CAPÍTULO I

Generalidades sobre cuerpos

En este capítulo se introduce la noción de extensión de cuerpos, que surge de modo natural al estudiar raíces de polinomios. En la primera sección se señala que si $L|K$ es una extensión de cuerpos entonces L tiene una estructura natural de K-espacio vectorial. En la segunda se distinguen los elementos algebraicos de los transcendentes y se estudian las extensiones algebraicas, y entre ellas las finitas.

Guía para leer el capítulo. El Ejemplo I.1.5 pone de manifiesto porqué las extensiones algebraicas de cuerpos surgen de modo natural al estudiar ecuaciones algebraicas.

La transitividad del grado I.1.6, cuya prueba dice más que el enunciado, véase I.1.7, junto con el hecho de que $[E : F] = 1$ si y sólo si $E = F$, I.1.8, son dos instrumentos esenciales a lo largo del curso.

Es importante entender que $K(a_1, \ldots, a_r)$ es el cuerpo de fracciones de $K[a_1, \ldots, a_r]$ y, también, el menor cuerpo que contiene a K, $a_1, \ldots, a_r$, véase I.1.9. A este respecto, cabe mencionar que $K(a_1, \ldots, a_r) = K[a_1, \ldots, a_r]$ si y sólo si cada a_j es algebraico sobre K, I.2.3.

Algebricidad y finitud están fuertemente relacionadas, I.2.3, por lo que la transitividad de la finitud se traduce en la transitividad de la algebricidad, I.2.10.

Se empleará constantemente el Teorema del elemento primitivo para extensiones de cuerpos de característica cero, I.3.3, mientras que de I.3.5 es, a nuestro parecer, más interesante su demostración que el enunciado.

1. Definiciones y conceptos básicos de la teoría de cuerpos

El objetivo de esta sección es introducir parte de la terminología y notación que nos permitirán estudiar *extensiones de cuerpos*.

Definición I.1.1 (Extensión de cuerpos) (1) Una *extensión de cuerpos* es una terna $(K, \mathtt{j}, L)$, donde K y L son cuerpos y $\mathtt{j} : K \to L$ es un homomorfismo. Se suele abreviar $L|K$. Vimos en II.1.5, vol. II, que todo homomorfismo de cuerpos es inyectivo, por lo que podemos identificar K con su imagen $\mathtt{j}(K)$ y considerar las extensiones de cuerpos como inclusiones de cuerpos $K \subset L$. Diremos entonces que K es un *subcuerpo* de L.

(2) Dadas extensiones de cuerpos $(K, \mathtt{j}_1, L)$ y $(L, \mathtt{j}_2, E)$, la terna $(K, \mathtt{j}_3, E)$, donde $\mathtt{j}_3 := \mathtt{j}_2 \circ \mathtt{j}_1$, es una extensión, y se dice que $(K, \mathtt{j}_1, L)$ es una *subextensión* de $(K, \mathtt{j}_3, E)$. En tal caso siempre podemos suponer que $K \subset L \subset E$ y las operaciones en K y L son las restricciones de las operaciones en E. Abreviaremos lo anterior diciendo que $L|K$ es una subextensión de $E|K$.

Ejemplos I.1.2 (1) Denotemos $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$, respectivamente, los cuerpos de los números racionales, reales y complejos. Como $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ y las operaciones en cada uno de estos cuerpos son las inducidas por la suma y producto de números complejos, $\mathbb{C}|\mathbb{R}$ es una extensión de cuerpos y $\mathbb{R}|\mathbb{Q}$ es una subextensión de $\mathbb{C}|\mathbb{Q}$.

(2) Sean K un cuerpo y $f \in K[\mathtt{t}]$ irreducible. Como $K[\mathtt{t}]$ es un DIP, por V.1.5 vol. II, el polinomio f genera un ideal maximal en $K[\mathtt{t}]$ y por tanto el cociente $L := K[\mathtt{t}]/(f)$ es un cuerpo donde, por simplicidad, hemos denotado (f) el ideal principal $f \cdot K[\mathtt{t}]$. Se comprueba inmediatamente que la aplicación

$$\mathtt{j} : K \to L,\ a \mapsto a + (f)$$

es un homomorfismo, y por tanto $(K, \mathtt{j}, L)$ es una extensión de cuerpos.

(3) El siguiente ejemplo explica por qué conviene utilizar la notación $L|K$ en lugar de $K \subset L$. Sean $\sqrt{2}$ el único número real positivo cuyo cuadrado vale 2 y el homomorfismo *evaluación en* $\sqrt{2}$ definido por

$$\varphi : \mathbb{Q}[\mathtt{t}] \to \mathbb{R},\ f \mapsto f(\sqrt{2}).$$

Su imagen es $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. En efecto, $g(\mathtt{t}) := \mathtt{t}^2 - 2 \in \mathbb{Q}[\mathtt{t}]$, que es un polinomio irreducible en $\mathbb{Z}[\mathtt{t}]$, y por tanto en $\mathbb{Q}[\mathtt{t}]$, por el Criterio de

Eisenstein, VI.2.7 vol. II, cumple $\varphi(g) = 0$. Al dividir cada $f \in \mathbb{Q}[\mathtt{t}]$ entre $g(\mathtt{t})$ existen $q \in \mathbb{Q}[\mathtt{t}]$ y $a, b \in \mathbb{Q}$ tales que $f(\mathtt{t}) = g(\mathtt{t})q(\mathtt{t}) + b\mathtt{t} + a$. En consecuencia, $\varphi(f) = a + b\sqrt{2}$.

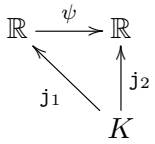
Además $(g) = \ker\varphi$ pues es obvio que $(g) \subset \ker\varphi$ y la igualdad se deduce por ser el ideal (g) maximal. Así, por el Primer Teorema de isomorfía,

$$\mathbb{Q}[\mathtt{t}]/(g) = \mathbb{Q}[\mathtt{t}]/\ker\varphi \simeq \operatorname{im}\varphi = \mathbb{Q}[\sqrt{2}],$$

de donde en particular se deduce que $K := \mathbb{Q}[\sqrt{2}]$ es un cuerpo. Consideramos los homomorfismos de cuerpos

$$\mathtt{j}_1 : K \to \mathbb{R},\ a + b\sqrt{2} \mapsto a + b\sqrt{2} \quad \& \quad \mathtt{j}_2 : K \to \mathbb{R},\ a + b\sqrt{2} \mapsto a - b\sqrt{2}.$$

Las extensiones $(K, \mathtt{j}_1, \mathbb{R})$ y $(K, \mathtt{j}_2, \mathbb{R})$ son distintas, pues no existe ningún homomorfismo de cuerpos $\psi : \mathbb{R} \to \mathbb{R}$ que haga conmutativo el diagrama:



En efecto, si existiese tal homomorfismo se tendría

$$-\sqrt{2} = \mathtt{j}_2(\sqrt{2}) = \psi(\mathtt{j}_1(\sqrt{2})) = \psi\big(\sqrt{2}\big) = \psi\big((\sqrt[4]{2})^2\big) = \big(\psi(\sqrt[4]{2})\big)^2 > 0,$$

que es una contradicción.

(4) Sean K un cuerpo y el homomorfismo $\varphi : \mathbb{Z} \to K$, $k \mapsto k \cdot 1_K$. Su núcleo es un ideal primo de $\mathbb{Z}$, luego, o bien $\ker\varphi = (0)$, o bien existe un número primo $p \in \mathbb{Z}$ tal que $\ker\varphi = p\mathbb{Z}$. En el primer caso, $\operatorname{char}(K) = 0$ y el homomorfismo φ se extiende al cuerpo de fracciones $\mathbb{Q}$ de $\mathbb{Z}$ mediante

$$\overline{\varphi} : \mathbb{Q} \to K,\ \frac{m}{n} \mapsto \frac{\varphi(m)}{\varphi(n)}$$

donde $m, n \in \mathbb{Z}$ y $n \neq 0$.

Si $\ker\varphi = p\mathbb{Z}$ entonces $\operatorname{char}(K) = p$ y, por el Primer Teorema de isomorfía, existe un homomorfismo inyectivo $\overline{\varphi} : \mathbb{Z}_p = \mathbb{Z}/\ker\varphi \to K$, $k + p\mathbb{Z} \mapsto \varphi(k)$.

En el primer caso se dice que $\mathbb{Q}$ es *el cuerpo primo de* K, y en el segundo dicho cuerpo primo es $\mathbb{Z}_p$. Nótese que si un cuerpo K es finito su característica es un primo p, pues en otro caso contendría un cuerpo isomorfo a $\mathbb{Q}$, contra

la finitud de K. El recíproco es falso; el cuerpo de fracciones del anillo de polinomios $\mathbb{Z}_p[\mathtt{t}]$ es infinito y de característica p.

(5) La situación del ejemplo del apartado (3) no es la regla general, en el sentido de que, en ocasiones, fijados un cuerpo L y un subcuerpo suyo K existe un único homomorfismo $\mathtt{j} : K \to L$, lo que hace superflua la mención al homomorfismo $\mathtt{j}$. En efecto, acabamos de ver que todo cuerpo L de característica 0 contiene a $\mathbb{Q}$, y vamos a comprobar que todo homomorfismo $\mathtt{j} : \mathbb{Q} \to L$ cumple que $\mathtt{j}(q) = q$ para cada $q \in \mathbb{Q}$. Como $\mathtt{j}(1) = 1$, se tiene $\mathtt{j}(n) = n$ para cada entero positivo n pues si suponemos por inducción que $\mathtt{j}(n-1) = n-1$, entonces

$$\mathtt{j}(n) = \mathtt{j}((n-1)+1) = \mathtt{j}(n-1) + \mathtt{j}(1) = (n-1) + 1 = n.$$

Además $\mathtt{j}(0) = 0$ y si $m \in \mathbb{Z}$ es negativo su opuesto $n := -m$ es positivo, y

$$0 = \mathtt{j}(0) = \mathtt{j}(m+n) = \mathtt{j}(m) + \mathtt{j}(n) = \mathtt{j}(m) + n,$$

así que $\mathtt{j}(m) = -n = m$. Finalmente, para todo número racional $q := \frac{m}{n}$, donde $m, n \in \mathbb{Z}$ y $n \neq 0$ se tiene

$$m = \mathtt{j}(m) = \mathtt{j}(qn) = \mathtt{j}(q)\mathtt{j}(n) = \mathtt{j}(q)n \quad \rightsquigarrow \quad \mathtt{j}(q) = \frac{m}{n} = q.$$

(6) También sucede que el único homomorfismo $\mathtt{j} : \mathbb{R} \to \mathbb{R}$ es la identidad. En efecto, en caso contrario existiría $x \in \mathbb{R}$ tal que $\mathtt{j}(x) \neq x$, y cambiando x por $-x$ podemos suponer que $x < \mathtt{j}(x)$. Tomamos $q \in \mathbb{Q}$ tal que $x < q < \mathtt{j}(x)$. Así $q - x > 0$, luego existe $y \in \mathbb{R}$ tal que $q - x = y^2$ y, por lo probado en (5),

$$q = \mathtt{j}(q) = \mathtt{j}(x) + \mathtt{j}(y^2) = \mathtt{j}(x) + (\mathtt{j}(y))^2 \geq \mathtt{j}(x),$$

que es una contradicción.

(7) Se dice que las extensiones $(K, \mathtt{j}_1, E)$ y $(K, \mathtt{j}_2, L)$ son *isomorfas* si existe un isomorfismo $\varphi : E \to L$ tal que $\varphi \circ \mathtt{j}_1 = \mathtt{j}_2$. Si suponemos que $\mathtt{j}_1$ y $\mathtt{j}_2$ son inclusiones conjuntistas la condición anterior equivale a que la restricción de φ al cuerpo K es la identidad.

Observación I.1.3 Si $L|K$ es una extensión de cuerpos identificamos K como subcuerpo de L, por lo que L admite una estructura canónica de K-espacio vectorial. Para ello se consideran como operaciones la suma de L y el producto por escalares de K definido por

$$\cdot : K \times L \to L, (\lambda, x) \mapsto \lambda \cdot x = \lambda x,$$

donde el producto $\lambda \cdot x$ es su producto como elementos de L. Este hecho justifica las siguientes definiciones.

Definiciones I.1.4 (Grado de una extensión) Sea $L|K$ una extensión de cuerpos.

(1) Se llama *grado* $[L : K]$ de la extensión a la dimensión $\dim_K L$ de L como K-espacio vectorial.

(2) Se dice que la extensión $L|K$ es *finita* si lo es su grado. En caso contrario se dice que $L|K$ es *infinita.*

Ejemplo I.1.5 Sean K un cuerpo, $f \in K[\mathtt{t}]$ un polinomio irreducible en $K[\mathtt{t}]$ y $L := K[\mathtt{t}]/(f)$. La extensión $L|K$ es finita y su grado coincide con el del polinomio f. De hecho, si denotamos $n := \deg(f)$ entonces

$$\mathcal{B} := \{1 + (f),\ \mathtt{t} + (f), \ldots,\ \mathtt{t}^{n-1} + (f)\}$$

es una base de L como K-espacio vectorial. En efecto, para cada $\alpha \in L$ existe un polinomio $g \in K[\mathtt{t}]$ tal que $\alpha := g + (f)$. Dividiendo g entre f, existen $q, r \in K[\mathtt{t}]$ tales que $\deg(r) < n$ y $g = qf + r$, luego $\alpha = r + (f)$. Escribimos $r := \sum_{j=0}^{n-1} a_j \mathtt{t}^j$ donde cada $a_j \in K$, y así

$$\alpha = r + (f) = \sum_{j=0}^{n-1} a_j \mathtt{t}^j + (f) = \sum_{j=0}^{n-1} a_j (\mathtt{t}^j + (f)),$$

lo que demuestra que $\mathcal{B}$ es sistema generador de L como K-espacio vectorial. En cuanto a la independencia lineal, sean $b_0, b_1, \ldots, b_{n-1} \in K$ tales que

$$0 = \sum_{k=0}^{n-1} b_k (\mathtt{t}^k + (f)) = \sum_{k=0}^{n-1} b_k \mathtt{t}^k + (f)$$

o, equivalentemente, $g := b_0 + b_1\mathtt{t} + \cdots + b_{n-1}\mathtt{t}^{n-1} \in (f)$. Esto significa que f, que tiene grado n, divide al polinomio g, cuyo grado es menor o igual que $n - 1$. Por tanto $g = 0$, es decir, $b_j = 0$ para $0 \leq j \leq n - 1$.

Proposición I.1.6 (Transitividad del grado) *Sean $L|K$ y $E|L$ extensiones de cuerpos. Las siguientes afirmaciones son equivalentes:*

(1) *$L|K$ y $E|L$ son finitas.*

(2) *$E|K$ es finita.*

Si se cumplen las condiciones anteriores, entonces

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

Demostración. Podemos suponer que $K \subset L \subset E$, y así L es un subespacio vectorial de E como K-espacio vectorial.

(1) $\Longrightarrow$ (2) Sean $\mathcal{B}_1 := \{u_1, \ldots, u_n\}$ y $\mathcal{B}_2 := \{v_1, \ldots, v_m\}$ bases, respectivamente, de E como L-espacio vectorial y de L como K-espacio vectorial. Veamos que

$$\mathcal{B}_3 := \{u_i v_j : \ 1 \leq i \leq n, \ 1 \leq j \leq m\} \subset E$$

es una base de E como K-espacio vectorial. lo que prueba la finitud de la extensión $E|K$ y la igualdad $[E : K] = [E : L] \cdot [L : K]$ del enunciado, pues $\mathcal{B}_3$ tiene mn elementos.

En primer lugar, comprobaremos que $\mathcal{B}_3$ es sistema generador. Para cada $x \in E$ existen $\lambda_1, \ldots, \lambda_n \in L$ tales que

$$x = \sum_{i=1}^{n} \lambda_i u_i.$$

Como cada $\lambda_i \in L$ existen $\mu_{i1}, \ldots, \mu_{im} \in K$ tales que $\lambda_i = \sum_{j=1}^{m} \mu_{ij} v_j$. Así,

$$x = \sum_{i=1}^{n} \lambda_i u_i = \sum_{i=1}^{n} \sum_{j=1}^{m} \mu_{ij} v_j u_i = \sum_{i=1}^{n} \sum_{j=1}^{m} \mu_{ij} u_i v_j,$$

lo que demuestra que $\mathcal{B}_3$ es un sistema generador de E como K-espacio vectorial. Veamos a continuación que también es un conjunto de vectores K-linealmente independientes. En efecto, consideramos la ecuación

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_{ij} u_i v_j = 0,$$

donde cada $\lambda_{ij} \in K$. Denotamos $\alpha_i := \sum_{j=1}^{m} \lambda_{ij} v_j \in L$ para $1 \leq i \leq n$, por lo que la igualdad anterior se reescribe como

$$\sum_{i=1}^{n} \alpha_i u_i = 0,$$

y, por tanto, cada $\alpha_i = 0$, pues $\mathcal{B}_1$ es una base de E como L-espacio vectorial. De este modo, para $1 \leq i \leq n$ tenemos la igualdad

$$\sum_{j=1}^{m} \lambda_{ij} v_j = 0,$$

donde cada $\lambda_{ij} \in K$. Como $\mathcal{B}_2$ es una base de L como K-espacio vectorial, concluimos que cada $\lambda_{ij} = 0$ y, por tanto, $\mathcal{B}_3$ es un conjunto de vectores K-linealmente independientes.

(2) $\Longrightarrow$ (1) Observamos que $\dim_K L \leq \dim_K E < +\infty$ puesto que L es un K-subespacio vectorial de E. Por otro lado, como $K \subset L$, cualquier base de E como K-espacio vectorial genera E como L-espacio vectorial. Esto implica que $\dim_L E \leq \dim_K E$ o lo que es igual, $[E : L] \leq [E : K] < +\infty$. □

Observación I.1.7 Obsérvese que en la Proposición anterior hemos probado algo más de lo que dice el enunciado. Hemos demostrado que dadas bases $\mathcal{B}_1 := \{u_1, \ldots, u_n\}$ y $\mathcal{B}_2 := \{v_1, \ldots, v_m\}$, respectivamente, de E como L-espacio vectorial y de L como K-espacio vectorial, entonces

$$\mathcal{B}_3 := \{u_i v_j : \ 1 \leq i \leq n, \ 1 \leq j \leq m\} \subset E$$

es base de E como K-espacio vectorial.

Observaciones I.1.8 (1) Sean $L|K$ y $E|L$ dos extensiones finitas de cuerpos tales que $[E : L] = [E : K]$. Entonces $L = K$.

En efecto, por la transitividad del grado, I.1.6, L es un K-espacio vectorial de dimensión 1, luego cualquier elemento no nulo de L, por ejemplo 1, constituye una base de L como K-espacio vectorial. Por tanto, para cada $v \in L$ existe $\lambda \in K$ tal que $v = \lambda \cdot 1 = \lambda \in K$, lo que prueba que $L = K$.

(2) Si la extensión $E|K$ es finita y $[E : K]$ es un número primo, entonces no existe ningún cuerpo L tal que $K \subsetneq L \subsetneq E$, es decir, $E|K$ no admite ninguna *subextensión propia.* En caso contrario los enteros $m := [E : L]$ y $n := [L : K]$ serían mayores que 1 y $[E : K] = [E : L] \cdot [L : K] = mn$ no sería primo.

1.a. Subextensión generada por un conjunto. Sean $L|K$ una extensión de cuerpos y $A \subset L$ un subconjunto. Como siempre, podemos suponer que $K \subset L$. La familia Σ_A formada por todos los subcuerpos de L que contienen a $K \cup A$ es no vacía, pues $L \in \Sigma_A$, y se define $K(A) := \bigcap_{F \in \Sigma_A} F$. Desde luego $K \cup A \subset K(A) \subset L$, y de hecho $K(A)$ es el menor subcuerpo de L que contiene a $K \cup A$. Para comprobarlo es suficiente, por estar contenido en el cuerpo L, demostrar que $K(A)$ es un cuerpo. Pero, dados $x, y \in K(A)$ la resta $x - y$ y el producto xy^{-1} (este último si $y \neq 0$), pertenecen a cada cuerpo $F \in \Sigma_A$, luego pertenecen a $K(A)$. Se dice que $K(A)$ es el *cuerpo generado por A sobre K,* y también que $K(A)|K$ es la subextensión de $L|K$ *generada por A.*

Si $A := \{a_1, \ldots, a_r\}$ es un conjunto finito, el subcuerpo $K(A)$ se denota por $K(A) := K(a_1, \ldots, a_r)$ y se dice que $K(a_1, \ldots, a_r)|K$ es una extensión *finitamente generada.* Diremos en este caso que $a_1, \ldots, a_r$ son *unos generadores* de la extensión $K(A)|K$. Si $r = 1$, es decir, $A := \{a\}$, entonces se dice que $K(a)|K$ es una *extensión simple* y que a es un *elemento primitivo* de la extensión $K(a)|K$.

Proposición I.1.9 *Sean $L|K$ una extensión de cuerpos y $a, a_1, \ldots, a_r \in L$. Entonces,*

(1) $K(a_1, \ldots, a_r) = \left\{ \frac{f(a_1,\ldots,a_r)}{g(a_1,\ldots,a_r)} : \ f, g \in K[\mathtt{x}_1, \ldots, \mathtt{x}_r] \ \ \& \ \ g(a_1, \ldots, a_r) \neq 0 \right\}$.

(2) $K(a) = \left\{ \frac{f(a)}{g(a)} : \ f, g \in K[\mathtt{t}] \quad \& \quad g(a) \neq 0 \right\}$.

Demostración. El apartado (2) se deduce de (1) con $r = 1$. En cuanto al primer apartado, en VII.1.3, vol. II vimos que el menor subanillo de L que contiene a K y a $a_1, \ldots, a_r$ es

$$K[a_1, \ldots, a_r] := \{f(a_1, \ldots, a_r) : \ f \in K[\mathtt{x}_1, \ldots, \mathtt{x}_r]\},$$

por lo que su cuerpo de fracciones es el menor subcuerpo de L que contiene a K y a $a_1, \ldots, a_r$, y eso es lo que afirma el enunciado. □

Proposición I.1.10 *Sean $L|K$ una extensión de cuerpos, $A \subset L$ y $\{E_i\}_{i\in I}$ una familia de subcuerpos de L que contienen a K.*

(1) *Supongamos que para cada par de índices $i, j \in I$ existe $k \in I$ tal que $E_i \cup E_j \subset E_k$. Entonces $F := \bigcup_{i\in I} E_i$ es un subcuerpo de L que contiene a K.*

(2) *Un elemento $x \in L$ pertenece a $K(A)$ si y sólo si existen $a_1, \ldots, a_r \in A$ y $f, g \in K[\mathtt{x}_1, \ldots, \mathtt{x}_r]$ tales que $g(a_1, \ldots, a_r) \neq 0$ y*

$$x := \frac{f(a_1, \ldots, a_r)}{g(a_1, \ldots, a_r)}.$$

Demostración. (1) Sólo hay que probar que $x - y, xy^{-1} \in F$ para cada $x, y \in F$, (el segundo si $y \neq 0$). Como $x, y \in F$, existen $i, j \in I$ tales que $x \in E_i$ e $y \in E_j$. Por hipótesis existe $k \in I$ tal que $E_i \cup E_j \subset E_k$ y, por tanto, $x, y \in E_k$, que es un cuerpo. En consecuencia, $x - y, \ xy^{-1} \in E_k \subset F$.

(2) Sea $\mathcal{F} := \{K(M) : M \in \mathcal{P}_F(A)\}$, donde $\mathcal{P}_F(A)$ es el conjunto formado por todos los subconjuntos finitos de A. La familia $\mathcal{F}$ está en las condiciones

del apartado anterior, pues dados subconjuntos finitos M y N de A también $M \cup N \in \mathcal{P}_F(A)$, por lo que $K(M \cup N) \in \mathcal{F}$ es un cuerpo que contiene a $K(M) \cup K(N)$. Se deduce del apartado (1) que $F := \bigcup_{M \in \mathcal{P}_F(A)} K(M)$ es un subcuerpo de L que contiene a K.

De hecho $F = K(A)$. En efecto, si $M \in \mathcal{P}_F(A)$ se tiene $M \subset A$, luego $K \cup M \subset K \cup A$, por lo que $K(M) \subset K(A)$ y esto implica que $F \subset K(A)$. Además, $a \in K(a) \subset F$ para cada $a \in A$, luego F contiene a $K \cup A$, así que también contiene a $K(A)$. □

Observaciones I.1.11 (1) Toda extensión finita es finitamente generada. En efecto, si $L|K$ es una extensión finita y $\mathcal{B} := \{u_1, \ldots, u_n\} \subset L$ es una base de L como K-espacio vectorial, entonces $L = K(u_1, \ldots, u_n)$, por lo que $L|K$ es una extensión finitamente generada. En efecto, L contiene a $K \cup \mathcal{B}$, luego $K(u_1, \ldots, u_n) \subset L$. El contenido recíproco es evidente pues para cada $x \in L$ existen $\lambda_1, \ldots, \lambda_n \in K$ tales que $x = \sum_{j=1}^{n} \lambda_j u_j \in K(u_1, \ldots, u_n)$.

(2) Ls extensiones $\mathbb{C}|\mathbb{Q}$ y $\mathbb{R}|\mathbb{Q}$ no son finitamente generadas, porque $\mathbb{Q}$ es un conjunto numerable pero ni $\mathbb{R}$ ni $\mathbb{C}$ lo son.

(3) Sean $L|K$ una extensión y $A, B \subset L$. Entonces,

$$K(A)(B) = K(A \cup B) = K(B)(A).$$

En efecto, $K(A \cup B)$ es un cuerpo que contiene a $K \cup A$, luego contiene a $K(A)$. Como también contiene a B se deduce que $K(A)(B) \subset K(A \cup B)$. El otro contenido es evidente pues, por la definición, $K(A)(B)$ contiene a $K \cup (A \cup B)$. Hemos probado la igualdad $K(A)(B) = K(A \cup B)$ y la otra se deduce de ésta y de que $A \cup B = B \cup A$.

2. Extensiones algebraicas

En esta sección se introducen las nociones de elementos algebraicamente dependientes e independientes sobre un cuerpo y se obtienen algunos resultados básicos acerca de las llamadas *extensiones algebraicas.*

Definición I.2.1 (Dependencia algebraica) Sean $L|K$ una extensión de cuerpos, $a = (a_1, \ldots, a_n) \in L^n$ y

$$\mathrm{ev}_a : K[\mathtt{x}_1, \ldots, \mathtt{x}_n] \to L,\ f \mapsto f(a_1, \ldots, a_n)$$

el homomorfismo evaluación.

(1) Se dice que $a_1, \ldots, a_n$ son *algebraicamente independientes sobre* K si ev_a es inyectivo, esto es, $f(a_1, \ldots, a_n) \neq 0$ para cada $f \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ no nulo. En caso contrario $a_1, \ldots, a_n$ son *algebraicamente dependientes* sobre K.

(2) Se dice que $a = a_1$ es *transcendente* sobre K si es algebraicamente independiente sobre K, es decir, si $f(a) \neq 0$ para cada polinomio no nulo $f \in K[\mathtt{t}]$. En caso contrario se dice que a es *algebraico* sobre K.

(3) Se dice que una extensión $E|K$ es *algebraica* si cada $a \in E$ es algebraico sobre K. Si E contiene algún elemento transcendente sobre K, se dice que la extensión $E|K$ es *transcendente*. Nótese que si $L|K$ es una subextensión de una extensión algebraica $E|K$, entonces también $L|K$ es algebraica.

Observaciones y Ejemplos I.2.2 (1) Cada $a \in K$ es raíz de $\mathtt{t} - a \in K[\mathtt{t}]$, luego es algebraico sobre K.

(2) Si a es algebraico sobre K, el núcleo del homomorfismo evaluación

$$\mathrm{ev}_a : K[\mathtt{t}] \to L,\ g \to g(a)$$

es un ideal primo no nulo de $K[\mathtt{t}]$, pues L es un dominio. Como $K[\mathtt{t}]$ es un DIP, el núcleo $\ker \mathrm{ev}_a$ está generado por un polinomio irreducible $f \in K[\mathtt{t}]$. Así, por V.1.9, vol. II, $K[\mathtt{t}]/(f) \simeq \mathrm{im}\, \mathrm{ev}_a = K[a]$. Como $K[\mathtt{t}]$ es un DIP y f es irreducible, (f) es ideal maximal, luego $K[a]$ es un cuerpo que contiene a $K \cup \{a\}$. Como $K[a] \subset K(a)$ concluimos que $K[a] = K(a)$. El polinomio f que genera $\ker \mathrm{ev}_a$ es único salvo multiplicación por unidades de $K[\mathtt{t}]$, es decir, por elementos no nulos de K.

Para elegir sin ambigüedad un generador f de $\ker \mathrm{ev}_a$ exigimos que sea mónico, propiedad que lo hace único. El polinomio mónico f que genera $\ker \mathrm{ev}_a$ recibe el nombre de *polinomio mínimo* o *irreducible* de a sobre K y lo denotaremos $P_{K,a}$. El nombre de polinomio mínimo proviene de que es el polinomio mónico de grado mínimo entre los polinomios de $K[\mathtt{t}]$ que tienen a a por raíz.

(3) Por el Ejemplo I.1.5 y la Proposición I.1.9, si a es algebraico sobre K la extensión $K(a)|K$ es finita, y de hecho $[K(a) : K] = \deg(P_{K,a})$. Más aún, si denotamos $\mathfrak{m} := P_{K,a}K[\mathtt{t}]$ el ideal maximal generado por $P_{K,a}$, la aplicación

$$L := K[\mathtt{t}]/\mathfrak{m} \to K[a],\ f + \mathfrak{m} \mapsto f(a)$$

es, por el apartado (2), un isomorfismo de cuerpos que deja fijos los elementos de K, luego es un isomorfismo de K-espacios vectoriales. Vimos en el Ejemplo

I.1.5 que si $P_{K,a}$ tiene grado n,

$$\mathcal{B} := \{1 + \mathfrak{m},\ \mathtt{t} + \mathfrak{m}, \ldots,\ \mathtt{t}^{n-1} + \mathfrak{m}\}$$

es base de L, luego $\{1, a, \ldots, a^{n-1}\}$ es base de $K[a]$ como K-espacio vectorial.

(4) Sean $L|K$ una extensión, $a \in L$ algebraico sobre K y $f \in K[\mathtt{t}]$ un polinomio mónico e irreducible en $K[\mathtt{t}]$ tal que $f(a) = 0$. Entonces $f = P_{K,a}$. En efecto, $f \in P_{K,a} \cdot K[\mathtt{t}]$ por la propia definición de $P_{K,a}$ y, como f es irreducible, existe $\lambda \in K \setminus \{0\}$ tal que $f = \lambda P_{K,a}$. Esto implica, puesto que tanto f como $P_{K,a}$ son mónicos, que $\lambda = 1$, esto es, $f = P_{K,a}$.

(5) Supongamos que $\mathrm{char}(K) = 0$ y sea $f \in K[\mathtt{t}]$ un polinomio irreducible. Para cada extensión $L|K$ todas las raíces de f en L son simples. En efecto, en caso contrario existirían una extensión $L|K$ y $a \in L$ raíz múltiple de f en L. Dividiendo f por su coeficiente director podemos suponer que es mónico, luego $f = P_{K,a}$. Al ser a raíz múltiple de f es raíz de f' y $\deg(f') < \deg(f)$. Como $\mathrm{char}(K) = 0$ el polinomio f' no es nulo, y lo anterior contradice que f es el polinomio mínimo de a sobre K.

(6) Si $L|E$ y $E|K$ son extensiones de cuerpos y $a \in L$ es algebraico sobre K, entonces también es algebraico sobre E, pues el polinomio mínimo de a sobre K tiene coeficientes en E. De hecho $P_{K,a} \in E[\mathtt{t}]$ y se anula en a, luego es múltiplo en $E[\mathtt{t}]$ de $P_{E,a}$. En particular, dados elementos $a, b \in L$ algebraicos sobre K y tomando $E := K(b)$ se tiene

$$[K(a,b) : K(b)] = [E(a) : E] = \deg\left(P_{E,a}\right) \leq \deg\left(P_{K,a}\right) = [K(a) : K].$$

(7) Sean $L|K$ una extensión y $a \in L$ transcendente sobre K. Entonces el homomorfismo $\mathrm{ev}_a : K[\mathtt{t}] \to L,\ g \to g(a)$ es inyectivo, por lo que es un isomorfismo entre $K[\mathtt{t}]$ y $K[a]$, que en consecuencia se extiende a un isomorfismo entre los cuerpos de fracciones:

$$K(\mathtt{t}) \to K(a),\ \frac{f}{g} \mapsto \frac{f(a)}{g(a)}.$$

(8) El isomorfismo anterior es también un isomorfismo de K-espacios vectoriales, lo que implica que la extensión $K(a)|K$ es infinita. En efecto, basta probar que lo es $K(\mathtt{t})|K$, y esto es consecuencia de que las potencias $\{\mathtt{t}^j : j \in \mathbb{N}\}$ son K-linealmente independientes.

(9) En particular, toda extensión transcendente $L|K$ es infinita, pues existe un elemento $a \in L$ transcendente sobre K, luego el K-espacio vectorial L contiene

al subespacio $K(a)$, que tiene dimensión infinita, por lo que también $\dim_K L$ es infinita.

(10) Sean $L|K$ una extensión y $a_1, \ldots, a_n \in L$ algebraicamente independientes sobre K. Entonces, el homomorfismo evaluación

$$\mathrm{ev} : K[\mathtt{x}_1, \ldots, \mathtt{x}_n] \to L,\ g \to g(a_1, \ldots, a_n)$$

es inyectivo, luego se extiende a un isomorfismo entre sus cuerpos de fracciones

$$K(\mathtt{x}_1, \ldots, \mathtt{x}_n) \to K(a_1, \ldots, a_n),\ \frac{f}{g} \mapsto \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)}.$$

(11) En las condiciones del apartado anterior, y fijados $1 \leq i_1 < \cdots < i_r \leq n$, es claro que los elementos $a_{i_1}, \ldots, a_{i_r}$ son también algebraicamente independientes sobre K.

(12) Sean K un cuerpo, $\mathtt{t}$ una indeterminada sobre K y $L := K(\mathtt{t})$. Entonces, los elementos $a_1 := \mathtt{t},\ a_2 := \mathtt{t}^2 \in L$ son algebraicamente dependientes sobre K porque el polinomio $f := \mathtt{x}_1^2 - \mathtt{x}_2 \in K[\mathtt{x}_1, \mathtt{x}_2]$ es no nulo y $f(a_1, a_2) = 0$.

Corolario I.2.3 (Finitud y algebricidad) *Sea $L|K$ una extensión de cuerpos. Se cumplen las siguientes propiedades.*

(1) *Si $L|K$ es finita, entonces es algebraica.*

(2) *Si $a \in L$ es algebraico sobre K, entonces la extensión $K(a)|K$ es finita, luego algebraica. Además $K(a) = K[a]$.*

(3) *Si $a_1, \ldots, a_n \in L$ son algebraicos sobre K, entonces $K(a_1, \ldots, a_n)|K$ es una extensión finita y, por tanto, algebraica. Además,*

$$K(a_1, \ldots, a_n) = K[a_1, \ldots, a_n].$$

(4) *Dos elementos $a, b \in L$ son algebraicos sobre K si y sólo si $a + b$ y ab son algebraicos sobre K.*

Demostración. (1) Está demostrado en el Ejemplo I.2.2 (9).

(2) Hemos visto en I.2.2 (3) que la extensión $K(a)|K$ es finita, luego por (1) es también algebraica. También hemos probado $K(a) = K[a]$ en I.2.2 (2).

(3) El caso $n = 1$ es el que acabamos de probar, y procedemos por inducción sobre n. Supongamos el resultado cierto para $n - 1$ y veamos que también es

cierto para n. Nótese que como a_n es algebraico sobre K también lo es sobre el cuerpo $E := K(a_1, \ldots, a_{n-1})$. Por la hipótesis de inducción se cumple que $E = K[a_1, \ldots, a_{n-1}]$ y, por la Observación I.1.11 (6),

$$\begin{aligned} K(a_1, \ldots, a_n) &= K(a_1, \ldots, a_{n-1})(a_n) = E(a_n) = E[a_n] \\ &= K[a_1, \ldots, a_{n-1}][a_n] = K[a_1, \ldots, a_n]. \end{aligned}$$

Además, por hipótesis de inducción, las extensiones $E|K$ y $E(a_n)|E$ son finitas, luego también lo es $E(a_n)|K$, esto es, $K(a_1, \ldots, a_n)|K$ es una extensión finita.

(4) Si a, b son algebraicos sobre K, se sigue del apartado (3) que la extensión $K(a, b)|K$ es algebraica. Como $u := a + b,\ v := ab \in K(a, b)$, tanto u como v son algebraicos sobre K.

Supongamos ahora que u y v son algebraicos sobre K. Por el apartado (3) la extensión $K(u, v)|K$ es finita. Además, a y b son algebraicos sobre $E := K(u, v)$ por ser raíces del polinomio $f(\mathtt{t}) := \mathtt{t}^2 - u\mathtt{t} + v \in E[\mathtt{t}]$, luego se deduce del apartado (3) que la extensión $E(a, b)|E$ es finita. Como también $E|K$ lo es, se sigue de la Proposición I.1.6 que la extensión $E(a, b)|K$ es finita. Esto implica la finitud de $K(a, b)|K$, puesto que $K \subset K(a, b) \subset E(a, b)$. En particular a y b son, por el apartado (1), algebraicos sobre K. □

Proposición I.2.4 *Sea $L|K$ una extensión de cuerpos generada por un subconjunto $A = \{u_i : i \in I\}$ de L cuyos elementos son algebraicos sobre K. Entonces, la extensión $L|K$ es algebraica y*

$$L = K(A) = \{f(u_{i_1}, \ldots, u_{i_r}) :\ f \in K[\mathtt{x}_1, \ldots, \mathtt{x}_r],\ r \geq 1,\ i_1, \ldots, i_r \in I\}.$$

Demostración. Sea $b \in L$. Por la Proposición I.1.10 (2), existen $u_{i_1}, \ldots, u_{i_r}$ tales que $b \in K(u_{i_1}, \ldots, u_{i_r})$. Como $u_{i_1}, \ldots, u_{i_r}$ son algebraicos sobre K entonces, por el Corolario I.2.3, $K(u_{i_1}, \ldots, u_{i_r}) = K[u_{i_1}, \ldots, u_{i_r}]$ y, por tanto, existe $h \in K[\mathtt{x}_1, \ldots, \mathtt{x}_r]$ tal que

$$b = h(u_{i_1}, \ldots, u_{i_r}) \in K[u_{i_1}, \ldots, u_{i_r}].$$

Empleando de nuevo el Corolario I.2.3, se sigue que b es algebraico sobre K. Así, $L = K(A)$ es una extensión algebraica de K y se cumple la igualdad del enunciado. □

Ejemplos I.2.5 (1) Dada una extensión de cuerpos $E|K$ y dados $a, b \in E$ elementos algebraicos sobre K, escribimos $L := K(a, b)$ y denotamos

$$m := [K(a) : K] \quad \& \quad n := [K(b) : K].$$