

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	9

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 α

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

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, $K \subseteq K(X)$ ^a. 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 :

$$P = a_1 X^{-n_1} + a_2 X^{-n_2} + \dots + a_m X^{-n_m}, \quad n_1 \leq \dots \leq n_m$$

entonces,

$$P = 0 \iff X^{n_m} P = 0 \iff a_1 X^{n_m - n_1} + \dots + a_m = 0 \iff \forall i, a_i = 0$$

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

^aTambién 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: Clase de extensiones multiplicativa

Una clase de extensiones $\mathcal{C} = \{L_i/K_i\}_{i \in I}$ se dice multiplicativa si para cada torre $K_1 \subseteq K_2 \subseteq K_3$ se cumple

$$K_3/K_1 \in \mathcal{C} \iff K_3/K_2 \in \mathcal{C} \text{ y } K_2/K_1 \in \mathcal{C}.$$

Más adelante veremos ejemplos interesantes de torres de cuerpos y clases de extensiones multiplicativas.

Definición 1.1.12: 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

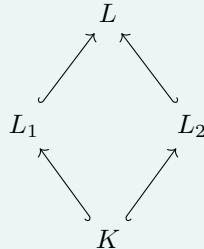
$$\text{Gal}(L/K).$$

Definición 1.1.13: 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 .

Veamos ahora diversas propiedades de los K -homomorfismos.

Proposición 1.1.14: Homomorfismos y grados

Sean L_1 y L_2 extensiones de K . Si existe un K -homomorfismo de cuerpos $\varphi : L_1 \rightarrow L_2$, entonces $[L_1 : K] \leq [L_2 : K]$.

Demostración

Todo homomorfismo de cuerpos es inyectivo. Como φ es K -lineal, es una transformación lineal inyectiva de L_1 a L_2 , considerados como K -espacios vectoriales. Por tanto,

$$\dim_K L_1 \leq \dim_K L_2,$$

es decir, $[L_1 : K] \leq [L_2 : K]$.

Proposición 1.1.15: Endomorfismos de extensiones finitas

Todo endomorfismo K -lineal $\sigma : L \rightarrow L$ de una extensión finita L/K es un automorfismo.

Demostración

σ es un homomorfismo de cuerpos, luego inyectivo. Como L/K es de dimensión finita, toda transformación lineal inyectiva $L \rightarrow L$ es también sobreductiva. Por tanto, σ es biyectivo, es decir, un automorfismo.

Proposición 1.1.16: Transitividad de grados

Sea $K \subseteq E \subseteq L$ una torre de cuerpos y sean B una base de E sobre K y B' una base de L sobre E . Entonces:

- $A = \{bb' : b \in B, b' \in B'\}$ es una base de L sobre K .
- En particular, $[L : K] = [L : E][E : K]$.
- La clase de extensiones finitas es multiplicativa.

Demostración

- Veamos primero que es conjunto generador. Dado $l \in L$, se escribe $l = \sum_i e_i b'_i$ con $e_i \in E$, $b'_i \in B'$. Cada $e_i = \sum_j k_{ij} b_{ij}$ con $k_{ij} \in K$, $b_{ij} \in B$. Luego

$$l = \sum_{i,j} k_{ij} b_{ij} b'_i,$$

combinación de elementos de A .

Para la independencia lineal, supongamos $\sum_{b \in B, b' \in B'} k_{b,b'} bb' = 0$ con $k_{b,b'} \in K$. Fijado b' , sea $e_{b'} = \sum_b k_{b,b'} b \in E$. Entonces $\sum_{b'} e_{b'} b' = 0$. Como B' es linealmente independiente sobre E , $e_{b'} = 0$ para todo b' . Como B es linealmente independiente sobre K , $k_{b,b'} = 0$ para todo b, b' .

- Se tiene $|A| = |B| \cdot |B'|$, luego de (a) deducimos

$$[L : K] = |A| = |B| \cdot |B'| = [E : K] \cdot [L : E].$$

(c) La clase $\mathcal{C} = \{L/K \mid [L : K] < \infty\}$ es multiplicativa: en una torre $K \subseteq E \subseteq L$,

$$L/K \in \mathcal{C} \iff E/K \in \mathcal{C} \text{ y } L/E \in \mathcal{C}$$

esto se sigue inmediatamente de (b).

Proposición 1.1.17: Compuesto de dos extensiones admisibles

Si L_1 y L_2 son extensiones admisibles de K y L es un cuerpo que contiene a L_1 y L_2 como subcuerpos, entonces

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

es el menor subcuerpo de L que contiene a L_1 y L_2 .

Demostración

Denotemos por F al conjunto de la derecha, que claramente está contenido en L . Veamos primero que es un cuerpo.

- Claramente contiene a $0 = \frac{0_{L_1} 0_{L_2}}{1_{L_1} 1_{L_2}}$ y $1 = \frac{1_{L_1} 1_{L_2}}{1_{L_1} 1_{L_2}}$.

- Dados $x, y \in F$, sean

$$x = \frac{\sum_{i=1}^n a_i b_i}{\sum_{i=1}^n a'_i b'_i}, \quad y = \frac{\sum_{j=1}^m c_j d_j}{\sum_{j=1}^m c'_j d'_j}$$

con $a_i, a'_i, c_j, c'_j \in L_1, b_i, b'_i, d_j, d'_j \in L_2$.

- Suma:

$$x + y = \frac{(\sum a_i b_i)(\sum c'_j d'_j) + (\sum c_j d_j)(\sum a'_i b'_i)}{(\sum a'_i b'_i)(\sum c'_j d'_j)}$$

que está en F porque numerador y denominador son sumas de productos ab con $a \in L_1, b \in L_2$.

- Producto:

$$xy = \frac{(\sum a_i b_i)(\sum c_j d_j)}{(\sum a'_i b'_i)(\sum c'_j d'_j)}$$

también de la misma forma.

- Inverso multiplicativo: si $x \neq 0$, entonces $x^{-1} = \frac{\sum a'_i b'_i}{\sum a_i b_i} \in F$.

Veamos ahora que F contiene a L_1 y L_2 :

- Para $a \in L_1$, $a = \frac{a_{1_{L_2}}}{1_{L_1} 1_{L_2}}$.

- Para $b \in L_2$, $b = \frac{1_{L_1} b}{1_{L_1} 1_{L_2}}$.

Finalmente, veamos que F es el menor. Sea F' un subcuerpo de L que contiene L_1 y L_2 . Entonces F' contiene todas las sumas finitas $\sum a_i b_i$ con $a_i \in L_1, b_i \in L_2$, y también sus cocientes. Luego $F \subseteq F'$. Como F es cuerpo que contiene L_1 y L_2 , es el menor.

Proposición 1.1.18: Subanillo y subcuerpo generados

Sean L/K una extensión de cuerpos y $S \subseteq L$. Entonces:

- (a) El menor subanillo de L que contiene a K y a S es

$$K[S] = \{p(s_1, \dots, s_n) \mid n \in \mathbb{N}, p \in K[X_1, \dots, X_n], s_i \in S\}.$$

- (b) El menor subcuerpo de L que contiene a K y a S es

$$K(S) = \left\{ \frac{p(s_1, \dots, s_n)}{q(s_1, \dots, s_n)} \mid n \in \mathbb{N}, p, q \in K[X_1, \dots, X_n], s_i \in S, q(s_1, \dots, s_n) \neq 0 \right\}.$$

Demostración

- (a) Denotemos $R = \{p(s_1, \dots, s_n) \mid \dots\}$.

- Claramente $K \subseteq R$ (polinomios constantes) y $S \subseteq R$ (polinomios X_i).
- R es cerrado bajo suma y producto: dados dos elementos, juntamos los conjuntos finitos de s_i usados y los expresamos como polinomios en esas variables. La suma/producto de polinomios es un polinomio.
- Luego R es un subanillo que contiene K y S .
- Si R' es otro subanillo con $K \cup S \subseteq R'$, entonces R' contiene todos los polinomios en elementos de S , luego $R \subseteq R'$.

Por tanto, $R = K[S]$.

- (b) Sea $F = \{p(s_1, \dots, s_n)/q(s_1, \dots, s_n) \mid \dots\}$.

- F es un subcuerpo: suma, producto e inversos se reducen a operaciones con polinomios.
- Claramente $K \cup S \subseteq F$.
- Si F' es un subcuerpo con $K \cup S \subseteq F'$, entonces F' contiene todos los polinomios $p(s_1, \dots, s_n)$ y sus cocientes, luego $F \subseteq F'$.

Por tanto, $F = K(S)$.

Bibliografía

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