

Capítulo 14

Cuerpos

En este capítulo vamos a estudiar algunas propiedades especiales de los cuerpos.

Primero revisemos un par de resultados que ya hemos visto de alguna manera en el capítulo 11.

Para un cuerpo K consideremos el homomorfismo canónico $\phi: \mathbb{Z} \rightarrow K$.

- Si ϕ es inyectivo, se dice que K tiene **característica** 0. En este caso K contiene un subanillo $\text{im } \phi$ que es isomorfo a \mathbb{Z} . Siendo un cuerpo, K también debe contener todos los inversos de los elementos no nulos de $\text{im } \phi$, así que K contiene un *subcuerpo* isomorfo a \mathbb{Q} .
- Si ϕ no es inyectivo, entonces $\text{im } \phi \cong \mathbb{Z}/n\mathbb{Z}$. Dado que K no tiene divisores de cero, el número $n = p$ es necesariamente primo. En este caso se dice que K tiene **característica** p . Notamos que $\mathbb{Z}/n\mathbb{Z} = \mathbb{F}_p$ es un cuerpo.

Podemos resumir que la característica de K corresponde al subcuerpo mínimo de K . Si este es isomorfo a \mathbb{Q} , entonces la característica es 0; si es isomorfo a \mathbb{F}_p , entonces la característica es p .

14.0.1. Ejemplo. Los cuerpos

$$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(X) := \left\{ \frac{f}{g} \mid f, g \in \mathbb{Q}[X], g \neq 0 \right\}$$

tienen característica 0. Los cuerpos \mathbb{F}_p y $\mathbb{F}_p(X)$ tienen característica p . ▲

Recordemos también que un cuerpo K tiene como sus ideales solamente (0) y K . Esto implica que todos los homomorfismos de cuerpos son inyectivos.

14.0.2. Observación. Sea $\phi: K \rightarrow R$ un homomorfismo donde K es un cuerpo y R es un anillo no nulo. Entonces, ϕ es inyectivo.

Demostración. El núcleo de ϕ es un ideal en K . Puesto que $R \neq 0$, tenemos $\phi(1) = 1 \neq 0^*$, así que $\ker \phi \neq K$. Luego, $\ker \phi = (0)$. ■

*Según nuestra convención, un homomorfismo de anillos preserva la identidad 1.

14.1 Extensiones de cuerpos

14.1.1. Definición. Si L es un cuerpo y $K \subseteq L$ es un subcuerpo (un subanillo que es también un cuerpo), se dice que L es una **extensión** de K y se escribe " L/K "* o se dibuja el diagrama

$$\begin{array}{c} L \\ | \\ K \end{array}$$

El lector puede comprobar que en la situación de arriba L satisface los axiomas de espacio vectorial sobre K .

14.1.2. Definición. La dimensión de L como un espacio vectorial sobre K se llama el **grado** de la extensión y se denota por

$$[L : K] := \dim_K L.$$

Si el grado es finito, se dice que L/K es una **extensión finita**. Cuando el grado no es finito, a veces se suele escribir " $[L : K] = \infty$ ".

14.1.3. Ejemplo. Los números complejos \mathbb{C} es una extensión de grado 2 de los números reales \mathbb{R} . Los números 1 y $\sqrt{-1}$ forman una base de \mathbb{C} sobre \mathbb{R} . ▲

14.1.4. Ejemplo. Los números reales \mathbb{R} forman una extensión infinita de los números racionales \mathbb{Q} . En efecto, para toda extensión finita K/\mathbb{Q} se tiene un isomorfismo $K \cong \mathbb{Q}^n$ de espacios vectoriales sobre \mathbb{Q} , donde $n = [K : \mathbb{Q}]$. Luego, \mathbb{Q}^n es numerable, puesto que \mathbb{Q} lo es. Sin embargo, \mathbb{R} no es numerable. De hecho, todo espacio vectorial sobre \mathbb{Q} de dimensión *numerable* es un conjunto numerable, así que este argumento nos dice que la dimensión de \mathbb{R} sobre \mathbb{Q} no es numerable.

Sin analizar las cardinalidades, se puede encontrar un subconjunto infinito de \mathbb{R} que es linealmente independiente sobre \mathbb{Q} . Consideremos los números $\log p$ donde $p = 2, 3, 5, 7, 11, \dots$ son primos. Si tenemos

$$a_1 \log p_1 + \dots + a_n \log p_n = 0$$

para diferentes primos p_1, \dots, p_n y algunos $a_1, \dots, a_n \in \mathbb{Q}$, entonces podemos primero cancelar los denominadores y asumir que $a_1, \dots, a_n \in \mathbb{Z}$. Luego,

$$p_1^{a_1} \dots p_n^{a_n} = 1,$$

lo que implica $a_1 = \dots = a_n = 0$. ▲

14.1.5. Ejemplo. Si K/\mathbb{F}_p es una extensión de grado n del cuerpo finito \mathbb{F}_p , entonces $|K| = p^n$. En el siguiente capítulo vamos a describir todas las extensiones finitas de \mathbb{F}_p . ▲

14.1.6. Proposición. Para una cadena de cuerpos $F \subseteq K \subseteq L$ se tiene

$$[L : F] = [L : K] \cdot [K : F].$$

Específicamente,

- 1) si $[L : K] < \infty$ y $[K : F] < \infty$, entonces $[L : F] = [L : K] \cdot [K : F]$; además, $[L : F] = \infty$ si y solo si se cumple $[L : K] = \infty$ o $[K : F] = \infty$;
- 2) si $\alpha_1, \dots, \alpha_m \in K$ es una base de K sobre F y $\beta_1, \dots, \beta_n \in L$ es una base de L sobre K , entonces los productos $\alpha_i \beta_j$ forman una base de L sobre F .

*Cuidado: es solamente una notación estándar que no significa ningún tipo de cociente.

$$\begin{array}{c}
 L \quad \beta_1, \dots, \beta_n \\
 [L:K]=n \mid \\
 K \quad \alpha_1, \dots, \alpha_m \\
 [K:F]=m \mid \\
 F
 \end{array}$$

Demostración. Todo elemento de L puede ser escrito como

$$x = \sum_{1 \leq j \leq n} b_j \beta_j$$

para algunos $b_1, \dots, b_n \in K$. Luego, los coeficientes b_j pueden ser expresados como

$$b_j = \sum_{1 \leq i \leq m} a_{ij} \alpha_i$$

para algunos $a_{ij} \in F$. Luego,

$$x = \sum_{1 \leq j \leq n} \sum_{1 \leq i \leq m} a_{ij} \alpha_i \beta_j,$$

lo que significa que los productos $\alpha_i \beta_j$ generan a L como un espacio vectorial sobre F . Para ver que esto es una base, hay que ver que los elementos $\alpha_i \beta_j$ son linealmente independientes. Si la combinación lineal de arriba es igual a 0, entonces se tiene $\sum_{1 \leq j \leq n} b_j \beta_j = 0$, de donde $b_j = 0$ para todo j por la independencia lineal de los β_j . Pero la independencia lineal de los α_i implica entonces que $a_{ij} = 0$ para todo i .

Notamos que si $[K : F] = \infty$, entonces existe un número infinito de elementos $\alpha \in K$ linealmente independientes sobre F . En particular, $\alpha \in L$ y esto significa que $[L : F] = \infty$. De la misma manera, si $[L : K] = \infty$, entonces existe un número infinito de elementos $\beta \in L$ que son linealmente independientes sobre K . En particular, son linealmente independientes sobre F y $[L : F] = \infty$. En fin, si $[L : F] = \infty$, entonces $[L : K] = \infty$ o $[K : F] = \infty$. En efecto, el argumento de arriba nos dice que $[L : K] < \infty$ y $[K : F] < \infty$ implica $[L : F] < \infty$. ■

En práctica muchas extensiones se obtienen “añadiendo” al cuerpo de base K una raíz de algún polinomio irreducible $f \in K[X]$. Por ejemplo, \mathbb{C} es el resultado de añadir a \mathbb{R} una raíz del polinomio $X^2 + 1$ que es irreducible en $\mathbb{R}[X]$. En general, se tiene el siguiente resultado.

14.1.7. Teorema. *Sea K un cuerpo y $f \in K[X]$ un polinomio irreducible de grado n . Entonces,*

- 1) *el anillo cociente $L := K[X]/(f)$ es un cuerpo;*
- 2) *el homomorfismo canónico $\phi: K \hookrightarrow K[X] \twoheadrightarrow K[X]/(f)$ es inyectivo e identifica a K con un subcuerpo de L y entonces a $K[X]$ con un subanillo de $L[X]$;*
- 3) *si $\alpha := X \pmod{f} \in L$ es la imagen de la variable X en el cociente, entonces $[L : K] = n$ y los elementos $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ forman una base de L sobre K ; en particular,*

$$L = \{a_0 + a_1 \alpha + \dots + a_{n-1} \alpha^{n-1} \mid a_0, a_1, \dots, a_{n-1} \in K\};$$

- 4) *considerando a f como un elemento de $L[X]$, se tiene $f(\alpha) = 0$.*

Demostración. Como sabemos, $K[X]$ es un dominio de ideales principales, y entonces si f es irreducible, el ideal $(f) \subset K[X]$ es maximal (si f es irreducible, entonces f es primo, así que el ideal (f) es primo, y luego todo ideal primo no nulo en $K[X]$ es maximal). Esto significa que $K[X]/(f)$ es un cuerpo.

Ahora $\phi: K \hookrightarrow K[X] \twoheadrightarrow K[X]/(f)$ es un homomorfismo de cuerpos y por ende es inyectivo.

Todo elemento de $K[X]/(f)$ puede ser representado por algún polinomio $g \in K[X]$ considerado módulo f . La división con resto en $K[X]$ nos permite escribir

$$g = qf + r, \quad \deg r < \deg f,$$

así que $g \equiv r \pmod{f}$. Esto significa que los elementos del cociente $K[X]/(f)$ se representan por polinomios

$$g = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$$

para algunos $a_0, a_1, \dots, a_{n-1} \in K$. La reducción de g módulo f nos da

$$\begin{aligned} \bar{g} &= \overline{a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}} = a_0 + a_1 \bar{X} + \cdots + a_{n-1} \bar{X}^{n-1} \\ &= a_0 + a_1 \alpha + \cdots + a_{n-1} \alpha^{n-1} \in L. \end{aligned}$$

Entonces, $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ generan a L como un espacio vectorial sobre K y solo falta ver que son linealmente independientes. Si tenemos

$$a_0 + a_1 \alpha + \cdots + a_{n-1} \alpha^{n-1} = 0,$$

esto significa que el polinomio

$$g = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} \in K[X]$$

se reduce a 0 módulo f ; es decir, $f \mid g$. Pero todos los múltiplos no nulos de f tienen grado $\geq n$, mientras que $\deg g \leq n-1$, así que necesariamente $g = 0$ y $a_0 = a_1 = \cdots = a_{n-1} = 0$.

De la construcción está claro que $f(\alpha) = 0$. ■

14.1.8. Ejemplo. Sea d un número entero libre de cuadrados diferente de 1. El polinomio $X^2 - d$ es irreducible en $\mathbb{Q}[X]$ (por ejemplo, porque sus raíces son irracionales para $d > 1$ o imaginarias para $d < 0$). Por el resultado de arriba, el anillo cociente $K := \mathbb{Q}[X]/(X^2 - d)$ es un cuerpo y $[K : \mathbb{Q}] = 2$. Denotando la imagen de X en el cociente por $\alpha \in K$, se tiene

$$K = \{a + b\alpha \mid a, b \in \mathbb{Q}\}.$$

La adición evidentemente viene dada por

$$(a_1 + b_1\alpha) + (a_2 + b_2\alpha) = (a_1 + a_2) + (b_1 + b_2)\alpha.$$

Para la multiplicación, hay que notar que en K se cumple la relación $\alpha^2 = d$:

$$(a_1 + b_1\alpha) \cdot (a_2 + b_2\alpha) = a_1 a_2 + (a_1 b_2 + a_2 b_1)\alpha + b_1 b_2 \alpha^2 = (a_1 a_2 + d b_1 b_2) + (a_1 b_2 + a_2 b_1)\alpha.$$

Para invertir un elemento $a + b\alpha \neq 0$, se puede primero notar que

$$(a + b\alpha)(a - b\alpha) = a^2 - b^2 \alpha^2 = a^2 - b^2 d,$$

y puesto que d es libre de cuadrados, este es un número racional no nulo. Luego,

$$(a + b\alpha)^{-1} = \frac{a}{a^2 - b^2 d} - \frac{b}{a^2 - b^2 d} \alpha.$$

▲

14.1.9. Ejemplo. El polinomio ciclotómico Φ_n es irreducible en $\mathbb{Q}[X]$ y tiene grado $\phi(n)$, así que el cuerpo $K := \mathbb{Q}[X]/(\Phi_n)$ es una extensión de grado $\phi(n)$ de \mathbb{Q} . ▲

14.1.10. Ejemplo. El polinomio $X^3 - 2$ es irreducible en $\mathbb{Q}[X]$, por ejemplo, gracias al criterio de Eisenstein para $p = 2$. El cociente $K := \mathbb{Q}[X]/(X^3 - 2)$ es una extensión de grado 3 de \mathbb{Q} ; tenemos

$$K = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\},$$

donde como siempre, α denota la imagen de X en el cociente. La multiplicación de los elementos se sigue de la relación $\alpha^3 = 2$, pero la fórmula general no es muy instructiva:

$$\begin{aligned} (a_1 + b_1\alpha + c_1\alpha^2)(a_2 + b_2\alpha + c_2\alpha^2) &= a_1a_2 + (a_1b_2 + a_2b_1)\alpha + (a_1c_2 + a_2c_1 + b_1b_2)\alpha^2 + (b_1c_2 + b_2c_1)\alpha^3 + c_1c_2\alpha^4 \\ &= a_1a_2 + 2(b_1c_2 + b_2c_1) + (a_1b_2 + a_2b_1 + 2c_1c_2)\alpha + (a_1c_2 + a_2c_1 + b_1b_2)\alpha^2. \end{aligned}$$

▲

14.1.11. Ejemplo. El polinomio $X^2 + X + 1$ es irreducible en $\mathbb{F}_2[X]$. Consideremos el cociente

$$K := \mathbb{F}_2[X]/(X^2 + X + 1).$$

Denotando por α la imagen de X , se ve que

$$K = \{0, 1, \alpha, \alpha + 1\}.$$

Tenemos $[K : \mathbb{F}_2] = 2$ y los elementos 1 y α forman una base de K sobre \mathbb{F}_2 . Las tablas de adición y multiplicación correspondientes son

+	0	1	α	$\alpha + 1$
0	0	0	0	0
1	0	1	α	$\alpha + 1$
α	0	α	$\alpha + 1$	1
$\alpha + 1$	0	$\alpha + 1$	1	α

×	0	1	α	$\alpha + 1$
0	0	1	α	$\alpha + 1$
1	1	0	$\alpha + 1$	α
α	α	$\alpha + 1$	0	1
$\alpha + 1$	$\alpha + 1$	α	1	0

De la misma manera se obtienen todos los cuerpos finitos. Si K es un cuerpo finito, entonces necesariamente $\text{char } K = p$ para algún primo p , lo que significa que K es una extensión finita de \mathbb{F}_p . Resulta que \mathbb{F}_p tiene una sola extensión de grado n salvo isomorfismo que se obtiene como $\mathbb{F}_p[X]/(f)$, donde $f \in \mathbb{F}_p[X]$ es un polinomio irreducible de grado n . La existencia de este f es algo que vamos a probar en el siguiente capítulo. ▲

Hemos visto cómo añadir a un cuerpo K una raíz de un polinomio irreducible $f \in K[X]$ de manera formal: hay que pasar al cociente $K[X]/(f)$. En muchos casos estas raíces ya están en una extensión específica de K y pueden ser añadidas en el siguiente sentido.

14.1.12. Definición. Para una extensión de cuerpos L/K y elementos $\alpha_1, \alpha_2, \dots \in L$ el subcuerpo mínimo de L que contiene a $\alpha_1, \alpha_2, \dots$ y todos los elementos de K se llama el subcuerpo **generado** por $\alpha_1, \alpha_2, \dots$ sobre K y se denota por

$$K(\alpha_1, \alpha_2, \dots) = \bigcap_{\substack{K \subseteq K' \subseteq L \\ \alpha_1, \alpha_2, \dots \in K'}} K'.$$

Las extensiones de la forma $K(\alpha)/K$ para un solo elemento $\alpha \in L$ se llaman las **extensiones simples** de K . En este caso α se llama un **elemento primitivo** de $K(\alpha)$.

En general, las extensiones de la forma $K(\alpha_1, \dots, \alpha_n)/K$ se llaman las **extensiones finitamente generadas** de K .

14.1.13. Ejemplo. Para un entero libre de cuadrados $d \neq 1$ consideremos $\sqrt{d} \in \mathbb{C}$ (si $d > 1$, entonces $\sqrt{d} \in \mathbb{R}$). Tenemos entonces

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

En efecto, la parte derecha está contenida en $\mathbb{Q}(\sqrt{d})$. Se ve fácilmente que es un subanillo de \mathbb{C} , y de hecho, es un subcuerpo: para $(a, b) \neq (0, 0)$ se tiene

$$\frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - db^2} = \frac{a}{a^2 - db^2} - \frac{b}{a^2 - db^2} \sqrt{d} \in \mathbb{Q}(\sqrt{d})$$

(note que $a^2 \neq db^2$, puesto que d es libre de cuadrados). ▲

Toda extensión finita K/\mathbb{Q} es simple: es de la forma $\mathbb{Q}(\alpha)$ para algún $\alpha \in \mathbb{C}$, pero lo veremos más adelante, después de desarrollar la teoría general adecuada. Por el momento, podemos ver algunos ejemplos sencillos.

14.1.14. Ejemplo. Consideremos el cuerpo $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Denotemos

$$\alpha := \sqrt{2} + \sqrt{3}.$$

Obviamente, tenemos $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Luego, calculamos que

$$\alpha^2 = 5 + 2\sqrt{6}, \quad \alpha^3 = 11\sqrt{2} + 9\sqrt{3}, \quad \alpha^4 = 49 + 20\sqrt{6},$$

de donde

$$\sqrt{2} = \frac{1}{2}(\alpha^3 - 9\alpha), \quad \sqrt{3} = -\frac{1}{2}(\alpha^3 - 11\alpha),$$

así que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\alpha)$ y podemos concluir que

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

▲

14.1.15. Ejemplo. Consideremos los elementos

$$\zeta_3 := e^{2\pi\sqrt{-1}/3} = \frac{-1 + \sqrt{-3}}{2}, \quad \sqrt[3]{2}, \quad \alpha := \zeta_3 + \sqrt[3]{2}.$$

Tenemos

$$2 = (\alpha - \zeta_3)^3 = \alpha^3 + 3\alpha\zeta_3^2 - 3\alpha^2\zeta_3 - \zeta_3^3.$$

Dado que $\zeta_3^3 = 1$ y $\zeta_3^2 = -1 - \zeta_3$, esto nos da la ecuación

$$3 = \alpha^3 - 3\alpha - 3\alpha(1 + \alpha)\zeta_3,$$

de donde se puede expresar

$$\zeta_3 = \frac{\alpha^3 - 3\alpha - 3}{3\alpha(1 + \alpha)},$$

así que $\zeta_3 \in \mathbb{Q}(\alpha)$, y luego $\sqrt[3]{2} = \alpha - \zeta_3 \in \mathbb{Q}(\alpha)$. Podemos concluir que

$$\mathbb{Q}(\zeta_3, \sqrt[3]{2}) = \mathbb{Q}(\zeta_3 + \sqrt[3]{2}).$$

▲

14.1.16. Comentario. Los últimos dos ejemplos fueron escogidos para facilitar los cálculos. Aunque más adelante vamos a probar que para cualquier extensión finita $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ se tiene $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$ para algún número γ , en general este no tiene por qué ser la suma de α y β .

14.1.17. Observación. Sea L/K una extensión de cuerpos. Para $\alpha, \beta \in L$ se tiene $K(\alpha, \beta) = (K(\alpha))(\beta)$.

Demostración. Tenemos $K \subset K(\alpha, \beta)$ y $\alpha \in K(\alpha, \beta)$, así que $K(\alpha) \subseteq K(\alpha, \beta)$ por la minimalidad de $K(\alpha)$. Además, $\beta \in K(\alpha, \beta)$ y por ende $(K(\alpha))(\beta) \subseteq K(\alpha, \beta)$.

De la misma manera, $K \subseteq (K(\alpha))(\beta)$ y $\alpha, \beta \in (K(\alpha))(\beta)$, así que $K(\alpha, \beta) \subseteq (K(\alpha))(\beta)$ por la minimalidad de $K(\alpha, \beta)$. ■

Por inducción se sigue que toda extensión finitamente generada $K(\alpha_1, \dots, \alpha_n)$ se obtiene como una sucesión de extensiones simples:

$$\begin{array}{rcl}
 K_n := K_{n-1}(\alpha_n) & = & K(\alpha_1, \dots, \alpha_n) \\
 & & | \\
 K_{n-1} := K_{n-2}(\alpha_{n-1}) & = & K(\alpha_1, \dots, \alpha_{n-1}) \\
 & & | \\
 & & \vdots \\
 & & | \\
 K_2 := K_1(\alpha_2) & = & K(\alpha_1, \alpha_2) \\
 & & | \\
 K_1 & := & K(\alpha_1) \\
 & & | \\
 & & K
 \end{array}$$

(En este caso también se dice que $K \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_n$ es una **torre de extensiones**.)

14.2 Extensiones algebraicas

14.2.1. Definición. Para una extensión L/K se dice que un elemento $\alpha \in L$ es **algebraico** sobre K si $f(\alpha) = 0$ para algún polinomio no nulo $f \in K[X]$. Cuando α no es algebraico, se dice que es **trascendente** sobre K .

Se dice que L/K es una extensión algebraica si todo elemento de L es algebraico sobre K .

14.2.2. Ejemplo. Los números $\sqrt[n]{2} \in \mathbb{R}$ y $\zeta_n := e^{2\pi\sqrt{-1}/n} \in \mathbb{C}$ son algebraicos sobre \mathbb{Q} : son raíces de los polinomios $X^n - 2$ y $X^n - 1$ respectivamente. ▲

14.2.3. Ejemplo. Los números $e = 2,718281828\dots$ y $\pi = 3,1415926\dots$ son trascendentes sobre \mathbb{Q} ; es un resultado clásico pero muy difícil. Es mucho más fácil (¡pero tampoco es trivial!) probar que $e, \pi \notin \mathbb{Q}$. ▲

14.2.4. Observación. Para una cadena de extensiones $F \subseteq K \subseteq L$, si $\alpha \in L$ es algebraico sobre F , entonces es algebraico sobre K .

Demostración. Si $f(\alpha) = 0$ para algún polinomio no nulo $f \in F[X]$, en particular $f \in K[X]$. ■

14.2.5. Observación. Toda extensión finita es algebraica.

Demostración. Si L/K es una extensión finita de grado n , entonces para cualquier $\alpha \in L$ los elementos $1, \alpha, \alpha^2, \dots, \alpha^n$ son necesariamente linealmente independientes, así que existen algunos coeficientes $a_0, a_1, a_2, \dots, a_n \in K$, no todos nulos, tales que

$$a_0 + a_1 \alpha + a_2 \alpha^2 + \dots + a_n \alpha^n = 0.$$

Esto significa que α es una raíz de un polinomio no nulo

$$f = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n \in K[X].$$

■

Hay extensiones algebraicas infinitas, pero las veremos un poco más adelante. Voy a mencionar un par de extensiones que no son algebraicas.

14.2.6. Ejemplo. Para un cuerpo K la extensión $K(T)/K$, donde

$$K(T) := \left\{ \frac{f}{g} \mid f, g \in k[T], g \neq 0 \right\}$$

es el cuerpo de las funciones racionales, no es algebraica. Por ejemplo, para cualesquiera $a_0, a_1, a_2, \dots, a_n$ el elemento

$$a_0 + a_1 T + a_2 T^2 + \dots + a_n T^n \in K(T)$$

es nulo si y solo si $a_0 = a_1 = a_2 = \dots = a_n = 0$, lo que significa que T no es algebraico sobre K . ▲

14.2.7. Ejemplo. La extensión \mathbb{R}/\mathbb{Q} no es algebraica. Esto puede ser probado sin construir ningún número trascendente específico. En efecto, todo elemento algebraico $\alpha \in \mathbb{R}$ es una raíz de algún polinomio no nulo $f \in \mathbb{Q}[X]$. El cuerpo \mathbb{Q} es numerable, luego el anillo $\mathbb{Q}[X]$ es numerable, y el conjunto de las raíces de estos polinomios es también numerable (todo polinomio racional de grado n tiene a lo sumo n raíces). Sin embargo, \mathbb{R} no es numerable. Se sigue que hay elementos de \mathbb{R} que no son algebraicos sobre \mathbb{Q} . ▲

14.2.8. Teorema (El polinomio mínimo). Sean L/K una extensión de cuerpos y $\alpha \in L$ un elemento.

1) α es algebraico sobre K si y solamente si el homomorfismo de evaluación

$$\text{ev}_\alpha: K[X] \rightarrow K(\alpha), \quad f \mapsto f(\alpha)$$

tiene núcleo no trivial.

2) En este caso $\ker \text{ev}_\alpha = (m_{\alpha, K})$, donde $m_{\alpha, K} \in K[X]$ es un polinomio mónico irreducible definido de modo único; a saber, $m_{\alpha, K}$ es el polinomio mónico de grado mínimo posible que tiene α como su raíz.

3) Hay un isomorfismo natural $K[X]/(m_{\alpha, K}) \cong K(\alpha)$.

4) Un polinomio $f \in K[X]$ tiene al elemento α como su raíz si y solamente si $m_{\alpha, K} \mid f$. Si f es irreducible, entonces $K[X]/(f) \cong K(\alpha)$.

5) Tenemos $[K(\alpha) : K] = \deg m_{\alpha, K}$.

Demostración. Puesto que $K[X]$ es un dominio de ideales principales, se tiene necesariamente $\ker \text{ev}_\alpha = (f)$ para algún polinomio $f \in K[X]$. Si $f = 0$, entonces α es trascendente. Si $f \neq 0$, entonces de nuestra prueba de que todo dominio euclidiano es un dominio de ideales principales (véase el capítulo anterior) se sigue que f es un polinomio de mínimo grado posible tal que $f(\alpha) = 0$.

Notamos que tal f es necesariamente irreducible: si $f = gh$ para algunos $g, h \in K[X]$ de grado menor que f , entonces $g(\alpha)h(\alpha) = f(\alpha) = 0$ implica que $g(\alpha) = 0$ o $h(\alpha) = 0$, pero f es un polinomio de mínimo grado posible que tiene a α como su raíz.

Ahora si f_1 y f_2 son dos polinomios que cumplen $(f_1) = (f_2) = \ker \text{ev}_\alpha$, entonces $f_1 \sim f_2$, así que $f_2 = c f_1$ para alguna constante $c \in K^\times$. Esto significa que la condición de que f sea mónico lo define de modo único. Denotemos este polinomio mónico por $m_{\alpha, K}$.

Dado que $m_{\alpha, K}$ es irreducible, el ideal $(m_{\alpha, K})$ es primo. El anillo $K[X]$ es un dominio de ideales principales y todo ideal primo no nulo en $K[X]$ es maximal. Esto implica que $K[X]/(m_{\alpha, K})$ es un cuerpo. El primer teorema de isomorfía nos da entonces un isomorfismo de cuerpos

$$K[X]/(m_{\alpha, K}) \cong \text{im } \text{ev}_\alpha.$$

Calculemos $\text{im } \text{ev}_\alpha$. Primero,

$$\text{im } \text{ev}_\alpha = \{a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0 \mid a_i \in K\} \subseteq K(\alpha).$$

Evaluando los polinomios constantes, se ve que $K \subseteq \text{im } \text{ev}_\alpha$. Además, $\alpha \in \text{im } \text{ev}_\alpha$. Se sigue que $\text{im } \text{ev}_\alpha = K(\alpha)$, puesto que $\text{im } \text{ev}_\alpha$ es un cuerpo que contiene a K y α e $\text{im } \text{ev}_\alpha$ está contenido en $K(\alpha)$. Entonces,

$$K[X]/(m_{\alpha, K}) \cong K(\alpha).$$

Ahora $f(\alpha) = 0$ si y solamente si $f \in \ker \text{ev}_\alpha = (m_{\alpha, K})$, lo que significa que $m_{\alpha, K} \mid f$. Si f es también irreducible como $m_{\alpha, K}$, entonces $f \sim m_{\alpha, K}$; es decir $(f) = (m_{\alpha, K})$ y

$$K[X]/(f) = K[X]/(m_{\alpha, K}) \cong K(\alpha).$$

En fin, hemos visto en 14.1.7 que el cuerpo $K[X]/(m_{\alpha, K})$ tiene grado $\deg m_{\alpha, K}$ sobre K . ■

14.2.9. Definición. Para una extensión L/K y un elemento $\alpha \in L$ algebraico sobre K , el polinomio mónico $m_{\alpha, K} \in K[X]$ de mínimo grado posible tal que $m_{\alpha, K}$ se llama el **polinomio mínimo** de α sobre K . Como acabamos de notar, $m_{\alpha, K}$ es necesariamente irreducible. El número

$$\deg_K(\alpha) := [K(\alpha) : K] = \deg m_{\alpha, K}$$

se llama el **grado** de α sobre K .

14.2.10. Observación. Si L/K es una extensión finita, entonces para todo $\alpha \in L$ el grado $\deg_K(\alpha)$ divide al grado $[L : K]$.

Demostración. Tenemos $[L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K]$. ■

14.2.11. Observación. Sea $F \subseteq K \subseteq L$ una cadena de extensiones y $\alpha \in L$ un elemento algebraico sobre F . Entonces, en el anillo de polinomios $K[X]$ se cumple

$$m_{\alpha, K} \mid m_{\alpha, F}.$$

En particular,

$$[K(\alpha) : K] = \deg_K(\alpha) \leq \deg_F(\alpha) = [F(\alpha) : F].$$

Demostración. Tenemos $m_{\alpha, F}(\alpha) = 0$. Puesto que $m_{\alpha, F} \in F[X] \subseteq K[X]$, se cumple $m_{\alpha, K} \mid m_{\alpha, F}$. ■

Antes de volver a los resultados generales sobre los elementos algebraicos, veamos algunos ejemplos de polinomios mínimos.

14.2.12. Ejemplo (Trivial). Para una extensión L/K , si $\alpha \in K$, entonces $m_{\alpha, K} = X - \alpha$. ▲

14.2.13. Ejemplo. Para $\sqrt{-1} \in \mathbb{C}$ el polinomio mínimo sobre \mathbb{Q} es $m_{\sqrt{-1}, \mathbb{Q}} = X^2 + 1$. Tenemos $\mathbb{Q}(\sqrt{-1}) \cong \mathbb{Q}[X]/(X^2 + 1)$. De la misma manera, $m_{\sqrt{-1}, \mathbb{R}} = X^2 + 1$ y $\mathbb{C} = \mathbb{R}(\sqrt{-1}) \cong \mathbb{R}[X]/(X^2 + 1)$. ▲

14.2.14. Ejemplo. Sea $d \neq 1$ un entero libre de cuadrados. Para $\sqrt{d} \in \mathbb{C}$ el polinomio mínimo sobre \mathbb{Q} es $X^2 - d$. En efecto, este polinomio tiene a d como su raíz y su grado es igual a $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$. Tenemos $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[X]/(X^2 - d)$. ▲

14.2.15. Ejemplo. Consideremos el número

$$(14.1) \quad \zeta_3 := e^{2\pi\sqrt{-1}/3} = \frac{-1 + \sqrt{-3}}{2} \in \mathbb{C}.$$

Aunque tenemos $\zeta_3^3 - 1 = 0$, el polinomio $X^3 - 1$ no es el polinomio mínimo de ζ_3 sobre \mathbb{Q} : se tiene $X^3 - 1 = (X - 1)(X^2 + X + 1)$, donde $f = X^2 + X + 1$ es un polinomio irreducible (por ejemplo, porque $\bar{f} \in \mathbb{F}_2[X]$ es irreducible o porque $f(X + 1) = X^3 + 3X + 3$ es irreducible por el criterio de Eisenstein) y $f(\zeta_3) = 0$. Entonces,

$$m_{\zeta_3, \mathbb{Q}} = X^2 + X + 1.$$

Notamos que

$$\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$$

—de la ecuación (14.1) se ve que $\zeta_3 \in \mathbb{Q}(\sqrt{-3})$ y $\sqrt{-3} \in \mathbb{Q}(\zeta_3)$. ▲

Para una generalización de este ejemplo, véase §14.4.

14.2.16. Ejemplo. El polinomio $X^3 - 2$ es irreducible en $\mathbb{Q}[X]$ y tiene tres raíces en \mathbb{C} :

$$\alpha_1 = \sqrt[3]{2}, \quad \alpha_2 = \sqrt[3]{2} \frac{-1 + \sqrt{-3}}{2} = \sqrt[3]{2} \zeta_3, \quad \alpha_3 = \sqrt[3]{2} \frac{-1 - \sqrt{-3}}{2} = \sqrt[3]{2} \bar{\zeta}_3 = \sqrt[3]{2} \zeta_3^2;$$

donde α_1 es real y α_2 y α_3 son números complejos conjugados. El teorema 14.2.8 nos dice que hay isomorfismos de cuerpos

$$\mathbb{Q}[X]/(X^3 - 2) \cong \mathbb{Q}(\alpha_1) \cong \mathbb{Q}(\alpha_2) \cong \mathbb{Q}(\alpha_3).$$

Sin embargo, $\mathbb{Q}(\alpha_1) \subset \mathbb{R}$, mientras que $\mathbb{Q}(\alpha_2), \mathbb{Q}(\alpha_3) \not\subset \mathbb{R}$, así que hay cierta diferencia entre $\mathbb{Q}(\alpha_1)$ y $\mathbb{Q}(\alpha_2), \mathbb{Q}(\alpha_3)$ que no puede ser expresada en términos de isomorfismos de cuerpos abstractos. ▲

14.2.17. Ejemplo. Volvamos al ejemplo 14.1.14. Para el cuerpo

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

hemos calculado las potencias de $\alpha := \sqrt{2} + \sqrt{3}$:

$$\alpha^2 = 5 + 2\sqrt{6}, \quad \alpha^3 = 11\sqrt{2} + 9\sqrt{3}, \quad \alpha^4 = 49 + 20\sqrt{6}.$$

Se ve que

$$\alpha^4 - 10\alpha^2 + 1 = 0,$$

así que α es una raíz del polinomio $f = X^4 - 10X^2 + 1$. El polinomio mínimo $m_{\alpha, \mathbb{Q}}$ necesariamente divide a f , lo que implica que

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 4.$$

Luego, tenemos

$$[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}],$$

donde $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, así que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ o 4.

Ahora si $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] = 1$ y $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2})$. Sin embargo, esto es imposible: $\sqrt{3} \in \mathbb{Q}(\alpha)$, pero $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. En efecto, si $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, entonces $\sqrt{3} = a + b\sqrt{2}$ para algunos $a, b \in \mathbb{Q}$, pero en este caso $3 = a^2 + 2ab\sqrt{2} + 2b^2$, lo que demostraría que $\sqrt{2} \in \mathbb{Q}$.

Podemos concluir que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, $m_{\alpha, \mathbb{Q}} = f$ y

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) \cong \mathbb{Q}[X]/(X^4 - 10X^2 + 1).$$

Notamos que sin estas consideraciones, no es obvio por qué $f = X^4 - 10X^2 + 1$ es un polinomio irreducible en $\mathbb{Q}[X]$. ▲

* * *

He aquí una caracterización de los elementos algebraicos.

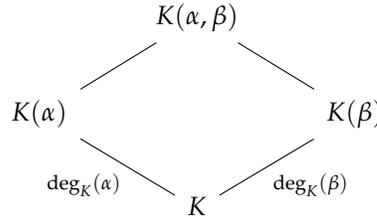
14.2.18. Observación. Para una extensión L/K un elemento $\alpha \in L$ es algebraico sobre K si y solo si $\deg_K(\alpha) := [K(\alpha) : K] < \infty$.

Demostración. Ya hemos visto que si α es algebraico, entonces existe un polinomio mínimo y $[K(\alpha) : K] = \deg m_{\alpha, K} < \infty$. Viceversa, si $[K(\alpha) : K] < \infty$, entonces la extensión $K(\alpha)/K$ es algebraica, como notamos en 14.2.5. ■

14.2.19. Observación. Sea L/K una extensión de cuerpos y $\alpha, \beta \in L$ elementos de grado finito sobre K . Entonces,

$$[K(\alpha, \beta) : K] \leq \deg_K(\alpha) \cdot \deg_K(\beta).$$

Demostración. Consideremos las extensiones



La desigualdad de 14.2.11 aplicada a las extensiones $K \subseteq K(\alpha) \subseteq K(\alpha, \beta)$ y $\beta \in K(\alpha, \beta)$ nos da

$$[(K(\alpha))(\beta) : K(\alpha)] \leq [K(\beta) : K],$$

de donde

$$[K(\alpha, \beta) : K] = [(K(\alpha))(\beta) : K(\alpha)] \cdot [K(\alpha) : K] \leq [K(\beta) : K] \cdot [K(\alpha) : K].$$

■

Por inducción se sigue que en general,

$$[K(\alpha_1, \dots, \alpha_n) : K] \leq \deg_K(\alpha_1) \cdots \deg_K(\alpha_n).$$

14.2.20. Comentario. Puede suceder que el grado $[K(\alpha, \beta) : K]$ es estrictamente menor que el producto $\deg_K(\alpha) \cdot \deg_K(\beta)$. Para un contraejemplo trivial, considere $\alpha = \beta$.

14.2.21. Ejemplo. Volvamos al ejemplo 14.1.15. Hemos visto que

$$\mathbb{Q}(\zeta_3, \sqrt[3]{2}) = \mathbb{Q}(\zeta_3 + \sqrt[3]{2}).$$

Tenemos

$$[\mathbb{Q}(\zeta_3 + \sqrt[3]{2}) : \mathbb{Q}] \leq \deg_{\mathbb{Q}}(\zeta_3) \cdot \deg_{\mathbb{Q}}(\sqrt[3]{2}) = 2 \cdot 3 = 6.$$

Pero el grado $[\mathbb{Q}(\zeta_3 + \sqrt[3]{2}) : \mathbb{Q}]$ tiene que ser divisible por 2 y 3, así que es exactamente 6. ▲

Tenemos la siguiente caracterización de extensiones finitas.

14.2.22. Proposición. Una extensión L/K es finita si y solo si $L = K(\alpha_1, \dots, \alpha_n)$, donde $\alpha_1, \dots, \alpha_n \in K$ es un número finito de elementos algebraicos sobre K .

Demostración. Si L/K es una extensión finita de grado n , sea $\alpha_1, \dots, \alpha_n$ una base de L sobre K . Tenemos $\deg_K(\alpha_i) \leq n$, así que $\alpha_1, \dots, \alpha_n$ son algebraicos. Está claro que $L = K(\alpha_1, \dots, \alpha_n)$.

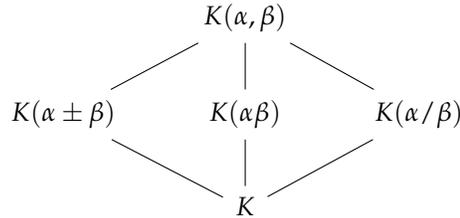
Viceversa, si $L = K(\alpha_1, \dots, \alpha_n)$ donde $\alpha_1, \dots, \alpha_n$ son algebraicos sobre K , entonces

$$[L : K] \leq \deg_K(\alpha_1) \cdots \deg_K(\alpha_n),$$

así que la extensión es finita. ■

14.2.23. Proposición. Para una extensión de cuerpos L/K sean $\alpha, \beta \in L$ elementos algebraicos sobre K . Entonces, $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ (donde $\beta \neq 0$) son también algebraicos sobre K .

Demostración. Si α y β son algebraicos sobre K , entonces la extensión $K(\alpha, \beta)/K$ es finita. Luego, tenemos



así que $K(\alpha \pm \beta), K(\alpha\beta), K(\alpha/\beta)$ son también extensiones finitas de K . Toda extensión finita es algebraica, lo que implica en particular que los números $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ son algebraicos sobre K . ■

14.2.24. Comentario. Si α y β son algebraicos, aunque la prueba de arriba nos dice que $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ son también algebraicos, esta no revela cómo obtener los polinomios mínimos de $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ a partir de los polinomios mínimos $m_{\alpha,K}$ y $m_{\beta,K}$. Veremos esto más adelante.

14.2.25. Corolario. Para una extensión de cuerpos L/K los elementos de L que son algebraicos sobre K forman un subcuerpo de L .

Terminemos por un ejemplo de extensiones algebraicas infinitas.

14.2.26. Ejemplo. Según 14.2.25, todos los números complejos que son algebraicos sobre \mathbb{Q} forman un cuerpo. Denotémoslo por $\overline{\mathbb{Q}}$. Notamos que $\sqrt[n]{2} \in \overline{\mathbb{Q}}$ y

$$\deg_{\mathbb{Q}}(\sqrt[n]{2}) = n.$$

Esto implica que la extensión $\overline{\mathbb{Q}}/\mathbb{Q}$ es infinita. En efecto, si $[L : K] < \infty$, entonces $\deg_K(\alpha) \mid [L : K]$ para todo $\alpha \in L$. En nuestro caso, la existencia de elementos $\alpha \in \overline{\mathbb{Q}}$ de grado arbitrariamente grande nos permite concluir que $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Puesto que $\sqrt[n]{2} \in \mathbb{R}$, esto demuestra que el cuerpo $\overline{\mathbb{Q}} \cap \mathbb{R}$ es una extensión algebraica infinita de \mathbb{Q} .

De hecho, lo que probamos es que la extensión

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \sqrt[5]{2}, \dots)/\mathbb{Q}$$

es infinita. Tenemos un cuerpo generado por elementos algebraicos sobre \mathbb{Q} , pero el número de estos generadores es infinito. ▲

14.3 Extensiones de grado 2

Sea K un cuerpo y sea L/K una extensión de grado 2. Para un elemento $\alpha \in L$ tal que $\alpha \notin K$ tenemos necesariamente $1 < [K(\alpha) : K] \leq [L : K] = 2$, así que $L = K(\alpha)$ y el polinomio mínimo de α es de grado 2:

$$m_{\alpha, K} = X^2 + bX - c$$

para algunos $b, c \in K$. Hay dos casos diferentes.

1) Si $b = 0$, entonces se trata de la extensión

$$K(\alpha) = K(\sqrt{c}) \cong K[X]/(X^2 - c).$$

2) Si $b \neq 0$, podemos hacer un cambio de variables

$$\begin{aligned} K[Y] &\xrightarrow{\cong} K[X], \\ Y &\mapsto X/b, \\ Y^2 + Y - c/b^2 &\mapsto \frac{1}{b^2} (X^2 + bX - c) \end{aligned}$$

que nos da un isomorfismo

$$K[X]/(X^2 + bX - c) \cong K[Y]/(Y^2 + Y - c') \cong K(\beta)$$

donde $c' := c/b^2 \in K$ y β denota la imagen de Y en el cociente. Notamos que en este caso $\beta^2 \notin K$, puesto que $\beta = c' - \beta^2 \notin K$.

Cuando $\text{char } K \neq 2$, el caso 2) siempre se reduce al caso 1): se puede hacer un cambio de variables ("completar el cuadrado")

$$\begin{aligned} K[Y] &\xrightarrow{\cong} K[X], \\ Y &\mapsto X + \frac{b}{2}, \\ Y^2 - c - \frac{b^2}{4} &\mapsto \left(X + \frac{b}{2}\right)^2 - c - \frac{b^2}{4} = X^2 + bX - c, \end{aligned}$$

así que

$$K[Y]/(Y^2 - c') \cong K[X]/(X^2 + bX - c),$$

donde $c' := c + b^2/4 \in K$.

Cuando $\text{char } K = 2$, los casos 1) y 2) son diferentes: en el caso 1) todo cuadrado de $x + y\sqrt{-c} \in K(\sqrt{c})$ pertenece a K :

$$(x + y\sqrt{c})^2 = x^2 + cy^2 \in K$$

(¡usando que $\text{char } K = 2$!), mientras que en el caso 2), tenemos $\beta^2 \notin K$.

Podemos concluir que si $\text{char } K \neq 2$, entonces toda extensión de grado 2 es de la forma $K(\sqrt{d})/K$ para algún $d \in K$ que no es un cuadrado en K .

Si $\text{char } K = 2$, puede haber extensiones distintas de la forma $K[X]/(Y^2 + Y + c)$, donde $c \in K$ e $Y^2 + Y + c \in K[Y]$ es algún polinomio irreducible. Por ejemplo, si $K = \mathbb{F}_2$, el polinomio $Y^2 + Y + 1$ es irreducible en $\mathbb{F}_2[Y]$. De hecho, \mathbb{F}_2 no puede tener extensiones de la forma $\mathbb{F}_2(\sqrt{c})$: todos los elementos de \mathbb{F}_2 son cuadrados.

En general, si $K = \mathbb{F}_{2^n}$ es un cuerpo finito de 2^n elementos*, entonces el homomorfismo

$$\mathbb{F}_{2^n}^\times \rightarrow \mathbb{F}_{2^n}^\times, \quad x \mapsto x^2$$

es sobreyectivo. Esto se sigue del hecho de que $\mathbb{F}_{2^n}^\times$ sea un grupo cíclico de orden impar $2^n - 1$. Por esto todos los elementos de \mathbb{F}_{2^n} son cuadrados.

14.4 Cuerpos ciclotómicos

Hemos probado en el capítulo anterior que los polinomios ciclotómicos Φ_{p^k} son irreducibles en $\mathbb{Q}[X]$ usando el criterio de Eisenstein. Para probar el caso general de Φ_n para cualquier n , podemos usar las factorizaciones de Φ_n en $\mathbb{F}_p[X]$. De hecho, sería más fácil considerar las factorizaciones de

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

Por ejemplo, para $n = p$ se tiene

$$X^p - 1 = (X - 1)^p.$$

Si $n = p - 1$, entonces el pequeño teorema de Fermat nos dice que cualquier elemento $x \in \mathbb{F}_p^\times$ satisface $x^{p-1} = 1$, así que se tiene

$$X^{p-1} - 1 = (X - 1)(X - 2) \cdots (X - (p - 1)).$$

Normalmente los polinomios $X^n - 1$ y en particular Φ_n se vuelven *reducibles* en $\mathbb{F}_p[X]$.

Primero, necesitamos la siguiente construcción.

14.4.1. Definición. Sea k un cuerpo. Para un polinomio

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_2 X^2 + a_0 \in k[X]$$

su *derivada* viene dada por

$$f' = n a_n X^{n-1} + (n - 1) a_{n-1} X^{n-2} + \cdots + a_2 X + a_1.$$

Dejo al lector como un ejercicio comprobar que esta definición cumple las propiedades habituales: para cualesquiera $f, g \in k[X]$ se cumple

$$(f + g)' = f' + g', \quad (fg)' = f'g + fg'.$$

14.4.2. Lema. En la factorización de $X^n - 1$ en $\mathbb{F}_p[X]$ hay factores repetidos si y solamente si $p \mid n$.

Demostración. Primero notamos que si $p \mid n$, entonces $n = pm$ para algún m y luego en $\mathbb{F}_p[X]$ se tiene

$$(X^n - 1) = ((X^m)^p - 1^p) = (X^m - 1)^p.$$

Ahora supongamos que en $\mathbb{F}_p[X]$

$$X^n - 1 = f^2 g$$

para algunos polinomios no constantes $f, g \in \mathbb{F}_p[X]$. Luego, tomando las derivadas se obtiene

$$n X^{n-1} = 2 f f' g + f^2 g' = f (2 f' g + f g').$$

*Véase el siguiente capítulo.

Entonces, $f \mid (X^n - 1)$ y $f \mid nX^{n-1}$. Si $p \nmid n$, esto es imposible: en este caso

$$1 = -1 \cdot (X^n - 1) + \frac{1}{n} X \cdot (nX^{n-1}),$$

así que

$$\text{mcd}(X^n - 1, nX^{n-1}) = 1.$$

■

La siguiente página contiene algunas factorizaciones de $X^n - 1$ en $\mathbb{F}_p[X]$. El lector debe fijarse en los factores repetidos.

Factorizaciones en $\mathbb{Z}[X]$

$$\begin{aligned}
X^2 - 1 &= (X - 1)(X + 1), \\
X^3 - 1 &= (X - 1)(X^2 + X + 1), \\
X^4 - 1 &= (X - 1)(X + 1)(X^2 + 1), \\
X^5 - 1 &= (X - 1)(X^4 + X^3 + X^2 + X + 1), \\
X^6 - 1 &= (X - 1)(X + 1)(X^2 + X + 1)(X^2 - X + 1), \\
X^7 - 1 &= (X - 1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1), \\
X^8 - 1 &= (X - 1)(X + 1)(X^2 + 1)(X^4 + 1), \\
X^9 - 1 &= (X - 1)(X^2 + X + 1)(X^6 + X^3 + 1), \\
X^{10} - 1 &= (X - 1)(X + 1)(X^4 + X^3 + X^2 + X + 1)(X^4 - X^3 + X^2 - X + 1).
\end{aligned}$$

Factorizaciones en $\mathbb{F}_p[X]$

$\frac{X^2 - 1}{p = 2: (X + 1)^2}$	$\frac{X^6 - 1}{p = 2: (X + 1)^2 (X^2 + X + 1)^2}$
$p = 3: (X - 1)(X + 1)$	$p = 3: (X + 1)^3 (X + 2)^3$
$p = 5: (X - 1)(X + 1)$	$p = 5: (X - 1)(X + 1)(X^2 + X + 1)(X^2 - X + 1)$
$p = 7: (X - 1)(X + 1)$	$p = 7: (X - 1)(X - 2)(X - 3)(X - 4)(X - 5)(X - 6)$
$p = 11: (X - 1)(X + 1)$	$p = 11: (X - 1)(X + 1)(X^2 + X + 1)(X^2 - X + 1)$
$\frac{X^3 - 1}{p = 2: (X + 1)(X^2 + X + 1)}$	$\frac{X^7 - 1}{p = 2: (X + 1)(X^3 + X + 1)(X^3 + X^2 + 1)}$
$p = 3: (X - 1)^3$	$p = 3: (X - 1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)$
$p = 5: (X - 1)(X^2 + X + 1)$	$p = 5: X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$
$p = 7: (X - 1)(X - 2)(X - 4)$	$p = 7: (X - 1)^7$
$p = 11: (X - 1)(X^2 + X + 1)$	$p = 11: (X - 1)(X^3 + 5X^2 + 4X - 1)(X^3 + 7X^2 + 6X - 1)$
$\frac{X^4 - 1}{p = 2: (X + 1)^4}$	$\frac{X^8 - 1}{p = 2: (X + 1)^8}$
$p = 3: (X - 1)(X + 1)(X^2 + 1)$	$p = 3: (X - 1)(X + 1)(X^2 + 1)(X^2 + X - 1)(X^2 - X - 1)$
$p = 5: (X - 1)(X - 2)(X - 3)(X - 4)$	$p = 5: (X - 2)(X - 3)(X - 4)(X^2 - 2)(X^2 - 3)$
$p = 7: (X - 1)(X + 1)(X^2 + 1)$	$p = 7: (X - 1)(X + 1)(X^2 + 1)(X^2 + 4X + 1)(X^2 - 4X + 1)$
$p = 11: (X - 1)(X + 1)(X^2 + 1)$	$p = 11: (X - 1)(X + 1)(X^2 + 1)(X^2 + 3X - 1)(X^2 - 3X - 1)$
$\frac{X^5 - 1}{p = 2: (X + 1)(X^4 + X^3 + X^2 + X + 1)}$	$\frac{X^9 - 1}{p = 2: (X + 1)(X^2 + X + 1)(X^6 + X^3 + 1)}$
$p = 3: (X - 1)(X^4 + X^3 + X^2 + X + 1)$	$p = 3: (X - 1)^9$
$p = 5: (X - 1)^5$	$p = 5: (X - 1)(X^2 + X + 1)(X^6 + X^3 + 1)$
$p = 7: (X - 1)(X^4 + X^3 + X^2 + X + 1)$	$p = 7: (X - 1)(X - 2)(X - 1)(X^3 - 2)(X^3 - 4)$
$p = 11: (X - 1)(X - 3)(X - 4)(X - 5)(X - 9)$	$p = 11: (X - 1)(X^2 + X + 1)(X^6 + X^3 + 1)$
$\frac{X^{10} - 1}{p = 2: (X + 1)^2 (X^4 + X^3 + X^2 + X + 1)^2}$	
$p = 3: (X - 1)(X + 1)(X^4 + X^3 + X^2 + X + 1)(X^4 - X^3 + X^2 - X + 1)$	
$p = 5: (X - 1)^5 (X + 1)^5$	
$p = 7: (X - 1)(X + 1)(X^4 + X^3 + X^2 + X + 1)(X^4 - X^3 + X^2 - X + 1)$	
$p = 11: (X - 1)(X - 2)(X - 3)(X - 4)(X - 5)(X - 6)(X - 7)(X - 8)(X - 9)(X - 10)$	

14.4.3. Lema. Para $g \in \mathbb{F}_p[X]$ se cumple $g(X^p) = g^p$.

Demostración. Usando la fórmula del binomio en característica p y el pequeño teorema de Fermat $a^p = a$ para todo $a \in \mathbb{F}_p$, tenemos

$$(a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0)^p = a_n (X^p)^n + a_{n-1} (X^p)^{n-1} + \cdots + a_1 X^p + a_0.$$

■

14.4.4. Teorema (Gauss). El polinomio ciclotómico Φ_n es irreducible en $\mathbb{Z}[X]$ para cualquier n .

Demostración. Escribamos

$$\Phi_n = fg$$

para algunos polinomios $f, g \in \mathbb{Z}[X]$ (necesariamente mónicos), donde f es irreducible. Sea ζ una raíz n -ésima primitiva. Tenemos entonces

$$\Phi_n(\zeta) = f(\zeta)g(\zeta) = 0.$$

Esto implica que $f(\zeta) = 0$ o $g(\zeta) = 0$. Puesto que f no es constante, algunas de las raíces n -ésimas primitivas deben ser raíces de f , y nuestro objetivo es probar que todas lo son.

Asumamos entonces que ζ es una raíz de f . Siendo un polinomio mónico irreducible, f debe ser el polinomio mínimo de ζ sobre \mathbb{Q} . Sea p un número primo tal que $p \nmid n$. Entonces, ζ^p es también una raíz n -ésima primitiva y

$$\Phi_n(\zeta^p) = f(\zeta^p)g(\zeta^p) = 0.$$

Asumamos que $g(\zeta^p) = 0$. Entonces, por las propiedades del polinomio mínimo, el polinomio $g(X^p)$ tiene que ser divisible por f en $\mathbb{Z}[X]$:

$$g(X^p) = fh \quad \text{para algún } h \in \mathbb{Z}[X].$$

Luego, reduciendo módulo p y aplicando 14.4.3, se obtiene

$$\bar{g}^p = \bar{f}\bar{h} \quad \text{en } \mathbb{F}_p[X].$$

Pero esto significa que \bar{f} y \bar{h} tienen un factor común en su factorización en $\mathbb{F}_p[X]$, así que $\bar{\Phi}_n = \bar{f}\bar{g}$ tiene un factor repetido en su factorización. Esto implica que la factorización de

$$X^n - 1 = \prod_{d|n} \bar{\Phi}_d$$

tiene un factor repetido, pero como vimos en 14.4.2, esto es imposible cuando $p \nmid n$. Esta contradicción nos permite concluir que $f(\zeta^p) = 0$.

Entonces, para cualquier primo p tal que $p \nmid n$ se tiene $f(\zeta^p) = 0$. Ahora todas las raíces n -ésimas primitivas son de la forma ζ^k donde $\text{mcd}(n, k) = 1$. Podemos factorizar entonces $k = p_1 \cdots p_s$ donde p_i son primos (no necesariamente diferentes) tales que $p_i \nmid n$, y luego

$$\zeta^k = (((\zeta^{p_1})^{p_2}) \cdots)^{p_s}.$$

El argumento de arriba nos dice que $f(\zeta^{p_1}) = 0$. Luego, el mismo argumento aplicado a ζ^{p_1} demuestra que $f((\zeta^{p_1})^{p_2}) = 0$, etcétera.

Entonces, todas las raíces n -ésimas primitivas son raíces de f y por ende $g = 1$. ■

14.4.5. Definición. Para $n = 1, 2, 3, 4, \dots$ el n -ésimo cuerpo ciclotómico es el cuerpo $\mathbb{Q}(\zeta_n)$, donde

$$\zeta_n := e^{2\pi\sqrt{-1}/n}.$$

Los cuerpos ciclotómicos tienen mucha importancia en la teoría de números. De los resultados anteriores siguen las siguientes propiedades básicas.

1) Dado que el polinomio ciclotómico $\Phi_n \in \mathbb{Z}[X]$ es un polinomio mónico irreducible y $\Phi_n(\zeta_n) = 0$, tenemos

$$m_{\zeta_n, \mathbb{Q}} = \Phi_n.$$

2) Hay un isomorfismo

$$\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[X]/(\Phi_n).$$

3) El grado de la extensión ciclotómica $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ viene dado por la función ϕ de Euler:

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n = \phi(n).$$

14.4.6. Observación. Si $m \mid n$, entonces $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n)$.

Demostración. Si $m \mid n$, entonces $\zeta_m = \zeta_n^{n/m} \in \mathbb{Q}(\zeta_n)$. ■

Una pregunta natural es si los cuerpos $\mathbb{Q}(\zeta_n)$ son diferentes para diferente n . Trivialmente,

$$\mathbb{Q}(\zeta_2) = \mathbb{Q}(\zeta_1) = \mathbb{Q},$$

pero un momento de reflexión nos da otros ejemplos más interesantes: se tiene

$$\zeta_6 = \zeta_7^2 = \zeta_6^3 \zeta_6^4 = \zeta_2 \zeta_3^2 = -\zeta_3^2 \in \mathbb{Q}(\zeta_3),$$

así que $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3)$. En general, tenemos el siguiente resultado.

14.4.7. Observación. Si m es un número impar, entonces $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$.

Demostración. Tenemos la inclusión obvia $\zeta_m = \zeta_{2m}^2 \in \mathbb{Q}(\zeta_{2m})$, y por otro lado, escribiendo $m = 2k + 1$,

$$\zeta_{2m} = \zeta_{2m}^{(2k+1)-2k} = \zeta_{2m}^m (\zeta_{2m}^2)^{-k} = \zeta_2 \zeta_m^{-k} = -\zeta_m^{-k} \in \mathbb{Q}(\zeta_m). \quad \blacksquare$$

14.4.8. Ejemplo. Tenemos

$$\mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3), \quad \mathbb{Q}(\zeta_{10}) = \mathbb{Q}(\zeta_5), \quad \mathbb{Q}(\zeta_{14}) = \mathbb{Q}(\zeta_7), \quad \mathbb{Q}(\zeta_{18}) = \mathbb{Q}(\zeta_9), \quad \dots \quad \blacktriangle$$

14.4.9. Comentario. Esto se refleja de la siguiente manera en los polinomios ciclotómicos: para $m > 1$ impar

$$\Phi_{2m}(X) = \Phi_m(-X),$$

mientras que para $m = 1$, tenemos $\Phi_1 = X - 1$ y $\Phi_2 = X + 1$, así que

$$\Phi_2(X) = -\Phi_1(-X).$$

(Haga el ejercicio 14.8.) Por ejemplo,

$$\begin{aligned} \Phi_3 &= X^2 + X + 1, & \Phi_6 &= X^2 - X + 1, \\ \Phi_5 &= X^4 + X^3 + X^2 + X + 1, & \Phi_{10} &= X^4 - X^3 + X^2 - X + 1, \\ \Phi_7 &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1, & \Phi_{14} &= X^6 - X^5 + X^4 - X^3 + X^2 - X + 1. \end{aligned}$$

La propiedad 14.4.7 se cumple por la razón banal de que $\zeta_2 = -1 \in \mathbb{Q}$. Resulta que en otras situaciones los cuerpos ciclotómicos no coinciden. Para probarlo, podemos investigar cuáles raíces de la unidad están en $\mathbb{Q}(\zeta_m)$.

14.4.10. Lema. *Si m es par y $m \mid r$, entonces $\phi(r) \leq \phi(m)$ implica $r = m$.*

Demostración. Primero, notamos que para cualesquiera $a, m \geq 1$ se cumple

$$\phi(am) = \frac{\phi(a) \phi(m) \text{mcd}(a, m)}{\phi(\text{mcd}(a, m))}$$

—esto se sigue de las fórmulas

$$\phi(a) = a \prod_{p|a} \left(1 - \frac{1}{p}\right),$$

$$\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right),$$

$$\phi(am) = am \prod_{p|am} \left(1 - \frac{1}{p}\right),$$

$$\phi(\text{mcd}(a, m)) = \text{mcd}(a, m) \prod_{p|a, p|m} \left(1 - \frac{1}{p}\right).$$

(Notamos que cuando a y m son coprimos, se tiene $\text{mcd}(a, m) = \phi(\text{mcd}(a, m)) = 1$ y se recupera la fórmula conocida.) Ahora para m par y $m \mid r$, asumamos que $m < r$, así que $r = am$ para algún $a > 1$. Tenemos

$$\phi(r) = \phi(am) = \frac{\phi(a) \phi(m) \text{mcd}(a, m)}{\phi(\text{mcd}(a, m))}.$$

Si $a = 2$, entonces $\phi(a) = \phi(2) = 1$ y $\text{mcd}(a, m) = 2$. Luego,

$$\frac{\phi(a) \phi(m) \text{mcd}(a, m)}{\phi(\text{mcd}(a, m))} = 2 \phi(m) > \phi(m).$$

Si $a > 2$, entonces $\phi(a) \geq 2$, y luego

$$\frac{\phi(a) \phi(m) \text{mcd}(a, m)}{\phi(\text{mcd}(a, m))} \geq \phi(a) \phi(m) > \phi(m).$$

En ambos casos, $m < r$ implica $\phi(m) < \phi(r)$. ■

14.4.11. Proposición. *Las raíces de la unidad en el cuerpo $\mathbb{Q}(\zeta_m)$ son precisamente*

$$\mu_\infty(\mathbb{C}) \cap \mathbb{Q}(\zeta_m)^\times = \begin{cases} \mu_m(\mathbb{C}), & \text{si } m \text{ es par,} \\ \mu_{2m}(\mathbb{C}), & \text{si } m \text{ es impar.} \end{cases}$$

Demostración [Mar1977]. Si $m = 2k + 1$ es un número impar, entonces ya notamos en 14.4.7 que $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$. Por esto sería suficiente considerar el caso cuando m es un número par.

Tenemos $\zeta_m \in \mathbb{Q}(\zeta_m)$, y por ende todas las raíces m -ésimas de la unidad, siendo potencias de ζ_m , están en $\mathbb{Q}(\zeta_m)$:

$$\mu_m(\mathbb{C}) \subseteq \mu_\infty(\mathbb{C}) \cap \mathbb{Q}(\zeta_m)^\times.$$

Hay que ver que en $\mathbb{Q}(\zeta_m)$ no hay raíces de la unidad de orden $k \nmid m$. Bastaría considerar las raíces k -ésimas primitivas.

Supongamos que $\zeta_k^\ell \in \mathbb{Q}(\zeta_m)$ donde ζ_k^ℓ es una raíz k -ésima primitiva; es decir, $\text{mcd}(k, \ell) = 1$. Pongamos

$$r := \text{mcm}(k, m) = \frac{km}{d}, \quad d = \text{mcd}(k, m).$$

Luego,

$$\text{mcd}(k, \ell m) = \text{mcd}(k, m) = d,$$

lo que significa que existen $a, b \in \mathbb{Z}$ tales que

$$d = ak + b\ell m.$$

Ahora,

$$\zeta_r = \zeta_{km}^d = \zeta_{km}^{ak+b\ell m} = \zeta_{km}^{ak} \zeta_{km}^{b\ell m} = \zeta_m^a (\zeta_k^\ell)^b \in \mathbb{Q}(\zeta_m)$$

y

$$\phi(r) \leq \phi(m), \quad m \text{ es par}, \quad m \mid r,$$

así que el lema 14.4.10 nos permite concluir que

$$r = \text{mcd}(k, m) = m,$$

lo que significa que $k \mid m$. ■

14.4.12. Corolario. Si $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$ para $m < n$, entonces m es impar y $n = 2m$.

Demostración. Si m es par, entonces las raíces de la unidad en $\mathbb{Q}(\zeta_m)$ son de orden m , mientras que las raíces de la unidad en $\mathbb{Q}(\zeta_n)$ son de orden n o $2n$, dependiendo de la paridad de n . Pero en ambos casos la hipótesis $m < n$ nos lleva a una contradicción.

Entonces, m es impar y las raíces de la unidad en $\mathbb{Q}(\zeta_m)$ son de orden m . La única posibilidad es $n = 2m$. ■

14.4.13. Comentario. Para enumerar los cuerpos ciclotómicos sin redundancias, a veces se consideran $\mathbb{Q}(\zeta_n)$ tales que $n \not\equiv 2 \pmod{4}$.

14.5 Perspectiva: números trascendentes

Hasta el momento, hemos estudiado las propiedades de extensiones algebraicas, con énfasis en los ejemplos de números algebraicos sobre \mathbb{Q} . Es extremadamente difícil probar que algún número específico es trascendente sobre \mathbb{Q} . Voy a mencionar solo algunos resultados clásicos y conjeturas.

- 1) El primer ejemplo explícito (aunque artificial) de un número trascendente fue construido por Liouville en 1844. Se dice que $\alpha \in \mathbb{R}$ es un **número de Liouville** si para todo entero positivo n existen $p, q \in \mathbb{Z}$, $q > 1$, tales que

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^n}.$$

Se puede demostrar que ningún número algebraico sobre \mathbb{Q} puede cumplir esta propiedad. Por ejemplo, el número

$$\alpha = \sum_{k \geq 1} \frac{1}{10^{k!}} = 0,110001 \underbrace{00000000000000000}_{17 \text{ ceros}} 1000 \dots$$

es un número de Liouville, y por ende es trascendente.

- 2) Lindemann* probó en 1882 que e^α es trascendente sobre \mathbb{Q} para cualquier número algebraico no nulo α . Para $\alpha = 1$ esto en particular establece la trascendencia de e . Para deducir la trascendencia de π , notamos que si π fuera algebraico, entonces $\pi\sqrt{-1}$ también lo sería y luego $e^{\pi\sqrt{-1}} = -1$ sería trascendente, lo que es absurdo.

De la misma manera del teorema de Lindemann se deduce la trascendencia de $\cos \alpha$, $\sin \alpha$, $\tan \alpha$ para cualquier número algebraico $\alpha \neq 0$ y la trascendencia de $\log \alpha$ para cualquier número algebraico $\alpha \neq 0, 1$.

- 3) Para la función zeta de Riemann

$$\zeta(s) := \sum_{n \geq 1} \frac{1}{n^s}, \quad (\operatorname{Re} s > 1)$$

Euler calculó que para cualquier $k = 1, 2, 3, \dots$ se tiene

$$\zeta(2k) := 1 + \frac{1}{2^{2k}} + \frac{1}{3^{2k}} + \frac{1}{4^{2k}} + \dots = (-1)^{k+1} B_{2k} \frac{2^{2k-1}}{(2k)!} \pi^{2k},$$

donde B_{2k} son ciertos números racionales, llamados los **números de Bernoulli**. Por ejemplo,

$$\zeta(2) = \frac{\pi^2}{6} \approx 1,644934 \dots,$$

$$\zeta(4) = \frac{\pi^4}{90} \approx 1,082323 \dots,$$

$$\zeta(6) = \frac{\pi^6}{945} \approx 1,017343 \dots,$$

$$\zeta(8) = \frac{\pi^8}{9450} \approx 1,004077 \dots,$$

$$\zeta(10) = \frac{\pi^{10}}{93\,555} \approx 1,000994 \dots,$$

$$\zeta(12) = \frac{691 \pi^{12}}{638\,512\,875} \approx 1,000246 \dots$$

Se supone que los números $\zeta(3), \zeta(5), \zeta(7), \zeta(9), \zeta(11), \dots$ son también trascendentes, pero a diferencia de los $\zeta(2k)$, entre los $\zeta(2k+1)$ no hay ninguna relación algebraica para diferentes k . Sin embargo, hasta el momento no se conoce ni siquiera si los $\zeta(2k+1)$ son irracionales. Para $\zeta(3)$ esto fue establecido en 1977 por el matemático francés ROGER APÉRY y hay impresionantes resultados más recientes sobre la irracionalidad. Por ejemplo el matemático francés TANGUY RIVOAL demostró en 2000 que entre los números $\zeta(3), \zeta(7), \zeta(9), \dots$ hay una infinidad de irracionales, mientras que el matemático ruso WADIM ZUDILIN demostró en 2001 que por lo menos un número entre $\zeta(5), \zeta(7), \zeta(9)$ y $\zeta(11)$ es irracional (¡y la prueba no revela cuál!). Sin embargo, parece que la humanidad está muy lejos de probar la trascendencia de los $\zeta(2k+1)$.

- 4) La serie armónica $\sum_{k \geq 1} \frac{1}{k}$ diverge lentamente, pero el límite

$$\gamma := \lim_{n \rightarrow \infty} \left(\sum_{1 \leq k \leq n} \frac{1}{k} - \log n \right)$$

*FERDINAND VON LINDEMANN (1852–1939), matemático alemán, conocido principalmente por sus pruebas de la trascendencia de e y π . Director de tesis de Hilbert.

existe. El número $\gamma = 0,5772156649\dots$ se conoce como la **constante de Euler–Mascheroni**** y aparece en muchos contextos importantes, inclusive aritméticos. Por ejemplo, el **tercer teorema de Mertens*** afirma que

$$\lim_{n \rightarrow \infty} \log n \prod_{p \leq n} \left(1 - \frac{1}{p}\right) = e^{-\gamma},$$

donde el producto se toma sobre los primos menores que n .

Otra aparición de la constante de Euler–Mascheroni es la serie de Laurent para la función zeta de Riemann

$$\zeta(s) = \frac{1}{s-1} + \sum_{n \geq 0} \frac{(-1)^n}{n!} \gamma_n (s-1)^n,$$

donde $\gamma_0 = \gamma$.

Se supone que el número γ es trascendente, pero hasta el momento no ha sido probado ni siquiera que es irracional.

Los números trascendentes se estudian en la **teoría de números trascendente**, mientras que los números algebraicos se estudian en la **teoría de números algebraica**. En este curso, naturalmente, nos van a interesar los números algebraicos. *Para conocer el lado trascendente*, el lector puede consultar el libro de texto [Bak1990].

14.6 La norma, traza y polinomio característico

Para endender mejor esta sección, el lector debe de revisar el apéndice C para las definiciones y resultados relevantes de álgebra lineal. Sea L/K una extensión finita de grado n . Para $\alpha \in L$ consideremos la aplicación de multiplicación por α sobre L :

$$\mu_\alpha : L \rightarrow L, \quad x \mapsto \alpha x.$$

Esto es un endomorfismo del espacio K -vectorial L . Notamos que para cualesquiera $\alpha, \beta \in L$, $a, b \in K$ se cumple

$$\mu_{\alpha\beta} = \mu_\alpha \circ \mu_\beta, \quad \mu_{a\alpha+b\beta} = a\mu_\alpha + b\mu_\beta.$$

14.6.1. Definición. Sean L/K una extensión finita de cuerpos y $\alpha \in L$.

1) La **norma** y **traza** de α son el determinante y traza del endomorfismo $\mu_\alpha : L \rightarrow L$ respectivamente:

$$N_{L/K}(\alpha) := \det \mu_\alpha, \quad T_{L/K}(\alpha) := \text{tr} \mu_\alpha.$$

2) El **polinomio característico** de α es el polinomio característico de μ_α :

$$p_{\alpha, L/K} := p_{\mu_\alpha} := p_A := \det(X I_n - A) \in K[X],$$

donde $A \in M_n(K)$ es una matriz que representa a ϕ en alguna base (véase el apéndice C).

14.6.2. Comentario. La norma, traza y el polinomio característico no solamente dependen de α , sino también de la extensión L/K . Cuando la última está clara a partir del contexto, vamos a omitirla por simplicidad y escribir “ N, T, p_α ” en lugar de “ $N_{L/K}, T_{L/K}, p_{\alpha, L/K}$ ”.

**LORENZO MASCHERONI (1750–1800), matemático italiano.

*FRANZ MERTENS (1840–1927), teórico de números polaco.

14.6.3. Proposición. Si $[L : K] = n$, entonces para cualquier $\alpha \in L$ el polinomio característico de α es mónico de grado n :

$$p_{\alpha, L/K} = X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0.$$

Además,

$$a_{n-1} = -T_{L/K}(\alpha), \quad a_0 = (-1)^n N_{L/K}(\alpha).$$

Demostración. Esto es una propiedad general del polinomio característico, probada en el apéndice C: tenemos

$$p_{\alpha, L/K} := p_{\mu_\alpha} = X^n - \text{tr}(\mu_\alpha) X^{n-1} + \cdots + a_1 X + (-1)^n \det(\mu_\alpha).$$

■

14.6.4. Ejemplo. Para $a \in K$ la aplicación $\mu_a : L \rightarrow L$ se representa en cualquier base por la matriz escalar de $n \times n$

$$\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix},$$

así que

$$N_{L/K}(a) = a^n, \quad T_{L/K}(a) = na, \quad p_{a, L/K} = (X - a)^n.$$

▲

14.6.5. Ejemplo. Para un cuerpo K , sea $d \in K$ un elemento tal que d no es un cuadrado; es decir, el polinomio $X^2 - d$ es irreducible en $K[X]$. Consideremos la extensión

$$K(\sqrt{d}) = K[X]/(X^2 - d),$$

donde \sqrt{d} denota la imagen de X en el cociente. La extensión $K(\sqrt{d})/K$ tiene grado 2 y los elementos $1, \sqrt{d}$ forman una base de $K(\sqrt{d})$ como un espacio vectorial sobre K . Para un elemento fijo $\alpha = a + b\sqrt{d}$ tenemos

$$\alpha \cdot 1 = \alpha = a + b\sqrt{d}, \quad \alpha \cdot \sqrt{d} = db + a\sqrt{d},$$

así que la multiplicación por α sobre $K(\sqrt{d})$ corresponde a la matriz

$$A = \begin{pmatrix} a & db \\ b & a \end{pmatrix}.$$

Luego,

$$N(\alpha) = \det A = a^2 - db^2, \quad T(\alpha) = \text{tr} A = 2a.$$

El polinomio característico de la matriz de arriba es

$$p_\alpha = \det \begin{pmatrix} X - a & db \\ b & X - a \end{pmatrix} = (X - a)^2 - db^2 = X^2 - 2aX + a^2 - db^2 = X^2 - T(\alpha)X + N(\alpha).$$

▲

14.6.6. Ejemplo. Consideremos la extensión $K(\sqrt[3]{d})/K$ donde d no es un cubo en K ; es decir, el polinomio $X^3 - d$ es irreducible en $K[X]$. Esta es una extensión de grado 3 y como una base de $K(\sqrt[3]{d})$ sobre K se puede tomar

$$1, \quad \sqrt[3]{d}, \quad \sqrt[3]{d^2}.$$

Para el elemento $\sqrt[3]{d}$ calculamos la aplicación $\mu_{\sqrt[3]{d}}: K(\sqrt[3]{d}) \rightarrow K(\sqrt[3]{d})$:

$$1 \mapsto \sqrt[3]{d}, \quad \sqrt[3]{d} \mapsto \sqrt[3]{d^2}, \quad \sqrt[3]{d^2} \mapsto d.$$

Entonces, $\mu_{\sqrt[3]{d}}$ se representa en la base $1, \sqrt[3]{d}, \sqrt[3]{d^2}$ por la matriz

$$\begin{pmatrix} 0 & 0 & d \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

de donde

$$N(\sqrt[3]{d}) = d, \quad T(\sqrt[3]{d}) = 0.$$

El polinomio característico correspondiente es

$$\det \begin{pmatrix} X & 0 & -d \\ -1 & X & 0 \\ 0 & -1 & X \end{pmatrix} = X \det \begin{pmatrix} X & 0 \\ -1 & X \end{pmatrix} - d \det \begin{pmatrix} -1 & X \\ 0 & -1 \end{pmatrix} = X^3 - d.$$

(Note que la norma y traza de α también pueden extraerse de los coeficientes del polinomio característico.)
Por otro lado, la aplicación

$$\mu_{\sqrt[3]{d^2}} = \mu_{\sqrt[3]{d}} \circ \mu_{\sqrt[3]{d}}$$

se representa por la matriz

$$\begin{pmatrix} 0 & 0 & d \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & d \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & d & 0 \\ 0 & 0 & d \\ 1 & 0 & 0 \end{pmatrix},$$

de donde

$$N(\sqrt[3]{d^2}) = d^2, \quad T(\sqrt[3]{d^2}) = 0.$$

El polinomio característico correspondiente es

$$\det \begin{pmatrix} X & -d & 0 \\ 0 & X & -d \\ -1 & 0 & X \end{pmatrix} = X \det \begin{pmatrix} X & -d \\ 0 & X \end{pmatrix} + d \det \begin{pmatrix} 0 & -d \\ -1 & X \end{pmatrix} = X^3 - d^2.$$

▲

14.6.7. Proposición. Sea L/K una extensión finita. Para todo $\alpha \in L$ el polinomio característico de α tiene a α como su raíz:

$$p_{\alpha, L/K}(\alpha) = 0.$$

Demostración. Primero notamos que gracias a las identidades

$$\mu_\alpha \circ \mu_\beta = \mu_{\alpha\beta}, \quad a\mu_\alpha + b\mu_\beta = \mu_{a\alpha + b\beta}$$

para cualesquiera $\alpha, \beta \in L$, $a, b \in K$, se sigue que para cualquier polinomio

$$f = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_1 X + a_0 \in K[X]$$

se cumple

$$f(\mu_\alpha) := a_m \mu_\alpha^m + a_{m-1} \mu_\alpha^{m-1} + \cdots + a_1 \mu_\alpha + a_0 \text{id} = \mu_{f(\alpha)}.$$

Por simplicidad, escribamos “ p ” en lugar de “ $p_{\alpha, L/K}$ ”. Tenemos

$$\mu_{p(\alpha)} = p(\mu_\alpha) = 0$$

por el teorema de Cayley–Hamilton (véase el apéndice C). En particular,

$$p(\alpha) = \mu_{p(\alpha)}(1) = 0.$$

■

14.6.8. Corolario. Si $L = K(\alpha)$, entonces el polinomio característico $p_{\alpha, L/K}$ coincide con el polinomio mínimo $m_{\alpha, K}$.

Demostración. El polinomio característico es un polinomio mónico de grado $[L : K]$ que, como acabamos de ver, tiene a α como su raíz. Luego, si $L = K(\alpha)$, entonces $[L : K] = \deg_K(\alpha)$ y $p_{\alpha, K}$ debe ser el polinomio mínimo de α sobre K . ■

14.6.9. Ejemplo. Sean m y n dos enteros tales que m, n, mn no son cuadrados. En este caso

$$\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m} + \sqrt{n}), \quad [\mathbb{Q}(\sqrt{m}, \sqrt{n}) : \mathbb{Q}] = 4$$

(véase el ejercicio 14.7). Como una base se puede tomar

$$1, \sqrt{m}, \sqrt{n}, \sqrt{mn}.$$

Calculemos el polinomio característico de $\sqrt{m} + \sqrt{n}$. Tenemos

$$\begin{aligned} 1 \cdot (\sqrt{m} + \sqrt{n}) &= \sqrt{m} + \sqrt{n}, \\ \sqrt{m} \cdot (\sqrt{m} + \sqrt{n}) &= m + \sqrt{mn}, \\ \sqrt{n} \cdot (\sqrt{m} + \sqrt{n}) &= n + \sqrt{mn}, \\ \sqrt{mn} \cdot (\sqrt{m} + \sqrt{n}) &= n\sqrt{m} + m\sqrt{n}. \end{aligned}$$

Entonces, la multiplicación por $\sqrt{m} + \sqrt{n}$ en la base de arriba corresponde a la matriz

$$A = \begin{pmatrix} 0 & m & n & 0 \\ 1 & 0 & 0 & n \\ 1 & 0 & 0 & m \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Su polinomio característico viene dado por

$$\det \begin{pmatrix} X & -m & -n & 0 \\ -1 & X & 0 & -n \\ -1 & 0 & X & -m \\ 0 & -1 & -1 & X \end{pmatrix} = X^4 - 2(m+n)X^2 + (m-n)^2$$

(el ejercicio 14.7 da otro modo de obtener el mismo polinomio). Puesto que $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m} + \sqrt{n})$, lo que acabamos de encontrar es el polinomio mínimo de $\sqrt{m} + \sqrt{n}$ sobre \mathbb{Q} . ▲

Multiplicatividad de la norma, linealidad de la traza

14.6.10. Observación.

1) La norma $N_{L/K}: L \rightarrow K$ es multiplicativa: para cualesquiera $\alpha, \beta \in L$ se tiene

$$N_{L/K}(\alpha\beta) = N_{L/K}(\alpha) \cdot N_{L/K}(\beta).$$

2) La traza $T_{L/K}: L \rightarrow K$ es K -lineal: para cualesquiera $\alpha, \beta \in L, a, b \in K$ se tiene

$$T_{L/K}(a\alpha + b\beta) = a T_{L/K}(\alpha) + b T_{L/K}(\beta).$$

Demostración. Se sigue del hecho de que el determinante es multiplicativo y la traza es K -lineal:

$$N_{L/K}(\alpha\beta) = \det(\mu_{\alpha\beta}) = \det(\mu_\alpha \circ \mu_\beta) = \det(\mu_\alpha) \cdot \det(\mu_\beta) = N_{L/K}(\alpha) \cdot N_{L/K}(\beta),$$

y

$$T_{L/K}(a\alpha + b\beta) = T_{L/K}(\mu_{a\alpha+b\beta}) = \text{tr}(a\mu_\alpha + b\mu_\beta) = a \text{tr}(\mu_\alpha) + b \text{tr}(\mu_\beta) = a T_{L/K}(\alpha) + b T_{L/K}(\beta).$$

■

14.6.11. Ejemplo. Probemos que $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$. Asumamos que $\sqrt[3]{3} \in \mathbb{Q}(\sqrt[3]{2})$. Dado que

$$[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{6}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3,$$

en este caso tendríamos

$$\mathbb{Q}(\sqrt[3]{3}) = \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{6}) = K.$$

En particular, existen algunos $a, b, c \in \mathbb{Q}$ tales que

$$\sqrt[3]{3} = a + b\sqrt[3]{2} + c\sqrt[3]{4}.$$

En el ejemplo 14.6.6 hemos calculado que $T_{K/\mathbb{Q}}(\sqrt[3]{2}) = T_{K/\mathbb{Q}}(\sqrt[3]{4}) = 0$. De aquí se sigue que

$$T_{K/\mathbb{Q}}(\sqrt[3]{3}) = T_{K/\mathbb{Q}}(a) + b T_{K/\mathbb{Q}}(\sqrt[3]{2}) + c T_{K/\mathbb{Q}}(\sqrt[3]{4}) = 3a.$$

Luego, tenemos

$$\sqrt[3]{6} = a\sqrt[3]{2} + b\sqrt[3]{4} + 2c,$$

de donde

$$T_{K/\mathbb{Q}}(\sqrt[3]{6}) = 2T_{K/\mathbb{Q}}(c) = 6c.$$

Sin embargo, los cálculos de 14.6.6 aplicados a las extensiones $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$ y $\mathbb{Q}(\sqrt[3]{6})/\mathbb{Q}$ nos dicen que

$$T_{K/\mathbb{Q}}(\sqrt[3]{3}) = T_{K/\mathbb{Q}}(\sqrt[3]{6}) = 0.$$

Entonces, $a = c = 0$ y se tiene

$$\sqrt[3]{3} = b\sqrt[3]{2}.$$

Esto significa que el número $\sqrt[3]{3/2} = b$ es racional, pero no es el caso. Esta contradicción implica que $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$. ▲

14.6.12. Comentario. Para apreciar el argumento de arriba, el lector puede tratar de probar de manera directa que $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$, sin usar trazas.

14.6.13. Ejemplo. Consideremos la extensión $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$. Probemos que el número $1 + \sqrt{-5}$ no es un cuadrado en $\mathbb{Q}(\sqrt{-5})$; es decir, no existe $\alpha \in \mathbb{Q}(\sqrt{-5})$ tal que $\alpha^2 = 1 + \sqrt{-5}$. En efecto, en este caso tendríamos

$$N(\alpha)^2 = N(\alpha^2) = N(1 + \sqrt{-5}) = 1^2 + 5 \cdot 1^2 = 6,$$

pero 6 no es un cuadrado en \mathbb{Q} . ▲

14.6.14. Comentario. Si para $\alpha \in L$ la norma $N(\alpha)$ es una potencia n -ésima en K , esto *no implica* en general que α es una potencia n -ésima en L .

He aquí un contraejemplo fácil: consideremos la extensión $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$. La norma viene dada por $N(a + b\sqrt{-1}) = a^2 + b^2$. Luego, el número 2 tiene norma 4, pero no es un cuadrado en $\mathbb{Q}(\sqrt{-1})$: si $\alpha^2 = 2$, entonces necesariamente $N(\alpha) = 2$. Sin embargo, los elementos de norma 2 son

$$\pm(1 + \sqrt{-1}), \quad \pm(1 - \sqrt{-1}),$$

y sus cuadrados no son iguales a 2:

$$(1 \pm \sqrt{-1})^2 = \pm 2\sqrt{-1}.$$

Polinomio característico y el polinomio mínimo

En general, el polinomio característico y el polinomio mínimo están relacionados de la siguiente manera.

14.6.15. Teorema. Sean L/K una extensión finita y $\alpha \in L$. Luego,

$$p_{\alpha, L/K} = m_{\alpha, K}^{n/d},$$

donde

$$n := [L : K], \quad d := \deg_K(\alpha) := [K(\alpha) : K].$$

Demostración. Consideremos las extensiones

$$n \begin{pmatrix} L \\ |m \\ K(\alpha) \\ |d \\ K \end{pmatrix}$$

Como una base de $K(\alpha)$ sobre K podemos tomar las potencias de α :

$$1, \alpha, \alpha^2, \dots, \alpha^{d-1}.$$

Sea

$$\beta_1, \beta_2, \dots, \beta_m$$

una base de L sobre $K(\alpha)$. Entonces, como vimos en 14.1.6, se pueden tomar como una base de L sobre K los productos

$$\alpha^i \beta_j. \quad (0 \leq i \leq d-1, 1 \leq j \leq m)$$

Sean c_{ij} los coeficientes de la matriz que representa el endomorfismo $\mu_\alpha : K(\alpha) \rightarrow K(\alpha)$:

$$\alpha \cdot \alpha^i = \sum_{0 \leq i \leq d-1} c_{ij} \alpha^i.$$

Tenemos entonces

$$m_{\alpha,K} = p_{\alpha,K(\alpha)/K} = \det(X \cdot I_d - A),$$

(véase 14.6.8) donde

$$A = \begin{pmatrix} c_{00} & c_{01} & \cdots & c_{0,d-1} \\ c_{10} & c_{11} & \cdots & c_{1,d-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{d-1,0} & c_{d-1,1} & \cdots & c_{d-1,d-1} \end{pmatrix}.$$

Luego,

$$\alpha \cdot \alpha^j \beta_k = \sum_{0 \leq i \leq d-1} c_{ij} \alpha^i \beta_k,$$

de donde se ve que la multiplicación por α sobre L se representa en la base $\alpha^j \beta_k$ por la matriz diagonal por bloques

$$\begin{pmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{pmatrix}.$$

Su polinomio característico viene dado por

$$\det \begin{pmatrix} X I_d - A & & & \\ & X I_d - A & & \\ & & \ddots & \\ & & & X I_d - A \end{pmatrix} = \det(X I_d - A)^m = m_{\alpha,K}^{n/d}.$$

■

14.6.16. Corolario. En la situación del teorema anterior, si el polinomio mínimo de α viene dado por

$$m_{\alpha,K} = X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0,$$

entonces

$$T_{L/K}(\alpha) = -\frac{n}{d} a_{d-1}, \quad N_{L/K}(\alpha) = (-1)^n a_0^{n/d}.$$

Demostración. Tenemos

$$p_{\alpha,L/K} = m_{\alpha,K}^{n/d} = \left(X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0 \right)^{n/d} = X^n + \frac{n}{d} a_{d-1} X^{n-1} + \cdots + a_0^{n/d}.$$

■

14.6.17. Corolario. Si en una extensión L/K de grado n para $\alpha \in L$ el polinomio mínimo se descompone en factores lineales

$$m_{\alpha,K} = (X - \alpha_1) \cdots (X - \alpha_d),$$

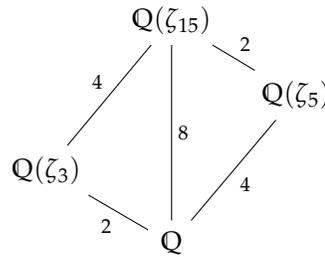
para algunos $\alpha_1, \dots, \alpha_d \in L$, entonces

$$T_{L/K}(\alpha) = \frac{n}{d} (\alpha_1 + \cdots + \alpha_d), \quad N_{L/K}(\alpha) = (\alpha_1 \cdots \alpha_d)^{n/d}.$$

Demostración. Se sigue inmediatamente del corolario anterior.

■

14.6.18. Ejemplo. Consideremos las extensiones ciclotómicas



Tenemos

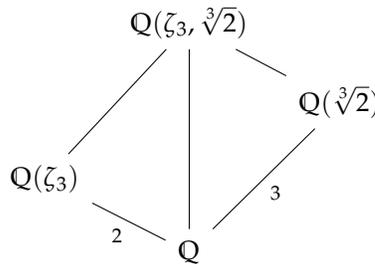
$$m_{\zeta_3, \mathbb{Q}} = \Phi_3 = X^2 + X + 1, \quad m_{\zeta_5, \mathbb{Q}} = \Phi_5 = X^4 + X^3 + X^2 + X + 1.$$

Luego, del resultado de 14.6.15 sabemos que

$$p_{\zeta_3, \mathbb{Q}(\zeta_{15})/\mathbb{Q}} = (X^2 + X + 1)^4, \quad p_{\zeta_5, \mathbb{Q}(\zeta_{15})/\mathbb{Q}} = (X^4 + X^3 + X^2 + X + 1)^2.$$



14.6.19. Ejemplo. Volvamos al ejemplo 14.1.15. Consideremos las extensiones



donde

$$K = \mathbb{Q}(\zeta_3, \sqrt[3]{2}) = \mathbb{Q}(\zeta_3 + \sqrt[3]{2}).$$

Sabemos que

$$[K : \mathbb{Q}] \leq \deg_{\mathbb{Q}}(\zeta_3) \cdot \deg_{\mathbb{Q}}(\sqrt[3]{2}) = 6,$$

pero este número tiene que ser divisible por 2 y 3, así que es precisamente 6. Como una base se puede tomar

$$1, \quad \zeta_3, \quad \sqrt[3]{2}, \quad \sqrt[3]{2}^2, \quad \zeta_3 \sqrt[3]{2}, \quad \zeta_3 \sqrt[3]{2}^2.$$

Calculamos

$$\begin{aligned} 1 \cdot (\zeta_3 + \sqrt[3]{2}) &= \zeta_3 + \sqrt[3]{2}, \\ \zeta_3 \cdot (\zeta_3 + \sqrt[3]{2}) &= -1 - \zeta_3 + \zeta_3 \sqrt[3]{2}, \\ \sqrt[3]{2} \cdot (\zeta_3 + \sqrt[3]{2}) &= \sqrt[3]{2}^2 + \zeta_3 \sqrt[3]{2}, \\ \sqrt[3]{2}^2 \cdot (\zeta_3 + \sqrt[3]{2}) &= 2 + \zeta_3 \sqrt[3]{2}^2, \\ \zeta_3 \sqrt[3]{2} \cdot (\zeta_3 + \sqrt[3]{2}) &= -\sqrt[3]{2} - \zeta_3 \sqrt[3]{2} + \zeta_3 \sqrt[3]{2}^2, \\ \zeta_3 \sqrt[3]{2}^2 \cdot (\zeta_3 + \sqrt[3]{2}) &= 2\zeta_3 - \sqrt[3]{2}^2 - \zeta_3 \sqrt[3]{2}^2. \end{aligned}$$

La matriz correspondiente es

$$A = \begin{pmatrix} 0 & -1 & 0 & 2 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 1 & -1 \end{pmatrix}.$$

Su polinomio característico es**

$$X^6 + 3X^5 + 6X^4 + 3X^3 + 9X + 9.$$

Este polinomio tiene grado 6 y tiene $\zeta_3 + \sqrt[3]{2}$ como su raíz, así que es el polinomio mínimo de $\zeta_3 + \sqrt[3]{2}$ sobre \mathbb{Q} .

Tenemos

$$m_{\zeta_3, \mathbb{Q}} = X^2 + X + 1, \quad m_{\sqrt[3]{2}, \mathbb{Q}} = X^3 - 2,$$

de donde

$$p_{\zeta_3, K/\mathbb{Q}} = (X^2 + X + 1)^3, \quad p_{\sqrt[3]{2}, K/\mathbb{Q}} = (X^3 - 2)^2.$$

▲

14.7 Cuerpos de descomposición

Recordemos que un polinomio $f \in K[X]$ tiene una raíz $\alpha \in K$ si y solo si $(X - \alpha) \mid f$. En particular, esto implica que si $\deg f = n > 0$, entonces f tiene a lo sumo n raíces. Si todas las raíces de f están en K , entonces f se descompone en factores lineales en $K[X]$:

$$f = c(X - \alpha_1) \cdots (X - \alpha_n).$$

14.7.1. Definición. Para un polinomio $f \in K[X]$ se dice que una extensión L/K es un **cuerpo de descomposición*** de f si

- 1) f se descompone en factores lineales en $L[X]$;
- 2) ninguna subextensión $K \subseteq L' \subsetneq L$ satisface esta propiedad.

14.7.2. Observación. Sea $f \in K[X]$ un polinomio de grado n y L/K una extensión tal que en $L[X]$ se tiene una descomposición

$$f = c(X - \alpha_1) \cdots (X - \alpha_n)$$

para algunos $\alpha_1, \dots, \alpha_n \in L$. Entonces, el subcuerpo

$$K(\alpha_1, \dots, \alpha_n) = \bigcap_{\substack{K' \subseteq L \\ \alpha_1, \dots, \alpha_n \in K'}} K'$$

es un cuerpo de descomposición de f .

Demostración. Está claro de la definición. ■

**Se puede hacer este cálculo en el programa PARI/GP (<http://pari.math.u-bordeaux.fr/>):

```
? charpoly([0,-1,0,2,0,0;1,-1,0,0,0,2;1,0,0,0,-1,0;0,0,1,0,0,-1;0,1,1,0,-1,0;0,0,0,1,1,-1])
% = x^6 + 3*x^5 + 6*x^4 + 3*x^3 + 9*x + 9
```

*Splitting field en inglés.

14.7.3. Ejemplo. Sean K un cuerpo y $d \in K$ un elemento que no es un cuadrado en K . Entonces, $K(\sqrt{d}) := K[X]/(X^2 - d)$ es un cuerpo de descomposición del polinomio $X^2 - d$. ▲

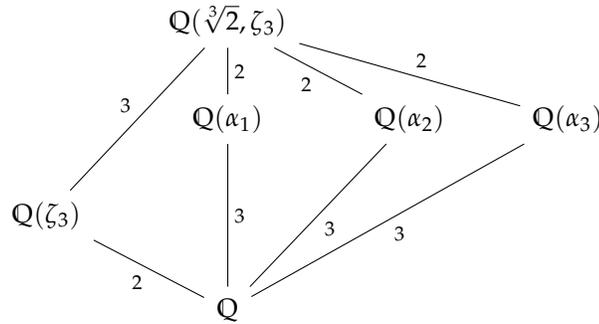
14.7.4. Ejemplo. Para el polinomio $X^n - 1 \in \mathbb{Q}[X]$ el cuerpo ciclotómico $\mathbb{Q}(\zeta_n)$ es un cuerpo de descomposición. En efecto, las raíces complejas de $X^n - 1$ son las raíces n -ésimas de la unidad, generadas por la raíz primitiva $\zeta_n := e^{2\pi\sqrt{-1}/n}$. ▲

14.7.5. Ejemplo. Consideremos el polinomio $X^3 - 2 \in \mathbb{Q}[X]$. Sus raíces complejas son

$$\alpha_1 = \sqrt[3]{2}, \quad \alpha_2 = \zeta_3 \sqrt[3]{2}, \quad \alpha_3 = \zeta_3^2 \sqrt[3]{2}.$$

El cuerpo de descomposición es el cuerpo

$$\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\alpha_1, \alpha_3) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3).$$



▲

Un polinomio $f \in \mathbb{Q}[X]$ siempre tiene raíces complejas $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ y esto nos permite tomar $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ como un cuerpo de descomposición de f . En la situación general abstracta, un cuerpo de descomposición se construye de la siguiente manera.

14.7.6. Proposición. Para un polinomio $f \in K[X]$ existe un cuerpo de descomposición L/K . Además, $[L : K] \leq n!$ donde $n := \deg f$.

Demostración. Gracias a la observación 14.7.2, bastaría probar que existe una extensión L/K de grado $\neq n!$ tal que f se descompone en factores lineales en $L[X]$.

Procedamos por inducción sobre n . Si $n = 1$, entonces, siendo un polinomio lineal, f tiene una raíz en K y podemos tomar $L = K$.

Ahora si $n > 1$, sea $p \mid f$ algún factor irreducible de f en $K[X]$. Consideremos el cuerpo $L' := K[X]/(p)$. Denotemos por α la imagen de X en el cociente. Tenemos $[L' : K] = \deg p \leq n$. Además, $p(\alpha) = 0$ y por ende $f(\alpha) = 0$. Se sigue que en $L'[X]$ tenemos una factorización

$$f = (X - \alpha)g$$

para algún polinomio $g \in L'[X]$. Tenemos $\deg g = n - 1$, así que por la hipótesis de inducción, existe una extensión L/L' de grado $\leq (n - 1)!$ tal que g (y entonces f) se descompone en factores lineales en $L[X]$. Luego,

$$[L : K] = [L : L'] \cdot [L' : K] \leq (n - 1)! \cdot n \leq n!$$

■

Nuestro próximo objetivo es probar que todos los cuerpos de descomposición de f son isomorfos. Empecemos por el siguiente lema.

14.7.7. Lema. Sea $\phi: K_1 \xrightarrow{\cong} K_2$ un isomorfismo de cuerpos y

$$\begin{aligned} \phi: K_1[X] &\rightarrow K_2[X], \\ \sum_{i \geq 0} a_i X^i &\mapsto \sum_{i \geq 0} \phi(a_i) X^i \end{aligned}$$

el isomorfismo correspondiente de los anillos de polinomios. Sean $f_1 \in K_1[X]$ y $f_2 \in K_2[X]$ polinomios irreducibles donde $f_2 = \phi(f_1)$ y sean L_1/K_1 y L_2/K_2 extensiones y $\alpha_1 \in L_1$, $\alpha_2 \in L_2$ elementos tales que $f_1(\alpha_1) = 0$ y $f_2(\alpha_2) = 0$. Entonces, el isomorfismo $K_1 \xrightarrow{\cong} K_2$ se extiende de manera canónica a un isomorfismo $K_1(\alpha_1) \xrightarrow{\cong} K_2(\alpha_2)$.

$$\begin{array}{ccc} L_1 & & L_2 \\ | & & | \\ K_1(\alpha_1) & \xrightarrow{\cong} & K_2(\alpha_2) \\ | & & | \\ K_1 & \xrightarrow{\cong} & K_2 \end{array}$$

Demostración. El isomorfismo entre $K_1[X]$ y $K_2[X]$ envía el ideal maximal $(f_1) \subset K_1[X]$ al ideal maximal $(f_2) \subset K_2[X]$ y entonces induce un isomorfismo

$$K_1[X]/(f_1) \xrightarrow{\cong} K_2[X]/(f_2).$$

Basta considerar el diagrama conmutativo

$$\begin{array}{ccc} K_1(\alpha_1) & \xrightarrow{\cong} & K_2(\alpha_2) \\ \cong \uparrow & & \cong \uparrow \\ K_1[X]/(f_1) & \xrightarrow{\cong} & K_2[X]/(f_2) \\ \uparrow & & \uparrow \\ K_1[X] & \xrightarrow{\cong} & K_2[X] \\ \uparrow & & \uparrow \\ K_1 & \xrightarrow{\cong} & K_2 \end{array}$$

■

14.7.8. Lema. Sea $\phi: K_1 \xrightarrow{\cong} K_2$ un isomorfismo de cuerpos. Sean $f_1 \in K_1[X]$ un polinomio irreducible y $f_2 \in K_2[X]$ el polinomio que corresponde a f_1 bajo el isomorfismo $K_1[X] \xrightarrow{\cong} K_2[X]$ inducido por ϕ . Sean L_1/K_1 y L_2/K_2 cuerpos de descomposición de f_1 y f_2 respectivamente. Entonces, el isomorfismo entre K_1 y K_2 se extiende a un isomorfismo entre L_1 y L_2 :

$$\begin{array}{ccc} L_1 & \xrightarrow{\cong} & L_2 \\ | & & | \\ K_1 & \xrightarrow{\cong} & K_2 \end{array}$$

Demostración. Procedamos por inducción sobre $n = \deg f_1$. Notamos que los factores irreducibles de f_1 en $K_1[X]$ corresponden a los factores irreducibles de f_2 en $K_2[X]$.

Si $n = 1$, o en general si f_1 se descompone en factores lineales en $K_1[X]$, se tiene $L_1 = K_1$, $L_2 = K_2$ y no hay que probar nada.

Si $n > 1$, sea $p_1 \in K_1[X]$ un factor irreducible de f y $p_2 \in K_2[X]$ el factor irreducible correspondiente de f_2 . Si $\alpha_1 \in L_1$ es una raíz de p_1 y $\alpha_2 \in L_2$ es una raíz de p_2 , entonces el lema anterior nos permite extender el isomorfismo $K_1 \xrightarrow{\cong} K_2$ a un isomorfismo $K_1(\alpha_1) \xrightarrow{\cong} K_2(\alpha_2)$. Ahora

$$f_1 = (X - \alpha_1) g_1 \text{ en } K_1(\alpha_1)[X], \quad f_2 = (X - \alpha_2) g_2 \text{ en } K_2(\alpha_2)[X].$$

Notamos que L_1 y L_2 son cuerpos de descomposición para g_1 y g_2 sobre $K_1(\alpha_1)$ y $K_2(\alpha_2)$ respectivamente. Puesto que $\deg g_1 = \deg g_2 = n - 1$, por la hipótesis de inducción, el isomorfismo $K_1(\alpha_1) \xrightarrow{\cong} K_2(\alpha_2)$ se extiende a un isomorfismo $L_1 \xrightarrow{\cong} L_2$.

$$\begin{array}{ccc} L_1 & \xrightarrow{\cong} & L_2 \\ | & & | \\ K_1(\alpha_1) & \xrightarrow{\cong} & K_2(\alpha_2) \\ | & & | \\ K_1 & \xrightarrow{\cong} & K_2 \end{array}$$

■

14.7.9. Corolario. Para un polinomio $f \in K[X]$, si L_1/K y L_2/K son dos cuerpos de descomposición, entonces existe un isomorfismo

$$\begin{array}{ccc} L_1 & \xrightarrow{\cong} & L_2 \\ & \swarrow & \searrow \\ & K & \end{array}$$

Demostración. Basta aplicar el resultado anterior a $K_1 = K_2 = K$, $\phi = \text{id}$ y $f_1 = f_2 = f$. ■

14.8 Extensiones separables

14.8.1. Definición. Sea K un cuerpo y $f \in K[X]$ un polinomio. En un cuerpo de descomposición L/K tenemos

$$f = c (X - \alpha_1)^{m_1} \cdots (X - \alpha_k)^{m_k},$$

donde $\alpha_1, \dots, \alpha_k \in L$ son diferentes elementos y $m_i \geq 1$. Si $m_i = 1$, se dice que α_i es una **raíz simple** de f y si $m_i > 1$, se dice que α_i es una **raíz múltiple** de **multiplicidad** m_i . Si todas las raíces de f son simples, se dice que f es un **polinomio separable**.

Notamos que diferentes cuerpos de descomposición son isomorfos y las multiplicidades de las raíces no dependen de la elección de L .

14.8.2. Proposición. Un polinomio $f \in K[X]$ tiene una raíz múltiple $\alpha \in K$ si y solo si $f'(\alpha) = 0$.

Demostración. Si α es una raíz múltiple, entonces

$$f = (X - \alpha)^2 g$$

para algún polinomio $g \in K[X]$. Luego, tomando las derivadas, se obtiene

$$f' = 2(X - \alpha)g + (X - \alpha)^2 g',$$

de donde $f'(\alpha) = 0$. Viceversa, si $\alpha \in K$ es una raíz común de f y f' , entonces tenemos

$$f = (X - \alpha)g$$

para algún $g \in K[X]$, y luego

$$f' = g + (X - \alpha)g'.$$

De aquí se sigue que $g = f' - (X - \alpha)g'$ tiene α como su raíz; es decir, $(X - \alpha) \mid g$. Entonces,

$$f = (X - \alpha)^2 h$$

para algún $h \in K[X]$. ■

14.8.3. Corolario. *Un polinomio $f \in K[X]$ es separable si y solo si $\text{mcd}(f, f') = 1$.*

Demostración. Sea L/K un cuerpo de descomposición de f .

Si $\text{mcd}(f, f') \neq 1$, entonces existe un polinomio no constante $g \in K[X]$ tal que $g \mid f$ y $g \mid f'$. El polinomio g tiene una raíz $\alpha \in L$, y luego $f(\alpha) = f'(\alpha) = 0$, lo que significa que α es una raíz múltiple de f en L .

Viceversa, si f no es separable, entonces existe $\alpha \in L$ tal que $f(\alpha) = f'(\alpha) = 0$. Esto implica que el polinomio mínimo $m_{\alpha, K}$ divide a f y f' , y por ende $\text{mcd}(f, f') \neq 1$. ■

14.8.4. Corolario. *Sea $f \in K[X]$ un polinomio irreducible. Si $f' \neq 0$, entonces f es separable.*

Demostración. Si $g \mid f$ y $g \mid f'$ y f es irreducible, entonces $g \in K^\times$ o $g \sim f$. Sin embargo, en el segundo caso tenemos $\deg f' < \deg f$, así que $g \nmid f'$. Se sigue que $\text{mcd}(f, f') = 1$, y por lo tanto f es separable. ■

14.8.5. Ejemplo. Consideremos el cuerpo

$$K := \mathbb{F}_p(T) := \left\{ \frac{f}{g} \mid f, g \in \mathbb{F}_p[T], g \neq 0 \right\}.$$

El polinomio $X^p - T$ es irreducible por el criterio de Eisenstein: el elemento T es irreducible en $\mathbb{F}_p[T]$ y $\mathbb{F}_p(T)$ es el cuerpo de fracciones de $\mathbb{F}_p[T]$. Sin embargo, $X^p - T$ no es separable: su derivada es nula, ya que trabajamos en característica p . ▲

14.8.6. Definición. Para una extensión de cuerpos L/K se dice que un elemento $\alpha \in L$ es **separable** sobre K si

- 1) α es algebraico sobre K ,
- 2) el polinomio mínimo de α sobre K es separable.

Si todo elemento de L es separable sobre K , se dice que L/K es una **extensión separable**.

Para ciertos cuerpos todas las extensiones algebraicas son automáticamente separables.

14.8.7. Definición. Se dice que un cuerpo K es **perfecto** si se cumple una de las siguientes condiciones:

- 1) $\text{char } K = 0$;
- 2) $\text{char } K = p$ y todo elemento de K es una p -ésima potencia.

14.8.8. Ejemplo. Todo cuerpo finito es perfecto. En efecto, si K es finito, entonces es una extensión finita de \mathbb{F}_p . Consideremos la aplicación

$$F: K \rightarrow K, \\ \alpha \mapsto \alpha^p.$$

Esto es un homomorfismo: tenemos claramente $(\alpha\beta)^p = \alpha^p \beta^p$ para cualesquiera $\alpha, \beta \in K$, y luego, dado que estamos en la característica p , tenemos también $(\alpha + \beta)^p = \alpha^p + \beta^p$. Siendo un homomorfismo de cuerpos, F es inyectivo, pero K es finito, así que F es también sobreyectivo. Para más información sobre los cuerpos finitos y la aplicación F , véase el siguiente capítulo. ▲

14.8.9. Ejemplo. El cuerpo $\mathbb{F}_p(T)$ no es perfecto: en este caso $\sqrt[p]{T} \notin \mathbb{F}_p(T)$. ▲

14.8.10. Proposición. Si K es un cuerpo perfecto, entonces todo polinomio irreducible $f \in K[X]$ es separable.

Demostración. Gracias a 14.8.4, sería suficiente probar que para todo polinomio irreducible

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in K[X]$$

donde $a_n \neq 0$ se tiene

$$f' = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \cdots + a_1 \neq 0.$$

Si $\text{char } K = 0$, entonces $n a_n \neq 0$ y por ende $f' \neq 0$. Asumamos que $\text{char } K = p$ y todo elemento de K es una p -ésima potencia. Notamos que si $f' = 0$, entonces $i \cdot a_i = 0$ para todo $i = 1, \dots, n$; es decir, $a_i = 0$ o $p \mid i$. Esto significa que el polinomio tiene forma

$$f = b_m X^{mp} + b_{m-1} X^{(m-1)p} + \cdots + b_1 X^p + b_0$$

para algunos $b_0, b_1, \dots, b_m \in K$. Por nuestra hipótesis, todo b_i es una potencia p -ésima en K , así que

$$f = c_m^p X^{mp} + c_{m-1}^p X^{(m-1)p} + \cdots + c_1^p X^p + c_0^p = (c_m X^m + c_{m-1} X^{m-1} + \cdots + c_1 X + c_0)^p$$

(usando que $\text{char } K = p$). Pero esto contradice la irreducibilidad de f . Entonces, $f' \neq 0$. ■

14.8.11. Corolario. Si K es un cuerpo perfecto, entonces toda extensión algebraica L/K es separable.

Teorema del elemento primitivo

El siguiente resultado simplifica mucho el estudio de extensiones de cuerpos K/F : resulta que en muchos casos son **simples**; es decir de la forma $K = F(\theta)$ para algún $\theta \in K$.

14.8.12. Teorema del elemento primitivo. Sea K/F una extensión finita de cuerpos tal que $K = F(\alpha_1, \dots, \alpha_n)$, donde $\alpha_2, \dots, \alpha_n \in K$ son separables*. Luego, existe un elemento $\theta \in K$ tal que $K = F(\theta)$.

Demostración [vdW1991, §6.10]. Consideremos primero el caso de $n = 2$. Sea entonces $K = F(\alpha, \beta)$, donde β es separable sobre F . Sea $f := m_{\alpha, F}$ el polinomio mínimo de α sobre F y $g := m_{\beta, F}$ el polinomio mínimo de β sobre F . Sea L/K una extensión donde f y g se descomponen en factores lineales y sean

$$\alpha_1 := \alpha, \alpha_2, \dots, \alpha_r \in L$$

las raíces diferentes de f en L y sean

$$\beta_1 := \beta, \beta_2, \dots, \beta_s \in L$$

*Sic. La separabilidad de α_1 no será necesaria en la prueba.

las raíces de g (son todas diferentes, dado que β es separable).

Notamos que sin pérdida de generalidad, se puede asumir que F es un cuerpo infinito. En el caso contrario, K también sería un cuerpo finito, y luego $K = F(\theta)$ donde θ es un generador del grupo cíclico K^\times .

Notamos que $\beta_j \neq \beta_1$ para $j \neq 1$, así que la ecuación

$$\alpha_i + x \beta_j = \alpha_1 + x \beta_1$$

tiene a lo sumo una raíz $x \in F$ para cualesquiera $i = 1, \dots, r$ y $j = 2, \dots, s$. Gracias a nuestra hipótesis de que F sea infinito, existe un elemento $c \in F$ que es distinto de las raíces de las ecuaciones de arriba:

$$\alpha_i + c \beta_j \neq \alpha_1 + c \beta_1 \quad \text{para } i = 1, \dots, r, j = 2, \dots, s.$$

Pongamos

$$\theta := \alpha_1 + c \beta_1 = \alpha + c \beta.$$

Tenemos $\theta = F(\alpha, \beta)$. Si logramos probar que $\beta \in F(\theta)$, entonces también $\alpha = \theta - c \beta \in F(\theta)$ y $F(\alpha, \beta) = F(\theta)$. Notamos que

$$g(\beta) = 0, \quad f(\alpha) = f(\theta - c \beta) = 0$$

y los polinomios $g \in F[X]$ y $f(\theta - c X) \in F(\theta)[X]$ no pueden tener más de una raíz común por nuestra elección de c : se tiene

$$\theta - c \beta_j \neq \alpha_i \quad \text{para } i = 1, \dots, r, j = 2, \dots, s,$$

así que $f(\theta - c \beta_j) \neq 0$ para $j \neq 1$. Calculamos

$$\text{mcd}(g, f(\theta - c X)) = h \quad \text{en } F(\theta)[X]$$

para algún polinomio mónico $h \in F(\theta)[X]$. Notamos que $\deg h > 0$: dado que $g(\beta) = f(\theta - c \beta) = 0$, ambos polinomios g y $f(\theta - c X)$ deben ser divisibles por el polinomio mínimo $m_{\beta, F(\theta)}$. En $L[X]$ el polinomio h se descompone en factores lineales y toda raíz de h es una raíz de g y $f(\theta - c X)$. Pero β es la única raíz común de g y $f(\theta - c X)$ y g no tiene raíces múltiples, así que necesariamente $h = X - \beta$. Esto nos permite concluir que $\beta \in F(\theta)$.

Esto termina la prueba en el caso de $n = 2$. En el caso general, podemos proceder por inducción sobre n . Asumamos que el resultado es válido para $n - 1$ y se tiene

$$F(\alpha_1, \dots, \alpha_{n-1}) = F(\eta)$$

para algún $\eta \in K$. Luego,

$$F(\alpha_1, \dots, \alpha_n) = F(\eta, \alpha_n) = F(\theta)$$

por el caso de dos generadores. ■

14.8.13. Corolario. Si F es un cuerpo perfecto, entonces toda extensión finita K/F es simple: existe $\theta \in K$ tal que $K = F(\theta)$.

14.8.14. Ejemplo. Consideremos la extensión $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Los polinomios mínimos de $\sqrt[3]{2}$ y ζ_3 sobre \mathbb{Q} son

$$X^3 - 2 \quad \text{y} \quad X^2 + X + 1$$

respectivamente. Sus raíces complejas son

$$\alpha_1 = \sqrt[3]{2}, \quad \alpha_2 = \zeta_3 \sqrt[3]{2}, \quad \alpha_3 = \zeta_3^2 \sqrt[3]{2}, \quad \beta_1 = \zeta_3, \quad \beta_2 = \zeta_3^2.$$

La prueba del teorema nos dice que hay que escoger $c \in \mathbb{Q}$ tal que

$$\begin{aligned}\sqrt[3]{2} + c\zeta_3^2 &\neq \sqrt[3]{2} + c\zeta_3, \\ \zeta_3 \sqrt[3]{2} + c\zeta_3^2 &\neq \sqrt[3]{2} + c\zeta_3, \\ \zeta_3^2 \sqrt[3]{2} + c\zeta_3^2 &\neq \sqrt[3]{2} + c\zeta_3.\end{aligned}$$

Se ve que funciona $c = 1$, y luego

$$\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\sqrt[3]{2} + \zeta_3).$$

▲

14.8.15. Ejemplo. Consideremos la extensión $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ donde m, n y mn no son cuadrados. Tenemos polinomios mínimos $X^2 - m$ y $X^2 - n$ y sus raíces

$$\alpha_1 = \sqrt{m}, \quad \alpha_2 = -\sqrt{m}, \quad \beta_1 = \sqrt{n}, \quad \beta_2 = -\sqrt{n}.$$

Necesitamos encontrar $c \in \mathbb{Q}$ tal que

$$\begin{aligned}\sqrt{m} - c\sqrt{n} &\neq \sqrt{m} + c\sqrt{n}, \\ -\sqrt{m} - c\sqrt{n} &\neq \sqrt{m} + c\sqrt{n}.\end{aligned}$$

Basta tomar $c = 1$, así que

$$\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m} + \sqrt{n}).$$

▲

14.9 Cerradura algebraica

En §14.7 para un polinomio $f \in K[X]$ hemos construido una extensión L/K donde f se descompone en factores lineales; es decir, una extensión que contiene todas las raíces de f . En general, para cualquier cuerpo K se puede construir su **cerradura algebraica** que es una extensión \bar{K}/K que contiene las raíces de todos los polinomios $f \in K[X]$.

14.9.1. Proposición. Sea K un cuerpo. Las siguientes condiciones son equivalentes:

- 1) todo polinomio no constante en $K[X]$ tiene una raíz en K ;
- 2) todo polinomio de grado $n > 0$ en $K[X]$ tiene n raíces en K , contándolas con multiplicidades; es decir,

$$f = c(X - \alpha_1) \cdots (X - \alpha_n)$$

para $\alpha_1, \dots, \alpha_n \in K$;

- 3) todo polinomio irreducible en $K[X]$ es lineal;
- 4) K no tiene extensiones algebraicas propias: si L/K es una extensión algebraica, entonces $L = K$.

Demostración. 1) \Rightarrow 2): si f es un polinomio de grado $n > 0$ y f tiene una raíz $\alpha \in K$, entonces $f = (X - \alpha)g$, donde $\deg g = n - 1$. Luego, g también debe tener una raíz, etcétera. Continuando de esta manera, se obtiene una descomposición $f = c(X - \alpha_1) \cdots (X - \alpha_n)$.

2) \Rightarrow 3): está claro.

3) \Rightarrow 4): si L/K es una extensión algebraica, entonces para todo $\alpha \in L$ el polinomio mínimo $m_{\alpha, K}$ debe ser lineal según 3), lo que significa que $\alpha \in K$.

4) \Rightarrow 1): para un polinomio no constante f , escribamos $f = gh$ donde g es irreducible. Luego, $L := K[X]/(g)$ es una extensión finita de grado $[L : K] = \deg g$, pero según 4), tenemos $L = K$, así que $\deg g = 1$. ■

14.9.2. Definición. Un cuerpo K que satisface las condiciones equivalentes de la proposición anterior se llama **algebraicamente cerrado**.

El siguiente resultado debe de ser conocido al lector.

14.9.3. “Teorema fundamental del álgebra”. *El cuerpo de los números complejos \mathbb{C} es algebraicamente cerrado.*

La construcción de los números complejos es *analítica*: primero hay que construir los números reales \mathbb{R} como la completación de los números racionales \mathbb{Q} considerando las sucesiones de Cauchy en \mathbb{Q} respecto a la relación de equivalencia

$$(x_n) \equiv (x'_n) \iff \lim_{n \rightarrow \infty} (x_n - x'_n) = 0,$$

y luego pasar al cuerpo $R(\sqrt{-1}) := \mathbb{R}[X]/(X^2 + 1)$. Se conocen muchas pruebas del teorema fundamental del álgebra, y una de estas puede ser encontrada en el apéndice E.

14.9.4. Digresión. Se puede tomar la completación de los números racionales \mathbb{Q} respecto a la **norma p -ádica**

$$\left| \frac{x}{y} \right|_p := v_p(x) - v_p(y)$$

—véase el capítulo anterior para una breve discusión de las valuaciones p -ádicas y mis apuntes

<http://cadadr.org/san-salvador/2018-04-topologia-p-adica/topologia-p-adica.pdf>

El resultado de esta completación es el cuerpo de los **números p -ádicos** \mathbb{Q}_p . Este cuerpo no es algebraicamente cerrado y se puede tomar su cerradura algebraica $\overline{\mathbb{Q}_p}$. Sin embargo, $\overline{\mathbb{Q}_p}$ deja de ser completo (no todas sucesiones de Cauchy convergen en $\overline{\mathbb{Q}_p}$). Luego, se puede tomar de nuevo la completación de $\overline{\mathbb{Q}_p}$ que se denota por \mathbb{C}_p . Resulta que \mathbb{C}_p es un cuerpo algebraicamente cerrado.

$$\mathbb{Q} \rightsquigarrow \mathbb{Q}_p \text{ compl., no alg. cerr.} \rightsquigarrow \overline{\mathbb{Q}_p} \text{ no compl., alg. cerr.} \rightsquigarrow \mathbb{C}_p \text{ compl., alg. cerr..}$$

Para los detalles, véase [Kob1984].

14.9.5. Definición. Para un cuerpo K , se dice que una extensión \overline{K}/K es una **cerradura algebraica** de K si

- 1) \overline{K}/K es una extensión algebraica;
- 2) el cuerpo \overline{K} es algebraicamente cerrado.

14.9.6. Ejemplo. Los números complejos \mathbb{C} forman una cerradura algebraica de los números reales \mathbb{R} . ▲

Existencia de cerradura algebraica

14.9.7. Teorema. *Para todo cuerpo K existe una cerradura algebraica \overline{K} .*

Demostración. Consideremos el anillo de polinomios $K[X_f]$, donde cada variable X_f corresponde a un polinomio mónico no constante $f \in K[X]$. (Este anillo es muy grande.)

Sea I el ideal en $K[X_f]$ generado por los polinomios $f(X_f)$ para todo polinomio mónico irreducible $f \in K[X]$. Este ideal es propio. En efecto, en el caso contrario existen algunos polinomios $g_1, \dots, g_n \in K[X_f]$ y $f_1, \dots, f_n \in K[X]$ tales que

$$1 = g_1 f_1(X_{f_1}) + \dots + g_n f_n(X_{f_n}).$$

Sea L/K una extensión finita donde cada uno de los polinomios f_i tiene una raíz $\alpha_i \in L$. Consideremos el homomorfismo de evaluación

$$\begin{aligned} \phi: K[X_f] &\rightarrow L, \\ X_{f_i} &\mapsto \alpha_i, \text{ para } i = 1, \dots, n, \\ X_f &\mapsto 0, \text{ si } f \neq f_i \text{ para } i = 1, \dots, n. \end{aligned}$$

Luego,

$$\phi(g_1 f_1(X_{f_1}) + \dots + g_n f_n(X_{f_n})) = 0,$$

pero esto significa que

$$g_1 f_1(X_{f_1}) + \dots + g_n f_n(X_{f_n}) \neq 1.$$

Siendo un ideal propio, I está contenido en un ideal maximal $\mathfrak{m} \subset K[X_f]$. Consideremos el cuerpo $K_1 := K[X_f]/\mathfrak{m}$. Por la construcción, todo polinomio no constante $f \in K[X]$ tiene una raíz en K_1 . En efecto, bastaría considerar el caso cuando f es mónico. Denotemos por $\alpha_f \in K_1$ la imagen de X_f en el cociente. Entonces, $f(\alpha_f) = 0$. Notamos que los elementos α_f son algebraicos sobre K , y entonces el cuerpo K_1 , siendo generado por los α_f , es una extensión algebraica de K .

De la misma manera, se puede construir una extensión K_2/K_1 tal que todo polinomio no constante $f \in K_1[X]$ tiene una raíz en K_2 , etcétera. Esto nos da una torre de extensiones algebraicas

$$K \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \dots$$

Pongamos

$$\bar{K} := \bigcup_{i \geq 1} K_i.$$

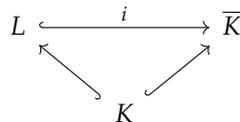
Esto es una extensión algebraica de K . Además, para cualquier polinomio no constante $f \in \bar{K}[X]$ sus coeficientes pertenecen a algún K_n para n suficientemente grande, así que f tiene una raíz en K_{n+1} . Entonces, \bar{K} es un cuerpo algebraicamente cerrado. ■

14.9.8. Comentario. La prueba de arriba pertenece a Emil Artin. En efecto, un análisis más cuidadoso demuestre que no es necesario iterar la construcción y el cuerpo K_1 ya es algebraicamente cerrado. Para los detalles, véase la nota de Keith Conrad

<http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/algclosure.pdf>

“Unicidad” de cerradura algebraica

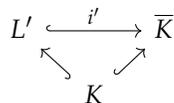
14.9.9. Lema. Sean \bar{K}/K una cerradura algebraica de K y L/K una extensión algebraica. Entonces, existe un encajamiento



La prueba es una aplicación típica del lema de Zorn*.

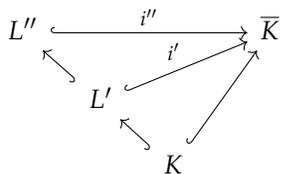
*Nuestra construcción de una cerradura algebraica también usa el lema de Zorn, pero escondido en el resultado sobre la existencia de ideales maximales.

Demostración. Sea \mathcal{P} el conjunto que consiste en pares de elementos (L', i') donde $K \subseteq L' \subseteq L$ es una subextensión e i' es un encajamiento de L' en \bar{K} :



Este conjunto no es vacío: $(K, i) \in \mathcal{P}$. Este conjunto es parcialmente ordenado por la relación

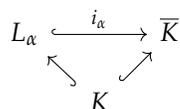
$$(L', i') \preceq (L'', i'') \iff L' \subseteq L'' \text{ y } i''|_{L'} = i'.$$



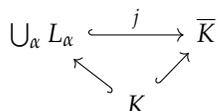
Es fácil comprobar que toda cadena ascendente en \mathcal{P} tiene una cota superior: para una cadena $\{(L_\alpha, i_\alpha)\}_\alpha$ podemos tomar

$$\bigcup_\alpha L_\alpha.$$

Puesto que L_α es una cadena, se ve que la unión es un cuerpo. Las inclusiones



inducen una inclusión



definida por $j(\alpha) := i_\alpha(\alpha)$ si $\alpha \in L_\alpha$ (esta aplicación está bien definida y hace parte del diagrama conmutativo de arriba, dado que $\{(L_\alpha, i_\alpha)\}_\alpha$ es una cadena).

Entonces, el lema de Zorn nos dice que \mathcal{P} tiene un elemento maximal (F, i) . Para concluir la prueba, vamos a ver que $F = L$. Todo elemento $x \in L$ es algebraico sobre K , y entonces es algebraico sobre F . Sea $f := m_{x,F} \in F[X]$ el polinomio mínimo de x sobre F . Tenemos

$$F(x) \cong F[X]/(f).$$

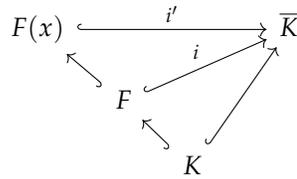
El polinomio f tiene una raíz $\alpha \in \bar{K}$. Consideremos el homomorfismo

$$\begin{aligned} \text{ev}_\alpha: F[X] &\rightarrow \bar{K}, \\ \sum_{k \geq 0} a_k X^k &\mapsto \sum_{k \geq 0} i(a_k) \alpha^k. \end{aligned}$$

Tenemos $f \in \ker \text{ev}_\alpha$, así que este homomorfismo induce un homomorfismo

$$i': F(x) \cong F[X]/(f) \rightarrow \bar{K}$$

que es necesariamente inyectivo, dado que $F(x)$ es un cuerpo, y que extiende a i :



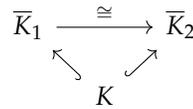
Entonces,

$$(F, i) \preceq (F(x), i').$$

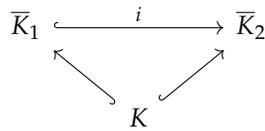
Sin embargo, la maximalidad de (F, i) implica que $F = F(x)$. Esto se cumple para cualquier $x \in L$, así que $F = L$. ■

De este lema se deduce que las cerraduras algebraicas son isomorfas entre sí.

14.9.10. Teorema. Sean $K \hookrightarrow \bar{K}_1$ y $K \hookrightarrow \bar{K}_2$ dos cerraduras algebraicas. Entonces, existe un isomorfismo



Demostración. Aplicando el lema anterior a $L = \bar{K}_1$ y $\bar{K} = \bar{K}_2$, se obtiene un encajamiento



Sin embargo, i es necesariamente sobreyectivo. En efecto, un elemento $y \in \bar{K}_2$ es una raíz de algún polinomio mónico irreducible $f \in K[X]$. Luego, f se factoriza como $(X - x_1) \cdots (X - x_n)$ en $\bar{K}_1[X]$, así que $y = i(x_k)$ para algún $k = 1, \dots, n$. ■

El isomorfismo $\bar{K}_1 \cong \bar{K}_2$ que acabamos de obtener no es único en ningún sentido y por este motivo no hay que hablar de “la cerradura algebraica”, sino de elección de *una cerradura algebraica*. De hecho, normalmente una cerradura algebraica \bar{K}/K tiene muchos automorfismos no triviales $\bar{K} \xrightarrow{\cong} \bar{K}$; para un ejemplo particular, véase el siguiente capítulo.

14.10 Ejercicios

Ejercicio 14.1. Sea K un cuerpo y

$$f = X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in K[X]$$

un polinomio irreducible. Denotemos por α la imagen de X en el cociente $L := K[X]/(f)$. Encuentre una fórmula explícita para α^{-1} en términos de la base $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$.

Ejercicio 14.2. Consideremos el polinomio $f := X^3 + X^2 + X + 2 \in \mathbb{Q}[X]$.

- 1) Demuestre que f es irreducible.
- 2) Denotemos por α la imagen de X en el cociente $K := \mathbb{Q}[X]/(f)$. Expresé los elementos

$$(\alpha^2 + \alpha + 1)(\alpha^2 + \alpha), \quad (\alpha - 1)^{-1} \in K$$

en términos de la base $1, \alpha, \alpha^2$.

Ejercicio 14.3. Encuentre un polinomio cúbico irreducible $f \in \mathbb{F}_2[X]$ y considere el cuerpo $k := \mathbb{F}_2[X]/(f)$. Verifique directamente que el grupo k^\times es cíclico mostrando que todos sus elementos son potencias de un generador.

Ejercicio 14.4. Sea n un número entero. Encuentre el polinomio mínimo sobre \mathbb{Q} para $n + \sqrt{-1} \in \mathbb{C}$.

Ejercicio 14.5. Para una extensión L/K y un elemento algebraico $\alpha \in L$ asumamos que el grado $[K(\alpha) : K]$ es impar. Demuestre que $K(\alpha) = K(\alpha^2)$.

Ejercicio 14.6. Para $p = 2, 3$ demuestre que el polinomio $X^3 - p$ es irreducible en $K[X]$ donde $K = \mathbb{Q}(\sqrt{-1})$. Sugerencia: considere la extensión $\mathbb{Q}(\sqrt{-1}, \sqrt[3]{p})/\mathbb{Q}$.

Ejercicio 14.7. Sean $m, n \in \mathbb{Z}$ dos números enteros tales que $\sqrt{m}, \sqrt{n} \notin \mathbb{Q}$. Consideremos $\alpha := \sqrt{m} + \sqrt{n} \in \mathbb{C}$.

- 1) Demuestre que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{m}, \sqrt{n})$.
- 2) Para

$$\alpha_1 := \alpha, \quad \alpha_2 := -\sqrt{m} + \sqrt{n}, \quad \alpha_3 := -\alpha_1, \quad \alpha_4 := -\alpha_2,$$
 demuestre que el polinomio $f := (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4)$ tiene coeficientes enteros.
- 3) Demuestre que si $\sqrt{mn} \notin \mathbb{Q}$, entonces f es el polinomio mínimo de α sobre \mathbb{Q} .
- 4) Demuestre que si $\sqrt{mn} \in \mathbb{Q}$, entonces $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$.

Polinomios y cuerpos ciclotómicos

Ejercicio 14.8. Demuestre que si $m > 1$ es impar, entonces $\Phi_{2m} = \Phi_m(-X)$.

Sugerencia: compare las expresiones

$$\prod_{d|2m} \Phi_d = X^{2m} - 1 = (X^m - 1)(X^m + 1) = -(X^m - 1)((-X)^m - 1) = - \prod_{d|m} \Phi_d(X) \Phi_d(-X)$$

usando la inducción sobre m .

Ejercicio 14.9. Encuentre un par de cuerpos ciclotómicos $\mathbb{Q}(\zeta_m)$ y $\mathbb{Q}(\zeta_n)$ tales que $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ pero $\mathbb{Q}(\zeta_m) \not\cong \mathbb{Q}(\zeta_n)$.

Ejercicio 14.10. Demuestre que toda extensión finita K/\mathbb{Q} contiene un número finito de las raíces de la unidad.

Ejercicio 14.11. Denotemos por $\mathbb{Q}(\zeta_\infty) = \mathbb{Q}(\zeta_3, \zeta_4, \zeta_5, \zeta_6, \dots)$ la extensión de \mathbb{Q} generada por todas las raíces de la unidad. Demuestre que $\mathbb{Q}(\zeta_\infty) = \bigcup_{n \geq 1} \mathbb{Q}(\zeta_n)$.

Derivadas formales

Ejercicio 14.12. Sea R un anillo conmutativo. Para una serie de potencias $f = \sum_{n \geq 0} a_n X^n \in R[[X]]$ definamos su *derivada formal* como la serie

$$f' := \sum_{n \geq 1} n a_n X^{n-1}.$$

1) Demuestre que para cualesquiera $f, g \in R[[X]]$ se cumple

$$(f + g)' = f' + g', \quad (fg)' = f'g + fg'.$$

2) Calcule las derivadas de las siguientes series formales en $\mathbb{Q}[[X]]$:

$$\begin{aligned} \exp(X) &:= \sum_{n \geq 0} \frac{X^n}{n!}, & \log(1 + X) &:= \sum_{n \geq 0} (-1)^{n+1} \frac{X^n}{n}, \\ \text{sen}(X) &:= \sum_{n \geq 0} (-1)^n \frac{X^{2n+1}}{(2n+1)!}, & \text{cos}(X) &:= \sum_{n \geq 0} (-1)^n \frac{X^{2n}}{(2n)!}. \end{aligned}$$

Ejercicio 14.13 (Serie de Taylor). Demuestre que si $\mathbb{Q} \subseteq R$, entonces para $f \in R[[X]]$ se cumple

$$f = \sum_{n \geq 0} \frac{f^{(n)}(0)}{n!} X^n,$$

donde $f^{(0)} := f$ y $f^{(n)} := (f^{(n-1)})'$ para $n \geq 1$.

Ejercicio 14.14. Si $\mathbb{Q} \subseteq R$, definamos las *integrales formales* por

$$\int_0^X \left(\sum_{n \geq 0} a_n X^n \right) dX := \sum_{n \geq 0} \frac{a_n}{n+1} X^{n+1}.$$

1) Demuestre que se cumple el **teorema fundamental del cálculo**:

$$\int_0^X f'(X) dX = f(X) - f(0) \quad \text{y} \quad \left(\int_0^X f(X) dX \right)' = f(X),$$

donde $f(0)$ denota el término constante de f .

2) Demuestre que se cumple la **integración por partes**:

$$f(X)g(X) - f(0)g(0) = \int_0^X f(X)g'(X) dX + \int_0^X f'(X)g(X) dX.$$

3) Calcule las series

$$\int_0^X \exp(X) dX, \quad \int_0^X \log(1 + X) dX, \quad \int_0^X X \exp(X) dX.$$

La traza, norma y el polinomio característico

Ejercicio 14.15. Consideremos la extensión ciclotómica $\mathbb{Q}(\zeta_3)/\mathbb{Q}$.

1) Usando la base $1, \zeta_3$, calcule el polinomio característico para un elemento $\alpha := a + b\zeta_3$, donde $a, b \in \mathbb{Q}$.

2) Note que $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. Verifique que el resultado de 1) coincide con el cálculo para las extensiones cuadráticas que hicimos en clase.

Ejercicio 14.16. Demuestre que $1 + \sqrt[3]{2}$ no es una n -ésima potencia en $\mathbb{Q}(\sqrt[3]{2})$ para ningún $n = 2, 3, 4, \dots$

Ejercicio 14.17. Consideremos $\alpha := \zeta_5 + \zeta_5^2$, donde $\zeta_5 := e^{2\pi\sqrt{-1}/5}$.

1) Calcule el polinomio característico de α respecto a la extensión ciclotómica $\mathbb{Q}(\zeta_5)/\mathbb{Q}$.

2) Demuestre que $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\alpha)$ y el polinomio obtenido es el polinomio mínimo de α .

Ejercicio 14.18. Encuentre el polinomio mínimo de $\sqrt{2} + \sqrt[3]{2}$ sobre \mathbb{Q} .

Separabilidad y el teorema del elemento primitivo

Ejercicio 14.19. Sea p un número primo. Consideremos el polinomio $f := X^2 + X + 1 \in \mathbb{F}_p[X]$.

1) Demuestre que f es irreducible si y solo si $p \equiv 2 \pmod{3}$.

Indicación: use la ley de reciprocidad cuadrática para ver cuándo $\sqrt{-3} \notin \mathbb{F}_p$; otra opción es notar que se trata del tercer polinomio ciclotómico.

2) ¿Para cuáles p el polinomio f es separable?

Ejercicio 14.20. ¿Para cuáles p el polinomio $f := X^2 + X + 2 \in \mathbb{F}_p[X]$ es irreducible? ¿separable?

Ejercicio 14.21. Sean p un número primo y $a \in \mathbb{F}_p$ un elemento no nulo. Consideremos el polinomio

$$f := X^p - X + a \in \mathbb{F}_p[X].$$

En este ejercicio vamos a probar que f es irreducible.

1) Demuestre que f es separable.

2) Sea L un cuerpo de descomposición de f y sea $\alpha \in L$ un elemento tal que $f(\alpha) = 0$. Demuestre que las raíces de f en L son $\alpha, \alpha + 1, \dots, \alpha + p - 1$.

3) Asumamos que $f = gh$ donde $g, h \in \mathbb{F}_p[X]$ son polinomios mónicos y $\deg g, \deg h < \deg f$. Analizando la suma de las raíces de g o h , concluya que $\alpha \in \mathbb{F}_p$.

4) Demuestre que en este caso f se descompone en factores lineales en $\mathbb{F}_p[X]$ y deduzca una contradicción.

Ejercicio 14.22. Sean p un primo impar y n un número natural tal que $p \nmid n$. Denotemos por $\Phi_n \in \mathbb{Z}[X]$ el n -ésimo polinomio ciclotómico. Demuestre que si $a \in \mathbb{Z}$ satisface $\Phi_n(a) \equiv 0 \pmod{p}$, entonces $p \nmid a$ y el orden de a en $(\mathbb{Z}/p\mathbb{Z})^\times$ es igual a n .

Indicación: factorice $X^n - 1 \in \mathbb{Z}[X]$ en polinomios ciclotómicos y note que el polinomio $X^n - 1 \in \mathbb{F}_p[X]$ es separable.

Ejercicio 14.23. Consideremos la extensión $K := \mathbb{Q}(\sqrt{-1}, \sqrt[3]{2})$. Encuentre $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$.

Bibliografía

- [Bak1990] Alan Baker, *Transcendental number theory*, second ed., Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1990. [MR1074572](#)
- [Kob1984] Neal Koblitz, *p -adic numbers, p -adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. [MR754003](#)
<http://dx.doi.org/10.1007/978-1-4612-1112-9>
- [Mar1977] Daniel A. Marcus, *Number fields*, Universitext, Springer-Verlag, New York, 1977.
<https://doi.org/10.1007/978-1-4684-9356-6>
- [vdW1991] Bartel Leendert van der Waerden, *Algebra*, vol. I, Springer-Verlag, New York, 1991.