ÁLGEBRA 3
Segundo cuatrimestre — 2014

Práctica 1: Extensiones

1. Sean E/K una extensión y $\alpha \in E$ un elemento algebraico sobre K. Si F/K es una subextensión de E/K, entonces $m(\alpha, F)$ divide a $m(\alpha, K)$. Muestre que $m(\alpha, F)$ y $m(\alpha, K)$ pueden ser tanto iguales como distintos.

Solución. Como $m(\alpha,K)(\alpha) = 0$ y $m(\alpha,K) \in K[X] \subseteq F[X]$, la propiedad característica de $m(\alpha, F)$ implica que $m(\alpha, F)$ divide a $m(\alpha, K)$, como queremos.

Para ver que $m(\alpha, F)$ y $m(\alpha, K)$ pueden ser distintos, basta considerar el caso en que $K \neq F = E$ y $\alpha \in E \setminus K$, ya que en ese caso $m(\alpha, F) = X - \alpha$ tiene grado 1 mientras que $m(\alpha, K)$ tiene grado mayor que 1.

Para ver un ejemplo en el que se tiene $m(\alpha, F) = m(\alpha, K)$, sean $K = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt{2})$, $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ y $\alpha = \sqrt{3}$. Es claro que $m(\alpha, K) = X^2 - 3$, ya que este polinomio tiene a α como raíz y es irreducible sobre $\mathbb{Q}$. Como ese polinomio tiene coeficientes en F, es divisible por $m(\alpha, F)$. Luego o bien $m(\alpha, F) = m(\alpha, K)$ o bien $m(\alpha, F)$ tiene grado 1; pero esto último es imposible, ya que $\alpha \notin F$. □

2. Determine los siguientes polinomios minimales

(a) $m(\sqrt[4]{2}, \mathbb{Q})$; (c) $m(\sqrt[4]{-1}, \mathbb{Q}(i))$; (e) $m(\sqrt[4]{-1}, \mathbb{Q})$;
(b) $m(\sqrt{2-\sqrt{3}}, \mathbb{Q})$; (d) $m(\sqrt[4]{2}, \mathbb{Q}(\sqrt{2}))$; (f) $m(w, \mathbb{R})$, si $w \in \mathbb{C}$.

Solución. (a) Como $a = \sqrt[4]{2}$ es raíz de $X^4 - 2 \in \mathbb{Q}[X]$ y este polinomio es irreducible —porque satisface el criterio de Eisenstein sobre 2— vemos que $m(a, \mathbb{Q}) = X^4 - 2$.

(b) Sea $b = \sqrt{2-\sqrt{3}}$, que es raíz de $f(X) = (X^2-2)^2 - 3 = X^4 - 4X^2 + 1$. Notemos que $f(X+1) = X^4 + 4X^3 + 2X^2 - 4X - 2$, que satisface la condición de Eisenstein para 2, así que f es irreducible. Concluimos de esta forma que $m(b, \mathbb{Q}) = f$.

(c) Sea $c = \sqrt[4]{-1}$. Como c es raíz de $f = X^4 + 1$ y $f(X+1) = X^4 + 4X^3 + 6X^2 + 4X + 2$ satisface la condición de Eisenstein sobre 2, vemos que $[\mathbb{Q}(c) : \mathbb{Q}] = 4$. Es $\mathbb{Q}(x) \supseteq \mathbb{Q}(i)$ y $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. La multiplicatividad del grado implica entonces que $[\mathbb{Q}(c) : \mathbb{Q}(i)] = 2$. Como c es raíz de $X^2 - i \in \mathbb{Q}(i)[X]$, este es el polinomio minimal $m(c, \mathbb{Q}(i))$.

(d) El mismo razonamiento se aplica a $d = \sqrt[4]{2}$. En efecto, es claro que tenemos una cadena $\mathbb{Q}(d) \supseteq \mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}$ y que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Como d es raíz de $X^4 - 2 \in \mathbb{Q}[X]$ y este polinomio satisface el criterio de Eisenstein sobre 2, vemos que $[\mathbb{Q}(d) : \mathbb{Q}] = 4$ y, en consecuencia, que $[\mathbb{Q}(d) : \mathbb{Q}(\sqrt{2})] = 2$. Como d satisface al polinomio $X^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[X]$, vemos que éste es $m(d, \mathbb{Q}(\sqrt{2}))$.

(e) Ya calculamos $m(\sqrt[4]{-1}, \mathbb{Q})$ en la solución de (c).

(f) Sea $w = x + iy$ con $x, y \in \mathbb{R}$ y supongamos que $y \neq 0$. Sabemos que w es raiz del polinomio $f = (X-(x+iy))(X-(x-iy)) = X^2 - 2xX + x^2 + y^2 = (X-x)^2 + y^2 \in \mathbb{R}[x]$. Como $y \neq 0$, este polinomio no se anula en $\mathbb{R}$, así que es irreducible en $\mathbb{R}[X]$ y $m(w, \mathbb{R}) = f$. □

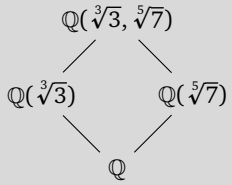
3. Determine los grados de las siguientes extensiones:

(*a*) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$; (*b*) $\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}$; (*c*) $\mathbb{Q}(\sqrt[3]{3},\sqrt[5]{7})/\mathbb{Q}$.

Solución. (*a*) Como en el ejercicio anterior calculamos que $\deg m(\sqrt[4]{2},\mathbb{Q}(\sqrt{2}))=2$, entonces $[\mathbb{Q}(\sqrt[4]{2}),\mathbb{Q}(\sqrt{2})]=2$.

(*b*) Tenemos una cadena $\mathbb{Q}(\sqrt{2},i)\supseteq\mathbb{Q}(\sqrt{2})\supseteq\mathbb{Q}$ y sabemos que $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$. El elemento i es raiz de $X^2+1\in\mathbb{Q}(\sqrt{2})[X]$, así que $[\mathbb{Q}(\sqrt{2},i):\mathbb{Q}(\sqrt{2})]\leq 2$. Para ver que $[\mathbb{Q}(\sqrt{2},i):\mathbb{Q}]=4$ bastará entonces mostrar que $\mathbb{Q}(\sqrt{2},i)\neq\mathbb{Q}(\sqrt{2})$. Pero esto es inmediato: $\mathbb{Q}(\sqrt{2})$ está contenido en $\mathbb{R}$, así que ninguno de sus elementos tiene cuadrado estrictamente negativo y, en consecuencia, $i\notin\mathbb{Q}(\sqrt{2})$.

(*c*) Sean $K=\mathbb{Q}(\sqrt[3]{3})$, $K'=\mathbb{Q}(\sqrt[5]{7})$ y $L=\mathbb{Q}(\sqrt[3]{3},\sqrt[5]{7})$.



Es $[K:\mathbb{Q}]=3$ porque el polinomio $X^3-3\in\mathbb{Q}[X]$ satisface el criterio de Eisenstein sobre 3 y, de manera similar, es $[K':\mathbb{Q}]=5$ porque X^5-7 porque satisface ese criterio sobre 7. Por otro lado, como $\sqrt[5]{7}$ satisface el polinomio $X^5-7\in K[X]$, vemos que $[L:K]\leq 5$. Tenemos que

$$3[L:K]=[L:K][K:\mathbb{Q}]=[L:\mathbb{Q}]=[L:K'][K':\mathbb{Q}]=5[L:K'],$$

así que 5 divide a $[L:K]$. Como $[L:K]\geq 1$, esto implica que $[L:K]=5$ y, entonces, que $[L:\mathbb{Q}]=3\cdot 5$. □

4. (*a*) Determine el grado de $\mathbb{Q}(\sqrt{2},\sqrt{3})$ y de $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ sobre $\mathbb{Q}$ y concluya que $\mathbb{Q}(\sqrt{2}+\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$.

(*b*) Encuentre un $\alpha\in\mathbb{C}$ tal que $\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt[3]{2},\sqrt{3})$ y calcule su polinomio minimal sobre $\mathbb{Q}$.

Solución. (*a*) En la cadena de cuerpos $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$ tenemos $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ y $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]\leq 2$, ya que $\sqrt{3}$ es raiz del polinomio $X^2-3\in\mathbb{Q}(\sqrt{2})[X]$. Si mostramos que $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$, esto implicará que $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]>1$ y, en consecuencia, que $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$.

Supongamos, para llegar a un absurdo, que $\sqrt{3}\in\mathbb{Q}(\sqrt{2})$, de manera que existen enteros a, b, c con $c\neq 0$ y $\sqrt{3}=(a+b\sqrt{2})/c$. Entonces $3c^2=a^2+b^2+2ab\sqrt{2}$ y, como el conjunto $\{1,\sqrt{2}\}$ es linealmente independiente sobre $\mathbb{Q}$, esto implica que $ab=0$. Así, o $a=0$ o $b=0$, y entonces o $3=(b/c)^2$ o $3=(a/c)^2$. Por supuesto, esto es imposible.

Sea ahora $a=\sqrt{2}+\sqrt{3}$. Es $a^2=5+2\sqrt{6}$, así que a es raíz de

$$f=(X^2-5)^2-24=X^4-10X^2+1.$$

Supongamos que f es reducible sobre $\mathbb{Q}$, de manera que es reducible sobre $\mathbb{Z}$ como producto de dos polinomios no constantes y mónicos. El criterio de Gauss nos dice que las raíces racionalees de f están contenidas en $\{\pm 1\}$ y calculando vemos que entonces no tiene ninguna, y en consecuencia los dos factores tienen grado 2. Existen entonces enteros u, v, s y t tales que $f=(X^2+uX+v)(X^2+sX+t)$. Distribuyendo, vemos que $u+s=0$, $v+us+t=-10$ y

$vt = 1$. De la tercera ecuación vemos que $v = t = \pm 1$, de la primera que $s = -u$ y entonces de la segunda que $u^2 = 2v + 10 \in \{8, 12\}$. Esto es absurdo.

Así, vemos que $[\mathbb{Q}(a) : \mathbb{Q}] = 4$ y, como $\mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, que $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(*b*) Sea $a = \sqrt[3]{2} + \sqrt{3}$. Como

$$2 = (a - \sqrt{3})^3 = a^3 - 3a^2\sqrt{3} + 9a - 3\sqrt{3} = (a^3 + 9a) - 3(a^2 + 1)\sqrt{3}, \tag{1}$$

es $3(a^2 + 1)\sqrt{3} = a^3 + 9a - 2$, y entonces

$$27(a^2 + 1)^2 = (a^3 + 9a - 2)^2.$$

Esto nos dice que a es raíz de $f(X) = X^6 - 9X^4 - 4X^3 + 27X^2 - 36X - 23$.

La igualdad (1) nos dice que $\sqrt{3} \in \mathbb{Q}(a)$ y, más aún, que a es raíz del polinomio $g(X) = (X - \sqrt{3})^3 - 2 \in \mathbb{Q}(\sqrt{3})[X]$. Afirmamos que g es irreducible sobre $\mathbb{Q}(\sqrt{3})$; esto es equivalente a que $g(X + \sqrt{3}) = X^3 - 2$ sea irreducible sobre ese cuerpo y, como el polinomio es cúbico, a que no haya en $\mathbb{Q}(\sqrt{3})$ ninguna raíz cúbica de 2. Esto es consecuencia inmediata de lo que hicimos en la primera parte de este ejercicio. Así, $[\mathbb{Q}(a) : \mathbb{Q}(\sqrt{3})] = 3$ y entonces $[\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 6$. Esto implica que el polinomio f que encontramos arriba es el polinomio minimal de a sobre $\mathbb{Q}$. Como $\mathbb{Q}(a)/\mathbb{Q}$ es una subextensión de grado 6 de la extensión $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})/\mathbb{Q}$, que también tiene grado 6, vemos que de hecho $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) = \mathbb{Q}(a)$. □

5. Muestre que $\mathbb{Q}(\sqrt{2 - \sqrt{3}}) = \mathbb{Q}(\sqrt{2 + \sqrt{3}})$ y determine el grado de este cuerpo sobre $\mathbb{Q}$.

Solución. La igualdad es inmediata porque $\sqrt{2 - \sqrt{3}} \cdot \sqrt{2 + \sqrt{3}} = 1$. El número $a = \sqrt{2 - \sqrt{3}}$ es raíz del polinomio $f(X) = (X^2 - 2)^2 - 3 = X^4 - 4X^2 + 1$. Es $f(X + 1) = X^4 + 4X^3 + 2X^2 - 4X - 2$, que satisface el criterio de Eisenstein sobre 2, así que f es irreducible. Así, tenemos que $[\mathbb{Q}(a) : \mathbb{Q}] = 4$.

6. Sea E/K una extensión finita de cuerpos. Si $\alpha \in E$, consideremos la función $L_\alpha : x \in E \mapsto \alpha x \in E$, que es K-lineal. El polinomo minimal de α sobre K coincide con el polinomio minimal de L_α. ¿Cuándo es $m(\alpha, K)$ igual al polinomio *característico* de L_α?

Solución. Sea $\mu \in K[X]$ el polinomio minimal de L_α, de manera que $\mu(L_\alpha) = 0$, de manera que $\mu(L_\alpha)(e) = 0$ para todo $e \in E$. Como $\mu(L_\alpha)(e) = \mu(\alpha)e$, tomando $e = 1_E$ vemos que $\mu(\alpha) = 0$, así que $m(\alpha, K)$ divide a μ. Por otro lado, $m(\alpha, K)(L_\alpha)(e) = m(\alpha, K)(\alpha)e = 0$ para todo $e \in E$, así que $m(\alpha, K)(L_\alpha) = 0$ y entonces μ divide a $m(\alpha, K)$. Como ambos polinomios son mónicos, se sigue de esto que, de hecho, $\mu = m(\alpha, K)$, como queríamos.

Si $m(\alpha, K)$, que tiene grado $[K(\alpha) : K]$, es igual al polinomio característico de L_α, que tienen grado $[E : K]$, entonces claramente $E = K(\alpha)$. Recíprocamente, si $E = K(\alpha)$, entonces para todo polinomio $p \in K[X]$ de grado menor que $[E : K]$ es $p(\alpha) \neq 0$ y entonces $p(L_\alpha)(1_E) = p(\alpha) \neq 0$, de manera que $p(L_\alpha) \neq 0$ y p no es el polinomio minimal de L_α: esto implica que el polinomio minimal de L_α tiene grado al menos, y entonces igual a, $[E : K]$. Vemos así que el polinomio minimal de L_α tiene grado igual al de su característico, y, por lo ya probado, que $m(\alpha, K)$ es el polinomio característico de L_α. □

7. Una extensión E/K es algebraica sii todo anillo A con $K \subseteq A \subseteq E$ es un cuerpo.

Solución. Si en E hay un elemento x trascendente sobre K, entonces el anillo $K[x]$ no es un cuerpo. Recíprocamente, supongamos que se cumple la condición y sea $x \in E$ no nulo. Como la hipótesis nos dice que $K[x]$ es un cuerpo, existe $p \in K[X]$ tal que $xp(x) = 1$: esto nos dice que x es raíz de $Xp(X) - 1 \in K[X]$, así que es algebraico sobre K. □

8. Si $a \in \mathbb{Z}[i]$ es un elemento irreducible, determine el cuerpo primo K de $\mathbb{Z}[i]/(a)$ y el grado $[\mathbb{Z}[i]/(a) : K]$.

Solución. Supongamos que $a = x + iy$ con $x, y \in \mathbb{Z}$. Como $\mathbb{Z}[i]$ es un dominio de factorización única y a es irreducible, a es primo. Esto implica que el ideal (a) de $\mathbb{Z}[i]$ es primo y, en consecuencia, $(a) \cap \mathbb{Z}$ es un ideal primo de $\mathbb{Z}$. Como $x^2 + y^2 = a(x - iy)$ es un entero no nulo, vemos que $(a) \cap \mathbb{Z}$ es un ideal no nulo de $\mathbb{Z}$. Como $1 \notin (a)$ porque a no es una unidad, también $(a) \cap \mathbb{Z}$ es un ideal propio de $\mathbb{Z}$. Así, existe exactamente un primo $p \in \mathbb{N}$ tal que $(a) \cap \mathbb{Z} = (p)$. Se sigue de esto que la inclusión $\mathbb{Z} \to \mathbb{Z}[i]$ induce un morfismo inyectivo $\mathbb{Z}/(p) \to \mathbb{Z}[i]/(a)$ y esto nos dice que el cuerpo primo de $\mathbb{Z}[i]/(a)$ es $\mathbb{F}_p$.

- Supongamos que $xy = 0$. Sin pérdida de generalidad, podemos suponer que $y = 0$ porque (a) y (ia) son el mismo ideal, y entonces $a \in \mathbb{Z}$. En ese caso, p divide a a en $\mathbb{Z}$ y existe $q \in \mathbb{Z}$ tal que $a = pq$. Como a es irreducible en $\mathbb{Z}[i]$, esto implica que $a = p$. El determinante de la aplicación $L_a : \mathbb{Z}[i] \to \mathbb{Z}[i]$ es p^2, así que el cardinal del cociente $\mathbb{Z}[i]/(i)$ es p^2, y entonces $[\mathbb{Z}[i]/(a) : \mathbb{F}_p] = 2$.
- Supongamos ahora, por el contrario, que $xy \neq 0$. Si $t \in (a) \cap \mathbb{Z}$, existen $u, v \in \mathbb{Z}$ tales que $t = (x + iy)(u + iv)$ y, en particular, $xv + uy = 0$. Como x e y son coprimos y no nulos, esto implica que existe $w \in \mathbb{Z}$ tal que $v = -yw$ y $u = wx$, y entonces $t = (x^2 + y^2)w$. Vemos así que $x^2 + y^2$ es el generador positivo del ideal $(a) \cap \mathbb{Z}$, y entonces $p = x^2 + y^2$. El determinante de la aplicación $L_a : \mathbb{Z}[i] \to \mathbb{Z}[i]$ es p, así que el cardinal del cociente $\mathbb{Z}[i]/(i)$ es p, y entonces $[\mathbb{Z}[i]/(a) : \mathbb{F}_p] = 1$. □

9. Sean L/K y M/K subextensiones finitas de una extensión F/K.

(a) Si los grados de L/K y de M/K son coprimos, entonces

$$[LM : K] = [L : K][M : K].$$

(b) Si $[LM : K] = [L : K][M : K]$, entonces $L \cap M = K$. ¿Vale la afirmación recíproca?

Solución. (a) Tenemos que $[LM : L][L : K] = [LM : K] = [LM : M][M : K]$, así que $[M : K]$ divide a $[LM : L][L : K]$ y la hipótesis, entonces, nos dice que divide a $[LM : L]$. Como $1 \leq [LM : L] \leq [M : K]$, esto implica que $[LM : L] = [M : K]$, que es lo que queremos.

(b) Hay una función K-lineal $\mu : L \otimes_K M \to LM$ tal que $\mu(x \otimes y) = xy$ para cada $x \in L$ y cada $y \in M$. Sabemos que es sobreyectiva, ya que LM es el subgrupo de F generado por los elementos de la forma xy con $x \in L$ ee $y \in M$; por otro lado, la hipótesis implica que el dominio y el codominio de μ tienen la misma dimensión, así que μ es inyeciva.

Hay una función $\phi : L \cap M \to L \otimes_K M$ tal que $\phi(x) = x \otimes 1 - 1 \otimes x$ para cada $x \in L \cap M$, y es inmediato verifiar que $\mu \circ \phi = 0$, así que $\phi = 0$. Supongamos que $L \cap M \subsetneq K$ y sea $x \in (L \cap M) \setminus K$. Como 1_K y x son dos elementos de M linealmente independientes sobre K, existe una función K-lineal $\lambda : M \to K$ talque $\lambda(1_K) = 1_K$ y $\lambda(x) = 0$. Se sigue entonces que $0 = (\mathsf{id}_L \otimes \lambda)(\phi(x)) = (\mathsf{id}_L \otimes \lambda)(x \times 1 - 1 \otimes x) = x$. Esto es absurdo. Así, debe ser $L \cap M = K$.

Sean $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$ y $M = \mathbb{Q}(\rho\sqrt[3]{2})$, con ρ una raiz cúbica primitiva de la unidad. Entonces $L \cap M = K$, ya que $L \neq M$, de maneta que $[L : L \cap M] > 1$, y $[L : L \cap M]$ divide a 3. Como $LM = \mathbb{Q}(\rho, \sqrt[3]{2})$ tiene grado 6 sobre K, es $[LM : K] \neq 9 = [L : K][M : K]$. □

10. El polinomio $X^5 + 6X^3 + 15X^2 + 3$ es irreducible en $\mathbb{Q}(\sqrt{2}, \sqrt{3})[X]$.

Solución. Llamemos f a ese polinomio. Satisface el criterio de Eisenstein sobre 3, así que es irreducible en $\mathbb{Q}[X]$. Si α es una de sus raíces en $\mathbb{C}$, entonces $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. Como este grado es coprimo con $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, vemos que $[\mathbb{Q}(\alpha, \sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4 \cdot 5$ y, en consecuencia, $[\mathbb{Q}(\alpha, \sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 5$. Esto implica inmediatamente que el polinomio f sigue siendo irreducible sobre $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. □

11. Sea F/K una extensión finita de cuerpos.

(*a*) Si F/K tiene grado impar y $F = K(u)$, entonces también $F = K(u^2)$.

(*b*) Si F/K tiene grado primo, entonces F/K no posee cuerpos intermedios.

Solución. (*a*) Tenemos una torre $K \subseteq K(u^2) \subseteq K(u)$, así que

$$[K(u) : K] = [K(u) : K(u^2)][K(u^2) : K].$$

Sabemos que $[K(u) : K]$ es impar. Claramente $[K(u) : K(u^2)] \leq 2$, así que si $K(u) \neq K(u^2)$, es $[K(u) : K(u^2)] = 2$: esto es absurdo.

(*b*) Si E es un cuerpo intermedio de F/K, entonces $[F : E][E : K]$ es primo, y o bien $[F : E] = 1$ o bien $[E : K] = 1$.

12. (*a*) Describa todas las extensiones cuadráticas de un cuerpo de característica distinta de dos.

(*b*) Sea $f = X^2 + X + 1 \in \mathbb{F}_2[X]$ y sea α una raíz de f en una clausura algebraica de $\mathbb{F}_2$. Muestre que no existe $\beta \in \mathbb{F}_2(\alpha)$ tal que $m(\beta, \mathbb{F}_2) = X^2 + c$ con $c \in \mathbb{F}_2$.

†(*c*) Describa todas las extensiones cuadrática de un cuerpo de característica dos.

Solución. (*a*) Sea K un cuerpo de característica distinta de 2.

Sea L/K una extensión de grado 2 y sea $x \in L \setminus K$, de manera que $L = K(x)$. El polinomio minimal de x sobre K tiene grado 2, así que existen $a, b \in K$ tales que este polinomio es $f(X) = X^2 + aX + b$. El elemento $y = x - a/2$ es claramente tal que $L = K(y)$ y su polinomio minimal sobre K es $g(X) = f(X - a/2) = X^2 + a^2/4 - b$. Como g es irreducible, debe ser $a^2/4 - b \notin K^2$ Así, hemos mostrado que

> *Si L/K es una extensión cuadrática, entonces existe $y \in L \setminus K$ tal que $L = K(y)$ e $y^2 \in K \setminus K^2$.*

Supongamos ahora que L/K es una extensión cuadrática'y que $y, z \in L \setminus K$ son tales que $L = K(y) = K(z)$, e $y^2, z^2 \in K \setminus K^2$. Existen entonces $a, b \in K$ tales que $z = a + by$, y $z^2 = a^2 + 2aby + b^2y^2$, de manera que $ab = 0$. No puede ser que sea $b = 0$ porque en ese

caso tendríamos que $z \in K$, así que $a = 0$, y entonces $z^2/y^2 \in K^2$. Esto significa que las clases $[y]$ y $[z]$ en $K^\times/K^{\times 2}$ son iguales. Así, hemos probado que

> *Si L/K es una extensión, entonces existe $y \in L \setminus K$ tal que $L = K(y)$ e $y^2 \in K \setminus K^2$ y la clase $[y] \in K^\times/K^{\times 2}$ depende solamente de L/K y no de la elección de y en L.*

Sea $\bar{K}$ una clausura algebraica de K y sea $C_2(K)$ el conjunto de las subextensiones L/K de $\bar{K}/K$ que son cuadráticas. Estamos en posición de definir una función $\beta : C_2(K) \to K^\times/K^{\times 2}$: si L/K es un elemento de $C_2(K)$, sabemos que existe $y \in L \setminus K$ tal que $y^2 \in K \setminus K^2$ y la clase $[y] \in K^2/K^{\times 2}$ depende únicamente de L/K, así que podemos poner $\beta(L/K) = [y]$.

Probemos que

> *la función β da una biyección entre el conjunto $C_2(K)$ y los elementos de $K^\times/K^{\times 2}$ distintos de la unidad.*

Primero, veamos la sobreyectividad. Sea $u \in K^\times$ tal que su clase en el cociente $K^\times/K^{\times 2}$ es no trivial. Esto significa, precisamente, que $u \notin K^2$ y entonces el polinomio $f(X) = X^2 - u \in K[X]$ es irreducible. El cociente $L = K[X]/(f(X))$ es un cuerpo que contiene a K, la extensión L/K es cuadrática, y si $v \in L$ es la clase de X en L, entonces $v^2 = u$. Esto nos dice, precisamente, que $\beta(L/K)$ es la clase de u en $K^\times/K^{\times 2}$.

Para ver la inyectividad, sean L/K y L'/K dos extensiones cuadráticas de K contenidas en $\bar{K}$ tales que $\beta(L/K) = \beta(L'/K)$. Sean $u \in L$ tal que $u^2 \in K \setminus K^2$ y $v^2 \in K \setminus K^2$, de manera que $L = K(u)$ y $L' = K(v)$ y $\beta(L/K)$ y $\beta(L'/K)$ son las clases de u y de v en $K^\times/K^{\times 2}$. Como son iguales, existe $a \in K$ tal que $u = a^2 v$. Es inmediato, entonces, que $L = L'$.

(*b*) Sea $f(X) = X^2 + X + 1 \in \mathbb{F}_2[X]$ y α una raíz de f en una clausura algebraica de $\mathbb{F}_2$. Sea $\beta \in \mathbb{F}_2(\alpha)$, de manera que existen a, $b \in \mathbb{F}_2$ tales que $\beta = a + b\alpha$. Entonces $\beta^2 = a^2 + b^2\alpha^2 = a^2 + b^2 + b^2\alpha$ pertenece a $\mathbb{F}_2$ sii $b = 0$, es decir, sii $\beta \in \mathbb{F}_2$. □

13. Si $b \in \mathbb{Q}$, sea α_b una raíz de $f_b(X) = X^2 + bX + b^2$. Describa las extensiones $\mathbb{Q}(\alpha_b)/\mathbb{Q}$ y determine sus grados.

Solución. Las raíces del polinomio f_b son $(-b \pm \sqrt{b^2 - 4b^2})/2 = (-1 \pm \sqrt{-3})b/2$, así que $\mathbb{Q}(\alpha_b) = \mathbb{Q}(\sqrt{-3})$ cualquiera sea $b \in \mathbb{Q}$ y, en particular, $\mathbb{Q}(\alpha_b)$ tiene grado 2 sobre $\mathbb{Q}$. □

14. Si $n \in \mathbb{N}$, sea $\zeta_n \in \mathbb{C}$ una raíz n-ésima primitiva de la unidad.

(*a*) Determine $m(\zeta_p, \mathbb{Q})$ si p es primo.

(*b*) Calcule $m(\zeta_6, \mathbb{Q})$.

(*c*) Es $m(\zeta_n, \mathbb{Q}) = \sum_{i=0}^{n-1} X^i$ sii n es primo.

Solución. (*a*) Supongamos que $n = p$ es un número primo. El polinomio minimal $m(\zeta_p, \mathbb{Q})$ de ζ_p divide a $X^p - 1$ y, como $\zeta_p \neq 1$, que divide de hecho a $f = (X^p - 1)/(X - 1)$. Como $f(X+1) = ((X+1)^p - 1)/X = \sum_{i=0}^{p-1} \binom{p}{i+1} X^i$, y p divide a $\binom{p}{i+1}$ si $0 \leq i < p-1$ y p^2 no divide a $\binom{p}{1} = p$, $f(X+1)$ satisface el criterio de Eisenstein sobre p, de manera que es irreducible. Vemos así que $m(\zeta_p, \mathbb{Q}) = f$.

(*b*) Sabemos que $X^6 - 1$ es divisible por $(X-1)(X+1)(X^2+X+1)$ y que el cociente es $X^2 - X + 1$. Las raíces del factor son todas de orden menor que 6, así que la del cociente son las sextas primitivas. Usando el criterio de Gauss para las raíces racionales, vemos que ese polinomio es irreducible en $\mathbb{Q}$.

(*c*) Si $n = rs$ con $r, s > 1$, entonces $X^{rs}-1$ es divisible por X^r-1, así que $(X^{rs}-1)/(X-1)$ es divisible por $(X^r-1)/(X-1)$, que tiene grado estrictamente menor y no es constante. □

15. Muestre que $m(\zeta_5 + \zeta_5^{-1}, \mathbb{Q}) = X^2 + X - 1$, deduzca que $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ admite una subextensión cuadrática y determínela explícitamente.

Solución. El número $\zeta = \zeta_5$ es raíz de $1 + X + X^2 + X^3 + X^4$, así que anula al polinomio de Laurent $X^{-2} + X^{-1} + 1 + X + X^2$. Como

$$X^{-2} + X^{-1} + 1 + X + X^2 = (X^{-1} + X)^2 + (X^{-1} + X) - 1,$$

el número $\zeta^{-1} + \zeta$ es raíz del polinomio $X^2 + X - 1$, que es irreducible sobre $\mathbb{Q}$. Así, $\mathbb{Q}(\zeta + \zeta^{-1})$ es una subextensión cuadrática de $\mathbb{Q}(\zeta)/\mathbb{Q}$. □

16. Sea $p \in \mathbb{N}$ primo e impar y sea $a \in \mathbb{Q}$ tal que $a \notin \mathbb{Q}^p$.

(*a*) Muestre que $m(\sqrt[p]{a}, \mathbb{Q}) = X^p - a$.

(*b*) Sea $K \subseteq \mathbb{C}$ el subcuerpo de $\mathbb{Q}$ generado por las raíces de $X^p - a$. Determine el grado de K sobre $\mathbb{Q}$ y sobre $\mathbb{Q}(\sqrt[p]{a})$.

Solución. (*a*) Supongamos que $X^p - a = f_1(X) \cdots f_n(X)$ es la factorización como producto de irreducibles mónicos de $X^p - a$ en $\mathbb{Q}(\zeta)[X]$, con ζ una raíz p-ésima primitiva de la unidad. Sea $I = \{1, \ldots, n\}$. Como el polinomio $X^p - a$ es coprimo con su derivada, siempre que $i, j \in I$ son distintos, f_i no es un múltiplo escalar de f_j. Notemos que si $k \in \mathbb{Z}/p\mathbb{Z}$ es

$$f_1(\zeta^k X) \cdots f_n(\zeta^k X) = (\zeta^k X)^p - a = X^p - a = f_1(X) \cdots f_n(X)$$

así que para cada $i \in I$ existe $j \in I$ tal que $f_i(\zeta^k X)$ es un múltiplo escalar de $f_j(X)$, y este j está bien determinado. Obtenemos de esta forma una acción $\triangleright$ del grupo $g = \mathbb{Z}/p\mathbb{Z}$ sobre I tal que para cada $k \in G$ es $f_i(\zeta^k X)$ un múltiplo escalar de $f_{k \triangleright i}(X)$.

Como G no tiene subgrupos propios e I tiene a lo sumo p elementos, vemos que

(I) o bien la acción de G es trivial

(II) o bien I tiene exactamente p elementos y la acción es simplemente transitiva.

En el caso (II), cada uno de los polinomios f_i tiene que tener grado 1, y f tiene una raíz α en $\mathbb{Q}(\zeta)$. Esto significa que existe un polinomio $h \in \mathbb{Q}[X]$ tal que $h(\zeta)^p = a$, de manera que ζ es una raíz del polinomio $h(X)^p - a$, que tiene coeficients racionales; ese polinomio debe ser entonces divisible por Φ_p y en consecuencia tiene a *todas* las raíces p-ésimas primitivas como raíces. Así, esto nos dice que $h(\zeta^i)^p = a$ para cada $i \in \{1, \ldots, p-1\}$.

Consideremos el polinomio

$$H(Y_1, \ldots, Y_{p-1}, X) = \prod_{i=1}^{p-1} h(Y_i X) \in \mathbb{Q}[X, Y_1, \ldots, Y_n]$$

Cuando lo escribimos como polinomio en la variable X con coeficientes en $\mathbb{Q}[Y_1, \ldots, Y_n]$, esos coeficientes son claramente funciones simétricas de las variables $Y_1, \ldots, Y_{p-1}$ con coeficientes racionales. Esto implica que

$$H(\zeta, \zeta^2, \ldots, \zeta^{p-1}, X)$$

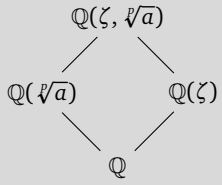
es un polinomio en X *con coeficientes racionales*, ya que las funciones simétricas elementales en $\zeta, \ldots, \zeta^{p-1}$ toman valores racionales —esos valores, en efecto, son salvo signo los coeficientes de Φ_p. Esto implica que

$$u := h(\zeta)\cdots h(\zeta^{p-1}) = H(\zeta, \ldots, \zeta^{p-1}, 1) \in \mathbb{Q}$$

Además, como $h(\zeta^i)^p = a$ para cada $i \in \{1, \ldots, p-1\}$, es $u^p = a^{p-1}$. Ahora bien, p y $p-1$ son coprimos, así que existen $x, y \in \mathbb{Z}$ tales que $xp + y(p-1) = 1$ y entonces $a = (u^y a^{-x})^p \in \mathbb{Q}^p$, contra la hipótesis. Vmos así que el caso (II) no puede ocurrir.

En el caso (I), en cambio, tenemos que $f_1(\zeta X)$ es un múltiplo escalar de $f_1(X)$. Si $f_1(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$, es $f_1(\zeta X) = \zeta^d X^d + \zeta^{d-1}a_{d-1}X^{d-1} + \cdots + a_0$. Como 0 no es raíz de $X^p - a$, $a_0 \neq 0$, y entonces vemos que debe ser, de hecho, $f_1(\zeta X) = f_1(X)$. Mirando el coeficiente de X^d, concluimos así que $\zeta^d = 1$, lo que sólo es posible si $d = p$. Así, $X^p - a$ es irreducible en $\mathbb{Q}(\zeta)$.

Consideremos el diagrama



Sabemos que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ y que $[\mathbb{Q}(\zeta, \sqrt[p]{a}) : \mathbb{Q}(\zeta)] = p$. Si $d = [\mathbb{Q}(\sqrt[p]{a}) : \mathbb{Q}]$ y $e = [\mathbb{Q}(\zeta, \sqrt[p]{a}) : \mathbb{Q}(\sqrt[p]{a})]$, es $d \leq p$ y $e \leq p - 1$, y de la multiplicatividad $p(p-1) = de$. En particular, p divide al producto de y no puede dividir a e, así que debe dividir a d: esto sólo es posible si, de hecho, $d = p$.

(*b*) Las raíces del polinomio son los números de la forma $\zeta^i \sqrt[p]{a}$ con $0 \leq i < p$. En particular, $\zeta = \zeta \sqrt[p]{a}/\sqrt[p]{a} \in K$, de manera que $\mathbb{Q}(\zeta, \sqrt[p]{a}) \subseteq K$; la inclusión recíproca es evidente, así que tenemos $K = \mathbb{Q}(\zeta, \sqrt[p]{a})$. De acuerdo a lo que hicimos en el punto anterior, es $[K : \mathbb{Q}] = p(p-1)$ y $[K : \mathbb{Q}(\sqrt[p]{a})] = p - 1$. □

17. El conjunto $\mathbb{Q}_{\mathsf{alg}}$ de los elementos de $\mathbb{C}$ que son algebraicos sobre $\mathbb{Q}$ es un subcuerpo de $\mathbb{C}$ y $\mathbb{Q}_{\mathsf{alg}}/\mathbb{Q}$ es una extensión algebraica que no es finita.

18. Sea $(p_i)_{i\in\mathbb{N}}$ una enumeración de los primos racionales.

(*a*) Encuentre el grado de $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ sobre $\mathbb{Q}$, y determine el número de subextesiones cuadráticas de esa extensión.

(*b*) Calcule $[\mathbb{Q}(\sqrt{p_i}, i \in \mathbb{N}) : \mathbb{Q}]$.

(*c*) ¿Es la extensión $\mathbb{Q}(\sqrt{p_i}, i \in \mathbb{N})/\mathbb{Q}$ finitamente generada?

(*d*) Si K es un cuerpo algebraicamente cerrado tal que $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$, ¿cuánto vale $[K : \mathbb{Q}]$?

19. Toda extensión algebraica de grado infinito contiene subextensiones finitas de grado arbitrariamente grande.

Solución. Sea E/K una extensión algebraica de grado infinito. Sea $x_1 \in E \setminus K$ arbitrario. Como $[K(x_1) : E]$ es finito, porque x_1 es algebraico sobre K, $E \neq K(x)$ y, de hecho, $E/K(x_1)$ es infinita y $d_1 = [K(x_1) : K] > 1$. De la misma forma, existe $x_2 \in E \setminus K(x_1)$ tal que

$E/K(x_1,x_2)$ es algebraica de grado infinito y $d_2 = [K(x_1,x_2) : K(x_1)] > 1$. Continuando de esta forma, podemos construir una sucesión $(x_i)_{i\geq 1}$ de elementos de E y una sucesión $(d_i)_{i\geq 1}$ de enteros tales que $[K(x_1,\dots,x_i) : K(x_1,\dots,x_{i-1})] = d_i > 1$ para todo $i \geq 1$. Pero entonces para todo $i \geq 1$ tenemos que $[K(x_1,\dots,xi) : K] = d_1 \cdots d_i \geq 2^i$. □

20. (*a*) Un cuerpo algebraicamente cerrado es infinito.

(*b*) Si E/K es una extensión algabraica, determine el cardinal de E en términos del de K.

(*c*) Existen cuerpos algebraicamente cerrados de todos los cardinales infinitos.

(*d*) El conjunto de elementos trascendentes de $\mathbb{R}$ es no numerable.

Solución. (*a*) Sea K un cuerpo finito y supongamos que tiene n elementos. Si p es un número primo mayor que n, entonces $X^p - 1 \in K[X]$ es un polinomio separable, ya que p es estrictamente más grande que la característica de K así que es coprimo con ella, que tiene que tener, entonces, exactamente p raíces distintas en K. Esto es claramente imposible.

(*b*) Todo elemento de E es algebraico sobre K, así que es raíz de algún polinomio de $K[X]$. Como cada polinomio tiene un número finito de raíces, esto implica que E tiene cardinal menor o igual que el de $K[X] \times \mathbb{N}$. Por supuesto, ese cardinal es al menos el de K.

Si K es infinito, entonces $K[X]$, que es la unión de una sucesión creciente de K-subespacios de dimensión finita (cada uno de los cuales tiene el mismo cardinal que K), tiene el cardinal de K. Se sigue entonces que $K[X] \times \mathbb{N}$ tiene el mismo cardinal que K. En este caso, entonces, K y E tienen el mismo cardinal.

Si en cambio K es finito, el conjunto $K[X] \times \mathbb{N}$ es numerable y, como sabemos que E es infinito, podemos concluir que E es numerable.

(*c*) Si $\mathscr{X}$ es un conjunto infinito, el anillo de polinomios $\mathbb{Q}[\mathscr{X}]$ con variables indexadas por el conjunto $\mathscr{X}$ tiene el mismo cardinal que $\mathscr{X}$, así que su cuerpo de fracciones $\mathbb{Q}(\mathscr{X})$ también. Pero entonces cualquier clausura algebraica de $\mathbb{Q}(\mathscr{X})$ tiene el cardinal de $\mathscr{X}$.

(*d*) Por lo anterior, el conjunto de elementos algebraicos sobre $\mathbb{Q}$ de $\mathbb{R}$ es necesariamente numerable, así que debe haber no numerables elementos trascendentes en $\mathbb{R}$. □

21. Sea K un cuerpo.

(*a*) Si t es trascendente sobre K y $n \in \mathbb{N}$, determine el polinomio $m(t, K(t^n))$ y el grado de la extensión $K(t)/K(t^n)$.

(*b*) Si $t_1,\dots,t_n$ es una familia algebraicamente independiente sobre K y $e_1,\dots,e_n$ son enteros no negativos, calcule

$$[K(t_1,\dots,t_n) : K(t_1^{e_1},\dots,t_n^{e_n})].$$

Solución. (*a*) El polinomio $X^n - t^n \in K(t^n)[X]$ tiene a t como raíz. Para ver que se trata de $m(t,K(t^n))$ basta mostrar que es irreducible. Del lema de Gauss, alcanza con mostrar que es irreducible en $K[t^n][X]$ y esto es claro, ya que satisface el criterio de Eisenstein sobre t^n. En particular vemos que $[K(t) : K(t^n)] = n$.

(*b*) Afirmamos que el grado es $e_1 \cdots e_n$ y lo probamos por inducción en n; notemos que cuando $n = 1$ esto es precisamente lo que hicimos en (*a*). Si $n > 1$, tenemos una torre

$$K(t_1^{e_1},\dots,t_n^{e_n}) \subseteq K(t_1,\dots,t_{n-1},t_n^{e_n}) \subseteq K(t_1,\dots,t_n).$$

Es $K(t_1,\dots,t_n) = K(t_1,\dots,t_{n-1})(t_n)$ y $K(t_1,\dots,t_{n-1},t_n^{e_n}) = K(t_1,\dots,t_{n-1})(t_n^{e_n})$, así que

$$[K(t_1,\dots,t_n) : K(t_1,\dots,t_{n-1},t_n^{e_n})] = [K(t_1,\dots,t_{n-1})(t_n) : K(t_1,\dots,t_{n-1})(t_n^{e_n})] = e_n$$

por lo que hicimos en (a). De manera similar, es $K(t_1,\dots,t_{n-1},t_n^{e_n}) = K(t_n^{e_n})(t_1,\dots,t_{n-1})$ y $K(t_1^{e_1},\dots,t_n^{e_n}) = K(t_n^{e_n})(t_1^{e_1},\dots,t_{n-1}^{e_{n-1}})$, así que

$$\begin{aligned}[K(t_1,\dots,t_{n-1},t_n^{e_n}) &: K(t_1^{e_1},\dots,t_n^{e_n})] \\ &= [K(t_n^{e_n})(t_1,\dots,t_{n-1}) : K(t_n^{e_n})(t_1^{e_1},\dots,t_{n-1}^{e_{n-1}})] = e_1\cdots e_{n-1}\end{aligned}$$

inductivamente. Tenemos entonces que

$$\begin{aligned}&[K(t_1,\dots,t_n) : K(t_1^{e_1},\dots,t_n^{e_n})] \\ &\quad = [K(t_1,\dots,t_n) : K(t_1,\dots,t_{n-1},t_n^{e_n})]\cdot[K(t_1,\dots,t_{n-1},t_n^{e_n} : K(t_1^{e_1},\dots,t_n^{e_n})] \\ &\quad = e_1\cdots e_n,\end{aligned}$$

y esto completa la inducción. □

22. Si K es un cuerpo y $f \in K[X]$ es un polinomio no constante, entonces

$$[K(X) : K(f)] = \deg f.$$

Solución. Es suficiente que mostremos que el polinomio minimal de X sobre $K(f(X))$ es $f(Y)-f(X) \in K(f(X))[Y]$. Es evidente que ese polinomio tiene a X como raíz, así que basta que probemos que es irreducible en $K(f(X))[Y]$. Como $f(X)$ es trascendente sobre K, hay un isomorfismo $K(f(X)) \to K(t)$, con t una variable, que manda $f(X)$ a t. Hay entonces un isomorfismo $K(f(X))[Y] \to K(t)[Y]$ que manda $f(Y)-f(X)$ a $f(Y)-t$, y basta que mostremos que $f(Y)-t$ es irreducible en $K(t)[Y]$. Como $K(t)$ es el cuerpo de fracciones de $K[t]$, que es un dominio de factorización única, el Lema de Gauss nos dice que esto es lo mismo que mostrar que $f(Y)-t$ es irreducible en $K[t][Y] = K[t,Y]$. Si $f(Y)-t = g(t,Y)h(t,Y)$ es una factorización en este último anillo, y teniendo en cuenta el grado en t, vemos que podemos suponer que $g(t,Y)$ no depende en realidad de t y que $h(t,Y)$ es de grado 1 en t. Así, existen $g, h_0, h_1 \in K[Y]$ tales que $f(Y)-t = g(Y)(h_0(Y)+th_1(Y))$. Se sigue de esto que $g(Y)h_1(Y) = -1$, con lo que g pertenece en realidad a K, y la factorización es trivial. □

23. Sea E/K una extensión de cuerpos y sean x e y elementos de E. Determine cuáles de las siguientes afirmaciones son verdaderas y, por supuesto, justifique sus respuestas:

(*a*) Si x e y son trascendentes sobre K, entonces los elementos xy y $x+y$ no son ambos algebraicos sobre K.

(*b*) Si x es trascendente sobre K e y e algebraico sobre K, entonces $x+y$ es trascendente sobre K.

(*c*) Si x es trascendente sobre K e y e algebraico sobre K, entonces xy es trascendente sobre K.

(*d*) Si x es trascendente sobre K e y es trascendente sobre $K(x)$, entonces el conjunto $\{x,y\}$ es algebraicamente independiente sobre K.

(*e*) Si x e y son trascendentes sobre K, entonces el conjunto $\{x,y\}$ es algebraicamente independiente sobre K.

24. (*a*) Si d un entero libre de cuadrados, entonces hay exactamente dos morfismos de cuerpos $\mathbb{Q}(\sqrt{d}) \to \mathbb{C}$ y ambos tienen a $\mathbb{Q}(\sqrt{d})$ como imagen.

(*b*) Si d es un entero libre de cubos, entonces hay exactamente tres morfismos de cuerpo $\mathbb{Q}(\sqrt[3]{d}) \to \mathbb{C}$, pero en general sus imagenes no están contenidas en $\mathbb{Q}(\sqrt[3]{d})$. ¿Cuántos morfismos $\mathbb{Q}(\sqrt[3]{d}, \zeta_3) \to \mathbb{C}$ hay y qué puede decir de sus imágenes?

Ernst Steinitz
1871–1928, Alemania

Steinitz escribió en 1910 un artículo llamado *Algebraische Theorie der Körper*, publicado en el *Journal de Crelle*, en el que estudió por primera vez a los cuerpos desde el punto de vista axiomático. Ahí se dieron por primera vez las definiciones de cuerpo primo, de cuerpo perfecto de grado de trascendencia y muchas otras. Fue el primero en probar que todo cuerpo posee una clausura algebraica. Suya es la idea que subyace a la prueba usual de que todo par de bases de un espacio vectorial tiene el mismo cardinal, y a la de que todo par de bases de trascendencia de un cuerpo tienen el mismo cardinal: el llamado lema de intercambio de Steinitz.

Un teorema famoso de Steinitz afirma que un cuerpo algebraicamente cerrado queda determinado por grado de trascendencia sobre su cuerpo primo y su característica.