

Cielo
Saga de la Divina Comedia

Universidad de Murcia

Jesús González Abril

24 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	11

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

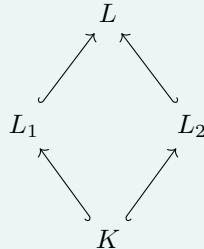
$$\text{Gal}(L/K).$$

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 , lo llamamos compuesto de L_1 y L_2 en L .

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, $F = K(S)$.

Analicemos el contenido de la Proposición 1.1.18. 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 . Por otro lado, el subcuerpo $K(S)$ 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

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

Por otro lado, el concepto de compuesto de dos subextensiones, presentado en la Proposición 1.1.17, 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 $\sum_{i=1}^m b_{1i} \dots b_{ni} \neq 0$.

Un caso importante se presenta cuando el conjunto S es finito. Si $S = \{a_1, \dots, a_n\}$, entonces escribimos $K[S] = K[a_1, \dots, a_n]$ y $K(S) = K(a_1, \dots, a_n)$. La siguiente definición muestra la importancia del caso S finito.

Definición 1.1.19: Extensión finitamente generada y extensión simple

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 .

Observación. Por lo general, una extensión finitamente generada no tiene que ser finita. En el Ejemplo 1.1.9 vimos que $K(X)$ es una extensión de K de grado infinito, pero esta extensión es finitamente generada, de hecho, es simple.

Por otro lado, el lector podrá comprobar fácilmente que toda extensión finita es finitamente generada. Para ello, solo hay que probar que dada una base $B = \{b_1, \dots, b_n\}$ de L_K , entonces $K(b_1, \dots, b_n) = L$.

Recordemos ahora el Ejemplo 1.1.8, en el que vimos que si $n \in \mathbb{Q}$ no es un cuadrado de un número racional, entonces $\mathbb{Q}(\sqrt{n})$ es una extensión de \mathbb{Q} de grado 2. De hecho, notemos que en este caso $\mathbb{Q}[\sqrt{n}] = \mathbb{Q}(\sqrt{n})$, ya que todo elemento de $\mathbb{Q}(\sqrt{n})$ se puede expresar de la forma $a + b\sqrt{n}$ con $a, b \in \mathbb{Q}$.

Demostración

Si consideramos un elemento arbitrario de $\mathbb{Q}(\sqrt{n})$, este es un cociente de polinomios en \sqrt{n} , es decir, un elemento de la forma

$$\frac{p(\sqrt{n})}{q(\sqrt{n})},$$

con $p(X), q(X) \in \mathbb{Q}[X]$ y $q(\sqrt{n}) \neq 0$. Como $\sqrt{n}^2 = n$, en realidad podemos suponer que $p(X)$ y $q(X)$ son polinomios de grado menor o igual que 1, pues todos los términos \sqrt{n}^k con $k \geq 2$ se pueden reducir a términos de grado 0 o 1. Por tanto, todo elemento de $\mathbb{Q}(\sqrt{n})$ se puede escribir como

$$\frac{a + b\sqrt{n}}{c + d\sqrt{n}},$$

con $a, b, c, d \in \mathbb{Q}$ y $c + d\sqrt{n} \neq 0$. Si $d = 0$, entonces $\frac{a+b\sqrt{n}}{c} = \frac{a}{c} + \frac{b}{c}\sqrt{n}$. Si $d \neq 0$, multiplicando numerador y denominador por $c - d\sqrt{n}$ obtenemos

$$\frac{a + b\sqrt{n}}{c + d\sqrt{n}} = \frac{(a + b\sqrt{n})(c - d\sqrt{n})}{c^2 - d^2n} = \frac{ac - bd}{c^2 - d^2n} + \frac{bc - ad}{c^2 - d^2n}\sqrt{n},$$

que también es de la forma $a' + b'\sqrt{n}$ con $a', b' \in \mathbb{Q}$. Por tanto, $\mathbb{Q}(\sqrt{n}) \subseteq \{a + b\sqrt{n} : a, b \in \mathbb{Q}\}$. La inclusión contraria es inmediata.

Notemos que el factor esencial para que funcione la demostración anterior es que $\sqrt{n}^2 = n$, es decir, \sqrt{n} es una raíz del polinomio irreducible $X^2 - n \in \mathbb{Q}[X]$. De hecho, este hecho es general y se recoge en el siguiente lema.

Lema 1.1.20: Propiedades de las raíces de polinomios irreducibles

Sea L/K una extensión. Si $\alpha \in L$ es una raíz de un polinomio irreducible p de grado n en $K[X]$ entonces

- (1) $K[\alpha] = K(\alpha)$
- (2) Si $q \in K[X]$, entonces $q(\alpha) = 0$ si y solo si p divide a q en $K[X]$
- (3) $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ es una base de $K(\alpha)_K$. En particular, $[K(\alpha) : K] = n$

Demostración

- (1) Consideremos el homomorfismo de evaluación en α

$$S : K[X] \rightarrow L, \quad S(q) = q(\alpha)$$

y sea $I = \ker S = \{q \in K[X] : q(\alpha) = 0\}$.

Notemos que I es un ideal propio de $K[X]$: $I \neq (0)$ puesto que $p(\alpha) = 0$ y p es irreducible, por tanto distinto de 0, por otro lado $I \neq K[X]$ pues $1 \notin I$ (ya que $1(\alpha) = 1 \neq 0$).

Como α es raíz de p se tiene $(p) \subseteq I \subset K[X]$. Pero (p) es un ideal maximal de $K[X]$, pues $K[X]$ es un DIP y p es irreducible. Concluimos que $I = (p)$ y, del Primer Teorema de Isomorfía deducimos que $K[\alpha] = \text{Im } S \simeq K[X]/(p)$, que es un cuerpo pues (p) es un ideal maximal de $K[X]$.

Finalmente, recordemos que $K[\alpha]$ es el menor subanillo de L que contiene a K y $\{\alpha\}$, y además hemos visto que es un cuerpo. Por otro lado, cualquier cuerpo que contenga a K y $\{\alpha\}$ es, en concreto, un subanillo que contiene a K y $\{\alpha\}$, y por tanto es mayor que $K[\alpha]$, por lo que este debe ser el menor cuerpo que contiene a K y $\{\alpha\}$. Esto prueba que $K[\alpha] = K(\alpha)$.

- (2) Si $q(\alpha) = 0$, entonces $q \in \ker S = (p)$, luego p divide a q . La implicación contraria es inmediata.
- (3) Si $\beta \in K(\alpha)$, como $K(\alpha) = K[\alpha]$, entonces $b = f(\alpha)$ para algún $f \in K[X]$. Como el grado define una función euclídea en $K[X]$, existen $q, r \in K[X]$ tales que $f = qp + r$ y $m = \text{gr}(r) < \text{gr}(p) = n$. Entonces $\beta = f(\alpha) = r(\alpha) = r_0 + r_1\alpha + r_2\alpha^2 + \dots + r_m\alpha^m$. Esto prueba que $1, \alpha, \dots, \alpha^{n-1}$ genera $K(\alpha)_K$. Para demostrar que son linealmente independientes ponemos $\sum_{i=0}^{n-1} a_i \alpha^i = 0$, con $a_i \in K$. Entonces α es raíz del polinomio $a = \sum_{i=0}^{n-1} a_i X^i$, es decir $a \in \ker S = (p)$. Como $n = \text{gr}(p) > \text{gr}(a)$, deducimos que $a = 0$, es decir $a_i = 0$ para todo i .

Bibliografía

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