

Cielo  
Saga de la Divina Comedia

Universidad de Murcia

Jesús González Abril

22 de enero de 2026

# Índice general

1. Extensiones de cuerpos	2
1.1. Extensiones de cuerpos . . . . .	2
1.1.1. Ejemplos de extensiones de cuerpos . . . . .	3
1.1.2. Torres de cuerpos y propiedades . . . . .	4
Bibliografía	8

# Capítulo 1

## Extensiones de cuerpos

### 1.1. Extensiones de cuerpos

Definición 1.1.1: Extensión de cuerpos

Sea  $K$  un cuerpo. Una extensión de  $K$  es un cuerpo  $L$  que contiene a  $K$  como subcuerpo. En tal caso decimos que  $L/K$  es una extensión de cuerpos o simplemente una extensión.

Observe que si  $L/K$  es una extensión de cuerpos, entonces  $L$  tiene una estructura natural de espacio vectorial sobre  $K$ . Los vectores son los elementos de  $L$  y los escalares son los elementos de  $K$ , la suma de vectores es la suma en  $L$  y el producto de escalares por vectores está bien definido puesto que los elementos de  $K$  están en  $L$ . Denotaremos este espacio vectorial como  $L_K$  y una base de la extensión  $L/K$  es simplemente una base de este espacio vectorial.

Definición 1.1.2: Grado de una extensión

La dimensión de  $L_K$  se llama grado de la extensión  $L/K$  y se representa por  $[L : K]$ . O sea

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

Ejemplo 1.1.3: Extensión de los reales

Tomemos  $K = \mathbb{R}$ ,  $L = \mathbb{C}$ . Entonces  $L/K$  es una extensión, en este caso los vectores del espacio vectorial son números complejos, y para construir una combinación lineal de ellos solo podemos emplear escalares reales.

El conjunto  $B = \{1, i\}$  genera a  $L_K$ : cualquier  $z \in L_K$  se puede expresar como

$$z = \operatorname{Re}(z)1 + \operatorname{Im}(z)i, \quad \operatorname{Re}(z), \operatorname{Im}(z) \in \mathbb{R}.$$

Además, si  $a, b \in \mathbb{R}$  cumplen  $a1 + bi = 0 \implies a, b = 0$ , por lo que  $B$  es una base. De aquí deducimos que  $[\mathbb{C} : \mathbb{R}] = 2$ .

Decimos que  $L/K$  es una extensión finita si  $[L : K] < \infty$ . Obsérvese que si  $L/K$  es una extensión de grado  $n$  entonces la base del espacio vectorial  $L_K$  tiene  $n$  vectores, por tanto, según un resultado conocido de álgebra lineal,

$$L_K \simeq K^n.$$

De aquí deducimos que,  $|L| = |K|^n$ . Gracias a este resultado obtenemos la siguiente proposición.

### Proposición 1.1.4

Sea  $L/K$  una extensión finita.

1. Si  $K$  es finito de orden  $q$ , entonces  $L$  es finito de orden  $q^n$ .
2. Si  $K$  es infinito entonces  $L$  tiene el mismo cardinal que  $K$ .

#### 1.1.1. Ejemplos de extensiones de cuerpos

##### Ejemplo 1.1.5

Si  $L/K$  es una extensión de cuerpos, entonces  $[L : K] = 1$  si y solo si  $K = L$ .

##### Demostración

Es inmediato que si  $K = L$  entonces una base de  $L_K$  es  $B = \{1\}$ , por lo que  $[L : K] = 1$ . Por otro lado, si las bases de  $L_K$  tiene un solo elemento, podemos fijar una base  $B = \{\alpha\}$ ,  $\alpha \neq 0$ . En concreto, la identidad debe expresarse como combinación lineal de elementos de esa base, es decir,

$$1 = \lambda\alpha$$

para cierto  $\lambda \in K$ , pero entonces debe ser  $\alpha = \lambda^{-1} \in K$ , por lo que cualquier elemento  $a \in L$  es combinación de un escalar  $b \in K$  con  $\alpha$

$$a = b\alpha \in K \quad \text{ya que } \alpha \in K$$

por tanto,  $L \subseteq K \implies L = K$ .

##### Ejemplo 1.1.6

Como hemos visto en el Ejemplo 1.1.3,  $\mathbb{C}/\mathbb{R}$  es una extensión finita de grado 2.

##### Ejemplo 1.1.7

$\mathbb{R}/\mathbb{Q}$  y  $\mathbb{C}/\mathbb{Q}$  son extensiones de grado infinito.

##### Demostración

Para verlo, supongamos que fueran de grado finito. Entonces, como  $\mathbb{Q}$  es infinito, por el apartado 2 de la Proposición 1.1.4,  $\mathbb{R}$  y  $\mathbb{C}$  deberían tener el mismo cardinal que  $\mathbb{Q}$ . Sin embargo, sabemos que  $\mathbb{R}, \mathbb{C}$  tienen mayor cardinal que  $\mathbb{Q}$ , luego ambas extensiones deben ser de grado infinito.

##### Ejemplo 1.1.8

Si  $n \in \mathbb{Q}$ , entonces  $\mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} : a, b \in \mathbb{Q}\}$  es una extensión que tiene grado 1 si  $n$  es un cuadrado de un número racional y grado 2 en caso contrario pues, en el segundo caso,  $\{1, \sqrt{n}\}$  es una base de  $\mathbb{Q}(\sqrt{n})/\mathbb{Q}$ .

### Ejemplo 1.1.9

El cuerpo de fracciones  $K(X)$  del anillo de polinomios  $K[X]$  es una extensión de  $K$  de grado infinito.

#### Demostración

Por un resultado sobre anillos, como  $K$  es un cuerpo, en concreto es un dominio, y entonces  $K[X]$  también lo es. Por tanto, tiene sentido considerar el cuerpo de fracciones de  $K[X]$ , que denotamos  $K(X)$ . Claramente,  $K \subseteq K(X)$ <sup>a</sup>. Para ver que la extensión es de grado infinito encontraremos un conjunto infinito de elementos linealmente independientes. De esto se deduce que cualquier base de  $K(X)$  debe tener infinitos elementos. Sea

$$C = \{1, X^{-1}, X^{-2}, \dots\},$$

consideremos una combinación lineal cualquiera de  $m$  elementos de  $C$ :

$$P = a_1X^{-n_1} + a_2X^{-n_2} + \dots + a_mX^{-n_m}, \quad n_1 \leq \dots \leq n_m$$

entonces,

$$P = 0 \iff X^{n_m}P = 0 \iff a_1X^{n_m-n_1} + \dots + a_m = 0 \iff \forall i, a_i = 0$$

ya que  $X^{n_m}P$  es un polinomio en  $K$  y solo puede ser cero si todos sus coeficientes son 0.

<sup>a</sup>También es cierto que  $K \subseteq K[X]$ , pero  $K[X]$  no tiene por qué ser un cuerpo.

### 1.1.2. Torres de cuerpos y propiedades

#### Definición 1.1.10: Torre de extensiones de cuerpos

Una torre de extensiones de cuerpos es una sucesión

$$K_1 \subseteq K_2 \subseteq \dots \subseteq K_n$$

de cuerpos, cada uno subcuerpo de los posteriores. Cada extensión  $K_{i+1}/K_i$  se llama subextensión de la torre.

#### Definición 1.1.11: $K$ -homomorfismo

Si  $L_1$  y  $L_2$  son dos extensiones de  $K$ , entonces un homomorfismo de  $L_1/K$  en  $L_2/K$  (también llamado  $K$ -homomorfismo) es un homomorfismo de cuerpos  $f : L_1 \rightarrow L_2$  tal que para todo  $a \in K$ ,  $f(a) = a$ .

Un endomorfismo de una extensión  $L/K$  es un homomorfismo de  $L/K$  en si misma. Un isomorfismo de extensiones (o  $K$ -isomorfismo) es un homomorfismo de extensiones que es isomorfismo de cuerpos y un automorfismo de extensiones (o  $K$ -automorfismo) es un isomorfismo de una extensión de  $K$  en si misma.

Obsérvese que el conjunto de los automorfismos de una extensión  $L/K$  es un grupo que llamaremos grupo de Galois de  $L/K$ , en el que el producto es la composición de aplicaciones, y que denotaremos por

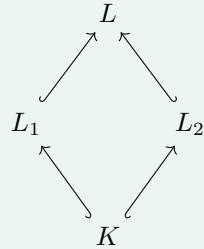
$$\text{Gal}(L/K).$$

### Definición 1.1.12: Subextensión

Una subextensión de una extensión de cuerpos  $L/K$  es un subcuerpo  $M$  de  $L$  que contiene a  $K$ :

$$K \subseteq M \subseteq L.$$

Dos extensiones  $L_1$  y  $L_2$  de un cuerpo  $K$  se dice que son admisibles si existe un cuerpo  $L$  que es extensión de  $L_1$  y  $L_2$ , o lo que es lo mismo, si ambas son subextensiones de una extensión común  $L/K$ .



Por convenio, en todos los cuerpos suponemos que  $0 \neq 1$ . Eso implica que todos los homomorfismos entre cuerpos son inyectivos.

### Demostración

Sea  $f : K \rightarrow L$  un homomorfismo de cuerpos. Sea  $x \in \ker f$ , si suponemos que  $x \neq 0$ , entonces

$$1_L = f(1_K) = f(xx^{-1}) = f(x)f(x^{-1}) = 0$$

lo cual es contradictorio. Por tanto,  $\ker f = \{1_K\}$ , por lo que

$$f(x) = f(y) \iff 0 = f(y) - f(x) = f(y-x) \iff y-x = 0 \iff y = x.$$

Además los  $K$ -homomorfismos son homomorfismos de  $K$ -espacios vectoriales. De esta forma siempre que exista un homomorfismo de cuerpos  $f : K \rightarrow L$ , el cuerpo  $L$  contiene un subcuerpo isomorfo a  $K$ , la imagen  $f(K)$  de  $f$ .

Por otro lado  $K$  admite una extensión isomorfa a  $L$ , a saber el conjunto  $K \cup (L \setminus f(K))$ , en el que se define el producto de la forma obvia. Abusaremos a menudo de la notación y cada vez que tengamos un homomorfismo de cuerpos  $f : K \rightarrow L$ , simplemente consideraremos  $K$  como subcuerpo de  $L$ , identificando los elementos de  $K$  y  $f(K)$ , a través de  $f$ .

Proposición 1.1.13: Propiedades básicas

- (1) Sean  $L_1$  y  $L_2$  extensiones de  $K$ . Si existe un homomorfismo de  $L_1/K$  en  $L_2/K$ , entonces  $[L_1 : K] \leq [L_2 : K]$ .
- (2) Todo endomorfismo de una extensión finita es un automorfismo.
- (3) Sea  $K \subseteq E \subseteq L$  una torre de cuerpos y sean  $B$  una base de  $E_K$  y  $B'$  una base de  $L_E$ . Entonces  $A = \{bb' : b \in B, b' \in B'\}$  es una base de  $L_K$ . En particular la clase de extensiones finitas es multiplicativa y si  $L/K$  es finita entonces

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

- (4) Si  $L_1$  y  $L_2$  son admisibles y  $L$  es un cuerpo que contiene a  $L_1$  y  $L_2$  como subcuerpos, entonces

$$L_1 L_2 = \left\{ \frac{a_1 b_1 + \cdots + a_n b_n}{a'_1 b'_1 + \cdots + a'_n b'_n} : a_i, a'_i \in L_1, b_i, b'_i \in L_2, a'_1 b'_1 + \cdots + a'_n b'_n \neq 0 \right\}$$

es el menor subcuerpo de  $L$  que contiene a  $L_1$  y  $L_2$ . Este cuerpo se llama compuesto de  $L_1$  y  $L_2$  en  $L$ .

- (5) Sean  $L/K$  una extensión de cuerpos y  $S$  un subconjunto de  $L$ . Entonces el menor subanillo de  $L$  que contiene a  $K$  y a  $S$  está formado por los elementos de la forma  $p(s_1, \dots, s_n)$  con  $p \in K[X_1, \dots, X_n]$  y  $s_1, \dots, s_n \in S$ . Además, el menor subcuerpo de  $L$  que contiene a  $K$  y a  $S$  está formado por los elementos de la forma

$$\frac{p(s_1, s_2, \dots, s_n)}{q(s_1, s_2, \dots, s_n)}$$

donde  $n$  es un número natural arbitrario,  $p, q \in K[X_1, \dots, X_n]$ ,  $s_1, \dots, s_n \in S$  y  $q(s_1, s_2, \dots, s_n) \neq 0$ .

Demostración

- (1) y (2) son una consecuencia inmediata de que todo  $K$ -homomorfismo de cuerpos  $L_1 \rightarrow L_2$  es un homomorfismo inyectivo de espacios vectoriales sobre  $K$  y de que todo endomorfismo inyectivo de un espacio vectorial de dimensión finita en sí mismo es un isomorfismo.
- (3) Si  $l \in L$ , entonces  $l = \sum_{i=1}^n e_i b'_i$  para ciertos  $e_i \in E$  y  $b'_i \in B'$ . Cada  $e_i$  es una combinación lineal  $e_i = \sum_{j=1}^{m_i} k_{ij} b_{ij}$ , con  $k_{ij} \in K$  y  $b_{ij} \in B$ . Por tanto

$$l = \sum_{i=1}^{m_i} k_{ij} b_{ij} b'_i$$

lo que muestra que  $A$  es un conjunto generador de  $L_K$ .

Supongamos que  $\sum_{b \in B, b' \in B'} k_{b,b'} bb' = 0$ , con  $k_{b,b'} \in K$  y  $k_{b,b'} = 0$  para casi todo  $(b, b') \in B \times B'$ . Para cada  $b' \in B'$ , ponemos  $e_{b'} = \sum_{b \in B} k_{b,b'} b \in E$ . Como  $k_{b,b'} = 0$  para casi todo  $(b, b') \in B \times B'$ , se tiene que  $e_b = 0$  para casi todo  $b \in B$ . Además,  $\sum_{b' \in B} e_{b'} b' = 0$ . Como  $B'$  es linealmente independiente sobre  $E$ , se tiene que  $e_{b'} = 0$  para todo  $b' \in B'$ . Utilizando que  $B$  es linealmente independiente sobre  $K$  deducimos que  $k_{b,b'} = 0$  para todo  $(b, b') \in B \times B'$ , lo que muestra que  $A$  es linealmente independiente.

(4) y (5) Ejercicio.

Si  $L/K$  es una extensión y  $S$  es un subconjunto de  $L$ , entonces  $K[S]$  denota el menor subanillo de  $L$  que contiene a  $K$  y lo llamamos subanillo de  $L$  generado por  $K$  y  $S$ . El subcuerpo  $K(S)$  descrito en el apartado (5) de la Proposición 1.3 se llama extensión de  $K$  generada por  $S$ . También diremos que  $K(S)$  es el cuerpo que se obtiene adjuntando a  $K$  los elementos de  $S$ . Observando que la intersección de subcuerpos de un cuerpo  $L$  es otro subcuerpo de  $L$ , se tiene que  $K(S)$  es la intersección de todos los subcuerpos de  $L$  que contienen a  $K$  y a  $S$ . Obsérvese que si  $S_1$  y  $S_2$  son dos subconjuntos de  $L$  entonces

$$K(S_1)K(S_2) = K(S_1 \cup S_2).$$

De la misma forma, si  $L_1/K$  y  $L_2/K$  son dos subextensiones de  $L$ , entonces  $L_1L_2$  es la intersección de todos los subcuerpos de  $L$  que contienen a  $L_1 \cup L_2$  y por tanto

$$L_1L_2 = K(L_1 \cup L_2).$$

El concepto de compuesto de dos subextensiones se puede generalizar de forma obvia a una familia arbitraria de subextensiones: Si  $C$  es una familia de subextensiones de  $L/K$  entonces el compuesto de  $C$  es el menor subcuerpo de  $L$  que contiene a todos los elementos de  $C$  y coincide con la intersección de todos los subcuerpos de  $L$  que contienen todos los elementos de  $C$  y con  $K(\cup_{E \in C} E)$ . Si  $C = \{L_1/K, \dots, L_n/K\}$ , entonces el compuesto de  $C$  se denota por  $L_1 \dots L_n$  y está formado por todos los elementos de la forma

$$\frac{\sum_{i=1}^m a_{1i} \dots a_{ni}}{\sum_{i=1}^m b_{1i} \dots b_{ni}}$$

con  $m$  arbitrario,  $a_{ji}, b_{ji} \in L_i$  y  $\sum_{i=1}^m b_{1i} \dots b_{ni} \neq 0$ .

Si  $S = \{a_1, \dots, a_n\}$ , entonces escribimos  $K[S] = K[a_1, \dots, a_n]$  y  $K(S) = K(a_1, \dots, a_n)$ . Decimos que  $L/K$  es una extensión finitamente generada si existen  $a_1, \dots, a_n \in L$  tales que  $L = K(a_1, \dots, a_n)$  y que es simple si  $L = K(a)$  para algún  $a \in L$ . En este último caso decimos que  $a$  es un elemento primitivo de  $L/K$ .

Cuidado: No confundir extensión finita con extensión finitamente generada. ¿Cuál es la diferencia?

# Bibliografía

[Hun03] Thomas Hungerford. Algebra. Springer, 2003.