ÁLGEBRA 3
Segundo cuatrimestre — 2014

Práctica 2: Extensiones normales

1. ¿Cuáles de las siguientes afirmaciones son válidas?

(*a*) Todo polinomio no constante se factoriza como producto de factores lineales sobre algún cuerpo.

(*b*) El cuerpo de descomposición de un polinomio es único a menos de isomorfismo.

(*c*) Toda extensión finita es el cuerpo de descomposición de algún polinomio.

(*d*) Sea $K \subseteq L \subseteq E$ una torre de cuerpos. Si E es el cuerpo de descomposición de un polinomio $f \in K[X]$, entonces E es el cuerpo de descomposición de f visto como polinomio en $L[X]$.

Solución. (*a*) Si K es un cuerpo, $f \in K[X]$ y $\bar{K}$ es una clausura algebraica de K, entonces f se factoriza en $\bar{K}[X]$ como producto de factores lineales.

(*b*) Sean E/K y L/K dos cuerpos de descomposición del polinomio $f \in K[X]$, y sea $\bar{L}$ una clausura algebraica de L. Como E/K es algebraica, la inclusión $K \to \bar{L}$ se extiende a un morfismo $\sigma : E \to \bar{L}$ sobre K. Si $f(X) = c(X-a_1)\cdots(X-a_n)$ es la factorización de f en E como factores lineales, entonces $c \in K$ y $a_1, \ldots, a_n \in E$, y vemos que $c(X-\sigma(a_1))\cdots(X-\sigma(a_n))$ es una factorización de f en $\bar{L}$. Como las raíces de f en $\bar{L}$ están en L, vemos así que $\sigma(a_1), \ldots, \sigma(a_n) \in L$ y, como las raíces de f en L generan a L sobre K, vemos que $\sigma(E) = L$. Así, el morfismo σ se restringe a un isomorfismo $E \to L$ sobre K.

(*c*) Consideremos el cuerpo $E = \mathbb{Q}(\sqrt[3]{2})$ y la extensión $K/\mathbb{Q}$. Si E fuese el cuerpo de descomposición de un polinomio $f \in \mathbb{Q}[X]$ y $\bar{E}$ un cuerpo algebraicamente cerrado que contiene a E, entonces todo morfismo $E \to \bar{E}$ sobre K tendría imagen contenida en E. Pero si ω es una raíz primitica cúbica de la unidad, hay un morfismo $\sigma : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\omega\sqrt[3]{2}) \subseteq \mathbb{C}$ que manda $\sqrt[3]{2}$ a $\omega\sqrt[3]{2}$.

(*d*) Por hipótesis, f se factoriza en factores lineales sobre E y E está generado sobre K por las raíces de f. Esto implica, evidentemente, que f se factoriza en factores lineales sobre E y que E está generado sobre L por las raíces de f, así que E es un cuerpo de descomposición de f sobre L. □

2. Para cada uno de los siguientes polinomios sobre los cuerpos indicados, exhiba un cuerpo de descomposición, determinando además el grado de la extensión correspondiente y generadores.

(*a*) $X^p - a$ sobre $\mathbb{Q}$, con $p \in \mathbb{N}$ primo y $a \in \mathbb{N} \setminus \mathbb{N}^p$;

(*b*) $X^3 - 10$ sobre $\mathbb{Q}$, sobre $\mathbb{Q}(\sqrt{2})$ y sobre $\mathbb{Q}(\sqrt{-3})$;

(*c*) $X^4 - 5$ sobre $\mathbb{Q}$, sobre $\mathbb{Q}(\sqrt{5})$, sobre $\mathbb{Q}(\sqrt{-5})$ y sobre $\mathbb{Q}(i)$;

(*d*) $X^4 + 2$ sobre $\mathbb{Q}$ y sobre $\mathbb{Q}(i)$;

(*e*) $\prod_{i=1}^{n}(X^2 - p_i)$ sobre $\mathbb{Q}$, con $p_1, \ldots, p_n \in \mathbb{N}$ primos distintos;

(*f*) $X^3 - 2$ sobre $\mathbb{F}_7$;

(*g*) $(X^3 - 2)(X^3 - 3)(X^2 - 2)$ sobre $\mathbb{Q}(\sqrt{-3})$ y sobre $\mathbb{F}_5$;

(*h*) $X^n - t$ sobre $\mathbb{C}(t)$, con t trascendente sobre $\mathbb{C}$ y $n \in \mathbb{N}$;
(*i*) $X^4 - t$ sobre $\mathbb{R}(t)$, con t trascendente sobre $\mathbb{R}$.

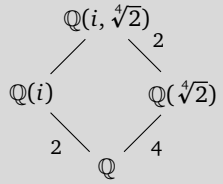
Solución. (*a*) Las raíces de $f(X) = X^p - a$ en $\mathbb{C}$ son los números de la forma $\omega^i \sqrt[p]{a}$ com ω una raíz p-ésima primitiva de la unidad y $0 \le i < p$. El subcuerpo que generan sobre $\mathbb{Q}$ es $E = \mathbb{Q}(\omega, \sqrt[p]{a})$. En la práctica anterior calculamos que $[E : \mathbb{Q}] = p(p-1)$.

(*b*) Si ω es una raíz cúbica primitiva de la unidad, entonces es claro que sobre el cuerpo $E = \mathbb{Q}(\sqrt[3]{10}, \omega\sqrt[3]{10}, \omega^2\sqrt[3]{10})$ el polinomio $f(X) = X^3 - 10$ se factoriza en factores lineales y que E está generado por raíces de f. Notemos que $E = \mathbb{Q}(\omega, \sqrt[3]{10})$ y que ya sabemos que $[E : \mathbb{Q}] = 3 \cdot 2$. Notemos que $\omega = (-1 + \sqrt{-3})/2$, así que $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-3}) \subseteq E$. Sabemos entonces que E es también un cuerpo de descomposición de f sobre $\mathbb{Q}(\sqrt{-3})$ y, como $[\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] = 2$, que $[E : \mathbb{Q}(\sqrt{-3})] = 3$.

El cuerpo $L = \mathbb{Q}(\sqrt{2}, \omega, \sqrt[3]{10})$ es un cuerpo de descomposición de f sobre $\mathbb{Q}(\sqrt{2})$. Como $\mathbb{Q}(\sqrt{2}, \omega) = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$, sabemos que $[\mathbb{Q}(\sqrt{2}, \omega) : \mathbb{Q}] = 4$. Como L es la extensión compuesta sobre $\mathbb{Q}$ de $\mathbb{Q}(\sqrt{2}, \omega)$ y de $\mathbb{Q}(\sqrt[3]{10})$, que tienen grados coprimos, vemos que $[L : \mathbb{Q}] = 4 \cdot 3$ y entonces de la torre $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq L$ vemos que $[L : \mathbb{Q}(\sqrt{2}] = 2 \cdot 3$.

(*c*) La raices de $f(X) = X^4 - 5$ son $\pm\sqrt[4]{5}$ y $\pm i\sqrt[4]{5}$, así que su cuerpo de descomposición sobre $\mathbb{Q}$ es $\mathbb{Q}(i, \sqrt[4]{5})$. Su grado es $2 \cdot 4$ sobre $\mathbb{Q}$, ya que $\mathbb{Q}(\sqrt[4]{5})$ tiene grado 4 sobre $\mathbb{Q}$ y no contiene a i. Este cuerpo contiene a los cuerpos $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-5})$ y $\mathbb{Q}(i)$, que son cuadráticos sobre $\mathbb{Q}$, así que sigue siendo el cuerpo de descomposición de f sobre cada un de ellos y sobre ellos tiene grado $2 \cdot 2$.

(*d*) Si $a = (1+i)/\sqrt[4]{2}$, las raices de $f(X) = X^4 + 2$ en $\mathbb{Q}$ son los cuatro números $\pm a$, $\pm ia$ y entonces un cuerpo de descomposición de f sobre $\mathbb{Q}$ es $E = \mathbb{Q}(i, a)$; este cuerpo es el mismo que $\mathbb{Q}(i, \sqrt[4]{2})$. Como $X^2 + 1$ es irreducible sobre $\mathbb{Q}(\sqrt[4]{2})$, porque este cuerpo está contenido en $\mathbb{R}$, de la consideración del diagrama



vemos que $[E : \mathbb{Q}] = 8$ y $[E : \mathbb{Q}(i)] = 4$.

(*e*) Sea $f(X) = \prod_{i=1}^{n}(X^2 - p_i)$ en $\mathbb{Q}[X]$ con $p_1, \ldots, p_n$ primos distintos. Claramente $E = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ es un cuerpo de descomposición de f sobre $\mathbb{Q}$ y en la práctica anterior calculamos que $[E : \mathbb{Q}] = 2^n$.

(*f*) Sea $f(X) = X^3 - 2 \in \mathbb{F}_7[X]$. Como 2 no es un cubo en $\mathbb{F}_7$, este polinomio no tiene raices en $\mathbb{F}_7$ y, considerando su grado, vemos que es irreducible en $\mathbb{F}_7[X]$. Por otro lado, 2 es una raíz cúbica primitiva de la unidad en $\mathbb{F}_7$, así que si a es una raíz cúbica de 2 en una clausura algebraica de $\mathbb{F}_7$, tenemos que $E = \mathbb{F}_7(a)$ es un cuerpo de descomposición de f sobre $\mathbb{F}_7$. Su grado es 3, ya que f es irreducible.

(*g*) Sabemos ya que $[\mathbb{Q}(\sqrt{2}, \sqrt{-3}) : \mathbb{Q}] = 4$. Mostremos que

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) : \mathbb{Q}] = 9. \tag{1}$$

Primero, sea $\alpha = \sqrt[3]{2}$ y supongamos que existe $\beta \in \mathbb{Q}(\alpha)$ tal que $\beta^3 = 3$. Como el polinomio $X^3 - 3$ es irreducible $\mathbb{Q}$, esto implica que $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Para cada $x \in \mathbb{Q}(\alpha)$ sea $L_x : y \in \mathbb{Q}(\alpha) \mapsto xy \in \mathbb{Q}(\alpha)$, que es un endomorfismo del $\mathbb{Q}$-espacio vectorial $\mathbb{Q}(\alpha)$, y pongamos $\mathsf{tr}(x) = \mathsf{tr}\, L_x \in \mathbb{Q}$; esto define una función $\mathbb{Q}$-lineal $\mathsf{tr} : \mathbb{Q}(\alpha) \to \mathbb{Q}$. El conjunto $B = \{1, \alpha, \alpha^2\}$ es una $\mathbb{Q}$-base de $\mathbb{Q}(\alpha)$, y $\|L_1\|_B = \left(\begin{smallmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{smallmatrix}\right)$, $\|L_\alpha\|_B = \left(\begin{smallmatrix} 0&0&2 \\ 1&0&0 \\ 0&1&0 \end{smallmatrix}\right)$ y $\|L_\alpha\|_B = \left(\begin{smallmatrix} 0&2&0 \\ 0&0&2 \\ 1&0&0 \end{smallmatrix}\right)$,

así que $\mathrm{tr}\,1 = 3$ y $\mathrm{tr}\,\alpha = \mathrm{tr}\,\alpha^2 = 0$. Procediendo de exactamente la misma forma pero usando la base $B' = \{1, \beta, \beta^2\}$ de $\mathbb{Q}(\alpha)$, calculamos que $\mathrm{tr}\,\beta = 0$. Notemos que $\alpha\beta$ es raíz del polinomio $X^3 - 6$, que es irreducible sobre $\mathbb{Q}$, así que $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha\beta)$ y calculando en la base $\{1, \alpha\beta, \alpha^2\beta^2\}$ vemos, otra vez, que $\mathrm{tr}\,\alpha\beta = 0$. Ahora bien, como $\beta \in \mathbb{Q}(\alpha)$, existen $a, b, c \in \mathbb{Q}$ tales que $\beta = a + b\alpha + c\alpha^2$. Aplicando la función tr a ambos lados de esta igualdad, vemos que $a = 0$. Multiplicando la igualdad por α obtenemos entonces que $\alpha\beta = 2c + b\alpha^2$, y aplicando tr otra vez vemos que $c = 0$. Así, debe ser $\beta = c\alpha$ y, elevando al cubo, $3 = 2c^3$. Como $c \in \mathbb{Q}$, esto es imposible: concluimos así que en $\mathbb{Q}(\sqrt[3]{2})$ no hay ninguna raíz cúbica de 3.

Ahora, esto implica que $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{2})] = 3$: en efecto, el polinomio $X^3 - 3$, si no fuese irreducible sobre $\mathbb{Q}(\sqrt[3]{2})$ tendría allí una raíz. Como $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, esto prueba (1).

Sea $f(X) = (X^3-2)(X^3-3)(X^2-2)$. Como $\mathbb{Q}(\sqrt{-3})$ contiene una raíz cúbica primitiva de la unidad, el cuerpo de descomposición de f sobre $\mathbb{Q}(\sqrt{-3})$ es $K = \mathbb{Q}(\sqrt{-3}, \sqrt{2}, \sqrt[3]{2}, \sqrt[3]{3})$, que es la extensión compuesta de $\mathbb{Q}(\sqrt{-3}, \sqrt{2})/\mathbb{Q}$ y de $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})/\mathbb{Q}$. Como los grados de estas dos extensiones, que son 4 y 9, son coprimos, es $[K : \mathbb{Q}] = 4 \cdot 9$. Como $[\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] = 2$, esto implica que $[K : \mathbb{Q}(\sqrt{-3})] = 2 \cdot 9$.

Consideremos ahora al polinomio $f(X) = (X^3 - 2)(X^3 - 3)(X^2 - 2)$ sobre $\mathbb{F}_7$. En este cuerpo 2 es una raíz cúbica primitiva de la unidad, 3 es una raíz cuadrada de 2, y 2 y 3 no tienen raíces cúbicas. Esto implica que el cuerpo de descomposición de f sobre $\mathbb{F}_7$ es $K = \mathbb{F}_7(\alpha, \beta)$ con $\alpha^3 = 2$ y $\beta^3 = 3$.

Mostremos que en $\mathbb{F}_7(\alpha)$ no contiene ninguna raíz cúbica de 3. Para llegar a un absurdo, supongamos que sí existe $\gamma \in \mathbb{F}_7(\alpha)$ tal que $\gamma^3 = 3$. Calculando trazas como antes, vemos que $\mathrm{tr}\,1 = 3$, $\mathrm{tr}\,\alpha = \mathrm{tr}\,\alpha^2 = \mathrm{tr}\,\gamma = \mathrm{tr}\,\alpha\gamma = 0$. Supongamos que $\gamma = a + b\alpha + c\alpha^2$ con $a, b, c \in \mathbb{F}_7$. Tomando trazas, vemos que $a = 0$; multiplicando por α y tomando trazas, vemos que $c = 0$, y entoncs $\gamma = b\alpha$. Elevando al cubo ambos lados de la igualdad, tenemos que $3 = b^3 2$, de manera que $b^3 = 3/2 = 4$. Como 4 no es un cubo en $\mathbb{F}_7$, esto es imposible.

Como $X^3 - 3$ no tiene raíces en $\mathbb{F}_7(\alpha)$ y es cúbico, es irreducible sobre ese cuerpo, y $[K : \mathbb{F}_7(\alpha)] = 3$. En consencuencia, $[K : \mathbb{F}_7] = [K : \mathbb{F}_7(\alpha)][\mathbb{F}_7(\alpha) : \mathbb{F}_7] = 9$.

(h) Como $\mathbb{C}$ tiene una raíz n-ésima de la unidad, alcanza con agregar a $\mathbb{C}(t)$ un raíz n-ésima de t para obtener un cuerpo E de descomposición de $f(X) = X^n - t$ sobre $\mathbb{C}(t)$. Como este polinomio es irreducible sobre $\mathbb{C}(t)$, porque este cuerpo es el cuerpo de fracciones del dominio de factorización única $\mathbb{C}[t]$ y el polinomio satisface el criterio de Eisenstein sobre t, vemos que $[E : \mathbb{C}(t)] = n$.

(i) Sea $f(X) = X^4 - t \in \mathbb{R}(t)[X]$, con t trascendente sobre $\mathbb{R}$. Tenemos un diagrama

$$\begin{array}{c} \mathbb{C}(\sqrt[4]{t}) \\ 4 \,\big|\, \\ \mathbb{R}(i,t) = \mathbb{C}(t) \\ 2 \,\big|\, \\ \mathbb{R}(t) \end{array}$$

Es $[\mathbb{C}(\sqrt[4]{t}) : \mathbb{C}(t)] = 4$ porque el polinomio $X^4 - t$ es irreducible sobre $\mathbb{C}(t)$ y, por otro lado, es $[\mathbb{R}(i,t) : \mathbb{R}(t)] = 2$ porque $X^2 + 1$ no tiene raíces en $\mathbb{R}(t)$: en efecto, el cuadrado de toda función racional en $\mathbb{R}(t)$ toma valores no negativos en los puntos de $\mathbb{R}$ en los que está definida. Luego el grado del cuerpo de descomposición de f sobre $\mathbb{R}(t)$ es 8. □

3. Describa los cuerpos de descomposición de los polinomios $X^3 + X^2 + X + 2$ y $X^3 + 2X + 1$ sobre $\mathbb{F}_3$ y muestre que son isomorfos en tanto extensiones de $\mathbb{F}_3$.

Solución. Calculando explicitamente, vemos que ninguno de los dos polinomios tiene raíces en $\mathbb{F}_3$, así que, como son cúbicos, son irreducibles sobre $\mathbb{F}_3$.

Sea $g(X) = X^3+2X+1$. Si $a \in \mathbb{F}_3$ es $g(X+a) = g(X)$, así que si α es una raíz de g en alguna clausura algebraica de $\mathbb{F}_3$, la factorización de g es, de hecho, $(X-\alpha)(X-\alpha-1)(X-\alpha-2)$. Esto significa que $\mathbb{F}_3(\alpha)$ es un cuerpo de descomposición de g y que $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = 3$.

Por otro lado, sea β una raíz de $f(X) = X^3 + X^2 + X + 2 \in \mathbb{F}_3[X]$. Entonces $f(\beta^3) = \beta^9 + \beta^6 + \beta^3 + 2 = f(\beta)^3 = 0$, así que β^3 también es una raíz de f. Es $\beta \neq \beta^3$: si no fuese ese el caso tendríamos que $\beta^2 = 1$ y f tendría un factor común con $X^2 - 1$, que no tiene porque es irreducible. Luego f tiene *dos* raíces distintas en $\mathbb{F}_3(\beta)$, así que tiene sus tres raíces allí: se trata, entonces, de un cuerpo de descomposición de f sobre $\mathbb{F}_3$. Vemos, además, que $\mathbb{F}_3(\beta)$ tiene grado 3 sobre $\mathbb{F}_3$.

Finalmente, como $\mathbb{F}_3(\alpha)$ y $\mathbb{F}_3(\beta)$ tienen ambos grado 3 sobre $\mathbb{F}_3$, sus elementos no nulos son raíces del polinomio $X^{3^3-1} - 1$ (porque sus grupos multiplicativos tienen orden $3^3 - 1$) y entonces ambos son cuerpos de descomposición de este polinomio: sabemos que esto implica que son isomorfos. □

4. Encuentre los cuerpos de descomposición de todos los polinomios irreducibles de grado 2 sobre $\mathbb{F}_5$ y clasifíquelos a menos de isomorfismo.

Solución. Si $f \in \mathbb{F}_5[X]$ es mónico cuadrático, de manera que $f(X) = X^2 + aX + b$ con $a, b \in \mathbb{F}_5$, entonces $f(X - a/2)$ es de la forma $X^2 - c$ para algún $c \in \mathbb{F}_2$ y, como este último polinomio es también irreducible, debe ser $c \in \{2, 3\}$, ya que este es el conjunto de los no-cuadrados de $\mathbb{F}_5$. Vemos así que los polinomios mónicos cuadráticos irreducibles son los de la forma $(X + t)^2 - 2$ o $(X + t)^2 - 3$ para algún $t \in \mathbb{F}_5$. El escalar t en estas representaciones queda claramente determinado por el polinomio, y entonces los 10 polinomios son distintos dos a dos. Hemos así obtenido la lista de los 10 polinomios mónicos cuadráticos irreducibles sobre $\mathbb{F}_5$. Sabemos que el cuerpo de descomposición de cada uno de ellos es de grado dos sobre $\mathbb{F}_5$, así que esos 10 cuerpos son isomorfos porque $\mathbb{F}_5$ tiene exactaente una extensión cuadrática. □

5. Si la extensión $E/\mathbb{Q}$ es el cuerpo de descomposición de un polinomio $f \in \mathbb{Q}[X]$ de grado n, entonces $[E : \mathbb{Q}]$ divide a $n!$. Dé ejemplos de extensiones para los que se cumpla la igualdad y otros para los que no se cumpla.

Solución. Más generalmente, probemos que si K es un cuerpo cualquiera y $f \in K[X]$ tiene grado n, entonces el grado de cualquier cuerpo L de descomposición de f sobre K es un divisor de $n!$.

Si f es irreducible en $K[X]$ y α es una raíz de f en alguna extensión algebraica de K que contiene a L, entonces $K \subseteq K(\alpha) \subseteq L$, $[K(\alpha) : K] = n$ y $g(X) = f(X)/(X - \alpha) \in K(\alpha)[X]$ tiene cuerpo de descomposición a L sobre $K(\alpha)$. Por inducción, $[L : K(\alpha)]$ divide a $(n-1)!$, así que $[L : K] = [L : K(\alpha)][K(\alpha) : K]$ divide a $n!$.

Si f no es irreducible y $f = gh$ con g irreducible en $K[X]$ y de grado m, entonces sabemos que g tiene un cuerpo de descomposición L' contenido en L e, inductivamente, que $[L' : K]$ divide a $m!$. Por otro lado, L es un cuerpo de descomposición de h sobre L', así que otra vez inductivamente tenemos que $[L : L']$ divide a $(n - m)!$. Así, vemos que $[L : K] = [L : L'][L' : K]$ divide a $m!(n-m)!$, y esto divide a $n!$ ya que $\binom{n}{m}$ es un entero.

Consideremos el polinomio $f(X) = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$, que es irreducible porque

es cúbico y no tiene raíces racionales. Si y es una raíz de f, es fácil ver que y^2-2 también lo es: para ello, alcanza con ver que $f(X^2-2) = X^6 - 5X^4 + 6X^2 - 1$ es divisible por $f(X)$. Esto implice que en $\mathbb{Q}(y)$ hay dos raíces de f, así que están las tres y se trata, en definitiva, de un cuerpo de descomposición de f. Su grado sobre $\mathbb{Q}$ es $3 < 3!$.

Por otro lado, sabemos que el cuerpo de descomposición de $g(X) = X^3 - 2$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\omega, \sqrt[3]{2})$, con $\omega \in \mathbb{C}$ una raíz cúbica primitiva de la unidad, y que su grado sobre $\mathbb{Q}$ es $6 = 3!$. □

6. ¿Cuáles de las siguientes afirmaciones son válidas?

(*a*) Toda extensión de grado finito es normal.

(*b*) Toda extensión de grado finito tiene una clausura normal de grado finito.

(*c*) Toda extensión de un cuerpo de característica cero es normal.

(*d*) Todo K-morfismo $f : L/K \to L/K$ es un K-automorfismo.

(*e*) Si L/K es una extensión algebraica, todo K-morfismo $f : L/K \to L/K$ es un K-automorfismo.

7. Sea K un cuerpo de característica p positiva.

(*a*) Para todo $n \in \mathbb{N}$ la función $f : x \in K \mapsto x^{p^n} \in K$ es un $\mathbb{F}_p$-morfismo de cuerpos.

(*b*) Si K es finito, ese morfismo f es un automorfismo.

(*c*) Dé ejemplos de cuerpos infinitos de característica positiva donde el morfismo sea un isomorfismo y otros donde no lo sea.

Solución. (*a*) Es inmediato que la función f es multiplicativa, y es aditiva porque $(x+y)^p = x^p + y^p$ en un cuerpo de característica p positiva. Esto nos dice que f es un morfismo de anillos, así que es un morfismo de cuerpos. Si $x \in K$ está en el cuerpo primo de K, entonces $x^p = x$, así que $f(x) = x$: esto es, f es un $\mathbb{F}_p$-morfismo.

(*b*) Para ver que cuando K es finito el morfismo f es un automorfimo basta mostrar que es inyectivo, y eso es evidente.

(*c*) Si $K = \mathbb{F}_p(t)$ con t trascendente sobre $\mathbb{F}_p$, entonces la función f no es sobreyectiva: en efecto, el polinomio $X^{p^n} - t$ no tiene ninguna raíz en $\mathbb{F}_p(t)$, ya que es irreducible. Por otro lado, si $\bar{\mathbb{F}}_p$ es una clausura algebraica de $\mathbb{F}_p$, entonces todo elemento de $\bar{\mathbb{F}}_p$ es una potencia p^n-ésima. □

8. El grado del cuerpo de descomposición de $X^{p^n} - X \in \mathbb{F}_p[X]$ sobre $\mathbb{F}_p$ es n.

Solución. Sea L el cuerpo de descomposición de $f(X) = X^{p^n} - X$ sobre $\mathbb{F}_p$. Como la característica de L es p, es inmediato que la suma, el producto y el cociente de dos raíces de f es una raíz de f, así que L es precisamente el conjunto de las raíces de f. En particular, tiene exactamente p^n elementos, porque $f(X) = X(X^{p^n-1} - 1)$ y el polinomio $X^{p^n-1} - 1$ es separable. Vemos así que $|L| = p^n$, de manera que $[L : \mathbb{F}_p] = n$, como queríamos. □

9. Describa los cuerpos de descomposición del polinomio $X^4 - 10X^2 + 5$ sobre $\mathbb{Q}$, sobre $\mathbb{F}_3$ y sobre $\mathbb{F}_7$.

Solución. Trabajemos primero sobre $\mathbb{Q}$. Si $f(X) = X^4 - 10X^2 + 5$ y $g(X) = X^2 - 10X + 5$, entonces las raíces de g son $a = 5+2\sqrt{5}$ y $b = 5-2\sqrt{5}$, y el cuerpo de descomposición de f es $E = \mathbb{Q}(c,d)$ con $c, d > 0$, $c^2 = a$ y $d^2 = b$. Notemos que $\sqrt{5} \in \mathbb{Q}(c)$ y que $(cd)^2 = ab = 5$, de manera que $d = \sqrt{5}/c$, así que $d \in \mathbb{Q}(c)$. Esto nos dice que $E = \mathbb{Q}(c)$ y, como f es irreducible, que $[E : \mathbb{Q}] = 4$.

TERMINAR

10. Sea K un cuerpo, sea $f \in K[X]$ un polinomio no nulo y sea E/K un cuerpo de descomposición para f. Si F/K es una subextensión de E/K, entonces todo morfismo $F/K \to E/K$ sobre K puede ser extendido a un automorfismo de E/K.

11. Determine cuáles de las siguientes extensiones son normales y determine todos los morfismos a una clausura algebraica de su base.

(*a*) $\mathbb{Q}(\sqrt[7]{5})/\mathbb{Q}$;
(*b*) $\mathbb{Q}(\sqrt[7]{5}, \sqrt{5})/\mathbb{Q}(\sqrt[7]{5})$;
(*c*) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})/\mathbb{Q}$;
(*d*) $\mathbb{Q}(\xi_p)/\mathbb{Q}$, con $p \in \mathbb{N}$ primo;
(*e*) $\mathbb{F}_3(a)/\mathbb{F}_3$, con a raíz de $X^3 + X^2 + 2X + 1$.

Solución. (*a*) No todas las raíces del polinomio minimal de $\sqrt[7]{5}$ sobre $\mathbb{Q}$, que es $X^7 - 5$, está en $\mathbb{Q}(\sqrt[7]{5})$: este cuerpo está contenido en $\mathbb{R}$ y el polinomio tiene raíces no reales. Esto nos dice que $\mathbb{Q}(\sqrt[7]{5})/\mathbb{Q}$ no es normal. Un morfismo $\mathbb{Q}(\sqrt[7]{5})/\mathbb{Q} \to \bar{\mathbb{Q}}/\mathbb{Q}$ queda deterinado por la imagen de $\sqrt[7]{5}$, que tiene que ser una raíz séptima de 5, y es claro que cada una de ellas aparece de esta forma.

(*b*) Como $\mathbb{Q}(\sqrt[7]{5})/\mathbb{Q}$ y $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ tienen grados coprimos 7 y 2, la extensión compuesta $\mathbb{Q}(\sqrt[7]{5}, \sqrt{5})/\mathbb{Q}$ tiene grado 14 y entonces la extensión $\mathbb{Q}(\sqrt[7]{5}, \sqrt{5})/\mathbb{Q}(\sqrt[7]{5})$ tiene grado 2. Es entonces normal y hay exactamente dos automorfismos a la clausura algebraica de $\mathbb{Q}(\sqrt[7]{5})$: la identidad y el que manda $\sqrt{5}$ a su opuesto.

(*c*) El cuerpo $E = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ no contiene todas las raices del polinomio minimal de $\sqrt[3]{3}$ sobre $\mathbb{Q}$, así que no es normal como extensión de $\mathbb{Q}$. Como sus generadores tienen grados coprimos sobre $\mathbb{Q}$, es $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) : \mathbb{Q}] = 6$. Consideremos el morfismo de $\mathbb{Q}$-álgebras $f : \mathbb{Q}[X,Y] \to \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ tal que $f(X) = \sqrt{2})$ y $f(Y) = \sqrt[3]{3}$. Claramente el ideal $I = (X^2 - 2, Y^3 - 3)$ está en el núcleo de f; como $\dim_{\mathbb{Q}} \mathbb{Q}[X,Y]/I = 6$, debe ser igual al núcleo, y entonces $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) = \mathbb{Q}[X,Y]/(X^2 - 2, Y^3 - 3)$. Esto implica que hay tantos $\mathbb{Q}$-morfismos $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) \to \bar{\mathbb{Q}}$ como morfismos de $\mathbb{Q}$-álgebras $\mathbb{Q}[X,Y] \to \bar{\mathbb{Q}}$ que tiene a $X^2 - 2$ y a $Y^3 - 3$ en su núcleo. Es claro que hay seis, que mandan X a alguna de las dos raíces cuadradas de 2 e Y a alguna de las tres raíces cúbicas de 3. Esto, por supuesto, determina los morfismos de cuerpos de $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ a $\bar{\mathbb{Q}}$.

(*d*) Sea $\xi = \xi_p$. Como $E = \mathbb{Q}(\xi)$ es el cuerpo de descomposición de Φ_p, es normal. COmo ξ genera a E, un automorfismo de E queda determinado por la imagen de ξ, que puede ser cualquiera de las raíces del polinomio minimal de ξ. Así, para cada $i \in \{1, \dots, p-1\}$ hay un automorfismo f_i de E tal que $f_i(\xi) = \xi^i$, y esos son todos.

(*e*) El polinomio del enunciado —llamémoslo f— es irreducible, así que $[\mathbb{F}_3(a) : \mathbb{F}_3] = 3$. Como f tiene coeficientes en $\mathbb{F}_3$, si x es una raíz de f entonces $f(x^3) = f(x)^3 = 0$ y entonces x^3 también es una raíz. Entonces a, a^3 y a^9 son raíces de f. Veamos que son distintas.

- Si $a = a^3$, entonces como $a \neq 0$ es $a^2 - 1 = 0$, y a es raíz de $X^2 - 1$, lo que es absurdo porque f es irreducible.

- Si $a^3 = a^9$, entonces $(a^2-1)^3 = a^6 - 1 = 0$, así que $a^2 - 1 = 0$, y ya vimos que eso es imposible.
- Finalmente, supongamos que $a = a^9$, de manera que $a^8 = 1$. Como $\mathbb{F}_3(a)^\times$ tiene $3^3 - 1 = 26$ elementos, $a^{26} = 1$ y entonces, como $(8, 26) = 2$, es $a^2 = 1$. Pero entonces $a = \pm 1 \in \mathbb{F}_3$, lo que es absurdo.

Vemos entonces que $\mathbb{F}_3(a)$ tiene a las tres raíces de f: se trata, así, del cuerpo de descomposición de f y es, en particular, normal. Todo automorfismo de ese cuerpo tiene que mandar a a a una de las raíces de f, es decir, a un elemento de $\{a, a^3, a^9\}$, y cada una de estas posibilidades ocurre. □

12. Si K es un cuerpo, $n \in \mathbb{N}$ y t es trascendente sobre K, entonces la extensión $K(t)/K(t^n)$ es normal sii el polinomio $X^n - 1$ se factoriza en $K[X]$ como producto de factores lineales.

Solución. Supongamos que la extensión es normal. El polinomio $f(X) = X^n - t^n$ es irreducible en $K(t^n)[X]$ y tiene una raíz en $K(t)$, así que se descompone totalmente sobre $K(t)$.

Sean $p(t), q(t) \in K[t]$ coprimos tales que $p(t)/q(t)$ es una raíz de f. Es $p(t)^n = t^n q(t)^n$ y, como $K[t]$ es un dominio de factorización única, esto nos dice que $p(t)/q(t) = at$ para algún escalar $a \in K$. Así, vemos que existen escalares $a_1, \ldots, a_n \in K$ tales que $X^n - t^n = \prod_{i=1}^n (X - a_i t)$. Esta es una igualdad en $K[t, X]$, y dividiendo por t^n y poniendo $u = X/t$, vemos que $u^n - 1 = \prod_{i=1}^n (u - a_i)$. Como u es trascendente sobre K, esto nos dice que $X^n - 1$ se factoriza completamente sobre K.

Recíprocamente, supongamos que $X^n - 1 = \prod_{i=1}^n (X - a_i)$ en K. Reemplazando a X por X/t y multiplicando por t^n, vemos que $X^n - t = \prod_{i=1}^n (X - a_i t)$, así que el polinomio $X^n - t^n$ se factoriza como producto de factores lineales en $K(t)$. Esto nos dice que $K(t)$ está generado, como extensión de $K(t^n)$, por las raíces del polinomio $X^n - t^n \in K(t^n)[X]$ y entonces que se trata de una extensión normal. □

13. (*a*) Las extensiones $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ son normales, pero la extensión $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ no lo es.

(*b*) Exhibir extensiones normales con subextensiones no normales.

Solución. (*a*) Ambas extensiones son cuadráticas, así que son automáticamente normals. Que $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ no es normal es claro, ya que no todas las raíces del polinomio minimal $X^4 - 2$ de $\sqrt[4]{2}$ sobre $\mathbb{Q}$ están contenidas en $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$.

(*b*) Si $\zeta \in \mathbb{C}$ es una raíz cúbica primitiva de la unidad, el cuerpo $\mathbb{Q}(\zeta, \sqrt[3]{2})$ es una extensión normal de $\mathbb{Q}$, ya que es el cuerpo de descomposición del polinomio $X^3 - 2$. Ese cuerpo contiene a $\mathbb{Q}(\sqrt[3]{2})$, que no es una extensión normal de $\mathbb{Q}$. □

14. Si E/K y F/K subextensiones normales de una extensión H/K, entonces EF/K y $E \cap F/K$ son extensiones normales.

Solución. Sea $\sigma : EF \to \bar{H}$ un K-morfismo a la clausura algebraica de H. Como E/K y F/K son normales, entonces $\sigma(E) \subseteq E$ y $\sigma(F) \subseteq F$, así que $\sigma(EF) \subseteq \sigma(E)\sigma(F) \subseteq EF$. Esto nos dice que EF/K es normal.

Por otro lado, sea $\sigma : E \cap F \to \bar{H}$ un K-morfismo. Sea $\sigma' : E \to \bar{H}$ una extensión de σ a E; como E/K es normal, es $\sigma(E \cap F) \subseteq \sigma'(E) \subseteq E$. De la misma forma vemos que $\sigma(E \cap F) \subseteq F$ y, entonces $\sigma(E \cap F) \subseteq E \cap F$. □

15. (*a*) Una extensión generada por elementos de grado 2 es normal.

(*b*) ¿Para qué valores de $n \in \mathbb{N}$ es cierto que toda extensión de grado n sobre $\mathbb{Q}$ es normal?

Solución. (*a*) Sea E/F una extensión generada por un conjunto A de elementos de grado 2 sobre F. Para cada $a \in A$, sea m_a su polinomio minimal sobre F, de manera que $\deg m_a = 2$.

Si $a \in A$, entonces a es raíz de m_a. Como m_a tiene grado dos, al tener una raíz en E tiene las dos, y entonces m_a se descompone totalmente en E. Vemos así que E es un cuerpo de descomposición de $\{m_a : a \in A\}$ y, entonces, que la extensión E/F es normal.

(*b*) Si $n \in \mathbb{N}$ es tal que $n \geq 3$, entonces la extensión $\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}$ no es normal. En efecto, contiene a $\sqrt[n]{2}$, que tiene polinomio minimal $X^n - 2$ sobre $\mathbb{Q}$, y contiene a lo sumo dos de las raíces de este polinoio. □

16. Sea $p \in \mathbb{N}$ primo impar y sea Sea $K = \mathbb{F}_p(u, v)$, con $\{u, v\}$ algebraicamente independientes sobre $\mathbb{F}_p$. Sea $f(X) = X^{2p} - uvX^p + v$ y sea α una raíz de f en una clausura algebraica de K.

(*a*) La extensión $K(\alpha)/K$ no es normal.

(*b*) Encuentre el grado del cuerpo de descomposición de f sobre K.

Solución. (*a*) Supongamos que la extensión es normal. Como $f(X) = (X^p - \alpha^p)(X^p - v/\alpha^p)$ es irreducible sobre K y tiene una raíz en $K(\alpha)$, las tiene todas y existe $\beta \in K(\alpha)$ tal que $\beta^p = v$. Tenemos que $uv = \alpha^p + v/\alpha^p = \alpha^p + \beta^p/\alpha^p$ y $v = \beta^p$, así que $u = \alpha^p/\beta^p + 1/\alpha^p = w^p$ si $w = \alpha/\beta + 1/\alpha$. Esto nos dice que $K(u^{1/p}, v^{1/p}) \subseteq K(\alpha)$. Esto es imposible porque $[K(u^{1/p}, v^{1/p}) : K] = p^2$ y $[K(\alpha) : K] = 2p$.

(*b*) Si α es una raíz de f, entonces $f(X) = (X^p - \alpha^p)(X^p - v/\alpha^p)$, así que en el cuerpo de descomposición E de f existe β tal que $\beta^p = v$ y, de hecho, $E = K(\alpha, \beta)$. Sabemos que $[K(\beta) : K] = p$ y es $[K(\alpha^p) : K] = 2$ porque α^p satisface al polinomio $X^2 - uvX + v$, que es irreducible sobre K. Esto nos dice que $[K(\alpha^p, \beta) : K] = 2p$, porque p es impar. Como la característica es p, el grado de $K(\alpha, \beta)$ sobre $K(\alpha^p, \beta)$ es o 1 o p. En el segundo caso tendremos que $[E : K] = [K(\alpha, \beta) : K] = 2p^2$.

Supongamos que estamos en el primer caso, de manera que $\alpha \in K(\alpha^p, \beta)$. Como $K(\alpha)/K$ no es normal y $K(\alpha^p, \beta)/K$ sí lo es, $K(\alpha) \subsetneq K(\alpha^p, \beta)$. Esto es absurdo, porque como f es irreducible, $[K(\alpha) : K] = 2p$. □

17. (*a*) Si E/K es una extensión algebraica tal que todo polinomio no constante en $K[X]$ se factoriza como producto de polinomios lineales en $E[X]$, entonces el cuerpo E es algebraicamente cerrado.

(*b*) Si E/K es una extensión algebraica de un cuerpo infinito K tal que todo polinomio no constante en $K[X]$ tiene una raíz en E, entonces el cuerpo E es algebraicamente cerrado.

Solución. (*a*) Sea E/K una extensión algebraica tal que todo irreducible de $K[X]$ se factoriza como producto de factores lineales en $E[X]$ y sea $f \in E[X]$ un irreducible. Sea a una raíz de f en alguna extensión de E. Como a es algebraico sobre E y la extensión E/P algebraica, la extensión $E(a)/P$ es algebraica. En particular, tenemos el polinomio minimal $m \in P[X]$ minimal de a sobre P, que es irreducible en $P[X]$. De acuerdo a la hipótesis hecha sobre E/K, el polinomio m se factoriza como producto de factores linales en $E[X]$, así que $a \in E$.

(*b*) Sea E/K una extensión algebraica de un cuerpo K que tiene la propiedad de que todo irreducible de $K[X]$ tiene una raíz en E. Bastará que probemos que

> *existe un subcuerpo $P \subseteq E$ que contiene a K y tal que todo irreducible de $P[X]$ se factoriza como producto de polinomios lineales en $E[X]$.* (2)

ya que eso nos reduce a la situación de la primera parte de este ejercicio. Para eso, consideramos dos casos.

- Si K es perfecto, podemos tomar simplemente $P = K$. Sea $f \in K[X]$ un irreducible y sea F/K un cuerpo de descomposición de f sobre K. Como K es perfecto, existe $a \in K$ tal que $F = K(a)$. Si $m \in K[X]$ es el polinomio minimal de a sobre K, la hipótesis nos dice que m tiene una raíz β en E, y entonces las extensiones $K(\alpha)/K$ y $K(\beta)/K$ son isomorfas. Como f se descompone completamente sobre $K(\alpha)$, también lo hace sobre $K(\beta) \subseteq E$.
- Supongamos ahora que K no es perfecto, de manera que, en particular, la caracteristica p de K es positiva. Sea $P = \{x \in E : \text{existe } n \geq 1 \text{ tal que } x^{p^n} \in K\}$. Es fácil ver que P es un subcuerpo de K que contiene a K.

  Este cuerpo P es perfecto. En efecto, si $x \in P$, existe $n \geq 1$ tal que $x^{p^n} \in K$. Por la hipótesis, el polinomio $X^{p^{n+1}} - x^{p^n} \in K[X]$ tiene alguna raíz en E, así que existe $b \in E$ tal que $b^{p^{n+1}} = x^{p^n}$. Claramente es $b \in P$ y, como $(b^p - x)^{p^n} = b^{p^{n+1}} - x^{p^n} = 0$, vemos que $x \in E^p$. Así, es $E = E^p$ y el cuerpo E es perfecto, como dijimos. De hecho, el cuerpo E también es perfecto: un irreducible de $E[X]$ divide a un irreducible de $P[X]$ y, como este último es separable, es separable; esto nos dice que todo irreducible de $E[X]$ es separable, esto es, que E es perfecto.

  Veamos ahora que la extensión E/P tiene la propiedad de que todo irreducible de $P[X]$ tiene una raíz en E. Sea $f(X) = \sum_{i=0}^{n} f_i X^i \in P[X]$ un irreducible. Como sus coeficientes están en P y son finitos en número, existe $m \geq 1$ tal que $g(X) = \sum_{i=0}^{n} f_i^{p^m} X^i \in K[X]$ y, por hipótesis, este polinomio g tiene una raíz a en E. Como E es perfecto, existe $b \in E$ tal que $b^{p^m} = a$, y entonces $f(b)^{p^m} = g(b^{p^m}) = g(a) = 0$, así que f tiene una raíz en E.

  Como P es perfecto, lo que hicimos en el punto anterior nos dice que de $P[X]$ se factoriza completamente en $E[X]$. □