Capítulo 14
Cuerpos

lección 25
17.10.18

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 $\phi\colon \mathbb{Z} \to K$.

- Si ϕ es inyectivo, se dice que K tiene **característica** 0. En este caso K contiene un subanillo $\operatorname{im}\phi$ que es isomorfo a $\mathbb{Z}$. Siendo un cuerpo, K también debe contener todos los inversos de los elementos no nulos de $\operatorname{im}\phi$, así que K contiene un *subcuerpo* isomorfo a $\mathbb{Q}$.

- Si ϕ no es inyectivo, entonces $\operatorname{im}\phi \cong \mathbb{Z}/n\mathbb{Z}$. 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

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

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 $\phi\colon K \to R$ 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 $p = 2, 3, 5, 7, 11, \ldots$ son primos. Si tenemos

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

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

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

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

14.1.5. Ejemplo. Si $K/\mathbb{F}_p$ es una extensión de grado n del cuerpo finito $\mathbb{F}_p$, entonces $|K| = p^n$. Más adelante 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 $\alpha_1, \ldots, \alpha_m \in K$ es una base de K sobre F y $\beta_1, \ldots, \beta_n \in L$ 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.

$$\begin{array}{rl} L & \beta_1, \ldots, \beta_n \\ {\scriptstyle [L:K]=n}\,\big| & \\ K & \alpha_1, \ldots, \alpha_m \\ {\scriptstyle [K:F]=m}\,\big| & \\ F & \end{array}$$

Demostración. Todo elemento de L puede ser escrito como

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

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

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

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

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

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 $\sum_{1 \le j \le n} b_j \, \beta_j = 0$, 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 $\phi\colon K \hookrightarrow K[X] \twoheadrightarrow K[X]/(f)$ es inyectivo e identifica a K con un subcuerpo de L y entonces a $K[X]$ con un subanillo de $L[X]$;*

3) *si $\alpha := X \mod f \in L$ es la imagen de la variable X en el cociente, entonces $[L : K] = n$ y los elementos $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ forman una base de L sobre K; en particular,*

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

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 $\phi\colon K \hookrightarrow K[X] \twoheadrightarrow K[X]/(f)$ 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 $a_0, a_1, \ldots, a_{n-1} \in K$. La reducción de g módulo f nos da

$$\overline{g} = \overline{a_0 + a_1\, X + \cdots + a_{n-1}\, X^{n-1}} = a_0 + a_1\, \overline{X} + \cdots + a_{n-1}\, \overline{X}^{n-1} \\ = a_0 + a_1\, \alpha + \cdots + a_{n-1}\, \alpha^{n-1} \in L.$$

Entonces, $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ 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:

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

▲

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

$\times$	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 $\operatorname{char} K = p$ 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 más adelante. ▲

lección 26
18.10.18

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 $\alpha_1, \alpha_2, \ldots \in L$ el subcuerpo mínimo de L que contiene a $\alpha_1, \alpha_2, \ldots$ y todos los elementos de K se llama el subcuerpo **generado** por $\alpha_1, \alpha_2, \ldots$ sobre K y se denota por

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

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 $K(\alpha_1, \ldots, \alpha_n)/K$ 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 $K(\alpha_1,\ldots,\alpha_n)$ se obtiene como una sucesión de extensiones simples:

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

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

14.2 Extensiones algebraicas

14.2.1. Definición. Para una extension 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 $e=2{,}718281828\ldots$ y $\pi=3{,}1415926\ldots$ 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 $1, \alpha, \alpha^2, \ldots, \alpha^n$ son necesariamente linealmente independientes, así que existen algunos coeficientes $a_0, a_1, a_2, \ldots, a_n \in K$, no todos nulos, tales que

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

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

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

■

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

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

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

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

es nulo si y solo si $a_0 = a_1 = a_2 = \cdots = a_n = 0$, 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*

$$\mathrm{ev}_\alpha \colon K[X] \to K(\alpha), \quad f \mapsto f(\alpha)$$

tiene núcleo no trivial.

2) *En este caso $\ker \mathrm{ev}_\alpha = (m_{\alpha,K})$, 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 $\ker \mathrm{ev}_\alpha = (f)$ 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 se un polinomio de mínimo grado posible tal que $f(\alpha) = 0$.

Notamos que tal f es necesariamente irreducible: si $f = g\,h$ 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 $(f_1) = (f_2) = \ker \mathrm{ev}_\alpha$, 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

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

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

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

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

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

Ahora $f(\alpha) = 0$ si y solamente si $f \in \ker \mathrm{ev}_\alpha = (m_{\alpha,K})$, 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.

lección 27
23.10.18

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

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

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 $\overline{f} \in \mathbb{F}_2[X]$ 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 $\mathbb{C}$:

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

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 $f = X^4 - 10\,X^2 + 1$. 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 $3 = a^2 + 2ab\sqrt{2} + 2b$, lo que demostraría que $\sqrt{2} \in \mathbb{Q}$.

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

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

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

* * *

He aquí una caracterización de los elementos algebraicos.

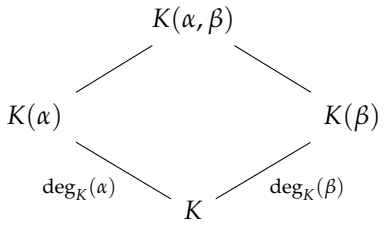
14.2.18. Observación. *Para una extensión L/K un elemento $\alpha \in L$ es algebraico sobre K si y solo si* $\deg_K(\alpha) := [K(\alpha) : K] < \infty$.

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,

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

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 $L = K(\alpha_1, \ldots, \alpha_n)$, donde $\alpha_1, \ldots, \alpha_n \in K$ es un número finito de elementos algebraicos sobre K.*

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

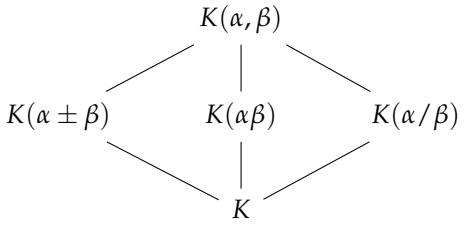
Viceversa, si $L = K(\alpha_1, \ldots, \alpha_n)$ donde $\alpha_1, \ldots, \alpha_n$ son algebraicos sobre K, entonces

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

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, $\alpha \pm \beta$, $\alpha\beta$, α/β (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 $\alpha \pm \beta$, $\alpha\beta$, α/β son algebraicos sobre K. ■

14.2.24. Comentario. Si α y β son algebraicos, aunque la prueba de arriba nos dice que $\alpha \pm \beta$, $\alpha\beta$, α/β son también algebraicos, esta no revela cómo obtener los polinomios mínimos de $\alpha \pm \beta$, $\alpha\beta$, α/β 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

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

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

lección 28–29 24.10.18 25.10.18

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:

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

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

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

que nos da un isomorfismo

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

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

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

así que

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

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

Cuando $\operatorname{char} K = 2$, 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 $\operatorname{char} K = 2$!), mientras que en el caso 2), tenemos $\beta^2 \notin K$.

Podemos concluir que si $\operatorname{char} K \neq 2$, 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 $\operatorname{char} K = 2$, 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

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

es sobreyecivo. 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

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

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

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

así que

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

■

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 $\mathbb{Z}[X]$

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

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

$\underline{X^2-1}$
- $p=2$: $(X+1)^2$
- $p=3$: $(X-1)(X+1)$
- $p=5$: $(X-1)(X+1)$
- $p=7$: $(X-1)(X+1)$
- $p=11$: $(X-1)(X+1)$

$\underline{X^3-1}$
- $p=2$: $(X+1)(X^2+X+1)$
- $p=3$: $(X-1)^3$
- $p=5$: $(X-1)(X^2+X+1)$
- $p=7$: $(X-1)(X-2)(X-4)$
- $p=11$: $(X-1)(X^2+X+1)$

$\underline{X^4-1}$
- $p=2$: $(X+1)^4$
- $p=3$: $(X-1)(X+1)(X^2+1)$
- $p=5$: $(X-1)(X-2)(X-3)(X-4)$
- $p=7$: $(X-1)(X+1)(X^2+1)$
- $p=11$: $(X-1)(X+1)(X^2+1)$

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

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

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

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

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

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

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

$$\Phi_n = f g$$

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 $\mathbb{Z}[X]$:

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

Luego, reduciendo módulo p y aplicando 14.4.3, se obtiene

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

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

$$X^n - 1 = \prod_{d|n} \overline{\Phi_n}$$

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 $\mathrm{mcd}(n,k) = 1$. 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 $n = 1, 2, 3, 4, \ldots$ 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

$$\zeta_6 = \zeta_6^7 = \zeta_6^3\,\zeta_6^4 = \zeta_2\,\zeta_3^2 = -\zeta_3^2 \in \mathbb{Q}(\zeta_3),$$

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 $m = 2k+1$,

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

■

14.4.8. Ejemplo. Tenemos

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

▲

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,

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

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

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

—esto se sigue de las fórmulas

$$\begin{aligned}
\phi(a) &= a \prod_{p \mid a} \left(1 - \frac{1}{p}\right), \\
\phi(m) &= m \prod_{p \mid m} \left(1 - \frac{1}{p}\right), \\
\phi(am) &= am \prod_{p \mid am} \left(1 - \frac{1}{p}\right), \\
\phi(\operatorname{mcd}(a,m)) &= \operatorname{mcd}(a,m) \prod_{p \mid a, p \mid m} \left(1 - \frac{1}{p}\right).
\end{aligned}$$

(Notamos que cuando a y m son coprimos, se tiene $\operatorname{mcd}(a,m) = \phi(\operatorname{mcd}(a,m)) = 1$ 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

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

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

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

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

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

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, $\operatorname{mcd}(k,\ell) = 1$. Pongamos

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

Luego,

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

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

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

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 $n \not\equiv 2 \pmod 4$.

lectura adicional

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

$$\alpha = \sum_{k\geq 1} \frac{1}{10^{k!}} = 0{,}1\,1\,000\,1\,\underbrace{0000000000000000}_{17\text{ ceros}}\,1\,000\cdots$$

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 $\cos\alpha$, $\operatorname{sen}\alpha$, $\tan\alpha$ 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 $k = 1, 2, 3, \ldots$ se tiene

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

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

$$\begin{aligned}
\zeta(2) &= \frac{\pi^2}{6} \approx 1{,}644934\ldots, \\
\zeta(4) &= \frac{\pi^4}{90} \approx 1{,}082323\ldots, \\
\zeta(6) &= \frac{\pi^6}{945} \approx 1{,}017343\ldots, \\
\zeta(8) &= \frac{\pi^8}{9450} \approx 1{,}004077\ldots, \\
\zeta(10) &= \frac{\pi^{10}}{93\,555} \approx 1{,}000994\ldots, \\
\zeta(12) &= \frac{691\,\pi^{12}}{638\,512\,875} \approx 1{,}000246\ldots
\end{aligned}$$

   Se supone que los números $\zeta(3), \zeta(5), \zeta(7), \zeta(9), \zeta(11), \ldots$ 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 $\zeta(3), \zeta(7), \zeta(9), \ldots$ 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 harmónica $\sum_{k\geq 1} \frac{1}{k}$ diverge lentamente, pero el límite

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

[*] 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 $\gamma = 0{,}5772156649\ldots$ 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

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

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

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

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

lección 31
31.10.18

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:

$$\mu_\alpha \colon L \to L, \quad x \mapsto \alpha x.$$

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 $\mu_\alpha \colon L \to L$ respectivamente:

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

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

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

■

14.6.4. Ejemplo. Para $a \in K$ la aplicación $\mu_a \colon L \to L$ 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,

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

El polinomio característico de la matriz de arriba es

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

▲

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 $\mu_{\sqrt[3]{d}}\colon K(\sqrt[3]{d}) \to K(\sqrt[3]{d})$:

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

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

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

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 $N_{L/K}\colon L \to K$ 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 $T_{L/K}\colon L \to K$ 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

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

■

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

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

Luego, tenemos

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

de donde

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

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:

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

lección 32
7.11.18

Polinomio característico y el polinomio mínimo

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

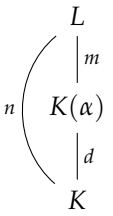
14.6.15. Teorema. *Sean L/K una extensión finita y $\alpha \in L$. Luego,*

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

donde

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

Demostración. Consideremos las extensiones



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

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

Sea

$$\beta_1, \beta_2, \ldots, \beta_m$$

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

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

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

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

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,

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

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*

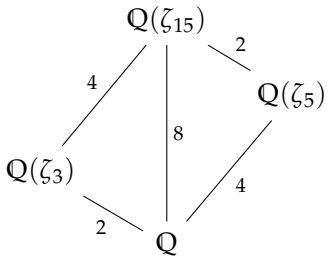
$$m_{\alpha,K} = (X - \alpha_1) \cdots (X - \alpha_d),$$

para algunos $\alpha_1, \ldots, \alpha_d \in L$, 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

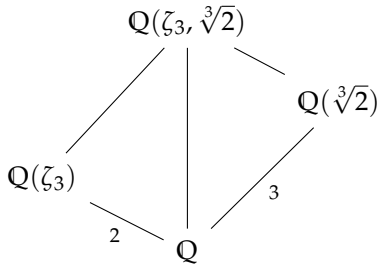
$$m_{\zeta_3,\mathbb{Q}} = \Phi_3 = X^2 + X + 1, \quad m_{\zeta_5,\mathbb{Q}} = \Phi_5 = X^4 + X^3 + X^2 + X + 1.$$

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[*]

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

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 $\alpha_1, \ldots, \alpha_n \in L$. Entonces, el subcuerpo

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

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 $X^2 - d$. ▲

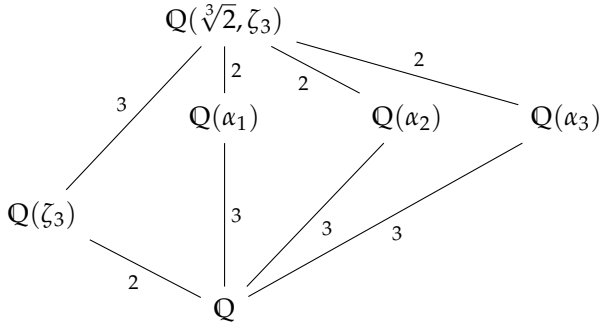
14.7.4. Ejemplo. Para el polinomio $X^n - 1 \in \mathbb{Q}[X]$ el cuerpo ciclotómico $\mathbb{Q}(\zeta_n)$ es un cuerpo de descomposición. En efecto, las raíces complejas de $X^n - 1$ son las raíces n-ésimas de la unidad, generadas por la raíz primitiva $\zeta_n := e^{2\pi\sqrt{-1}/n}$. ▲

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 $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ y esto nos permite tomar $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ 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,

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

■

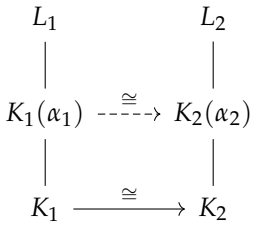
lección 33
8.11.18

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 $\phi\colon K_1 \xrightarrow{\cong} K_2$ un isomorfismo de cuerpos y*

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

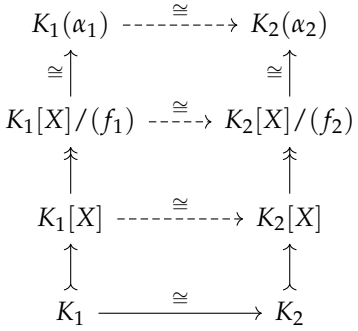
el isomorfismo correspondiente de los anillos de polinomios. Sean $f_1 \in K_1[X]$ y $f_2 \in K_2[X]$ polinomios irreducibles donde $f_2 = \phi(f_1)$ y sean L_1/K_1 y L_2/K_2 extensiones y $\alpha_1 \in L_1$, $\alpha_2 \in L_2$ elementos tales que $f_1(\alpha_1) = 0$ y $f_2(\alpha_2) = 0$. Entonces,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



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

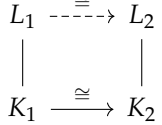
$$K_1[X]/(f_1) \xrightarrow{\cong} K_2[X]/(f_2).$$

Basta considerar el diagrama conmutativo



■

14.7.8. Lema. *Sea $\phi\colon K_1 \xrightarrow{\cong} K_2$ 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:*



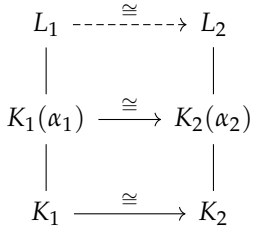
Demostración. Procedamos por inducción sobre $n = \deg f_1$. Notamos que los factores irreducibles de f_1 en $K_1[X]$ corresponden a los factores irreducibles de f_2 en $K_2[X]$.

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 $K_1(\alpha_1) \xrightarrow{\cong} K(\alpha_2)$. Ahora

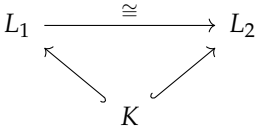
$$f_1 = (X - \alpha_1)\, g_1 \text{ en } K_1(\alpha_1)[X], \quad f_2 = (X - \alpha_2)\, g_2 \text{ en } K_2(\alpha_2)[X].$$

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 $L_1 \xrightarrow{\cong} L_2$.



■

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*



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

14.8 Cuerpos finitos

> ...as a longtime worker using only real or complex numbers, [Joseph F. Ritt] referred to finite fields as "monkey fields".
>
> Steven Krantz, "Mathematical Apocrypha Redux"

En esta sección vamos a construir los cuerpos finitos y ver sus propiedades básicas.

14.8.1. Observación. *Todo cuerpo finito tiene p^n elementos donde p es algún número primo y $n = 1, 2, 3, \ldots$*

Demostración. Un cuerpo finito necesariamente tiene característica p para algún número primo p, y entonces es una extensión finita de $\mathbb{F}_p$. En particular, es un espacio vectorial de dimensión finita n sobre $\mathbb{F}_p$ que tiene p^n elementos. ■

14.8.2. Teorema. *Para todo primo p y $n = 1, 2, 3, \ldots$ existe un cuerpo finito de p^n elementos; específicamente, es un cuerpo de descomposición del polinomio $X^{p^n} - X \in \mathbb{F}_p[X]$. En particular, es único salvo isomorfismo.*

Demostración. Consideremos una extensión $\mathbb{F}/\mathbb{F}_p$. Notamos que el polinomio $f := X^{p^n} - X \in \mathbb{F}_p[X]$ no tiene raíces múltiples en $\mathbb{F}$: en efecto, si en $\mathbb{F}[X]$ se tiene

$$X^{p^n} - X = (X - \alpha)^2 g$$

para algún X, entonces, tomando las derivadas formales en $\mathbb{F}[X]$, se obtiene

$$-1 = p^n X^{p^n-1} - 1 = 2(X - \alpha) g + (X - \alpha)^2 g',$$

de donde $(X - \alpha) \mid -1$, lo que es absurdo.

1) Sea $\mathbb{F}/\mathbb{F}_p$ un cuerpo de descomposición de f. Por lo que acabamos de probar, $\mathbb{F}$ contiene p^n raíces distintas de f. Notamos que las raíces de f forman un subcuerpo de $\mathbb{F}$. En efecto, está claro que $f(0) = f(1) = 0$. Sean $\alpha, \beta \in \mathbb{F}$ elementos tales que $f(\alpha) = f(\beta) = 0$; es decir, $\alpha^{p^n} = \alpha$ y $\beta^{p^n} = \beta$. Luego,
$$(\alpha\beta)^{p^n} = \alpha^{p^n} \beta^{p^n} = \alpha\beta,$$
y además
$$(\alpha + \beta)^{p^n} = \sum_{i+j=p^n} \binom{p^n}{i} \alpha^i \beta^j = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta,$$
usando que $p \mid \binom{p^n}{i}$ para todo $i = 1, \ldots, p^n - 1$. En fin, si $\alpha \neq 0$, entonces
$$(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}.$$
Por la minimalidad de los cuerpos de descomposición, esto significa que todos los elementos de $\mathbb{F}$ son raíces del polinomio f cuyo grado es p^n, así que $|\mathbb{F}| = p^n$.

2) Viceversa, notamos que si $\mathbb{F}$ es un cuerpo de p^n elementos, entonces $\mathbb{F}$ tiene característica p y $\mathbb{F}_p \subseteq \mathbb{F}$. El grupo multiplicativo $\mathbb{F}^\times$ tiene orden $p^n - 1$, así que todo elemento $\alpha \in \mathbb{F}^\times$ satisface $\alpha^{p^n-1} = 1$ según el teorema de Lagrange, así que $\alpha^{p^n} = \alpha$. Para $\alpha = 0$ esto también trivialmente se cumple. Luego, todos los p^n elementos de $\mathbb{F}$ son raíces del polinomio $f := X^{p^n} - X \in \mathbb{F}_p[X]$ de grado p^n, así que $\mathbb{F}$ es un cuerpo de descomposición de f. Recordemos que un cuerpo de descomposición es único salvo isomorfismo.

■

14.8.3. Notación. En vista del último resultado, se suele hablar de *el cuerpo* de p^n elementos y se usa la notación $\mathbb{F}_{p^n}$, o $\mathbb{F}_q$ donde $q = p^n$.

14.8.4. Comentario. Note que para $n > 1$ el anillo $\mathbb{Z}/p^n\mathbb{Z}$ (los restos módulo p^n) tiene divisores de cero, y en particular no es un cuerpo. Entonces, $\mathbb{F}_{p^n}$ es algo muy diferente de $\mathbb{Z}/p^n\mathbb{Z}$.

lección 34
13.11.18

Para construir los cuerpos finitos de manera más explícita, notamos que si $\mathbb{F}_{p^n}$ es un cuerpo de p^n elementos, entonces el grupo $\mathbb{F}_{p^n}^\times$ es cíclico (véase el capítulo 7); es decir, existe un generador $\alpha \in \mathbb{F}_{p^n}^\times$ tal que

$$\mathbb{F}_{p^n} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^n-2}\}.$$

Sea $f := m_{\alpha,\mathbb{F}_p}$ el polinomio mínimo de α sobre $\mathbb{F}_p$. Tenemos

$$\mathbb{F}_p[X]/(f) \cong \mathbb{F}_p(\alpha), \quad [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg f.$$

Pero $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$, así que $\deg f = n$. Esto nos da el siguiente resultado.

14.8.5. Teorema. *Para todo primo p y $n = 1, 2, 3, \ldots$ existe un polinomio irreducible $f \in \mathbb{F}_p[X]$ de grado n.*

14.8.6. Comentario. Si f es un polinomio irreducible en $\mathbb{F}_p[X]$ y $\mathbb{F} := \mathbb{F}_p[X]/(f)$, denotemos por α la imagen de X en el cociente. Este α *no tiene por qué* ser un generador del grupo multiplicativo $\mathbb{F}^\times$. Por ejemplo, consideremos un cuerpo finito de 9 elementos $\mathbb{F} := \mathbb{F}_3[X]/(X^2+1)$. En este caso $\alpha^2 = -1$, y luego $\alpha^4 = 1$. Siendo un grupo cíclico de 8 elementos, $\mathbb{F}^\times$ tiene $\phi(8) = 4$ diferentes generadores y son $\alpha+1$, $\alpha+2$, $2\alpha+1$, $2\alpha+2$.

14.8.7. Ejemplo. He aquí algunos polinomios irreducibles en $\mathbb{F}_p[X]$.

$\underline{p=2}$	$\underline{p=3}$	$\underline{p=5}$
X^2+X+1	X^2+X+2	X^2+X+1
X^3+X^2+1	X^3+X^2+X+2	X^3+X^2+3X+4
$X^4+X^3+X^2+X+1$	$X^4+X^3+X^2+X+1$	$X^4+X^3+2X^2+X+3$
$X^5+X^4+X^2+X+1$	$X^5+X^4+2X^3+1$	$X^5+X^4+X^3+2X^2+3X+1$
$X^6+X^5+X^3+X^2+1$	$X^6+X^5+X^4+X^3+X^2+X+1$	$X^6+X^5+X^4+X^3+X^2+X+1$

▲

Entonces, para construir un cuerpo de p^n elementos, se puede tomar un polinomio irreducible $f \in \mathbb{F}_p[X]$ de grado n y pasar al cociente $\mathbb{F}_p[X]/(f)$. Diferentes f dan el mismo resultado, salvo isomorfismo. Sería interesante saber cuántas posibilidades hay para escoger a f. Denotemos por N_n el número de los polinomios mónicos irreducibles en $\mathbb{F}_p[X]$ de grado n. Nuestro objetivo es deducir una fórmula explícita para N_n.

La fórmula de Gauss para el número de polinomios irreducibles

14.8.8. Lema.

1) *Sea k cualquier cuerpo. El polinomio $X^\ell - 1$ divide a $X^m - 1$ en $k[X]$ si y solo si $\ell \mid m$.*

2) *Sea a un entero ≥ 2. El número $a^\ell - 1$ divide a $a^m - 1$ en $\mathbb{Z}$ si y solo si $\ell \mid m$.*

3) *En particular, para un primo p y $d, n \geq 1$ se tiene $(X^{p^d} - X) \mid (X^{p^n} - X)$ si y solo si $d \mid n$.*

Demostración. En la primera parte, escribamos $m = q\ell + r$ donde $0 \leq r < \ell$. Tenemos en $k(X)$

$$\frac{X^m-1}{X^\ell-1} = \frac{(X^{q\ell+r} - X^r) + (X^r - 1)}{X^\ell - 1} = X^r \frac{X^{q\ell}-1}{X^\ell-1} + \frac{X^r-1}{X^\ell-1} = X^r \sum_{0 \leq i < q} X^{i\ell} + \frac{X^r-1}{X^\ell-1}.$$

Esto es un polinomio si y solamente si $\frac{X^r-1}{X^\ell-1}$ lo es. Pero $r < \ell$, así que la única opción es $r = 0$.

La segunda parte se demuestra de la misma manera. La última parte es una combinación de 1) y 2):

$$(X^{p^d} - X) \mid (X^{p^n} - X) \iff (X^{p^d-1} - 1) \mid (X^{p^n-1} - 1) \iff (p^d - 1) \mid (p^n - 1) \iff d \mid n.$$

■

14.8.9. Lema. *Denotemos por f_d el producto de todos los polinomios mónicos irreducibles de grado d en $\mathbb{F}_p[X]$. Luego,*

$$X^{p^n} - X = \prod_{d \mid n} f_d.$$

Demostración. Ya hemos notado en la prueba de 14.8.2 que el polinomio $X^{p^n} - X$ no tiene raíces múltiples en su cuerpo de descomposición. En particular, $X^{p^n} - X$ no puede tener factores irreducubles múltiples en $\mathbb{F}_p[X]$[*]. Sería entonces suficiente comprobar que un polinomio mónico irreducible $f \in \mathbb{F}_p[X]$ es de grado d divide a $X^{p^n} - X$ si y solo si $d \mid n$.

Consideremos el cuerpo finito

$$\mathbb{F} := \mathbb{F}_p[X]/(f)$$

y denotemos por $\alpha \in \mathbb{F}$ la imagen de X en el cociente. En este caso f es el polinomio mínimo de α sobre $\mathbb{F}_p$. Siendo un cuerpo de p^d elementos, $\mathbb{F}$ es un cuerpo de descomposición del polinomio $X^{p^d} - X \in \mathbb{F}_p[X]$.

1) Si $d \mid n$, entonces, según el lema anterior, $(X^{p^d} - X) \mid (X^{p^n} - X)$. Entonces, todas las raíces de $X^{p^d} - X$ son también raíces de $X^{p^n} - X$, y en particular $\alpha^{p^n} - \alpha = 0$. Tenemos entonces

$$f \mid (X^{p^n} - X).$$

2) Viceversa, si $f \mid (X^{p^n} - X)$, entonces $f(\alpha) = 0$ implica que $\alpha^{p^n} - \alpha = 0$. Además, para cualquier elemento

$$x = a_{d-1}\,\alpha^{d-1} + \cdots + a_1\,\alpha + a_0 \in \mathbb{F},$$

donde $a_0, a_1, \ldots, a_{d-1} \in \mathbb{F}_p$, se tiene

$$x^{p^n} = a_{d-1}\,(\alpha^{p^n})^{d-1} + \cdots + a_1\,(\alpha^{p^n}) + a_0 = x,$$

así que *todos* los elementos de $\mathbb{F}$ son raíces de $X^{p^n} - X$. Se sigue que $(X^{p^d} - X) \mid (X^{p^n} - X)$, y luego $d \mid n$ por el lema anterior.

■

14.8.10. Ejemplo. Se sigue que para obtener todos los polinomios irreducibles de grado $d \mid n$ en $\mathbb{F}_p[X]$, basta factorizar el polinomio $X^{p^n} - X$ en $\mathbb{F}_p[X]$. Por ejemplo, en $\mathbb{F}_2[X]$ se tiene

$$X^{16} - X = X\,(X+1)\,(X^2+X+1)\,(X^4+X+1)\,(X^4+X^3+1)\,(X^4+X^3+X^2+X+1).$$

y en $\mathbb{F}_3[X]$

$$X^9 - X = X\,(X+1)\,(X+2)\,(X^2+1)\,(X^2+X+2)\,(X^2+2\,X+2).$$

▲

14.8.11. Corolario. *Se cumple*

$$p^n = \sum_{d \mid n} d \cdot N_d.$$

Demostración. Basta comparar grados a ambos lados de la identidad $X^{p^n} - X = \prod_{d \mid n} f_d$ en $\mathbb{F}_p[X]$. ■

Para obtener una fórmula para N_n, se puede usar la fórmula de inversión de Möbius, revisada en el apéndice D.

[*]Sin pasar al cuerpo de descomposición, basta notar que si $X^{p^n} - X = f^2\,g$, entonces, tomando las derivadas formales en $\mathbb{F}_p[X]$, se obtiene $2f\,f'\,g + f^2\,g' = -1$, así que $f \mid -1$ y $f \in \mathbb{F}_p^\times$ es una constante invertible.

14.8.12. Teorema (Gauss). *El número de polinomios mónicos irreducibles de grado n en $\mathbb{F}_p[X]$ es igual a*

$$N_n := \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)\, p^d,$$

donde μ denota la ***función de Möbius****;*

$$\mu(1) := 1, \quad \mu(n) = 0 \text{ si } n \text{ no es libre de cuadrados},$$

y para n libre de cuadrados se pone

$$\mu(p_1 \cdots p_k) := (-1)^k,$$

donde k es el número de diferentes números primos que aparecen en la factorización de n.

Demostración. Consideremos la función $f(n) := n\, N_n$. Luego,

$$F(n) := \sum_{d|n} f(d) = \sum_{d|n} d\, N_d = p^n,$$

usando 14.8.11. La fórmula de inversión de Möbius nos da

$$f(n) = n\, N_n = \sum_{d|n}\mu\left(\frac{n}{d}\right)\, F(d) = \sum_{d|n}\mu\left(\frac{n}{d}\right)\, p^d.$$

■

14.8.13. Ejemplo. Hay

$$\frac{1}{6}\left(\mu(1)\cdot 2^6 + \mu(3)\cdot 2^2 + \mu(2)\cdot 2^3 + \mu(6)\cdot 2\right) = \frac{1}{6}\left(64 - 4 - 8 + 2\right) = 9$$

polinomios mónicos irreducibles en $\mathbb{F}_2[X]$ de grado 6. Factorizando el polinomio $X^{2^6} - X$ en $\mathbb{F}_2[X]$, se puede ver que son

$$\begin{array}{lll} X^6 + X + 1, & X^6 + X^4 + X^3 + X + 1, & X^6 + X^5 + X^3 + X^2 + 1, \\ X^6 + X^3 + 1, & X^6 + X^5 + 1, & X^6 + X^5 + X^4 + X + 1, \\ X^6 + X^4 + X^2 + X + 1, & X^6 + X^5 + X^2 + X + 1, & X^6 + X^5 + X^4 + X^2 + 1. \end{array}$$

He aquí algunos valores de N_n para diferentes p y n.

p \ n	1	2	3	4	5	6
2	2	1	2	3	6	9
3	3	3	8	18	48	116
5	5	10	40	150	624	2 580
7	7	21	112	588	3 360	19 544
11	11	55	440	3 630	32 208	295 020
13	13	78	728	7 098	74 256	804 076
17	17	136	1 632	20 808	283 968	4 022 064
19	19	171	2 280	32 490	495 216	7 839 780

El número de los polinomios mónicos irreducibles de grado n en $\mathbb{F}_p[X]$

▲

En particular, la fórmula de Gauss implica que para todo $n \geq 1$ existe un polinomio mónico irreducible $f \in \mathbb{F}_p[X]$ de grado n en $\mathbb{F}_p[X]$. En efecto,

$$N_n = \frac{1}{n}\left(p^n + \sum_{\substack{d|n \\ d\neq n}} \pm p^d\right) \geq \frac{1}{n}\left(p^n - (p^{n-1} + \cdots + p^2 + p)\right) > 0,$$

dado que

$$p^{n-1} + \cdots + p^2 + p = \frac{p^n - 1}{p - 1} - 1 < p^n.$$

14.9 Automorfismos de cuerpos finitos

La construcción de cuerpo finito de p^n elementos depende de una elección de un polinomio irreducible de grado n en $\mathbb{F}_p[X]$. Aunque probamos su existencia, no hay un modo canónico de escogerlo. Sin embargo, sabemos que todos los cuerpos de orden p^n son isomorfos entre sí. Esto nos lleva a la siguiente pregunta: ¿cuántos automorfismos tiene un cuerpo finito $\mathbb{F}_{p^n}$?

Para un cuerpo K los automorfismos $\sigma\colon K \xrightarrow{\cong} K$ forman un grupo $\mathrm{Aut}(K)$ respecto a la composición.

14.9.1. Teorema. *Para un cuerpo finito $\mathbb{F}_{p^n}$ el grupo de automorfismos $\mathrm{Aut}(\mathbb{F}_{p^n})$ es cíclico de orden n. Específicamente,*

$$\mathrm{Aut}(\mathbb{F}_{p^n}) = \langle F \rangle \cong \mathbb{Z}/n\mathbb{Z},$$

donde F denota el ***automorfismo de Frobenius***

$$F\colon x \mapsto x^p.$$

Demostración. Notamos primero que F es un automorfismo. Para cualesquiera $x, y \in \mathbb{F}_{p^n}$ tenemos obviamente

$$(xy)^p = x^p\, y^p.$$

Para las sumas, notamos que $\mathbb{F}_{p^n}$ es un cuerpo de característica p, así que

$$(x+y)^p = \sum_{i+j=p} \binom{p}{i} x^i\, y^j = x^p + y^p,$$

puesto que $p \mid \binom{p}{i}$ para $i = 1, \ldots, p-1$. Esto demuestra que F es un homomorfismo $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. Como todo homomorfismo de cuerpos, F es automáticamente inyectivo. Puesto que $\mathbb{F}_{p^n}$ es finito, F es sobreyectivo.

El grupo multiplicativo $\mathbb{F}_{p^n}^\times$ es cíclico y podemos escoger un generador $\alpha \in \mathbb{F}_{p^n}^\times$. Todo elemento $x \in \mathbb{F}_{p^n}^\times$ es de la forma α^i para $i = 0, 1, \ldots, p^n - 2$, y para cualquier automorfismo $\sigma\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ se tiene

$$\sigma(\alpha^i) = \sigma(\alpha)^i.$$

Esto demuestra que σ está definido por la imagen de α. Consideremos las potencias del automorfismo de Frobenius

$$F^k := \underbrace{F \circ \cdots \circ F}_{k}\colon x \mapsto x^{p^k}.$$

Tenemos $F^k = \mathrm{id}$ si y solo si $\alpha^{p^k} = \alpha$; es decir, $\alpha^{p^k - 1} = 1$ en $\mathbb{F}_{p^n}^\times$. Dado que α tiene orden $p^n - 1$ en el grupo $\mathbb{F}_{p^n}^\times$, lo último sucede si y solo si $(p^n - 1) \mid (p^k - 1)$; es decir, si y solo si $n \mid k$. Podemos concluir que

$$F^0 = \mathrm{id},\ F,\ F^2,\ \ldots,\ F^{n-1}$$

son n diferentes automorfismos de $\mathbb{F}_{p^n}$. Para terminar la prueba, hay que ver que $\mathbb{F}_{p^n}$ no tiene otros automorfismos.

Sea $f = m_{\alpha,\mathbb{F}_p}$ el polinomio mínimo de α sobre $\mathbb{F}_p$. Luego,

$$\mathbb{F}_p[X]/(f) \cong \mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}.$$

En particular,

$$\deg f = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n.$$

Tenemos $f(\alpha) = 0$, y para cualquier automorfismo $\sigma\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ necesariamente

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0,$$

así que $\sigma(\alpha)$ debe ser una raíz de f. Pero f, siendo un polinomio de grado n, tiene a lo sumo n raíces, y esto demuestra que $|\operatorname{Aut}(\mathbb{F}_{p^n})| \leq n$. ■

lección 35
14.11.18

14.9.2. Corolario. *En un cuerpo finito $\mathbb{F}_{p^n}$ todo elemento es una p-ésima potencia.*

Demostración. Se sigue de la sobreyectividad del automorfismo de Frobenius $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. ■

14.9.3. Teorema. *Los subcuerpos de un cuerpo finito $\mathbb{F}_{p^n}$ corresponden a los divisores de n: son precisamente*

$$\mathbb{F}_{p^d} := \{x \in \mathbb{F}_{p^n} \mid x^{p^d} = x\}.$$

Demostración. Primero, si tenemos un subcuerpo $\mathbb{F} \subseteq \mathbb{F}_{p^n}$, entonces necesariamente $\mathbb{F}_p \subseteq \mathbb{F}$ y $|\mathbb{F}| = p^d$ para algún d. Luego,

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}] \cdot [\mathbb{F} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}] \cdot d,$$

demuestra que $d \mid n$. Dado que el grupo multiplicativo $\mathbb{F}^\times$ es cíclico de orden $p^d - 1$, los elementos de $\mathbb{F}$ son precisamente las raíces del polinomio $X^{p^d} - X \in \mathbb{F}_p[X]$:

$$\mathbb{F} = \mathbb{F}_d := \{x \in \mathbb{F}_{p^n} \mid x^{p^d} - x = 0\} = \{x \in \mathbb{F}_{p^n} \mid F^d(x) = x\}.$$

donde $F\colon x \mapsto x^p$ denota el automorfismo de Frobenius. Viceversa, para cualquier $d \mid n$ el conjunto $\mathbb{F}_{d^n}$ de arriba tiene p^d elementos: tenemos $(X^{p^d} - X) \mid (X^{p^n} - X)$ y el polinomio $X^{p^n} - X$ se descompone en factores lineales en $\mathbb{F}_{p^n}[X]$. Además, para cualquier cuerpo K y un endomorfismo $\sigma\colon K \xrightarrow{\cong} K$, el conjunto

$$K^\sigma := \{x \in K \mid \sigma(x) = x\}$$

es un subcuerpo de K: esto se sigue de las identidades

$$\sigma(x+y) = \sigma(x) + \sigma(y), \quad \sigma(1) = 1, \quad \sigma(xy) = \sigma(x)\,\sigma(y), \quad \sigma(x^{-1}) = \sigma(x)^{-1}.$$

■

14.9.4. Ejemplo. Consideremos un cuerpo de $2^6 = 64$ elementos

$$\mathbb{F}_{64} = \mathbb{F}_2[X]/(X^6 + X^5 + X^3 + X^2 + 1).$$

Denotemos por α la imagen de X en el cociente. Tenemos

$$\mathbb{F}_{64} = \{a_5\,\alpha^5 + a_4\,\alpha^4 + a_3\,\alpha^3 + a_2\,\alpha^2 + a_1\,\alpha + a_0 \mid a_i = 0, 1\}.$$

Los elementos fijos bajo el automorfismo de Frobenius $F\colon x \mapsto x^2$ corresponden al subcuerpo

$$\mathbb{F}_2 = \{0, 1\}.$$

Los elementos fijos por $F^2\colon x \mapsto x^4$ corresponden al subcuerpo

$$\mathbb{F}_4 = \{0,\ 1,\ \alpha^4 + \alpha^2 + \alpha,\ \alpha^4 + \alpha^2 + \alpha + 1\}.$$

Los elementos fijos por $F^3\colon x \mapsto x^8$ corresponden al subcuerpo

$$\mathbb{F}_8 = \{0,\ 1,\ \alpha^2 + \alpha,\ \alpha^2 + \alpha + 1,\ \alpha^4 + \alpha,\ \alpha^4 + \alpha + 1,\ \alpha^4 + \alpha^2,\ \alpha^4 + \alpha^2 + 1\}.$$

▲

14.9.5. Comentario. Notamos que $\mathrm{Aut}(\mathbb{F}_{p^n}) = \langle F \rangle$ es el grupo cíclico de orden n generado por el automorfismo de Frobenius $F\colon x \mapsto x^p$. Los subgrupos de $\mathrm{Aut}(\mathbb{F}_{p^n})$ son precisamente $\langle F^d \rangle$ para $d \mid n$, y entonces hemos obtenido una biyección entre los subcuerpos de $\mathbb{F}_{p^n}$ y los subgrupos de $\mathrm{Aut}(\mathbb{F}_{p^n})$. Esto no es una coincidencia: es un caso particular de la **teoría de Galois**.

14.10 Cuerpos finitos y la reciprocidad cuadrática

Recordemos que para un número entero a y un primo p el **símbolo de Legendre** se define mediante

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & \text{si } p \nmid a \text{ y } a \text{ es un cuadrado módulo } p, \\ -1, & \text{si } p \nmid a \text{ y } a \text{ no es un cuadrado módulo } p, \\ 0, & \text{si } p \mid a. \end{cases}$$

Tenemos las siguientes propiedades elementales.

a) El símbolo de Legendre es multiplicativo: se tiene

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

para cualesquiera $a, b \in \mathbb{Z}$.

b) Si p es un primo impar, entonces entre los números $\{1, 2, \ldots, p-1\}$ precisamente la mitad son cuadrados módulo p y la mitad no son cuadrados módulo p; en particular,

$$\sum_{0 \le i \le p-1} \left(\frac{i}{p}\right) = 0. \tag{14.2}$$

c) El símbolo de Legendre puede ser interpretado mediante el **criterio de Euler**: si p es un primo impar, entonces

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Todas estas propiedades se deducen fácilmente del hecho de que $\mathbb{F}_p^\times$ sea un grupo cíclico: existe un generador $\alpha \in \mathbb{F}_p^\times$ tal que todo elemento de $\mathbb{F}_p^\times$ es de la forma α^i para algún $i \in \mathbb{Z}$. Luego, α^i es un cuadrado si y solo si i es par (véase el capítulo 7 para los detalles).

El objetivo de esta sección es presentar una aplicación de cuerpos finitos en una prueba de la **ley de reciprocidad cuadrática** de Gauss.

1) Si p y q son diferentes primos impares, entonces

$$\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{p}{q}\right) = \begin{cases} +\left(\frac{p}{q}\right), & \text{si } p \equiv 1 \text{ o } q \equiv 1 \pmod 4, \\ -\left(\frac{p}{q}\right), & \text{si } p \equiv 3 \text{ y } q \equiv 3 \pmod 4. \end{cases}.$$

2) La **primera ley suplementaria**: si p es un primo impar, entonces

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & \text{si } p \equiv 1 \pmod 4, \\ -1, & \text{si } p \equiv 3 \pmod 4. \end{cases}$$

3) La **segunda ley suplementaria**: si p es un primo impar, entonces

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & \text{si } p \equiv \pm 1 \pmod 8, \\ -1, & \text{si } p \equiv \pm 3 \pmod 8. \end{cases}$$

14.10.1. Ejemplo. He aquí una pequeña tabla de los valores de $\left(\frac{p}{q}\right)$.

p \ q	3	5	7	11	13	17	19	23	29	31
-1	$-$	$+$	$-$	$-$	$+$	$+$	$-$	$-$	$+$	$-$
2	$-$	$-$	$+$	$-$	$-$	$+$	$-$	$+$	$-$	$+$
3	0	$-$	$-$	$+$	$+$	$-$	$-$	$+$	$-$	$-$
5	$-$	0	$-$	$+$	$-$	$-$	$+$	$-$	$+$	$+$
7	$+$	$-$	0	$-$	$-$	$-$	$+$	$-$	$+$	$+$
11	$-$	$+$	$+$	0	$-$	$-$	$+$	$-$	$-$	$-$
13	$+$	$-$	$-$	$-$	0	$+$	$-$	$+$	$+$	$-$
17	$-$	$-$	$-$	$-$	$+$	0	$+$	$-$	$-$	$-$
19	$+$	$+$	$-$	$-$	$-$	$+$	0	$-$	$-$	$+$
23	$-$	$-$	$+$	$+$	$+$	$-$	$+$	0	$+$	$-$
29	$-$	$+$	$+$	$-$	$+$	$-$	$-$	$+$	0	$-$
31	$+$	$+$	$-$	$+$	$-$	$-$	$-$	$+$	$-$	0

▲

Notamos que la primera ley suplementaria se deduce inmediatamente del criterio de Euler. Otro modo de verlo: para $\alpha \in \mathbb{F}_p^\times$ se tiene $\alpha^2 = -1$ si y solamente si el orden de α es igual a 4. Entonces, -1 es un cuadrado si y solo si $4 \mid (p-1)$.

Vamos a probar la segunda ley suplementaria y luego la ley principal. Nuestra exposición sigue [IR1990, Chapter 6], pero en lugar de las raíces de la unidad ζ_n usamos los cuerpos finitos, según lo indicado en [IR1990, §7.3].

La segunda ley suplementaria

Antes de probar la ley principal, empecemos por la segunda ley suplementaria. Si p es un primo impar, entonces $p^2 \equiv 1 \pmod 8$, puesto que cualquier cuadrado de un número impar es congruente a 1 módulo 8:

$$1^2 = 1, \quad 3^2 = 9, \quad 5^2 = 25, \quad 7^2 = 49.$$

Consideremos el cuerpo finito $\mathbb{F}_{p^2}$. El grupo multiplicativo $\mathbb{F}_{p^2}^\times$ es cíclico de orden $p^2 - 1$, y dado que $8 \mid (p^2 - 1)$, existe un elemento $\alpha \in \mathbb{F}_{p^2}^\times$ de orden 8. Notamos que

$$(\alpha^4 - 1)(\alpha^4 + 1) = \alpha^8 - 1 = 0.$$

Dado que $\alpha^4 \neq 1$, tenemos $\alpha^4 = -1$, de donde se siguen las identidades

$$\alpha^2 + \alpha^{-2} = 0, \quad \alpha^3 = -\alpha^{-1}.$$

Pongamos

$$\tau := \alpha + \alpha^{-1}.$$

Notamos que $\tau \neq 0$. En efecto, si $\alpha^{-1} = -\alpha$, entonces $\alpha^2 = -1$ y luego $\alpha^4 = 1$, pero no es el caso.

Tenemos

$$\tau^{p-1} = (\tau^2)^{\frac{p-1}{2}} = (\alpha^2 + 2 + \alpha^{-2})^{\frac{p-1}{2}} = 2^{\frac{p-1}{2}} = \left(\frac{2}{p}\right),$$

donde la última igualdad se sigue del criterio de Euler. En consecuencia

$$\alpha^p + \alpha^{-p} = (\alpha + \alpha^{-1})^p = \tau^p = \left(\frac{2}{p}\right) \tau.$$

Dado que α tiene orden 8, la expresión a la izquierda depende solamente del residuo de p módulo 8:

$$\alpha^p + \alpha^{-p} = \left\{ \begin{array}{lll} \alpha + \alpha^{-1} = \tau, & p \equiv \pm 1 & \pmod 8 \\ \alpha^3 + \alpha^{-3} = -\tau, & p \equiv \pm 3 & \pmod 8 \end{array} \right\} = (-1)^{\frac{p^2-1}{8}} \tau.$$

Comparando las últimas dos identidades, se obtiene

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

14.10.2. Comentario. El mismo argumento funciona para la raíz de la unidad ζ_8 en lugar de α y el anillo $\mathbb{Z}[\zeta_8]$ en lugar de $\mathbb{F}_{p^2}$. En este caso hay que considerar identidades en $\mathbb{Z}[\zeta_8]$ módulo p.

lección 36
15.11.18

La ley principal

Sean p y q dos diferentes primos impares. Podemos escoger un número $n = 1, 2, 3, \ldots$ tal que

$$q^n \equiv 1 \pmod p$$

(por ejemplo, basta tomar $n = p - 1$). Consideremos el cuerpo finito $\mathbb{F}_{q^n}$. El grupo multiplicativo $\mathbb{F}_{q^n}^\times$ es cíclico de orden $q^n - 1$. Por nuestra elección de n, se tiene $p \mid (q^n - 1)$, así que existe un elemento $\alpha \in \mathbb{F}_{q^n}^\times$ de orden p.

Para $a \in \mathbb{Z}$ pongamos

$$\tau_a := \sum_{0 \leq i \leq p-1} \left(\frac{i}{p}\right) \alpha^{ai} \in \mathbb{F}_{q^n}.$$

En particular, definamos

$$\tau := \tau_1.$$

A partir de ahora y hasta el final de esta sección, todos los sumatorios serán entre 0 y $p-1$, así que por brevedad vamos a escribir "$\sum_i$" en lugar de "$\sum_{0\le i\le p-1}$".

14.10.3. Lema. *Tenemos*

$$\sum_i \alpha^{ai} = \begin{cases} p, & si\ p \mid a, \\ 0, & si\ p \nmid a. \end{cases}$$

Demostración. Si $p \mid a$, entonces $\alpha^{ai} = 1$ para todo $0 \le i \le p-1$, así que

$$\sum_i \alpha^{ai} = p.$$

Si $p \nmid a$, entonces $\alpha^a \neq 1$, y luego

$$\sum_i \alpha^{ai} = \frac{\alpha^{ap}-1}{\alpha^a - 1} = 0.$$

■

14.10.4. Proposición (Gauss). *En $\mathbb{F}_{q^n}$ se cumplen las identidades*

1) $\tau_a = \left(\frac{a}{p}\right)\tau$.

2) $\tau^2 = (-1)^{\frac{p-1}{2}}\, p$.

Demostración. Si $p \mid a$, entonces

$$\left(\frac{a}{p}\right) = 0.$$

Por otro lado, tenemos $\alpha^{ai} = 1$ para todo $0 \le i \le p-1$, dado que el orden de α es igual a p, y luego,

$$\tau_a = \sum_i \left(\frac{i}{p}\right) = 0$$

por (14.2). Si $p \nmid a$, entonces calculamos que

$$\left(\frac{a}{p}\right)\tau_a = \sum_i \left(\frac{ai}{p}\right)\alpha^{ai} = \sum_j \left(\frac{j}{p}\right)\alpha^j = \tau$$

—el símbolo de Legendre $\left(\frac{j}{p}\right)$ y el elemento α^j dependen solo del resto de j módulo p y los números ai para $0 \le i \le p-1$ nos dan todos los restos módulo p. Ahora $\left(\frac{a}{p}\right) = \pm 1$, así que al multiplicar la identidad de arriba por $\left(\frac{a}{p}\right)$ nos queda la identidad 1)

$$\tau_a = \left(\frac{a}{p}\right)\tau.$$

Probemos la segunda identidad. Notamos que si $p \nmid a$, entonces la identidad 1) nos da

$$\tau_a\,\tau_{-a} = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right)\tau^2 = \left(\frac{-1}{p}\right)\tau^2,$$

y si $p \mid a$, entonces $\tau_a \, \tau_{-a} = 0$. Luego,

$$\sum_a \tau_a \, \tau_{-a} = \left(\frac{-1}{p}\right) (p-1) \, \tau^2. \tag{14.3}$$

Por otro lado, tenemos

$$\tau_a \, \tau_{-a} = \sum_i \sum_j \left(\frac{i}{p}\right) \left(\frac{j}{p}\right) \alpha^{a\,(i-j)},$$

y sumando estas identidades para $0 \leq a \leq p-1$, se obtiene

$$\sum_a \tau_a \, \tau_{-a} = \sum_i \sum_j \left(\frac{i}{p}\right) \left(\frac{j}{p}\right) \sum_a \alpha^{a\,(i-j)}.$$

El cálculo del lema 14.10.3 nos dice que

$$\sum_a \alpha^{a\,(i-j)} = \begin{cases} p, & \text{si } i = j, \\ 0, & \text{si } i \neq j. \end{cases}$$

Entonces,

$$\sum_a \tau_a \, \tau_{-a} = \sum_i \left(\frac{i}{p}\right)^2 p = (p-1)\, p. \tag{14.4}$$

Comparando (14.3) y (14.4), tenemos

$$\left(\frac{-1}{p}\right) (p-1) \, \tau^2 = (p-1)\, p,$$

de donde

$$\tau^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} \, p.$$

■

Estamos listos para probar la ley de reciprocidad cuadrática. Denotemos

$$p^* := (-1)^{\frac{p-1}{2}} \, p.$$

La segunda identidad de 14.10.4 nos dice que

$$\tau^2 = p^* \quad \text{en } \mathbb{F}_{q^n}.$$

Entonces,

$$\left(\frac{p^*}{q}\right) = 1 \iff \tau \in \mathbb{F}_q \subset \mathbb{F}_{q^n} \iff \tau^q = \tau.$$

(En efecto, si p^* es un cuadrado en $\mathbb{F}_q$, entonces $p^* = x^2$ para algún $x \in \mathbb{F}_q$. Pero en este caso $\tau = \pm x$, así que $\tau \in \mathbb{F}_q$. Viceversa, si $\tau \in \mathbb{F}_q$, entonces $p^* = \tau^2$ es un cuadrado en $\mathbb{F}_q$.) Luego, tenemos en $\mathbb{F}_{q^n}$

$$\tau^q = \left(\sum_i \left(\frac{i}{p}\right) \alpha^i\right)^q = \sum_i \left(\frac{i}{p}\right)^q \alpha^{qi} = \sum_i \left(\frac{i}{p}\right) \alpha^{qi} = \tau_q = \left(\frac{q}{p}\right) \tau,$$

según la primera identidad 14.10.4. Entonces, la condición $\tau^q = \tau$ equivale a

$$\left(\frac{q}{p}\right) = 1.$$

Hemos probado que

$$\left(\frac{p^*}{q}\right) = 1 \iff \left(\frac{q}{p}\right) = 1.$$

Esto equivale a la identidad

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{p}{q}\right).$$

14.10.5. Comentario. Estos cálculos se pueden hacer con la raíz de la unidad ζ_p en lugar de α. En este caso la expresión

$$g_a := \sum_{0 \le a \le p-1} \left(\frac{a}{p}\right) \zeta_p^a, \quad g := g_1$$

se conoce como la **suma cuadrática de Gauss**. Muchas pruebas de la reciprocidad cuadrática, incluso una de las pruebas de Gauss, se basan en la identidad

$$g^2 = \left(\frac{-1}{p}\right) p.$$

En el tratado de Gauss "Disquisitiones Arithmeticae" aparecen ocho pruebas diferentes de la reciprocidad cuadrática, y hoy en día se conocen alrededor de 250[*]. Para más información sobre las leyes de reciprocidad en el contexto histórico, véase el libro [Lem2000].

[*]Véase http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html

14.11 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 $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$.

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 $K := \mathbb{Q}[X]/(f)$. Exprese 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 $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$.*

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 $\mathbb{Q}(\zeta_m) \ncong \mathbb{Q}(\zeta_n)$.*

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 $\mathbb{Q}(\zeta_\infty) = \mathbb{Q}(\zeta_3, \zeta_4, \zeta_5, \zeta_6, \ldots)$ 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 $\mathbb{Q}[\![X]\!]$:*

$$\exp(X) := \sum_{n\geq 0} \frac{X^n}{n!}, \quad \log(1+X) := \sum_{n\geq 0} (-1)^{n+1} \frac{X^n}{n},$$
$$\operatorname{sen}(X) := \sum_{n\geq 0} (-1)^n \frac{X^{2n+1}}{(2n+1)!}, \quad \cos(X) := \sum_{n\geq 0} (-1)^n \frac{X^{2n}}{(2n)!}.$$

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****:*

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

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*

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

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* $n = 2, 3, 4, \ldots$

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.

Cuerpos finitos

Ejercicio 14.18.

1) *Encuentre polinomios irreducibles de grado* 2

$$f \in \mathbb{F}_2[X] \quad y \quad g \in \mathbb{F}_3[X].$$

2) *Consideremos los cuerpos finitos*

$$\mathbb{F}_4 := \mathbb{F}_2[X]/(f) \quad y \quad \mathbb{F}_9 := \mathbb{F}_3[X]/(g)$$

de orden 4 *y* 9 *respectivamente. Escriba las tablas de adición y multiplicación para* $\mathbb{F}_4$ *y* $\mathbb{F}_9$.

3) *Encuentre el orden de cada elemento del grupo multiplicativo* $\mathbb{F}_4^\times$ *y* $\mathbb{F}_9^\times$.

4) *Consideremos la ecuación*

$$y^2 = x^3 - x.$$

Enumere todas sus soluciones $(x, y) \in R^2$, *donde*

$$R = \mathbb{F}_2,\ \mathbb{F}_3,\ \mathbb{F}_4,\ \mathbb{F}_9,\ \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/9\mathbb{Z}.$$

Ejercicio 14.19. *Sea* $q = p^k$ *donde* p *es primo y* $k = 1, 2, 3, \ldots$ *Demuestre que para cualquier* $n = 1, 2, 3, \ldots$ *existe un polinomio mónico irreducible* $f \in \mathbb{F}_q[X]$ *de grado* n. *(Lo probamos en clase para* $k = 1$.*)*

Ejercicio 14.20. *Encuentre isomorfismos explícitos entre los cuerpos*

$$\mathbb{F}_3[X]/(X^2 + 1), \quad \mathbb{F}_3[X]/(X^2 + X + 2), \quad \mathbb{F}_3[X]/(X^2 + 2X + 2).$$

Ejercicio 14.21. *Encuentre los polinomios mónicos irreducibles de grado* 3 *en* $\mathbb{F}_2[X]$ *factorizando* $X^8 - X$.

Ejercicio 14.22. *Sean* p *y* q *dos diferentes primos impares. Demuestre que el número de polinomios mónicos irreducibles de grado* q *en* $\mathbb{F}_p[X]$ *es igual a* $\frac{1}{q}(p^q - p)$.

Ejercicio 14.23. *Sea* k *un cuerpo.*

1) *Demuestre que los cuadrados en el grupo multiplicativo* $k^\times$ *forman un subgrupo*

$$(k^\times)^2 := \{\alpha \in k^\times \mid \alpha = x^2 \text{ para algún } x \in k^\times\} \subseteq k^\times.$$

2) *Enumere los cuadrados en el grupo* $\mathbb{F}_9^\times$ *para el cuerpo* $\mathbb{F}_9$ *construido en el ejercicio anterior.*

3) *Calcule el grupo cociente* $k^\times/(k^\times)^2$ *para* $k = \mathbb{R}$ *y* $k = \mathbb{F}_q$, *donde* $q = p^k$ *(considere por separado el caso de* $p = 2$ *y* p *impar).*

Ejercicio 14.24. *Sea $q = p^k$ donde p es un primo impar y $k = 1, 2, 3, \ldots$ Demuestre que -1 es un cuadrado en $\mathbb{F}_q$ si y solamente si -1 tiene orden 4 en el grupo cíclico $\mathbb{F}_q^\times$. Concluya que -1 es un cuadrado en $\mathbb{F}_q$ si y solamente si $q \equiv 1 \pmod 4$.*

Ejercicio 14.25 (generalización de 14.23). *Sea $q = p^k$ donde p es primo y $k = 1, 2, 3, \ldots$ Asumamos que $q \equiv 1 \pmod n$.*

1) *Demuestre que para todo $\alpha \in \mathbb{F}_q^\times$ la ecuación $x^n = \alpha$ o no tiene soluciones, o tiene n soluciones.*

2) *Demuestre que el subconjunto*

$$\{\alpha \in \mathbb{F}_q^\times \mid \alpha = x^n \text{ para algún } x \in \mathbb{F}_q^\times\}$$

es un subgrupo de $\mathbb{F}_q^\times$ de orden $\frac{q-1}{n}$.

3) *Por ejemplo, encuentre el subgrupo de cubos en $\mathbb{F}_{13}^\times$.*

Ejercicio 14.26. *Supongamos que p es un primo tal que $p \equiv 3 \pmod 4$. Demuestre que el anillo cociente $\mathbb{Z}[\sqrt{-1}]/(p)$ es un cuerpo de p^2 elementos.*

Bibliografía

[Bak1990] Alan Baker, *Transcendental number theory*, second ed., Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1990. MR1074572

[IR1990] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR1070716
https://doi.org/10.1007/978-1-4757-2103-4

[Lem2000] Franz Lemmermeyer, *Reciprocity laws: From Euler to Eisenstein*, Springer-Verlag Berlin Heidelberg, 2000.
http://dx.doi.org/10.1007/978-3-662-12893-0

[Mar1977] Daniel A. Marcus, *Number fields*, Universitext, Springer-Verlag, New York, 1977.
https://doi.org/10.1007/978-1-4684-9356-6