

2. EXTENSIONES FINITAS Y ALGEBRAICAS DE CUERPOS

2.1. Extensiones algebraicas.

Si E/K es una extensión de cuerpos, un elemento $\alpha \in E$ se dice **algebraico** sobre K si es raíz de algún polinomio no nulo con coeficientes en K . En otro caso, α se dice **trascendente** sobre K .

Por ejemplo, el número real $\sqrt{2}$ es algebraico sobre \mathbb{Q} , al ser raíz del polinomio $x^2 - 2$, y el número real π es trascendente sobre \mathbb{Q} (TEOREMA DE LINDEMANN-WEIERSTRASS).

Notemos que el concepto de algebraicidad de un elemento de un cuerpo E es relativo al cuerpo base. Por ejemplo, aunque π es trascendente sobre \mathbb{Q} , es algebraico sobre \mathbb{R} al ser raíz de $x - \pi \in \mathbb{R}[x]$.

Una **extensión** E/K se dice **algebraica** si todo elemento de E es algebraico sobre K .

Ejemplo 2.1. La extensión \mathbb{C}/\mathbb{R} es algebraica. Si $z = a + bi \in \mathbb{C}$, donde $a, b \in \mathbb{R}$, entonces z es raíz del polinomio $x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$:

$$z^2 - 2az + (a^2 + b^2) = (a + bi)^2 - 2a(a + bi) + a^2 + b^2 = a^2 + 2abi - b^2 - 2a^2 - 2abi + a^2 + b^2 = 0.$$

Los elementos algebraicos tienen asociado un particular polinomio:

Teorema 2.2. * Sea E/K una extensión y $\alpha \in E$ algebraico sobre K . Sea $f \in K[x]$ un polinomio mónico¹ que tiene a α como raíz.

- (1) Las siguientes propiedades sobre $f \in K[x]$ son equivalentes:
 - (a) f es irreducible;
 - (b) f es un divisor de cualquier polinomio no nulo en $K[x]$ que tenga a α como raíz;
 - (c) f es de grado mínimo entre los polinomios no nulos de $K[x]$ que tienen a α como raíz.
- (2) Existe un único $f \in K[x]$ verificando las condiciones anteriores, que es llamado **el polinomio irreducible de α sobre K** y es denotado por

$$\text{Irr}(\alpha, K).$$

DEMOSTRACIÓN. (1) (a) \Rightarrow (b). Sea $g \in K[x]$ tal que $g(\alpha) = 0$, si ocurriera que $f \nmid g$, sería $\text{mcd}(f, g) = 1$ y tendríamos una igualdad de polinomios en $K[x]$ de la forma $1 = uf + vg$. Evaluando en α , obtendríamos que $1 = u(\alpha)f(\alpha) + v(\alpha)g(\alpha) = 0$, lo que es imposible. Luego ha de ser f un divisor de g .

(b) \Rightarrow (c) es inmediato, pues cualquier múltiplo no nulo de f será de grado mayor o igual al de f .

(c) \Rightarrow (a) Supongamos, por el contrario, que $f = gh$ donde g y h son de grado positivo y, por tanto, estrictamente menor que el de f . Como $0 = f(\alpha) = g(\alpha)h(\alpha)$, ha de ser $g(\alpha) = 0$ o $h(\alpha) = 0$. Pero ninguna de esas posibilidades puede darse en virtud de la hipótesis (c).

(2) *Existencia.* Como α es algebraico, existe al menos un polinomio de grado positivo $g \in K[x]$ tal que $g(\alpha) = 0$. Supongamos que la descomposición en irreducibles mónicos de

¹de coeficiente líder 1, esto es de la forma $x^n + a_{n-1}x^{n-1} + \dots + a_0$.

ese polinomio es $g = af_1^{m_1} \cdots f_r^{m_r}$. Evaluando en α , resulta que $0 = af_1(\alpha)^{m_1} \cdots f_r(\alpha)^{m_r}$, de donde, para algún i , debe ser $f_i(\alpha) = 0$ y el polinomio f_i es el que buscamos.

Unicidad. Es consecuencia inmediata de la propiedad (b). \square

Ejemplo 2.3. El número real $1 + \sqrt[3]{2}$ es algebraico sobre \mathbb{Q} , y

$$\text{Irr}(1 + \sqrt[3]{2}, \mathbb{Q}) = x^3 - 3x^2 + 3x - 3.$$

En efecto, llamemos $\alpha = 1 + \sqrt[3]{2}$. Como $\alpha - 1 = \sqrt[3]{2}$, elevando al cubo obtenemos que $\alpha^3 - 3\alpha^2 + 3\alpha - 1 = 2$, lo que nos asegura que $\alpha = 1 + \sqrt[3]{2}$ es una raíz del polinomio $x^3 - 3x^2 + 3x - 3 \in \mathbb{Q}[x]$, que es mónico e irreducible sobre \mathbb{Q} (por el criterio de Eisenstein para $p = 3$).

Ejemplo 2.4. El número real $\sqrt{5} + \sqrt[4]{5}$ es algebraico sobre \mathbb{Q} y

$$\text{Irr}(\sqrt{5} + \sqrt[4]{5}, \mathbb{Q}) = x^4 - 10x^2 - 20x + 20.$$

En efecto, llamemos $\alpha = \sqrt{5} + \sqrt[4]{5}$. De las sucesivas igualdades siguientes $\alpha - \sqrt{5} = \sqrt[4]{5}$, $\alpha^2 - 2\sqrt{5}\alpha + 5 = \sqrt{5}$, $\alpha^2 + 5 = (1 + 2\alpha)\sqrt{5}$, $\alpha^4 + 10\alpha^2 + 25 = (1 + 4\alpha + 4\alpha^2)5$, $\alpha^4 - 10\alpha^2 - 20\alpha + 20 = 0$, vemos que $\sqrt{5} + \sqrt[4]{5}$ es raíz del polinomio $x^4 - 10x^2 - 20x + 20 \in \mathbb{Q}[x]$, que es mónico e irreducible (por el criterio de Eisenstein para el primo $p = 5$). Luego podemos concluir que $\text{Irr}(\sqrt{5} + \sqrt[4]{5}, \mathbb{Q}) = x^4 - 10x^2 - 20x + 20$.

El polinomio $\text{Irr}(\alpha, K)$ depende tanto de α como de K . Por ejemplo, $\text{Irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ y $\text{Irr}(\sqrt{2}, \mathbb{R}) = x - \sqrt{2}$. Una útil observación general es la siguiente.

Proposición 2.5. Dada una torre $K \leq F \leq E$, si $\alpha \in E$ es algebraico sobre K entonces α es algebraico sobre F y el polinomio $\text{Irr}(\alpha, F)$ es un divisor en $F[x]$ del polinomio $\text{Irr}(\alpha, K)$.

DEMOSTRACIÓN. El polinomio $\text{Irr}(\alpha, K) \in F[x]$ y tiene a α como raíz. Luego α es algebraico sobre F y el polinomio $\text{Irr}(\alpha, K)$ ha de ser un múltiplo del polinomio $\text{Irr}(\alpha, F)$. \square

2.2. Extensiones finitas.

Si E/K es una extensión de cuerpos, E es automáticamente un espacio vectorial sobre el cuerpo K . Esto es, los elementos de E pueden ser vistos como vectores sobre el cuerpo de escalares K , con las operaciones de suma $\alpha + \beta$, para $\alpha, \beta \in E$, y multiplicación por escalares $a\alpha$, para $a \in K$ y $\alpha \in E$, dadas por las propias operaciones de suma y multiplicación en E . Es claro que E con su adición es un grupo abeliano, y las igualdades $a(\beta + \gamma) = a\beta + a\gamma$, $(a + b)\alpha = a\alpha + b\alpha$, $(ab)\alpha = a(b\alpha)$, y $1\alpha = \alpha$ son trivialmente consecuencia de ser E un cuerpo y $K \leq E$ un subcuerpo suyo.

Una extensión E/K se dice **finita**, si E es un K -espacio vectorial finitamente generado. Recordemos que cualquier sistema de generadores finito de un espacio vectorial contiene una base, y que la cardinalidad común a todas ellas es la dimensión del espacio vectorial. Usualmente escribimos

$$[E : K]$$

para indicar la dimensión de E como espacio vectorial sobre K , al que llamamos **grado de la extensión**.

Ejemplo 2.6. $[\mathbb{C} : \mathbb{R}] = 2$, pues $1, i$ claramente forman una base de la extensión.

Proposición 2.7. *Todo extensión finita es algebraica.*

DEMOSTRACIÓN. Sea $[E : K] = n$ y $\alpha \in E$. Los elementos $1, \alpha, \alpha^2, \dots, \alpha^n$ han de ser linealmente dependientes (hay $n + 1$). Entonces existen $a_i \in K$, no todos nulos, tal que $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$. Entonces $f(\alpha) = 0$, donde $0 \neq f = \sum_i a_i x^i \in K[x]$. \square

Proposición 2.8 (Propiedad multiplicativa del grado). * Sea $K \leq F \leq E$ una torre de extensiones de cuerpos

(1) E/K es finita si y solo si E/F y F/K son finitas. En tal caso

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

(2) Si $\{\alpha_1, \dots, \alpha_m\}$ es una base de F/K y $\{\beta_1, \dots, \beta_n\}$ es una base de E/F , entonces $\{\alpha_i\beta_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ es una base de E/K .

DEMOSTRACIÓN. Supongamos primero que E/K es finita. Puesto que $K \leq F \leq E$, F es un K -subespacio vectorial de E , se sigue que F/K es finita. Además, cualquier sistema de generadores de E como K -espacio vectorial genera también a E como F -espacio vectorial, luego E/F también es finita. El resto del teorema se sigue de la demostración de la segunda parte:

Sea cualquier $\beta \in E$. Será $\beta = \sum_j z_j \beta_j$ para ciertos $z_j \in F$. Como cada z_j es expresable en la forma $z_j = \sum_i a_{ij} \alpha_i$ donde los $a_{ij} \in K$, obtenemos que $\beta = \sum_j \sum_i a_{ij} \alpha_i \beta_j$. Esto prueba que el conjunto de los productos $\alpha_i \beta_j$ generan E como K -espacio vectorial K . Para probar que son linealmente independientes, supongamos que $0 = \sum_j \sum_i a_{ij} \alpha_i \beta_j$ con $a_{ij} \in K$. Llamando $z_j = \sum_i a_{ij} \alpha_i$, tenemos que $0 = \sum_j z_j \beta_j$ donde los $z_j \in F$. Por la independencia lineal de los β_j concluimos que $z_j = 0$ para todo j , de donde, por la independencia de los α_i que $a_{ij} = 0$ para todo i y todo j . \square

Una elemental inducción nos demuestra el siguiente

Corolario 2.9. Si $K = E_0 \leq E_1 \leq \dots \leq E_n = E$ es una torre de extensiones de cuerpos, la extensión E/K es finita si y solo si cada peldaño E_i/E_{i-1} es una extensión finita. En tal caso,

$$[E : K] = \prod_{i=1}^n [E_i : E_{i-1}]$$

2.3. Extensiones algebraicas simples.

Sea E/K una extensión de cuerpos. Para cualquier elemento $\alpha \in E$, denotaremos por $K(\alpha)$ al menor subcuerpo de E que contiene a K y a α , y le llamamos el **subcuerpo generado sobre K por α** . Tal cuerpo existe y es único: es la intersección de todos los subcuerpos de E que contienen a K y a α . Si $E = K(\alpha)$, para algún α , la extensión E/K se dice **simple**, y a α un **generador** de la extensión.

Ejemplo 2.10. \mathbb{C}/\mathbb{R} es una extensión simple generada por i , esto es, $\mathbb{C} = \mathbb{R}(i)$. En efecto, puesto que en $\mathbb{R}(i)$ han de estar están todos los números reales y también i , y es un subcuerpo, por tanto cerrado para multiplicación y sumas, se sigue que todo número complejo $a + bi \in \mathbb{R}(i)$.

Ejemplo 2.11. Una extensión simple admite muchos generadores, por ejemplo tenemos las igualdades de subcuerpos de \mathbb{R} : $\mathbb{Q}(\frac{1+\sqrt{2}}{3}) = \mathbb{Q}(1 + \sqrt{2}) = \mathbb{Q}(\sqrt{2})$.

En el siguiente teorema se describe completamente una extensión simple de un cuerpo generada por un elemento algebraico en función del polinomio irreducible del generador.

Teorema 2.12 (* ESTRUCTURA DE LAS EXTENSIONES ALGEBRAICAS SIMPLES). *Sea $E = K(\alpha)$ una extensión simple de un cuerpo K generada por un elemento α algebraico sobre K . Supongamos que $f = \text{Irr}(\alpha, K)$ es de grado n . Entonces,*

- (1) *La extensión E/K es finita (y por tanto algebraica).*
- (2) *$[E : K] = n$.*
- (3) *Los elementos $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$, forman una base de E/K . Por tanto,*

$$E = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_i \in K\},$$

donde la expresión de cada elemento de E de tal forma es única.

- (4) *Todo elemento de E es expresable como $g(\alpha)$, para algún polinomio $g \in K[x]$. Si $g \in K[x]$ es cualquier polinomio tal que $g(\alpha) = \beta$, entonces la expresión de β en función de la base es*

$$\beta = r(\alpha) = \sum_{i=0}^{n-1} c_i \alpha^i,$$

donde $r = \sum_{i=0}^{n-1} c_i x^i$ es el resto de dividir g entre f .

- (5) *Si $g, h \in K[x]$ son polinomios tal que $g(\alpha) = \beta$ y $h(\alpha) = \gamma$, entonces*

$$\begin{cases} \beta + \gamma = (g + h)(\alpha), \\ \beta\gamma = (gh)(\alpha). \end{cases}$$

Además, si $0 \neq \beta = g(\alpha)$, existen polinomios $u, v \in K[x]$ tal que $1 = gu + fv$ y se verifica que

$$\beta^{-1} = u(\alpha).$$

DEMOSTRACIÓN. Sea $F = \{g(\alpha) \mid g \in K[x] \subseteq E$. Observemos que F es un subcuerpo de E : Si $\beta = g(\alpha)$ y $\gamma = h(\alpha)$, para ciertos $g, h \in K[x]$, entonces $\beta + \gamma = g(\alpha) + h(\alpha) = (g + h)(\alpha) \in F$ y $\beta\gamma = g(\alpha)h(\alpha) = (gh)(\alpha) \in F$. Así que F es cerrado para sumas y productos. Claramente contiene a 0 y a 1 (pues $0 = 0(\alpha)$ y $1 = 1(\alpha)$), y es cerrado para opuestos, pues si $\beta = g(\alpha)$, entonces $-\beta = (-g)(\alpha)$. Veamos finalmente que es cerrado para inversos: Supongamos que $0 \neq \beta = g(\alpha)$. Entonces $f \nmid g$ en $K[x]$ y, al ser f irreducible, $1 = \text{mcd}(g, f)$. Por el Teorema de Bezout, existen $u, v \in K[x]$ tal que $1 = gu + fv$, lo que nos asegura que $1 = g(\alpha)u(\alpha) = \beta u(\alpha)$; esto es $\beta^{-1} = u(\alpha) \in F$.

Tenemos pues que $F \leq E$ es un subcuerpo. Además $K \leq F$, pues para todo $a \in K$, $a = a(\alpha)$, y $\alpha \in F$, pues $\alpha = x(\alpha)$; luego $E = K(\alpha) \leq F$. Así que $F = E$.

Observemos ahora que $\{1, \alpha, \dots, \alpha^{n-1}\}$ es una base de E/K : Estos elementos son linealmente independientes, pues en otro caso existirían elementos $b_i \in K$, no todos nulos, tal que $b_{n-1}\alpha^{n-1} + \dots + b_1\alpha + b_0 = 0$. Pero esto indica que α es raíz del polinomio $b_{n-1}x^{n-1} + \dots + b_1x + b_0 \in K[x]$ cuyo grado es menor que el del polinomio irreducible de α sobre K , lo que es imposible. Finalmente vemos que es un sistema de generadores de E como espacio vectorial sobre K : Sea $\beta \in E$. Será $\beta = g(\alpha)$ para algún $g \in K[x]$. Dividiendo g entre f en $K[x]$, si q es el cociente y r el resto, será $g = fq + r$ donde $r = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$, para ciertos $c_i \in K$. Pero entonces

$$\beta = g(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha) = c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1}.$$

Nota. Del teorema anterior se deduce que una extensión simple $K(\alpha)$ generada por un elemento algebraico α , está completamente determinada por el polinomio $f = \text{Irr}(\alpha, K)$, pues conocemos como describir sus diferentes elementos y como estos se suman y se multiplican. Podemos expresar esto con otras palabras: Si $\text{Si} : K[x] \rightarrow K(\alpha)$, $g \mapsto g(\alpha)$, es el homomorfismo de evaluación en α , este es sobreyectivo (por (4)) y su núcleo es precisamente el ideal principal de $K[x]$ de los múltiplos de f . El Primer Teorema de Isomorfía, nos determina un isomorfismo

$$K[x]/f \cong K(\alpha), \quad [g] \mapsto g(\alpha).$$

Ejemplo 2.13. Puesto que $\text{Irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$, se tiene que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, que $\{1, \sqrt{2}\}$ es una base de la extensión $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, y que

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, \ a, b \in \mathbb{Q}\}.$$

Ejemplo 2.14. Puesto que $\text{Irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$, se tiene que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, que $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ es una base, y

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}.$$

Si queremos expresar en función de esta base, por ejemplo, el elemento $(\sqrt[3]{4} - 1)^{-1}$, podemos proceder así: Consideramos el polinomio $x^2 - 1$ (que al evaluar en $\sqrt[3]{2}$ nos da el elemento $\sqrt[3]{4} - 1$ del cual queremos calcular el inverso). Por el algoritmo de Euclides, obtenemos que

$$3 = -(x + 2)(x^3 - 2) + (x^2 - 1)(x^2 + 2x + 1),$$

de donde, evaluando en $\sqrt[3]{2}$, obtenemos

$$3 = (\sqrt[3]{4} - 1)(\sqrt[3]{4} + 2\sqrt[3]{2} + 1).$$

En definitiva,

$$(\sqrt[3]{4} - 1)^{-1} = \frac{1}{3}\sqrt[3]{4} + \frac{2}{3}\sqrt[3]{2} + \frac{1}{3}.$$

Supongamos ahora que queremos expresar en función de la base el número real

$$(1 - \sqrt[3]{2} + \sqrt[3]{4})^3.$$

Podríamos proceder así: Consideramos el polinomio $(1 - x + x^2)^3 = x^6 - 3x^5 + 6x^4 - 7x^3 + 6x^2 - 3x + 1$. Lo dividimos entre $x^3 - 2$ y obtenemos $x^3 - 3x^2 + 6x - 5$ como cociente y $9x - 9$ como resto. Esto es, la igualdad

$$(1 - x + x^2)^3 = (x^3 - 2)(x^3 - 3x^2 + 6x - 5) + 9x - 9,$$

que, evaluando en $\sqrt[3]{2}$ nos dice que

$$(1 - \sqrt[3]{2} + \sqrt[3]{4})^3 = 9\sqrt[3]{2} - 9.$$

Supongamos ahora que queremos expresar en función de la base el número real

$$(1 - \sqrt[3]{2} + \sqrt[3]{4})(\sqrt[3]{2} + \sqrt[3]{4}).$$

Podríamos hacerlo así: Consideramos el polinomio $(1 - x + x^2)(x + x^2) = x^4 + x$; lo dividimos entre $x^3 - 2$ y obtenemos la igualdad $(1 - x + x^2)(x + x^2) = (x^3 - 2)x + 3x$; y si evaluamos en $\sqrt[3]{2}$ obtenemos que

$$(1 - \sqrt[3]{2} + \sqrt[3]{4})(\sqrt[3]{2} + \sqrt[3]{4}) = 3\sqrt[3]{2}.$$

Aunque también podríamos haberlo hecho, en este caso, usando simples propiedades de cálculo con radicales:

$$(1 - \sqrt[3]{2} + \sqrt[3]{4})(\sqrt[3]{2} + \sqrt[3]{4}) = \sqrt[3]{2} - \sqrt[3]{4} + 2 + \sqrt[3]{4} - 2 + 2\sqrt[3]{2} = 3\sqrt[3]{2}.$$

□

2.4. Extensiones algebraicas finitamente generadas.

Sea E/K una extensión de cuerpos. Para cualesquiera elementos $\alpha_1, \dots, \alpha_r \in E$, denotaremos por $K(\alpha_1, \dots, \alpha_r)$ al menor subcuerpo de E que contiene a K y a todos los α_i , $i = 1, \dots, r$, y le llamamos el **subcuerpo generado sobre K por $\alpha_1, \dots, \alpha_r$** . Tal cuerpo existe y es único: es la intersección de todos los subcuerpos de E que contienen a K y a los α_i . Si $E = K(\alpha_1, \dots, \alpha_r)$ para ciertos $\alpha_i \in E$, la extensión E/K se dice **finitamente generada**.

Teorema 2.15. * Para E/K una extensión de cuerpos, son equivalentes

- (1) La extensión es finita.
- (2) La extensión es algebraica y finitamente generada.
- (3) La extensión es finitamente generada por elementos algebraicos.

DEMOSTRACIÓN. (1) \Rightarrow (2): Sabemos que toda extensión finita es algebraica. Además, si $\alpha_1, \dots, \alpha_r$ es una base de E/K , es claro que $E = K(\alpha_1, \dots, \alpha_r)$.

(2) \Rightarrow (3): Es obvio.

(3) \Rightarrow (1): Sea $E = K(\alpha_1, \dots, \alpha_n)$, donde los α_i son algebraicos sobre K . Hagamos inducción en n . Si $n = 1$, el hecho está probado en el teorema anterior. Suponiendo $n > 1$, y bajo hipótesis de inducción, llamemos $F = K(\alpha_1, \dots, \alpha_{n-1})$. Entonces tenemos la torre $K \leq F \leq E$, donde F/K es finita. Además $E = F(\alpha_n)$ donde α_n sabemos por hipótesis que es raíz de un polinomio no nulo con coeficientes en K y por tanto en F ; esto es, α_n es algebraico sobre F . Luego E/F es finita. Por la transitividad de las extensiones finitas, E/K es finita. □

Corolario 2.16. Sea E/K una extensión de cuerpos. Si $\alpha, \beta \in E$ son algebraicos sobre K , entonces $-\alpha$, $\alpha + \beta$, $\alpha\beta$ y, si $\alpha \neq 0$, α^{-1} son todos algebraicos sobre K .

DEMOSTRACIÓN. La subextensión $K(\alpha, \beta)/K$ es finita, luego algebraica. □

En general, manejar extensiones finitamente generadas es algo más complicado que el caso de extensiones simples. Para su tratamiento, lo más útil suele ser el mirar a una tal extensión $E = K(\alpha_1, \dots, \alpha_r)/K$ como el extremo de una torre de extensiones simples

$$K \leq K(\alpha_1) \leq K(\alpha_1, \alpha_2) \leq \dots \leq K(\alpha_1, \dots, \alpha_{r-1}) \leq K(\alpha_1, \dots, \alpha_r) = E$$

y estudiar cada eslabón de la cadena.

Ejemplo 2.17. Consideremos la extensión $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Es finita, pues es finitamente generada por elementos algebraicos. Tenemos una torre de extensiones

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2}, \sqrt{3}),$$

donde cada eslabón es una extensión simple, ya que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$. Hemos visto antes que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ y que $\{1, \sqrt{2}\}$ es una base de esta extensión. Notemos ahora que $\sqrt{3}$ es raíz del polinomio $x^2 - 3 \in \mathbb{Q}[x] \leq \mathbb{Q}(\sqrt{2})[x]$, por tanto el polinomio

$\text{Irr}(\sqrt{3}, \mathbb{Q}(\sqrt{2}))$ es un divisor de $x^2 - 3$, así que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leq 2$. Pero necesariamente ha de ser $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, pues en otro caso sería 1 lo que significaría que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})$, esto es, que $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Pero en tal caso existirían racionales $a, b \in \mathbb{Q}$ de tal manera que $\sqrt{3} = a + b\sqrt{2}$, lo que, elevando al cuadrado, nos llevaría a que $3 = a^2 + 2b^2 + 2ab\sqrt{2}$ y, necesariamente entonces a que $2ab = 0$, $3 = a^2 + 2b^2$. Si $a = 0$, sería $3 = 2b^2$ y b raíz del polinomio $2x^2 - 3$, pero este polinomio es irreducible sobre \mathbb{Q} por el criterio de Eisenstein y no tiene raíces en \mathbb{Q} . Análogamente, si es $b = 0$, sería $3 = a^2$ y a una raíz racional del polinomio $x^2 - 3$, lo que es imposible pues este polinomio es irreducible sobre \mathbb{Q} . Concluimos entonces que $\text{Irr}(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = x^2 - 3$ y, entonces, que una base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ como espacio vectorial sobre $\mathbb{Q}(\sqrt{2})$ es $\{1, \sqrt{3}\}$. En definitiva, tenemos que $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ es una base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ como espacio vectorial racional. En conclusión, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ y

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, a, b, c, d \in \mathbb{Q}\}.$$

La siguiente observación es de mucha utilidad práctica.

Proposición 2.18. *Sea $K \leq F \leq E$ una torre de extensiones, donde F/K es finita, y $\alpha \in E$ un elemento algebraico sobre K tal que el grado del polinomio $\text{Irr}(\alpha, K)$ es primo relativo con el grado $[F : K]$. Entonces, $\text{Irr}(\alpha, K) = \text{Irr}(\alpha, F)$.*

DEMOSTRACIÓN. Supongamos que $[F : K] = m$ y que $\text{Irr}(\alpha, K)$ es de grado n . Es claro que $\text{Irr}(\alpha, F)$ es un divisor en $F[x]$ del polinomio $\text{Irr}(\alpha, K)$ y, en particular, de grado menor o igual. Se trata de ver que son del mismo grado y, por tanto, el mismo polinomio. Consideremos la torre $K \leq F \leq F(\alpha)$. Puesto que $[F(\alpha) : F] = \text{gr}(\text{Irr}(\alpha, F)) \leq n$, tendremos que

$$[F(\alpha) : K] = [F : K] \cdot [F(\alpha) : F] = m \cdot \text{gr}(\text{Irr}(\alpha, F)) \leq m \cdot n.$$

De manera que el número $[F(\alpha) : K]$ ha de ser un múltiplo de m y $\leq mn$. Por otra parte, Considerando la torre $K \leq K(\alpha) \leq F(\alpha)$, vemos que $[F(\alpha) : K] = [K(\alpha) : K] \cdot [F(\alpha) : K(\alpha)] = n \cdot [F(\alpha) : K(\alpha)]$ es también un múltiplo de n . Pero entonces resulta que $[F(\alpha) : K]$ es múltiplo del $\text{mcm}(m, n) = mn$ y menor o igual que mn . Necesariamente es $[F(\alpha) : K] = mn$ y entonces $\text{gr}(\text{Irr}(\alpha, F)) = n$.

Ejemplo 2.19. Consideremos la extensión $\mathbb{Q}(\sqrt[3]{5}, \sqrt{2})/\mathbb{Q}$. Tenemos la torre la torre $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{5}) \leq \mathbb{Q}(\sqrt[3]{5}, \sqrt{2})$. La primera extensión es simple con $\text{Irr}(\sqrt[3]{5}, \mathbb{Q}) = x^3 - 5$, de manera que es de grado 3 y $\{1, \sqrt[3]{5}, \sqrt[3]{25}\}$ es una base. Puesto que $\text{Irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ y $\text{mcd}(2, 3) = 1$, por la proposición anterior, conocemos que también $\text{Irr}(\sqrt{2}, \mathbb{Q}(\sqrt[3]{5})) = x^2 - 2$ y la segunda extensión es de grado 2 con $\{1, \sqrt{2}\}$ una base de la misma. Entonces, la extensión $\mathbb{Q}(\sqrt[3]{5}, \sqrt{2})/\mathbb{Q}$ es de grado 6, con base

$$\{1, \sqrt[3]{5}, \sqrt[3]{25}, \sqrt{2}, \sqrt[3]{5}\sqrt{2}, \sqrt[3]{25}\sqrt{2}\}.$$

Queremos ahora expresar en función de ella el elemento $(\sqrt[3]{5} + \sqrt{2})^{-1}$. Para ello, vamos a utilizar de nuevo la torre $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{5}) \leq \mathbb{Q}(\sqrt[3]{5}, \sqrt{2})$ y, en primera instancia expresaremos $(\sqrt[3]{5} + \sqrt{2})^{-1}$ como combinación lineal de $\{1, \sqrt{2}\}$ con coeficientes en $\mathbb{Q}(\sqrt[3]{5})$ y, después expresaremos cada coeficiente de esa combinación en la base $\{1, \sqrt[3]{5}, \sqrt[3]{25}\}$ de la extensión $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$:

Para la primera cuestión, consideramos el polinomio $x + \sqrt[3]{5}$ (que al ser evaluado en $\sqrt{2}$ nos da el número del cual queremos calcular el inverso). Aplicamos entonces el algoritmo extendido de Euclides a los polinomios $x^2 - 2$ y $x + \sqrt[3]{5}$, obteniendo la igualdad

$$\sqrt[3]{25} - 2 = (x^2 - 2) + (x + \sqrt[3]{5})(\sqrt[3]{5} - x),$$

de donde, por evaluación en $\sqrt{2}$, deducimos que $\sqrt[3]{25} - 2 = (\sqrt{2} + \sqrt[3]{5})(\sqrt[3]{5} - \sqrt{2})$. Así que

$$(\sqrt[3]{5} + \sqrt{2})^{-1} = (\sqrt[3]{25} - 2)^{-1}(\sqrt[3]{5} - \sqrt{2}).$$

Calculamos ahora el inverso de $\sqrt[3]{25} - 2$ en $\mathbb{Q}(\sqrt[3]{5})$ en su base natural $\{1, \sqrt[3]{5}, \sqrt[3]{25}\}$. Para ello, consideramos el polinomio $x^2 - 2$ y, utilizando de nuevo el algoritmo extendido de Euclides, obtenemos que

$$\frac{17}{4} = -\left(\frac{1}{2}x + \frac{5}{4}\right)(x^2 - 2) + \left(\frac{1}{2}x^2 + \frac{5}{4}x + 1\right)(x^2 - 2).$$

Evaluando en $\sqrt[3]{5}$, obtenemos que

$$\frac{17}{4} = \left(\frac{1}{2}\sqrt[3]{25} + \frac{5}{4}\sqrt[3]{5} + 1\right)(\sqrt[3]{25} - 2),$$

de donde

$$(\sqrt[3]{25} - 2)^{-1} = \frac{2}{17}\sqrt[3]{25} + \frac{5}{17}\sqrt[3]{5} + \frac{4}{17}.$$

En conclusión,

$$\begin{aligned} (\sqrt[3]{5} + \sqrt{2})^{-1} &= (\sqrt[3]{5} - \sqrt{2}) \left(\frac{2}{17}\sqrt[3]{25} + \frac{5}{17}\sqrt[3]{5} + \frac{4}{17} \right) \\ &= \frac{10}{17} + \frac{4}{17}\sqrt[3]{5} + \frac{5}{17}\sqrt[3]{25} - \frac{4}{17}\sqrt{2} - \frac{5}{17}\sqrt[3]{5}\sqrt{2} - \frac{2}{17}\sqrt[3]{25}\sqrt{2}. \end{aligned}$$

□

Las siguientes observaciones nos serán de utilidad en el siguiente capítulo.

Lema 2.20. Sea $E = K(\alpha_1, \dots, \alpha_n)$ una extensión finita generada por elementos algebraicos $\alpha_1, \dots, \alpha_n$. Si dos homomorfismos de cuerpos $\sigma, \sigma' : E \rightarrow F$ son tales que $\sigma|_K = \sigma'|_K$ y $\sigma(\alpha_i) = \sigma'(\alpha_i)$ para $i = 1, \dots, n$, entonces $\sigma = \sigma'$.

DEMOSTRACIÓN. Procedemos por inducción en r . Supongamos primero que $r = 1$, esto es, que $E = K(\alpha)$ una extensión simple generada por un elemento algebraico α . Si r es el grado del polinomio $\text{Irr}(\alpha, K)$, cada elemento $\beta \in E$ se expresa de la forma $\beta = \sum_{i=0}^{r-1} a_i \alpha^i$, donde $a_i \in K$. Tenemos entonces que

$$\sigma(\beta) = \sum_i \sigma(a_i) \sigma(\alpha)^i = \sum_i \sigma'(a_i) \sigma'(\alpha)^i = \sigma'(\beta)$$

y $\sigma = \sigma'$. Supongamos ahora que $n > 1$. Sea $F = K(\alpha_1, \dots, \alpha_{r-1})$. Por hipótesis de inducción será $\sigma|_F = \sigma'|_F$. Como $E = F(\alpha_r)$, la conclusión $\sigma = \sigma'$ sigue por el caso $n = 1$ antes visto. □

Lema 2.21. Sea $E = K(\alpha_1, \dots, \alpha_n)$ una extensión finita generada por elementos algebraicos $\alpha_1, \dots, \alpha_n$. Si $\sigma : E \rightarrow F$ es un homomorfismo de cuerpos, entonces

$$\sigma(E) = \sigma(K)(\sigma(\alpha_1), \dots, \sigma(\alpha_n)).$$

DEMOSTRACIÓN. Hacemos inducción sobre el número de generadores de la extensión. Supongamos $n = 1$, o sea $E = K(\alpha)$ una extensión simple algebraica. El cuerpo $\sigma(E)$ contiene a $\sigma(K)$ y a $\sigma(\alpha)$ y por tanto al cuerpo $\sigma(K)(\sigma(\alpha))$. Para la inclusión recíproca, supongamos que $\text{Irr}(\alpha, K)$ es de grado r . Sabemos entonces que $\{1, \alpha, \dots, \alpha^{r-1}\}$ es una base de E como espacio vectorial sobre K , por tanto cualquier elemento β de este cuerpo es expresable de la forma $\beta = \sum a_i \alpha^i$, con los $a_i \in K$. Pero entonces $\sigma(\beta) = \sigma(\sum a_i \alpha^i) = \sum \sigma(a_i) \sigma(\alpha)^i \in \sigma(K)(\sigma(\alpha))$. El resto de la demostración se sigue entonces por inducción:

$$\begin{aligned} \sigma(E) &= \sigma(K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n)) = \sigma(K(\alpha_1, \dots, \alpha_{n-1}))(\sigma(\alpha_n)) \\ &= \sigma(K)(\sigma(\alpha_1), \dots, \sigma(\alpha_{n-1}))(\sigma(\alpha_n)) = \sigma(K)(\sigma(\alpha_1), \dots, \sigma(\alpha_n)). \end{aligned}$$

□