mathbb{R}$. Deberá ser:

$$a+bi=z^2,$$

y si $b = 0$, en virtud de 1.3 existen:

$$z=+\sqrt{a} \qquad \text{si} \quad a\geqslant 0$$
$$z=(+\sqrt{-a})i \quad \text{si} \quad a<0$$

y hemos terminado. Supondremos, pues, $b \neq 0$. Buscamos $x, y \in \mathbb{R}$ tales que

$$a+bi=z^2=(x+yi)^2=x^2-y^2+2xyi,$$

esto es,

$$\begin{cases} a=x^2-y^2 \\ b=2xy \end{cases}.$$

Es claro que si encontramos $x \neq 0$ tal que

(*) $$a=x^2-(b/2x)^2,$$

entonces $z = x + yi = x + (b/2x)i$ resuelve la ecuación. Pero (*) equivale, quitando denominadores, a

(**) $$4x^4-4ax^2-b^2=0,$$

y se comprueba inmediatamente que si

$$x^2=\frac{a+\sqrt{a^2+b^2}}{2},$$

entonces x cumple (**). Pero el numerador de la última fracción es > 0, pues como $b \neq 0$:

$$\sqrt{a^2+b^2} > \sqrt{a^2} = |a| \geqslant -a.$$

En consecuencia, 1.3 proporciona el $x \neq 0$ buscado.

Como se ha visto en la demostración anterior, la resolución de la ecuación compleja se ha podido reducir a una real, y entonces utilizar 1.3 que es una propiedad especial de $\mathbb{R}$, que en $\mathbb{C}$ no tiene significado al involucrar la ordenación de los números reales. Este proceso es, en cierta medida, generalizable.

(1.5) **Conjugación de polinomios.**—La conjugación de números complejos

$$\mathbb{C} \to \mathbb{C} : z = x + yi \mapsto \bar{z} = x - yi$$

es un isomorfismo de cuerpos y, por tanto, se extiende a un isomorfismo del anillo de polinomios:

$$\mathbb{C}[T] \to \mathbb{C}[T] : f = a_0 T^p + \ldots + a_p \mapsto \bar{f} = \bar{a}_0 T^p + \ldots + \bar{a}_p,$$

según se vio en el caso general (III.1.4). Es evidente que

$$\bar{\bar{f}} = f,$$

y también que

(1.5.1) $f \in \mathbb{R}[T]$ si y sólo si $f = \bar{f}$.

De esto se deduce:

(1.5.2) $f \cdot \bar{f} \in \mathbb{R}[T]$ para todo $f \in \mathbb{C}[T]$.

En efecto, se tiene:

$$\overline{f \cdot \bar{f}} = \bar{f} \cdot \bar{\bar{f}} = \bar{f} \cdot f = f \cdot \bar{f}$$

y por 1.5.1, $f \cdot \bar{f} \in \mathbb{R}[T]$. Obsérvese que la primera de las igualdades anteriores es válida por ser $f \mapsto \bar{f}$ *homomorfismo de anillos*.

Respecto de las raíces se tiene la siguiente propiedad, también inmediata, pero que pronto será útil:

(1.5.3) $\bar{z} \in \mathbb{C}$ es raíz de f si y sólo si z es raíz de $\bar{f}$.

En efecto, se tiene:

$$\bar{f}(z) = \bar{a}_0 z^p + \ldots + \bar{a}_p = \bar{a}_0 (\bar{\bar{z}})^p + \ldots + \bar{a}_p = \overline{a_0 (\bar{z})^p + \ldots + a_p} = \overline{f(\bar{z})},$$

lo que implica 1.5.3.

(1.6) *Reducción de 1.1 al caso de polinomios con coeficientes reales.*—Afirmamos que para probar el teorema 1.1 basta demostrar:

(1.6.1) Todo polinomio $g \in \mathbb{R}[T]$ de grado mayor o igual que 1 tiene alguna raíz en $\mathbb{C}$.

En efecto, asumamos 1.6.1 y sea $f \in \mathbb{C}[T]$. Entonces $g = f \cdot \bar{f} \in \mathbb{R}[T]$ tiene alguna raíz $z \in \mathbb{C}$, esto es:

$$0 = g(z) = f(z)\bar{f}(z).$$

Si $f(z) = 0$, z es raíz de f. Si $f(z) \neq 0$, entonces z es raíz de $\bar{f}$ y por 1.5.3 $\bar{z}$ es raíz de f. En todo caso, f tiene alguna raíz en $\mathbb{C}$.

(1.7) Demostración de 1.6.1 *(y, por tanto, del teorema fundamental del Álgebra).*—Pongamos $\partial g = q = 2^n m$, con $n \geqslant 0$ y m impar. Procederemos por inducción sobre n.

Para $n = 0$ es $\partial g = m$ impar, y g tiene incluso raíces reales:

(1.7.1) Todo polinomio con coeficientes reales y de grado impar tiene alguna raíz real.

En efecto, ésta es una consecuencia del teorema de Bolzano. Tendremos

$$g = c_0 T^m + c_1 T^{m-1} + \ldots + c_m, \quad c_0 \neq 0,$$

y elegimos $t_0 \in \mathbb{R}$ con

$$|t_0| > 1 + \left|\frac{c_1}{c_0}\right| + \ldots + \left|\frac{c_m}{c_0}\right|$$

de modo que se verifica

$$(*) \qquad c_0 t_0^m g(t_0) > 0.$$

Efectivamente, en primer lugar

$$\begin{aligned} c_0 t_0^m g(t_0) &= c_0 t_0^m (c_0 t_0^m + c_1 t_0^{m-1} + \ldots + c_m) = \\ &= c_0^2 t_0^{2m-1} \left(t_0 + \frac{c_1}{c_0} + \ldots + \frac{c_m}{c_0 t_0^{m-1}} \right). \end{aligned}$$

Ahora observamos que como $|t_0| > 1$, es $|t_0^k| \geqslant |t_0|$ para $k \geqslant 1$, luego

$$\left|\frac{c_k}{c_0 t_0^{k-1}}\right| = \left|\frac{c_k}{c_0}\right| \cdot \frac{1}{|t_0|^{k-1}} \leqslant \left|\frac{c_k}{c_0}\right| \cdot \left|\frac{1}{t_0}\right| \leqslant \left|\frac{c_k}{c_0}\right|, \text{ con } k \geqslant 2.$$

Así:

$$\left|\frac{c_1}{c_0}+\ldots+\frac{c_m}{c_0 t_0^{m-1}}\right| \leqslant \left|\frac{c_1}{c_0}\right|+\ldots+\left|\frac{c_m}{c_0 t_0^{m-1}}\right| \leqslant \left|\frac{c_1}{c_0}\right|+\ldots+\left|\frac{c_m}{c_0}\right| < |t_0|$$

y en consecuencia,

$$\alpha = t_0+\frac{c_1}{c_0}+\ldots+\frac{c_m}{c_0 t_0^{m-1}} \neq 0 \text{ tiene el signo de } t_0, \quad \text{esto es,} \quad t_0\cdot\alpha > 0.$$

En fin:

$$c_0 t_0^m g(t_0) = c_0^2 t_0^{2m-1}\alpha = c_0^2 t_0^{2(m-1)}(t_0\alpha) > 0.$$

Ahora aplicamos (*) con un $t_0 = \eta > 0$ y resulta

$$c_0\eta^m g(\eta) > 0,$$

y también con $t_0 = -\eta$, pues $|-\eta| = |\eta|$, y resulta

$$c_0(-\eta)^m g(-\eta) > 0.$$

En consecuencia:

$$c_0 g(\eta) > 0 \quad ; \quad c_0 g(-\eta) < 0 \ (m \text{ es impar}),$$

luego

$$g(\eta)g(-\eta) < 0,$$

y aplicando el teorema de Bolzano (1.2) a la función

$$[-\eta, \eta] \to \mathbb{R} : t \mapsto g(t),$$

concluimos que existe $c \in [-\eta, \eta]$ con $g(c) = 0$, esto es, existe alguna raíz real c de g.

Así queda probado el caso $n = 0$. Supondremos pues, $n > 0$, y válida la hipótesis de inducción, que se formula del modo siguiente.

(1.7.2) Si $h \in \mathbb{R}[T]$ tiene grado $\partial h = 2^{n-1}m'$ con m' impar, entonces h tiene alguna raíz compleja.

Veamos, en fin, que g también tiene raíces en $\mathbb{C}$. En primer lugar, elegimos un cuerpo $L \supset \mathbb{C}$ tal que

$$g = c_0(T-x_1)\ldots(T-x_q), \quad c_0, x_1, \ldots, x_q \in L, \quad c_0 \neq 0.$$

(tal cuerpo existe según se probó ya en III.2.13). Como $g \in \mathbb{R}[T]$, necesariamente $c_0 \in \mathbb{R}$.

Sean $X_1, \ldots, X_q$ nuevas indeterminadas, y para cada entero $s \geqslant 1$ se considera el polinomio

$$f_s = \prod_{k<\ell} (T + sX_kX_\ell - X_k - X_\ell) \in \mathbb{Z}[T][X_1, \ldots, X_q].$$

Es claramente simétrico en $X_1, \ldots, X_q$, luego por IV.1.3:

$$f_s(X_1, \ldots, X_q, T) = g_s(u_1, \ldots, u_q, T), \quad g_s \in \mathbb{Z}[T][U_1, \ldots, U_q].$$

siendo $u_1, \ldots, u_q$ las formas simétricas elementales en $X_1, \ldots, X_q$. Resulta que

$$h_s = f_s(x_1, \ldots, x_q, T) = g_s(u_1(x_1, \ldots, x_q), \ldots, u_q(x_1, \ldots, x_q), T)$$

es un polinomio de $\mathbb{R}[T]$, puesto que

$$-u_1(x_1, \ldots, x_q)\cdot c_0, \ldots, (-1)^q u_q(x_1, \ldots, x_q)\cdot c_0$$

son los coeficientes de $g \in \mathbb{R}[T]$ (IV.1.9) y $0 \neq c_0 \in \mathbb{R}$.

Ahora bien:

$$f_s(x_1, \ldots, x_q, T) = \prod_{1 \leq k < \ell \leq q} (T + sx_kx_\ell - x_k - x_\ell)$$

tiene grado $\binom{q}{2} = \dfrac{q(q-1)}{2} = 2^{n-1}(2^n m - 1)m = 2^{n-1}m'$, siendo

$$m' = (2^n m - 1)m$$

impar, ya que $n > 0$. Por tanto, por la hipótesis de inducción con $h = h_s$, alguna de las raíces de h_s, está en $\mathbb{C}$. Pero esas raíces son

$$-(sx_kx_\ell - x_k - x_\ell) \quad , \quad k < \ell,$$

luego existe algún par (k, ℓ) con

$$y_s = sx_kx_\ell - x_k - x_\ell \in \mathbb{C}.$$

Como hay una cantidad finita de pares (k, ℓ) posibles y una cantidad infinita de enteros $s \geqslant 1$, necesariamente existen enteros distintos s, s' a los que corresponde el mismo par (k, ℓ), esto es:

$$y_s = sx_kx_\ell - x_k - x_\ell \in \mathbb{C}$$
$$y_{s'} = s'x_kx_\ell - x_k - x_\ell \in \mathbb{C}.$$

Deducimos

$$x_k + x_\ell = \frac{s'y_s - sy_{s'}}{s - s'} \in \mathbb{C}$$

$$x_k x_\ell = \frac{y_s - y_{s'}}{s - s'} \in \mathbb{C}.$$

Esto significa que x_k y x_ℓ son las raíces del polinomio de segundo grado:

$$T^2 - (x_k + x_\ell)T + x_k x_\ell \in \mathbb{C}[T],$$

luego en virtud del lema 1.4, x_k y $x_\ell \in \mathbb{C}$. Esto es, g tiene al menos las raíces x_k y x_ℓ en $\mathbb{C}$.

La demostración de 1.6.1 ha terminado, y con ella la de 1.1.

Corolario 1.8.—Todo polinomio $f \in \mathbb{C}[T]$ de grado $p \geqslant 1$ factoriza en la forma

$$f = a_0(T - x_1)\ldots(T - x_p)$$

$a_0, x_1, \ldots, x_p \in \mathbb{C}, a_0 \neq 0.$

Demostración.—Por inducción sobre p. Si $p = 1$, es inmediato. Supongámoslo probado para grado $p - 1$ con $p > 1$. Por el teorema 1.1, existe $x_1 \in \mathbb{C}$ con $f(x_1) = 0$, luego por la regla de Ruffini:

$$f = (T - x_1)g, \quad g \in \mathbb{C}[T].$$

Necesariamente $\partial g = p - 1$, luego por hipótesis de inducción

$$g = a_0(T - x_2)\ldots(T - x_p), \quad a_0, x_2, \ldots, x_p \in \mathbb{C},$$

y por tanto,

$$f = a_0(T - x_1)(T - x_2)\ldots(T - x_p).$$

Corolario 1.9.—Sea $f \in \mathbb{R}[T]$ un polinomio de grado $p \geqslant 1$. La factorización de f en $\mathbb{R}[T]$ es de la forma:

$$f = c \prod_{1 \leq k \leq r} (T - z_k) \prod_{1 \leq \ell \leq s} ((T - x_\ell)^2 + y_\ell^2),$$

siendo $c, z_k, x_\ell, y_\ell \in \mathbb{R}$, $c \neq 0$, $y_\ell \neq 0$.

Demostración.—Procederemos, una vez más, por inducción sobre p, siendo el caso $p = 1$ trivial. Sea, pues, $p > 1$. Por el teorema fundamental 1.1 existe $z \in \mathbb{C}$ tal que $f(z) = 0$, y dos casos son posibles:

— Si $z \in \mathbb{R}$, entonces $f = (T - z)g$, siendo g un polinomio *con coeficientes reales,* de grado $p - 1$. Aplicando la hipótesis de inducción a g resulta la factorización deseada.

— Si $z = x + yi \notin \mathbb{R}$, esto es, $y \neq 0$, entonces $\overline{z} = x - yi \neq z$. Además $\overline{z}$ es raíz de $\overline{f} = f$ (1.5.3 y 1.5.1). En consecuencia, $T - z$ y $T - \overline{z}$ dividen a f, y por tanto, su producto también. Ese producto es:

$$h = (T - z)(T - \overline{z}) = T^2 - (z + \overline{z})T + z\overline{z} =$$
$$= T^2 - 2xT + x^2 + y^2 = (T - x)^2 + y^2 \in \mathbb{R}[T],$$

luego

$$f = ((T - x)^2 + y^2)g = hg, \quad g \in \mathbb{C}[T], \partial g = p - 2.$$

Ahora bien, puesto que $f, h \in \mathbb{R}[T]$ se tiene

$$gh = f = \overline{f} = \overline{gh} = \overline{g} \cdot \overline{h} = \overline{g}h,$$

y como $h \neq 0$, es $g = \overline{g}$, luego también $g \in \mathbb{R}[T]$ (1.5.1). Podemos, pues, aplicar la hipótesis de inducción a g, y obtenemos la factorización deseada.

(1.10) **Observación.**—La factorización de 1.9 es ciertamente la factorización de f en factores irreducibles. En efecto, se trata de ver que los factores que ahí aparecen son irreducibles en $\mathbb{R}[T]$. Pero

- $h = T - z$, $z \in \mathbb{R}$, es irreducible, pues es lineal.
- $h = (T - x)^2 + y^2$, $x, y \in \mathbb{R}$, $y \neq 0$, es irreducible, pues tiene grado $2 \leqslant 3$ y ninguna raíz es real (cf. III.3.4): sus raíces son $x \pm yi \notin \mathbb{R}$, ya que $y \neq 0$.

El corolario 1.9 nos dice simplemente que las raíces de un polinomio con coeficientes reales se distribuyen en: reales y no reales, estas últimas complejas dos a dos conjugadas. Por supuesto, puede haber sólo un tipo de raíces:

$$T^2 + 1 = (T - i)(T + i) \quad ; \quad T^2 - 3T + 2 = (T - 2)(T - 1).$$

Ya hemos señalado que en todo lo anterior se precisa el teorema de Bolzano 1.2, que tiene índole topológica. Resaltamos, sin embargo, que sólo se precisa dicho teorema para probar 1.3 y 1.7.1, y que en esos dos momentos se utiliza solamente para funciones *polinomiales*. Veamos ahora cómo se cierra el círculo, deduciendo la versión de 1.2 para funciones polinomiales a partir del teorema fundamental 1.1, o más exactamente, de su corolario 1.9.

Si $f \in \mathbb{R}[T]$, $a < b$ y $f(a)\, f(b) < 0$ *entonces f tiene alguna raíz en* $[a, b]$. Factorizamos f como en 1.9 y observamos que al evaluar en $t \in [a, b]$ los factores de grado 2 son siempre > 0, ya que