Teoría de Cuerpos y Teoría de Galois

Ana M. de Viola-Prioli \ Jorge E. Viola-Prioli

EDITORIAL REVERTÉ

Teoría de Cuerpos y Teoría de Galois

Ana M. de Viola-Prioli
Universidad Simón Bolívar
Caracas

Jorge E. Viola-Prioli
Florida Atlantic University
U. S. A.
Universidad Simón Bolívar
Caracas

EDITORIAL REVERTÉ, S. A.
Barcelona • Bogotá • Buenos Aires • Caracas • México

Teoría de Cuerpos y Teoría de Galois

Edición en papel:
© Editorial Reverté. S.A., 2006
ISBN: 978-84-291-5163-3

Edición en e-book:
© Editorial Reverté. S.A., 2020
ISBN: 978-84-291-9305-3

Propiedad de:
EDITORIAL REVERTÉ, S. A.
Loreto, 13-15, Local B
08029 Barcelona
Tel: (34) 93 419 33 36
Fax: (34) 93 419 51 89
reverte@reverte.com
www.reverte.com

Prólogo

Una parte importante de este libro está centrada en resultados fundamentales de dos jóvenes matemáticos: Niels Abel (Noruega, 1802-1829) y Évariste Galois (Francia, 1811-1832), cuyos trabajos revolucionaron el desarrollo del Álgebra a partir del Siglo XIX. Sin embargo, consideramos que una introducción a la Teoría de Cuerpos, como es ésta, no debe tener como único objetivo la demostración del Teorema de Abel (que prueba "la irresolubilidad de la ecuación de quinto grado", en términos que serán precisados en el texto), lo cual puede lograrse en unas pocas páginas. Más bien, pensamos que es beneficioso para el lector la exposición, junto con lo anterior, de otros temas incluidos en el texto, en cuya creación intervinieron otros matemáticos brillantes, como Newton, Lagrange, Gauss, Dedekind, Artin y Hilbert.

Aunque todas las demostraciones se presentan detalladamente, se espera del lector cierto grado de madurez matemática, así como suficientes conocimientos básicos de Teoría de Grupos y Álgebra Lineal para los Capítulos 1 a 12, y también de Álgebra Conmutativa para el Capítulo 13. Por ello, no incluimos Apéndices destinados a revisar estos temas, contribuyendo así a la brevedad del material. En cuanto a los ejercicios propuestos, algunos de los cuales vienen acompañados de sugerencias, deben interpretarse como parte fundamental del aprendizaje, ya que no solamente sirven para afianzar los conceptos nuevos y clarificar ideas, sino para estimular la creatividad del estudiante.

Con la finalidad de complementar el material presentado, hemos incluido un apartado de Comentarios al final de cada capítulo, algunos de naturaleza histórica y otros esencialmente técnicos.

Como lectura adicional recomendamos el tratamiento histórico dado por Bell [4], y el libro de Edwards [8] basado en las Memorias originales de E. Galois.

Nuestra experiencia en el dictado de este curso en la Universidad Simón Bolívar indica que el material puede ser tratado en cuarenta y ocho clases de cincuenta minutos cada una.

Para aclarar su lectura y comprensión y mejorar la presentación de esta obra se incorporaron sugerencias y observaciones hechas por Manuel Castellet, Ferrán Cedó y José Sosa, a quienes estamos profundamente agradecidos por ello.

La escritura en LaTeX 2_ε ha correspondido a Yolanda Perdomo y Jean Pierre Veiro, a quienes agradecemos su esmero y dedicación. Extendemos nuestro reconocimiento a los profesionales de Editorial Reverté, en especial a Julio Bueno por su continuo y acertado asesoramiento en las correcciones finales, y a Mercè Aicart por su eficiencia en la tarea de llevarlas a cabo, ya que sin la participación de ellos este proyecto no hubiera finalizado exitosamente.

Afirmaba D'Alembert que el Álgebra es muy generosa, pues con frecuencia nos da más que lo que se le pide. Estaremos satisfechos si al recorrer estas páginas el lector comprueba cuánto de cierto encierra esa afirmación.

Caracas

Ana M. de Viola-Prioli

Jorge E. Viola-Prioli

Índice general

Capítulo 1

Preliminares

En lo que sigue A indicará un anillo conmutativo con identidad no nula y $A[x]$ el anillo de polinomios con coeficientes en A. F indicará un cuerpo, $\mathbb{Z}$ representará el anillo de los números enteros, y $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ los cuerpos de los números racionales, reales y complejos, respectivamente, mientras que $\mathbb{Z}_p$ denotará el cuerpo de los enteros módulo p, si p es un número primo. Utilizaremos indistintamente las notaciones f y $f(x)$ para indicar los polinomios de $A[x]$.

Definición 1.1. Sea f un elemento no nulo de $A[x]$. Se dice que el *grado* de f es n si $f(x) = \sum_{i=0}^{n} a_i x^i$ con a_n no nulo, y se denota el grado de f por $\mathrm{gr}(f)$. Por definición, el polinomio nulo no tiene grado.

Definición 1.2. Se dice que un polinomio es *constante* si tiene grado cero o es el polinomio nulo.

Definición 1.3. Se dice que un polinomio es *mónico* si tiene grado n y el coeficiente de x^n es igual a 1.

A continuación recordamos algunos resultados y hechos conocidos.

I. Si D es un dominio de integridad y si f y $g \in D[x]$, entonces $\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$.

II. $F[x]$ es un DIP (dominio de ideales principales) y cada ideal de $F[x]$ está generado por un único generador mónico.

III. Algoritmo de División en $F[x]$: si $f, g \in F[x]$ y g es no nulo, entonces existen $t, r \in F[x]$ únicos tales que $f = tg + r$, con r nulo ó $\mathrm{gr}(r) < \mathrm{gr}(g)$.

IV. Si F es un cuerpo, el cuerpo de fracciones de $F[x]$ es

$$F(x) = \left\{ \frac{f}{g};\ f, g \in F[x], g \neq 0 \right\}.$$

Definición 1.4. Sea f un elemento no nulo de $A[x]$. Se dice que f es *irreducible* en $A[x]$ si se cumplen las dos condiciones siguientes:

1. f no es invertible en $A[x]$;
2. si $f = qp$ con $p, q \in A[x]$, entonces q es invertible o p lo es.

Diremos que f es *reducible* si f no es irreducible.

Ejemplos:

a. $p(x) = 2$ es irreducible en $\mathbb{Z}[x]$.

b. $p(x) = 2$ no es irreducible en $\mathbb{Q}[x]$, pues es invertible en $\mathbb{Q}[x]$.

c. $p(x) = 3x + 3$ es irreducible en $\mathbb{Q}[x]$, pero no en $\mathbb{Z}[x]$, pues $3 + 3x = 3(x + 1)$.

d. $p(x) = x^2 + 1$ es irreducible en $\mathbb{R}[x]$, pero no en $\mathbb{C}[x]$, pues $x^2 + 1 = (x + i)(x - i)$.

e. Todo polinomio de grado 1 es irreducible en $F[x]$.

Recordemos otros resultados conocidos.

V. Sea $p \in F[x]$. Entonces p es irreducible en $F[x]$ si, y sólo si, (p) (el ideal generado por p en $F[x]$) es maximal.

VI. Sea p un elemento no nulo de $F[x]$. Entonces p es irreducible en $F[x]$ si, y sólo si,

a) p no es constante,

b) p no es producto de dos polinomios de $F[x]$ de grado estrictamente menor que el grado de p.

VII. $F[x]$ es un DFU (dominio de factorización única), es decir: para todo polinomio no constante $f \in F[x]$ existen polinomios $p_1, \ldots, p_r$ irreducibles en $F[x]$ tales que $f = p_1 \ldots p_r$. Esta descomposición es única salvo invertibles y orden de los factores, o sea que, si $f = q_1, \ldots q_s$, con $q_1, \ldots, q_s$ irreducibles en $F[x]$, entonces $r = s$ y existe una permutación α del conjunto $\{1, \ldots, r\}$ tal que $p_i = u_i q_{\alpha(i)}$, con u_i invertible para todo $i = 1, \ldots, r$.

Definición 1.5. Se dice que $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$ es un *polinomio primitivo* si el ideal de A generado por los coeficientes de f es igual a A, es decir, $A = (a_0, a_1, \ldots, a_n)$.

Lema 1.1 (Lema de Gauss). Sean $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{i=0}^{m} b_i x^i$ elementos de $A[x]$. Entonces f y g son primitivos si, y sólo si, fg lo es.

Demostración. ($\Leftarrow$) Supongamos $f(x)g(x) = \sum_{i=0}^{m+n} c_i x^i$. Por hipótesis,

$$A = (c_0, c_1, \ldots, c_{m+n}) \subseteq (a_0, a_1, \ldots, a_n) \quad \text{y}$$
$$A = (c_0, c_1, \ldots, c_{n+m}) \subseteq (b_0, b_1, \ldots, b_m).$$

Luego $A = (a_0, a_1, \ldots, a_n) = (b_0, b_1, \ldots, b_m)$, es decir, f y g son primitivos.

($\Rightarrow$) Si fg no fuese primitivo existiría un ideal maximal $\mathcal{M}$ de A tal que $(c_0, c_1, \ldots, c_{n+m}) \subseteq \mathcal{M}$. Como f es primitivo, entonces existe algún $a_i \notin \mathcal{M}$. Sea a_r el primer elemento del conjunto $\{a_0, a_1, \ldots, a_n\}$ tal que $a_r \notin \mathcal{M}$. Análogamente, sea b_s el primer elemento del conjunto $\{b_0, b_1, \ldots, b_m\}$ tal que $b_s \notin \mathcal{M}$. Por lo tanto, $a_r b_s \notin \mathcal{M}$. Pero

$$c_{r+s} = a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{r-1} b_{s+1} + a_r b_s + a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0,$$

de donde, usando la elección de a_r y despejando, se obtiene que $a_r b_s$ está en $\mathcal{M}$, resultando una contradicción. Así pues, fg es primitivo. ∎

Lema 1.2. Para cada $f \in \mathbb{Z}[x]$ existen $d \in \mathbb{Z}$ y $p \in \mathbb{Z}[x]$ primitivo tales que $f(x) = dp(x)$ y $\text{gr}(f) = \text{gr}(p)$. Más aún, si $f(x) = eq(x)$, con $e \in \mathbb{Z}$ y $q \in \mathbb{Z}[x]$ primitivo, entonces $d = e$ ó $d = -e$.

Demostración. Si $f(x) = \sum_{i=0}^{n} a_i x^i$ y $d = \text{mcd}\{a_0, a_1, \ldots, a_n\}$, entonces $f(x) = dp(x)$, y $p(x) = \sum_{i=0}^{n} d^{-1} a_i x^i \in \mathbb{Z}[x]$.

Como $(d^{-1}a_0, d^{-1}a_1, \ldots, d^{-1}a_n) = d^{-1}(d) = (1)$, p es primitivo. Si $f(x) = d\sum_{i=0}^{n} b_i x^i = e\sum_{i=0}^{n} c_i x^i$, con b_i, c_i, d y $e \in \mathbb{Z}$, y si d y e son no

invertibles se tiene $d = (\pm 1)\ p_1 \cdots p_r$ y $e = (\pm 1)\ q_1 \cdots q_m$, con p_i y q_i primos positivos. Entonces

$$(\pm 1)\ p_1 \cdots p_r \left(\sum_{i=0}^{n} b_i x^i \right) = (\pm 1)\ q_1 \cdots q_m \left(\sum_{i=0}^{n} c_i x^i \right). \tag{1.1}$$

Supongamos $r < m$. Como q es primitivo, existe c_k tal que p_1 no divide a c_k. Pero p_1 divide a $p_1 \cdots p_r b_k = (\pm) q_1 \cdots q_m c_k$, y entonces $p_1 = q_i$, para algún i. Sin pérdida de generalidad se puede suponer $i = 1$. Cancelando p_1 en (1.1) se obtiene

$$(\pm 1) p_2 \cdots p_r \left(\sum_{i=0}^{n} b_i x^i \right) = (\pm 1)\ q_2 \cdots q_m \left(\sum_{i=0}^{m} c_i x^i \right).$$

Se continúa el proceso hasta agotar todos los p_i y se obtiene $p_i = q_i$ para todo $i = 1, ..., r$ y

$$(\pm)\ p(x) = (\pm 1)\ q_{r+1} \cdots q_m \left(\sum_{i=0}^{n} c_i x^i \right). \tag{1.2}$$

Pero entonces $q_{r+1} | b_i$ para todo i, y como $p(x)$ es primitivo resulta $q_{r+1} = 1$, que es una contradicción. Luego debe ser $r = m$, y entonces $e = (\pm 1)\ d$. Si d (ó e) es invertible, nos remitimos a (1.2). ∎

Proposición 1.3. Si $f \in \mathbb{Z}[x]$, $\mathrm{gr}(f)$ no es cero y f es reducible en $\mathbb{Q}[x]$, entonces f es reducible en $\mathbb{Z}[x]$. Más aún, si $f(x) = r(x)s(x)$ en $\mathbb{Q}[x]$, entonces $f(x) = r_1(x)s_1(x)$ en $\mathbb{Z}[x]$ con $\mathrm{gr}(r) = \mathrm{gr}(r_1)$ y $\mathrm{gr}(s) = \mathrm{gr}(s_1)$.

Demostración. Por hipótesis f no está en $\mathbb{Q}$, por lo que $f(x) = r(x)s(x)$ en $\mathbb{Q}[x]$, con $0 < \mathrm{gr}(r) < \mathrm{gr}(f)$ y $0 < \mathrm{gr}(s) < \mathrm{gr}(f)$. Si d es el mínimo común múltiplo de los denominadores de los coeficientes de r y de s, entonces $d^2 f(x) = r_2(x)s_2(x)$, con $r_2,\ s_2 \in \mathbb{Z}[x]$ y $\mathrm{gr}(r) = \mathrm{gr}(r_2)$ y $\mathrm{gr}(s) = \mathrm{gr}(s_2)$. Por el Lema 1.2 $f(x) = cg(x)$ con $c \in \mathbb{Z},\ g \in \mathbb{Z}[x]$ primitivo y $\mathrm{gr}(f) = \mathrm{gr}(g),\ r_2(x) = c_1 r_3(x)$ con $c_1 \in \mathbb{Z},\ r_3 \in \mathbb{Z}[x]$ primitivo y $\mathrm{gr}(r_2) = \mathrm{gr}(r_3)$ y $s_2(x) = c_2 s_3(x)$ con $c_2 \in \mathbb{Z},\ s_3 \in \mathbb{Z}[x]$ primitivo y $\mathrm{gr}(s_2) = \mathrm{gr}(s_3)$. Así,

$$d^2 cg(x) = d^2 f(x) = r_2(x)s_2(x) = c_1 c_2 r_3(x)s_3(x). \tag{1.3}$$

Pero por el Lema de Gauss $r_3(x)s_3(x)$ es primitivo, y entonces por el Lema 1.2 se tiene $d^2 c = (\pm) c_1 c_2$. Reemplazando en (1.3) y cancelando se obtiene

$$f(x) = cg(x) = (\pm) c r_3(x)s_3(x) = (\pm)\ r_3(x) c s_3(x),$$

con $\mathrm{gr}(r_3) = \mathrm{gr}(r) > 0$, $\mathrm{gr}(cs_3) = \mathrm{gr}(s) > 0$. Si denotamos $r_1 = \pm r_3$ y $s_1 = cs_3$, resulta $f = r_1 s_1$ y la proposición queda demostrada. ∎

Proposición 1.4. Si $f \in \mathbb{Z}[x]$ y si f es irreducible en $\mathbb{Q}[x]$ y primitivo en $\mathbb{Z}[x]$, entonces f es irreducible en $\mathbb{Z}[x]$.

Demostración. f no es constante, pues es irreducible en $\mathbb{Q}[x]$. Si $f(x) = p(x)q(x)$ con $p, q \in \mathbb{Z}[x]$, por hipótesis debe ser p ó q invertible en $\mathbb{Q}[x]$. Supongamos, por ejemplo, p invertible, o sea $p(x) = c \in \mathbb{Q}$. Pero $p \in \mathbb{Z}[x]$, por lo cual $f(x) = cq(x)$, con $c \in \mathbb{Z}$. Como f es primitivo, el Lema de Gauss implica que $p(x) = c$ es primitivo, es decir $(c)\mathbb{Z} = \mathbb{Z}$, y por lo tanto c es invertible en $\mathbb{Z}$. Como consecuencia $p(x)$ es invertible en $\mathbb{Z}[x]$. ∎

Corolario 1.5. Sea $f \in \mathbb{Z}[x]$ mónico con $\mathrm{gr}(f) \geq 1$. Entonces f es irreducible en $\mathbb{Q}[x]$ si, y sólo si, f es irreducible en $\mathbb{Z}[x]$.

Demostración. Es consecuencia inmediata de las proposiciones anteriores. ∎

Proposición 1.6. Para cada $f \in \mathbb{Q}[x]$ existen $d \in \mathbb{Q}$ y $p \in \mathbb{Z}[x]$ primitivo tales que $f(x) = dp(x)$. Más aún, si $f(x) = eq(x)$, con $e \in \mathbb{Q}$ y $q \in \mathbb{Z}[x]$ primitivo, entonces $d = e$ ó $d = -e$.

Demostración. Si $f(x) = \sum_{i=0}^{n} a_i x^i$ y si r es el producto de los denominadores de los a_i, entonces $f(x) = r^{-1}q(x)$, con $q(x) \in \mathbb{Z}[x]$. Por el Lema 1.2 $q(x) = sp(x)$, con $s \in \mathbb{Z}$ y $p(x) \in \mathbb{Z}[x]$ primitivo. Por lo tanto $f(x) = dp(x)$, con $d = r^{-1}s \in \mathbb{Q}$ y $p \in \mathbb{Z}[x]$ primitivo. Si $f(x) = eq(x)$, con $e \in \mathbb{Q}$ y $q(x) = \sum_{i=0}^{n} b_i x^i \in \mathbb{Z}[x]$ primitivo, y si $de^{-1} = \frac{m}{n} \in \mathbb{Q}$, con $(m, n) = 1$, entonces $mp = nq$. Si t es un divisor primo de m, como $(t, n) = 1$, resulta que t divide a b_i para todo i, lo cual es una contradicción. Por tanto $m = \pm 1$. Análogamente, $n = \pm 1$, y entonces $de^{-1} = \pm\, 1$. ∎

Corolario 1.7. Si en $\mathbb{Q}[x]$ se tiene $x^n - 1 = f(x)g(x)$ con f mónico, entonces $f \in \mathbb{Z}[x]$ y $g \in \mathbb{Z}[x]$.

Demostración. Por la Proposición 1.6

$$x^n - 1 = f(x)g(x) = (dp(x))(bq(x)) = dbp(x)q(x),$$

con $d, b \in \mathbb{Q}$ y $p, q \in \mathbb{Z}[x]$ primitivos. Por el Lema de Gauss pq es primitivo, y como $x^n - 1$ también lo es, por la unicidad debe ser $db = \pm 1$, o sea