Cielo
Saga de la Divina Comedia

Universidad de Murcia

Jesús González Abril

4 de febrero 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
1.2. Adjunción de raíces . . . 12
1.3. Extensiones algebraicas . . . 17
1.3.1. Polinomio mínimo . . . 18
1.3.2. Ejemplos de polinomios mínimos . . . 19
1.3.3. Caracterización de extensiones algebraicas . . . 19

2. Cuerpos algebraicamente cerrados y extensiones normales **23**
2.1. Cuerpos algebraicamente cerrados . . . 23
2.2. Clausura algebraica . . . 27

A. Polinomios **30**
A.1. Anillos de polinomios . . . 30
A.2. Propiedades de anillos de polinomios . . . 30
A.3. Divisibilidad en anillos de polinomios . . . 31
A.4. Polinomios sobre $\mathbb{Q}$ . . . 32

Bibliografía **34**

Capítulo 1

Extensiones de cuerpos

1.1. Extensiones de cuerpos

Definición 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 está 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 1.2: 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 1.3: 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

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

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 algebra lineal,

$$L_K \simeq K^n.$$

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

Proposición 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 1.5

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 1.6

Como hemos visto en el Ejemplo 1.3, $\mathbb{C}/\mathbb{R}$ es una extensión finita de grado 2.

Ejemplo 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 1.4, $\mathbb{R}$ 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 1.8

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 1.9

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:

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

entonces,

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

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

[a] 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 1.10: Torre de extensiones de cuerpos

Una torre de extensiones de cuerpos es una sucesión

$$K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n$$

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

Definición 1.11: 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

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

Ejemplo 1.12

Consideremos la torre de cuerpos $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. La extensión $\mathbb{C}/\mathbb{Q}$ es de grado infinito, y las extensiones $\mathbb{R}/\mathbb{Q}$ y $\mathbb{C}/\mathbb{R}$ también lo son. Consideremos la clase de extensiones $\mathcal{C} = \{\mathbb{R}/\mathbb{Q}, \mathbb{C}/\mathbb{R}, \mathbb{C}/\mathbb{Q}\}$, como solo hay una torre $K_1 \subseteq K_2 \subseteq K_3$ con $K_1 = \mathbb{Q}$, $K_2 = \mathbb{R}$, $K_3 = \mathbb{C}$, se cumple trivialmente que la clase $\mathcal{C}$ es multiplicativa.

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

Definición 1.13: 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 $f : L_1 \to L_2$ 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

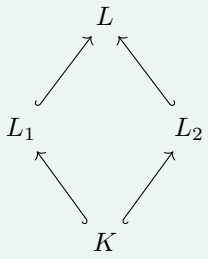
$$\mathrm{Gal}(L/K).$$

Definición 1.14: 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 $f : K \to L$ 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 $f : K \to L$, 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 $f : K \to L$, 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 1.15: Homomorfismos y grados

Sean L_1 y L_2 extensiones de K. Si existe un K-homomorfismo de cuerpos $\varphi : L_1 \to L_2$, 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 1.16: Endomorfismos de extensiones finitas

Todo endomorfismo K-lineal $\sigma : L \to L$ 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 $L \to L$ es también sobreyectiva. Por tanto, σ es biyectivo, es decir, un automorfismo.

Proposición 1.17: 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) $A = \{bb' : b \in B, b' \in B'\}$ es una base de L sobre K.

(b) En particular, $[L : K] = [L : E][E : K]$.

(c) La clase de extensiones finitas es multiplicativa.

Demostración

(a) 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'.

(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 1.18: 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

$$L_1L_2 = \left\{ \frac{a_1b_1 + \cdots + a_nb_n}{a_1'b_1' + \cdots + a_n'b_n'} : a_i, a_i' \in L_1, b_i, b_i' \in L_2, \sum a_i'b_i' \neq 0 \right\}$$

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
$$x = \frac{\sum_{i=1}^n a_ib_i}{\sum_{i=1}^n a_i'b_i'}, \quad y = \frac{\sum_{j=1}^m c_jd_j}{\sum_{j=1}^m c_j'd_j'}$$
con $a_i, a_i', c_j, c_j' \in L_1$, $b_i, b_i', d_j, d_j' \in L_2$.
- Suma:
$$x + y = \frac{(\sum a_ib_i)(\sum c_j'd_j') + (\sum c_jd_j)(\sum a_i'b_i')}{(\sum a_i'b_i')(\sum c_j'd_j')}$$
que está en F porque numerador y denominador son sumas de productos ab con $a \in L_1, b \in L_2$.
- Producto:
$$xy = \frac{(\sum a_ib_i)(\sum c_jd_j)}{(\sum a_i'b_i')(\sum c_j'd_j')}$$
también de la misma forma.
- Inverso multiplicativo: si $x \neq 0$, entonces $x^{-1} = \frac{\sum a_i'b_i'}{\sum a_ib_i} \in F$.

Veamos ahora que F contiene a L_1 y L_2:

- Para $a \in L_1$, $a = \frac{a1_{L_2}}{1_{L_1}1_{L_2}}$.
- 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 $\sum a_ib_i$ con $a_i \in L_1, b_i \in L_2$, y también sus cocientes. Luego $F \subseteq F'$.

Proposición 1.19: 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

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

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

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

Demostración

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

- Claramente $K \subseteq R$ (polinomios constantes) y $S \subseteq R$ (polinomios X_i).
- R es cerrado bajo suma y producto: dados dos elementos x, y

$$x = p(s_1, \ldots, s_n), y = q(s'_1, \ldots s'_m)$$

juntamos los s_i, s'_j usados y podemos ver x, y como polinomios en $n + m$ variables, donde las variables son $\{s_1, \ldots, s_n, s'_1, \ldots, s'_m\}$. Como la suma y el producto de polinomios en esas $n + m$ variables da polinomios del mismo tipo, R es cerrado bajo suma y producto.

- R contiene al 1 de L puesto que este es el mismo 1 de K, que es un polinomio constante.

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 las sumas y productos de elementos de S y K, es decir, todos los polinomios en elementos de S, luego $R \subseteq R'$, por tanto, $R = K[S]$.

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

- F es un subcuerpo: suma, producto e inversos se reducen a operaciones con polinomios en las variables $s_i \in S$, igual que en el apartado anterior. Hacemos solo el caso de los inversos, dado $x \in F \setminus \{0\}$

$$x = \frac{p(s_1, \ldots, s_n)}{q(s_1, \ldots, s_n)}, \quad p(s_1, \ldots, s_n) \neq 0$$

de donde vemos que $x^{-1} = \frac{q(s_1, \ldots, s_n)}{p(s_1, \ldots, s_n)} \in F$.

- $K \cup S \subseteq F$ por el mismo razonamiento del caso anterior tomando como cociente el polinomio constantemente igual a la unidad.
- Si F' es un subcuerpo con $K \cup S \subseteq F'$, entonces F' contiene todos los polinomios $p(s_1, \ldots, s_n)$ y sus cocientes, luego $F \subseteq F'$.

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

Analicemos el contenido de la Proposición 1.19. 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. Notemos que aunque S no tenga ninguna estructura, siempre es posible tomar el producto de elementos de S y elementos de K, así como inversos, puesto que todos los elementos con los que

se trata se encuentran dentro del cuerpo L.

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

$$K(S) = \bigcap_{\substack{K \cup S \subseteq E \\ E \leq L}} E.$$

Obsérvese que si S_1 y S_2 son dos subconjuntos de L entonces

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

Demostración

En primer lugar, $K(S_1)K(S_2)$ es un cuerpo que contiene a K, S_1, S_2, por lo que $K(S_1 \cup S_2) \subseteq K(S_1)K(S_2)$.
Para la otra inclusión basta notar que $K(S_1)K(S_2)$ es el menor cuerpo que contiene a $K(S_1)$ y $K(S_2)$, y ambos están contenidos en $K(S_1 \cup S_2)$,

$$K(S_1) \subseteq K(S_1 \cup S_2), \quad K(S_2) \subseteq K(S_1 \cup S_2),$$

luego $K(S_1 \cup S_2) \subseteq K(S_1)K(S_2)$.

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 1.18, 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 $C = \{L_1/K, \ldots, L_n/K\}$, entonces el compuesto de C se denota por $L_1 \ldots L_n$ y está formado por todos los elementos de la forma

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

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

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

Definición 1.20: Extensión finitamente generada y extensión simple

Decimos que L/K es una extensión finitamente generada si existen $a_1, \ldots, a_n \in L$ tales que $L = K(a_1, \ldots, a_n)$ 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 1.9 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 $B = \{b_1, \ldots, b_n\}$ de L_K, entonces $K(b_1, \ldots, b_n) = L$.

Ejemplo 1.21

Sea $K(a_1, \ldots, a_n)$ es una extensión finitamente generada, entonces $K(a_1, \ldots, a_n) = K(a_1)(a_2)\ldots(a_n)$, es decir, se puede construir la extensión adjuntando un elemento cada vez. La demostración es inmediata por inducción en n. El único caso importante es el caso $n = 2$, que se sigue de la definición de cuerpo generado.

Demostración

Claramente $K, \{a_1, a_2\} \subseteq K(a_1)(a_2)$, por lo que $K(a_1, a_2) \subseteq K(a_1)(a_2)$. Por otro lado, $K(a_1) \subseteq K(a_1, a_2)$ ya que $K, \{a_1\} \subseteq K(a_1, a_2)$, y $a_2 \in K(a_1, a_2)$, por lo tanto $K(a_1)(a_2) \subseteq K(a_1, a_2)$.

Recordemos ahora el Ejemplo 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

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

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 se cumpla $\mathbb{Q}[\sqrt{n}] = \mathbb{Q}(\sqrt{n})$ es que $\sqrt{n}^2 = n$, es decir, $\sqrt{n}$ es una raíz del polinomio irreducible $X^2 - n \in \mathbb{Q}[X]$. No solo eso, además vemos que el orden de la extensión $\mathbb{Q}(\sqrt{n})/\mathbb{Q}$ es 2, lo que coincide con el grado del polinomio irreducible. De hecho, este hecho es general y se recoge en el siguiente lema.

Lema 1.22: 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) $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ es una base de $K(\alpha)_K$. En particular, $[K(\alpha) : K] = n$

Demostración

(1) Consideremos el homomorfismo de evaluación en α

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

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 $K[\alpha] = \operatorname{Im} S \simeq K[X]/(p)$, 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 $m = \operatorname{gr}(r) < \operatorname{gr}(p) = n$. Entonces $\beta = f(\alpha) = r(\alpha) = r_0 + r_1\alpha + r_2\alpha^2 \cdots + r_m\alpha^m$. Esto prueba que $1, \alpha, \ldots, \alpha^{n-1}$ 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 $a = \sum_{i=0}^{n-1} a_iX^i$, es decir $a \in \ker S = (p)$. Como $n = \operatorname{gr}(p) > \operatorname{gr}(a)$, deducimos que $a = 0$, es decir $a_i = 0$ para todo i.

1.2. Adjunción de raíces

Una de las maneras más "sensatas" de extender los números reales es buscar un cuerpo en el que el polinomio X^2+1 tenga raíces, de esta forma llegamos a los números complejos. El siguiente teorema muestra que todos los polinomios no constantes tienen alguna raíz en algún cuerpo.

Teorema 1.23: Teorema de Kronecker

Si K es un cuerpo y $p \in K[X] \setminus K$, entonces existe una extensión L de K que contiene una raíz de p.

Demostración

Como p es un elemento no nulo ni invertible de $K[X]$ y este es un DFU, p es divisible en $K[X]$ por un polinomio irreducible y todas las raíces de este divisor son raíces de p. Por tanto podemos suponer que p es irreducible. Eso implica que (p) es un ideal maximal de $K[X]$, pues este último es un DIP.
Entonces $L = K[X]/(p)$ es un cuerpo. La composición de la inclusión $\iota : K \to K[X]$ y la proyección $\pi : K[X] \to L = K[X]/(p)$ es un homomorfismo de cuerpos, al que llamaremos $f : K \to L$. Para ver que es homomorfismo de cuerpos basta notar que

$$f(1_K) = \pi(1_K[X]) = 1_{K[X]} + (p) = 1_L,$$

$$f(a+b) = \pi(a+b) = (a+b) + (p) = (a+(p)) + (b+(p)) = f(a) + f(b),$$
$$f(ab) = \pi(ab) = (ab) + (p) = (a+(p))(b+(p)) = f(a)f(b).$$

Por tanto, podemos considerar L como una extensión de K.
Para acabar la demostración basta ver que $a = X + (p)$ es una raíz de p (teniendo en cuenta que no vamos a evaluar p en un elemento de K como haríamos usualmente, sino en un elemento de L, que es un anillo cociente). En efecto, si ponemos $p = \sum_{i=0}^{n} a_i X^i$, entonces

$$p(a) = p(X + (p)) = \sum_{i=0}^{n} a_i (X + (p))^i = p + (p) = (p)$$

que es el cero del anillo L.

Por tanto, si $p \in K[X]$ es un polinomio no constante, entonces existe una extensión L/K que contiene una raíz α de p y $K(\alpha)$ es la menor subextensión de L/K que contiene a α.

Definición 1.24: Polinomio completamente factorizable y raíces

Decimos que un polinomio $p \in K[X] \setminus K$ es completamente factorizable sobre K si es producto de polinomios de grado 1, o lo que es lo mismo si $p = a(X - \alpha_1) \dots (X - \alpha_n)$ para ciertos $a, \alpha_1, \dots, \alpha_n \in K$. En tal caso las raíces de p son $\alpha_1, \dots, \alpha_n$.

Ejemplo 1.25

Un polinomio puede ser completamente factorizable sobre un cuerpo pero no sobre otro. Por ejemplo,

$$X^3 - 1 = (X-1)(X^2 + X + 1) = (X-1)\left(X - \frac{-1+\sqrt{-3}}{2}\right)\left(X - \frac{-1-\sqrt{-3}}{2}\right)$$

es completamente factorizable sobre $\mathbb{C}$, pero no sobre $\mathbb{Q}$ ni $\mathbb{R}$.

El Teorema de Kronecker afirma que cada polinomio no constante tiene una raíz en alguna extensión. De hecho podemos decir algo más.

Corolario 1.26: Factorización completa en alguna extensión

Si K es un cuerpo y $p \in K[X] \setminus K$, entonces p es completamente factorizable en alguna extensión de K.

Demostración

Lo demostraremos por inducción sobre el grado de p. Si el grado de p es 1, no hay nada que demostrar.
Supongamos que el resultado se cumple para polinomios de grado $n-1$. Si el grado de p es n entonces p tiene una raíz α en alguna extensión E de K. Entonces $p = (X-\alpha)q$ para algún $q \in E[X] \setminus E$. Por hipótesis de inducción, q es completamente factorizable en alguna extensión L de E, es decir, q es producto de polinomios de $L[X]$ de grado menor o igual que 1. Por tanto, también p es producto de polinomios de $L[X]$ de grado menor o igual que 1.

Nuestro objetivo principal es establecer un criterio para determinar cuándo un polinomio es resoluble por radicales. Como se detalla en las siguientes definiciones, un polinomio es resoluble por radicales precisamente cuando sus raíces se pueden expresar en sucesivas extensiones en las que en cada paso se adjunta una raíz n-ésima de elementos del cuerpo anterior.

Definición 1.27: Torre radical y extensión radical

Una torre radical es una torre de cuerpos

$$E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n$$

tales que para cada $i = 1, \ldots, n$, existen $n_i \geq 1$ y $\alpha_i \in E_i$ tal que $E_i = E_{i-1}(\alpha_i)$ y $\alpha_i^{n_i} \in E_{i-1}$.
Una extensión de cuerpos L/K se dice que es radical si existe una torre radical

$$K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = L.$$

Definición 1.28: Ecuación resoluble por radicales

Una ecuación polinómica $P(X) = 0$, con $P \in K[X]$, se dice que es resoluble por radicales sobre K si existe una extensión radical L/K tal que P es completamente factorizable en L. En tal caso también se dice que el polinomio P es resoluble por radicales sobre K.

O sea, si suponemos que $P \in K[X]$ entonces P es resoluble por radicales sobre K si K tiene una extensión radical que contiene todas las raíces de P y queremos descubrir cuándo pasa eso. Para llegar a ello tenemos que recorrer un largo camino que se completará en los dos últimos capítulos.

Recordemos que si $\sigma : K \to E$ es un homomorfismo de anillos, entonces σ tiene una única extensión a un homomorfismo entre los anillos de polinomios, que seguiremos denotando por $\sigma : K[X] \to E[X]$ tal que $\sigma(X) = X$. Este homomorfismo se comporta bien sobre las raíces, como recoge el siguiente lema.

Lema 1.29: Comportamiento de homomorfismos con raíces

Sean $\sigma : E \to L$ un homomorfismo de cuerpos y $p \in E[X]$.

1. Si α es una raíz de p en E entonces $\sigma(\alpha)$ es una raíz de $\sigma(p)$.
2. Si E/K y L/K son extensiones de un cuerpo K, $p \in K[X]$ y $\sigma : E \to L$ es un K-homomorfismo entonces σ se restringe a una aplicación inyectiva del conjunto de las raíces de p en E al conjunto de las raíces de p en L.
3. En particular, si $E = L$ (es decir, si $\sigma \in \mathrm{Gal}(L/K)$), entonces esta restricción de σ es una permutación del conjunto de las raíces de p en L.

Demostración

1. Supongamos que $p = p_0 + p_1X + \cdots + p_nX^n$, entonces $\sigma(p) = \sigma(p_0) + \sigma(p_1)X + \cdots + \sigma(p_n)X^n$. Si α es una raíz de p, entonces

$$\begin{aligned}\sigma(p)(\sigma(\alpha)) &= (\sigma(p_0) + \sigma(p_1)X + \sigma(p_1)X^2 + \cdots + \sigma(p_n)X^n)(\sigma(\alpha)) \\ &= \sigma(p_0) + \sigma(p_1)\sigma(\alpha) + \sigma(p_1)\sigma(\alpha)^2 + \cdots + \sigma(p_n)\sigma(\alpha)^n \\ &= \sigma(p_0 + p_1\alpha + p_1\alpha^2 + \cdots + p_n\alpha^n) \\ &= \sigma(p(\alpha)) = \sigma(0) = 0.\end{aligned}$$

   Esto prueba la primera afirmación.

2. Sean R_E, R_L los conjuntos de raíces de p en E y L respectivamente. Si $\alpha \in R_E$, entonces por la primera parte $\sigma(\alpha) \in R_L$, luego σ restringido a R_E es una aplicación de R_E en R_L. Para la inyectividad, basta notar que $R_E \subseteq E, R_L \subseteq L$ y que σ es inyectiva como homomorfismo de E a L por ser un homomorfismo de cuerpos.
3. Si $E = L$, entonces la aplicación de la parte 2 es una aplicación de R_L en sí mismo. Como σ es inyectiva, esta aplicación también lo es, y como R_L es un conjunto finito (de tamaño a lo sumo $\mathrm{gr}(p)$), la aplicación es sobreyectiva, luego es una permutación de R_L.

Lema 1.30: Lema de Extensión

Sea $\sigma : K_1 \to K_2$ un homomorfismo de cuerpos y sea $p \in K_1[X]$ un polinomio irreducible. Sean L_1/K_1 y L_2/K_2 dos extensiones de cuerpos y sean $\alpha_1 \in L_1$ y $\alpha_2 \in L_2$ con α_1 una raíz de p.
Entonces existe un homomorfismo $\hat{\sigma} : K_1(\alpha_1) \to K_2(\alpha_2)$ tal que $\hat{\sigma}|_{K_1} = \sigma$ y $\hat{\sigma}(\alpha_1) = \alpha_2$ si y solo si α_2 es una raíz del polinomio $\sigma(p)$. En tal caso sólo hay un homomorfismo $\hat{\sigma}$ que satisfaga la condición indicada y si además, σ es un isomorfismo, entonces también $\hat{\sigma}$ es un isomorfismo.

$$\begin{array}{ccc} K_1 & \xrightarrow{\sigma} & K_2 \\ \downarrow & & \downarrow \\ K_1(\alpha_1) & \xrightarrow{\hat{\sigma}} & K_2(\alpha_2) \end{array}$$

Demostración

Si existe el homomorfismo $\hat{\sigma}$ satisfaciendo la propiedad indicada entonces del Lema 1.29 se tiene que $\alpha_2 = \hat{\sigma}(\alpha_1)$ es una raíz de $\hat{\sigma}(p) = \sigma(p)$.
Recíprocamente, supongamos que α_2 es una raíz de $\sigma(p)$. Consideremos los homomorfismos de sustitución en α_1 y α_2: $S_{\alpha_1} : K_1[X] \to K_1(\alpha_1)$ y $S_{\alpha_2} : K_2[X] \to K_2(\alpha_2)$. Por el Lema 1.22, $K_1[\alpha_1] = K_1(\alpha_1)$, $[K(\alpha_1) : K] = \mathrm{gr}(p)$ y $(p) = \ker S_{\alpha_1}$. Además, por el Lema 1.29, $\sigma(p) \in \ker S_{\alpha_2}$.
Todo esto implica que la aplicación $\hat{\sigma} : K_1(\alpha_1) \to K_2(\alpha_2)$, dada por $\hat{\sigma}(f(\alpha_1)) = \sigma(f)(\alpha_2)$, para $f \in K_1[X]$, está bien definida pues si $f(\alpha_1) = g(\alpha_1)$, con $f, g \in K_1[X]$, entonces $f - g \in \ker S_{\alpha_1}$, con lo que p divide a $f - g$ en $K_1[X]$ ya que $\ker S_{\alpha_1} = (p)$. Esto quiere decir que existen $q \in K_1[X]$ tal que $f - g = qp$. Aplicando σ obtenemos

$$\sigma(f) - \sigma(g) = \sigma(q)\sigma(p).$$

Luego $\sigma(p)$ divide a $\sigma(f) - \sigma(g)$ en $K_2[X]$ y por tanto $\sigma(f) - \sigma(g) \in \ker S_{\alpha_2}$, es decir $\sigma(f)(\alpha_2) = \sigma(g)(\alpha_2)$. Una vez que hemos visto que $\hat{\sigma}$ está bien definida, es fácil ver que es un homomorfismo de cuerpos (queda como ejercicio) y que satisface las condiciones del Lema: si $k \in K_1$ entonces $k = f(\alpha_1)$ con $f(X) = k$, luego $\sigma(f) = \sigma(k)$ y

$$\hat{\sigma}(k) = \hat{\sigma}(f(\alpha_1)) = \sigma(f)(\alpha_2) = \sigma(k),$$

por otro lado, para α_1 tenemos $\alpha_1 = g(\alpha_1)$ con $g(X) = X$, luego $\sigma(g)(X) = X$ y

$$\hat{\sigma}(\alpha_1) = \hat{\sigma}(g(\alpha_1)) = \sigma(g)(\alpha_2) = \alpha_2.$$

Para la unicidad supongamos que $\tau : K_1(\alpha_1) \to K_2(\alpha_2)$ es un homomorfismo que cumple las condiciones, es decir $\tau|_K = \sigma$ y $\tau(\alpha_1) = \alpha_2$. Si $f = f_0 + f_1X + \cdots + f_nX^n$, entonces

$$\tau(f(\alpha_1)) = \tau(f_0 + f_1\alpha_1 + \cdots + f_n\alpha_1^n) = \tau(f_0) + \tau(f_1)\tau(\alpha_1) + \cdots + \tau(f_n)\tau(\alpha_1)^n$$

$$= \sigma(f_0) + \sigma(f_1)\alpha_2 + \cdots + \sigma(f_n)\alpha_2^n = \hat{\sigma}(f)(\alpha_2).$$

Por tanto $\tau = \hat{\sigma}$.
Si además σ es un isomorfismo, entonces $\hat{\sigma}$ es un isomorfismo pues todo homomorfismo de cuerpos es inyectivo y además K_2 y α_2 están en la imagen de $\hat{\sigma}$,[a] lo que muestra que $\hat{\sigma}$ es suprayectivo.

[a] K_2 está en la imagen de $\hat{\sigma}$ ya que $\hat{\sigma}(k) = \sigma(k)$ para todo $k \in K_1$ y σ es un isomorfismo, en concreto suprayectivo

Si aplicamos el Lema 1.30 al caso en que σ es la aplicación identidad en K entonces obtenemos que si α y β son dos raíces de p entonces $K(\alpha)$ y $K(\beta)$ son K-isomorfos. Eso y algo más es lo que dice la siguiente proposición.

Proposición 1.31: Extensiones por raíces del mismo polinomio irreducible

Sea $p \in K[X]$ un polinomio irreducible y sean α y β dos raíces de p en dos extensiones de K (tal vez dos extensiones diferentes). Entonces existe un único K-isomorfismo $f : K(\alpha) \to K(\beta)$ tal que $f(\alpha) = \beta$. En particular las dos extensiones $K(\alpha)/K$ y $K(\beta)/K$ son isomorfas.

Demostración

Aplicando el Lema 1.30 con $\sigma = \mathrm{id}_K$ (que es un isomorfismo) y p el polinomio irreducible obtenemos la existencia y unicidad del K-isomorfismo $f : K(\alpha) \to K(\beta)$ tal que $f(\alpha) = \beta$.

Observación. La hipótesis de que el polinomio p sea irreducible en la Proposición 1.31 es imprescindible. Por ejemplo, si $p = X(X^2 + 1)$, entonces 0 e i son dos raíces de p y obviamente $\mathbb{Q}(0) = \mathbb{Q}$ no es isomorfo a $\mathbb{Q}(i)$.

A la vista de la Proposición 1.31, si $p \in K[X]$ es irreducible, hablaremos de la extensión de K obtenida adjuntando a K una raíz del polinomio irreducible p, como la extensión $K(\alpha)/K$ donde α es cualquier raíz de p en una extensión arbitraria de K.

Ejemplo 1.32

Consideremos $K = \mathbb{Q}$ y el polinomio $p = X^3 - 2 \in \mathbb{Q}[X]$. Este polinomio es irreducible en $\mathbb{Q}[X]$ por el Criterio de Eisenstein con $p = 2$. Si $\alpha = \sqrt[3]{2}$ es una raíz real de p, entonces la extensión $\mathbb{Q}(\alpha)/\mathbb{Q}$ es la extensión obtenida al adjuntar a $\mathbb{Q}$ una raíz del polinomio irreducible $X^3 - 2$.
Por otro lado, si $\omega = e^{2\pi i/3}$ es una raíz primitiva cúbica de la unidad, entonces las otras dos raíces de p son $\omega\alpha$ y $\omega^2\alpha$ y las extensiones $\mathbb{Q}(\omega\alpha)/\mathbb{Q}$ y $\mathbb{Q}(\omega^2\alpha)/\mathbb{Q}$ son isomorfas a $\mathbb{Q}(\alpha)/\mathbb{Q}$.

Un aspecto reseñable del último ejemplo es que si bien las extensiones $\mathbb{Q}(\alpha)/\mathbb{Q}$, $\mathbb{Q}(\omega\alpha)/\mathbb{Q}$ y $\mathbb{Q}(\omega^2\alpha)/\mathbb{Q}$ son isomorfas, no son iguales vistas como subconjuntos de $\mathbb{C}$, pues por ejemplo $\omega\alpha \notin \mathbb{Q}(\alpha)$. Sin embargo, en el caso de $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(-\sqrt{2})$ sí que son iguales como subconjuntos de $\mathbb{R}$. Más tarde veremos que esto no es una casualidad.

1.3. Extensiones algebraicas

En un contexto informal hablamos de números trascendentes como aquellos que no son raíces de ningún polinomio con coeficientes enteros (o racionales), por ejemplo π o e. En contraposición, los números algebraicos son aquellos que sí son raíces de algún polinomio con coeficientes enteros (o racionales), por ejemplo $\sqrt{2}$ o $\sqrt[3]{5}$. Esta idea se puede generalizar al contexto de extensiones de cuerpos como se recoge en las siguientes definiciones.

Definición 1.33: Elemento algebraico y trascendente

Sea L/K una extensión de cuerpos. Un elemento $\alpha \in L$ se dice que es algebraico sobre K si existe un polinomio no nulo $0 \neq p \in K[X]$ tal que $p(\alpha) = 0$. En caso contrario se dice que α es trascendente sobre K.

Definición 1.34: Extensión algebraica y trascendente

Decimos que L/K es una extensión algebraica si todo elemento de L es algebraico sobre K. En caso contrario decimos que la extensión es trascendente.

Si un elemento es algebraico, entonces podemos elegir un polinomio irreducible que lo anule, de esta manera, según el Lema 1.22, obtenemos una extensión finita. De igual manera, si $K(\alpha)/K$ es finita de grado n, entonces el conjunto

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n\}$$

debe ser linealmente dependiente sobre K, luego existen $a_0, a_1, \ldots, a_n \in K$, no todos nulos, tales que

$$a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n = 0,$$

es decir, α es raíz del polinomio $p(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$. Esto muestra que un elemento es algebraico si y solo si la extensión que genera es finita. Más tarde recogeremos esta idea (y otras equivalencias) en la Proposición 1.37.

Ejemplo 1.35

El cuerpo de fracciones de $K[X]$ es $K(X)$ y $K(X)/K$ es una extensión de grado infinito pues las potencias de X son linealmente independientes sobre K. Por tanto X es trascendente sobre K.

Ejemplo 1.36

Decidir si un número real o complejo es algebraico sobre el cuerpo de los números racionales es un problema normalmente muy difícil. El carácter algebraico o trascendente del número π sobre $\mathbb{Q}$ fue un problema sin resolver durante muchos años hasta que Lindemann demostró en 1882 que es trascendente. También es trascendente la base e del logaritmo neperiano, lo que fue demostrado por Hermite en 1873.

La siguiente proposición caracteriza cuándo un elemento es algebraico.

Proposición 1.37: Caracterización de elemento algebraico

Si L/K es una extensión de cuerpos y $\alpha \in L$, entonces las siguientes condiciones son equivalentes:

(1) α es algebraico sobre K.

(2) El homomorfismo de sustitución

$$\begin{aligned} S_\alpha : K[X] &\to L \\ p &\mapsto p(\alpha) \end{aligned}$$

no es inyectivo.

(3) $K[\alpha] = K(\alpha)$.

(4) $K[\alpha]$ es un subcuerpo de L.

(5) $K(\alpha)/K$ es finita.

Demostración

- (1) $\Leftrightarrow$ (2): Si α es algebraico, existe un polinomio no nulo $f \in K[X]$ tal que $f(\alpha) = 0$, luego $f \in \ker S_\alpha$ y por tanto S_α no es inyectivo. Recíprocamente, si S_α no es inyectivo, existe un polinomio no nulo $f \in K[X]$ tal que $f(\alpha) = 0$, luego α es algebraico sobre K.
- (3) $\Leftrightarrow$ (4): Si $K[\alpha] = K(\alpha)$, es inmediato puesto que $K(\alpha)$ es un subcuerpo de L. Recíprocamente, si $K[\alpha]$ es un subcuerpo de L, entonces $K(\alpha)$, que es el menor subcuerpo de L que contiene a K y $\{\alpha\}$, debe estar contenido en $K[\alpha]$. Por tanto, $K(\alpha) = K[\alpha]$.
- (1) $\Rightarrow$ (3), (5): Supongamos que α es algebraico sobre K y sea $0 \neq f \in K[X]$ tal que $f(\alpha) = 0$. Si $f = p_1 \dots p_n$ es una factorización de f es producto de irreducibles de $K[X]$, entonces $p_1(\alpha) \dots p_n(\alpha) = f(\alpha) = 0$ y por tanto $p_i(\alpha) = 0$ para algún i. Eso implica que α es una raíz de un polinomio irreducible de $K[X]$ y del Lema 1.22 se deduce que $K[\alpha] = K(\alpha)$, lo que prueba (3). De este mismo Lema se deduce también que $K(\alpha)/K$ es finita, lo que prueba (5).
- (4) $\Rightarrow$ (2): Supongamos que el homomorfismo de sustitución $S = S_\alpha : K[X] \to K[\alpha]$ es inyectivo. Entonces $K[X] \cong K[\alpha]$ y por tanto $K[\alpha]$ no es cuerpo. Por tanto no se verifica (4).
- (5) $\Rightarrow$ (2): Supongamos que el homomorfismo de sustitución $S = S_\alpha : K[X] \to K[\alpha]$ es inyectivo. Entonces $K[X] \cong K[\alpha]$ y por tanto $K[\alpha]$ no es de dimensión finita sobre K. Por tanto no se verifica (5).

1.3.1. Polinomio mínimo

Sean L/K una extensión y α un elemento de L algebraico sobre K. Entonces el núcleo I del homomorfismo de sustitución $S = S_\alpha : K[X] \to L$ es un ideal no nulo que es primo pues $K[X]/I \simeq \mathrm{Im}(S) = K[\alpha]$ es un dominio. Por tanto $I = (p)$ para un polinomio irreducible p de $K[X]$. De todos los generadores de I, hay uno sólo que sea mónico.

Definición 1.38

Se llama polinomio irreducible o mínimo de α sobre K, denotado $\mathrm{Min}_K(\alpha)$, al único generador mónico de $I = \ker S_\alpha$.

Notemos que I puede estar generado por otros polinomios irreducibles que no son mónicos, pero el polinomio mínimo es el único mónico. Además, como cualquier otro polinomio en I es múltiplo de $\mathrm{Min}_K(\alpha)$ deducimos que $\mathrm{Min}_K(\alpha)$ tiene grado mínimo en I. Juntando estos dos hechos, encontramos que $\mathrm{Min}_K(\alpha)$ es el único polinomio mónico de grado mínimo en I.

Del Lema 1.22 se deduce que si $\mathrm{Min}_K(\alpha)$ tiene grado n, entonces $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ es una base de $K(\alpha)/K$. En resumen:

Lema 1.39: Grado del polinomio mínimo

Si α es algebraico sobre K, entonces $[K(\alpha) : K] = \mathrm{gr}(\mathrm{Min}_K(\alpha))$ y si este grado es n entonces $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ es una base de $K(\alpha)_K$.

1.3.2. Ejemplos de polinomios mínimos

Para decidir si un polinomio es irreducible podemos usar distintas herramientas. En $\mathbb{Q}[X]$ tenemos el Criterio de Eisenstein. En $\mathbb{R}[X]$ y $\mathbb{C}[X]$ tenemos el Teorema Fundamental del Álgebra que nos dice que todo polinomio en $\mathbb{C}[X]$ es producto de polinomios de grado 1 y que en $\mathbb{R}[X]$ es producto de polinomios de grado 1 o 2.

Además, cualquier polinomio de grado 1 es irreducible en cualquier cuerpo. En los siguientes ejemplos se ilustran algunos polinomios mínimos.

Ejemplo 1.40

$\mathrm{Min}_{\mathbb{Q}}(\sqrt{2}) = X^2 - 2$, $\mathrm{Min}_{\mathbb{R}}(\sqrt{2}) = X - \sqrt{2}$ y $\mathrm{Min}_{\mathbb{Q}}(i) = \mathrm{Min}_{\mathbb{R}}(i) = X^2 + 1$. Más generalmente, si $q \in \mathbb{Q}$ y $\sqrt{q} \notin \mathbb{Q}$, entonces $\mathrm{Min}_{\mathbb{Q}}(\sqrt{q}) = X^2 - q$.

Demostración

Las afirmaciones sobre $\mathrm{Min}_{\mathbb{R}}(\sqrt{2})$, $\mathrm{Min}_{\mathbb{Q}}(i)$ y $\mathrm{Min}_{\mathbb{R}}(i)$ se dejan como ejercicio.
Para el caso $q \in \mathbb{Q}$ y $\sqrt{q} \notin \mathbb{Q}$ solo tenemos que probar que $X^2 - q$ es irreducible en $\mathbb{Q}[X]$ cuando $\sqrt{q} \notin \mathbb{Q}$. Si $X^2 - q$ fuera reducible en $\mathbb{Q}[X]$, entonces

$$X^2 - q = (aX - b)(cX - d)$$

y por tanto tendría una raíz en $\mathbb{Q}$, digamos $r = b/a$. Pero entonces $r^2 = q$ y por tanto $\sqrt{q} = r \in \mathbb{Q}$, lo que contradice la hipótesis. Luego $X^2 - q$ es irreducible en $\mathbb{Q}[X]$.

Ejemplo 1.41

Si $\alpha = \sqrt{5 + \sqrt{5}}$, entonces $\alpha^2 - 5 = \sqrt{5}$, con lo que $5 = (\alpha^2 - 5)^2 = \alpha^4 - 10\alpha^2 + 25$, es decir α es una raíz del polinomio $X^4 - 10X + 20$. Aplicando el Criterio de Eisenstein a este polinomio para el primo 5, deducimos que es irreducible sobre $\mathbb{Q}$ y por tanto $\mathrm{Min}_{\mathbb{Q}}(\alpha) = X^4 - 10X + 20$.

1.3.3. Caracterización de extensiones algebraicas

Una consecuencia de la Proposición 1.37 es el siguiente corolario que caracteriza las extensiones finitas.

Corolario 1.42: Caracterización de extensiones finitas

Las siguientes condiciones son equivalentes para una extensión de cuerpos.

(1) L/K es finita.

(2) L/K es algebraica y finitamente generada.

(3) Existen $\alpha_1, \ldots, \alpha_n \in L$ algebraicos sobre K tales que $L = K(\alpha_1, \ldots, \alpha_n)$.

Demostración

(1) $\Rightarrow$ (2). Supongamos que L/K es finita. Entonces de la igualdad $[L : K] = [L : K(\alpha)][K(\alpha) : K]$ tenemos que

$$[K(\alpha) : K] \leq [L : K] < \infty$$

para todo $\alpha \in L$. De la Proposición 1.37 se deduce que α es algebraico sobre K. Por otro lado, si $\alpha_1, \ldots, \alpha_n$ es una base de L_K, entonces $L = K(\alpha_1, \ldots, \alpha_n)$ y por tanto L/K es finitamente generada.
(2) $\Rightarrow$ (3) es obvio.
(3) $\Rightarrow$ (1). Si $\alpha_1, \ldots, \alpha_n$ son algebraicos entonces existen polinomios no nulos $p_1, \ldots, p_n \in K[X]$ tales que $p_i(\alpha_i) = 0$ para $i = 1, \ldots, n$. Como cada $K \subseteq K(\alpha_1, \ldots, \alpha_{i-1})$, podemos ver cada polinomio p_i como elemento de $K(\alpha_1, \ldots, \alpha_{i-1})[X]$.
Además, es inmediato que

$$K(\alpha_1, \ldots, \alpha_i) = K(\alpha_1, \ldots, \alpha_{i-1})(\alpha_i).$$

Entonces, cada α_i es algebraico sobre $L_i = K(\alpha_1, \ldots, \alpha_{i-1})$, ya que el polinomio $p_i \in L_i[X]$ anula a α_i. De ahí, $K(\alpha_1, \ldots, \alpha_i)/K(\alpha_1, \ldots, \alpha_{i-1})$ es una extensión finita por la Proposición 1.37.
Aplicando que la clase de extensiones finitas es multiplicativa (Proposición 1.17) deducimos que $L = K(\alpha_1, \ldots, \alpha_n)/K$ es finita.

Notemos que el Corolario que acabamos de demostrar es bastante importante, pues nos dice que para construir extensiones finitas basta con adjuntar elementos algebraicos. De hecho, si α, β son algebraicaos sobre K, entonces $K(\alpha, \beta)/K$ es algebraica y finitamente generada, en concreto, $\alpha + \beta, \alpha\beta, \alpha^1$ son todos algebraicos sobre K (es decir, raices de polinomios con coeficientes en K). Esto es, desde luego, algo que no parece obvio a primera vista, puesto que dadas dos raíces de polinomios distintos $p(X), q(X)$, no hay ninguna razón aparente para que su suma o producto deban ser raíces de algún polinomio con coeficientes en el mismo cuerpo base.

Corolario 1.43: Multiplicatividad de extensiones algebraicas

La clase de extensiones algebraicas es multiplicativa.

Demostración

Sea $K \subseteq E \subseteq L$ una torre de extensiones.
Si L/K es algebraica, entonces un elemento cualquiera $\alpha \in L$ es algebraico sobre K, luego existe un polinomio $p \in K[X]$ con coeficientes en K que lo anula. Ahora basta notar que ese polinomio también pertenece a $E[X]$, y por tanto α también es algebraico sobre E, luego L/E es algebraica. Por otro lado, si tomamos un elemento cualquiera $\alpha \in E$, entonces $\alpha \in L$, por lo que es algebraico sobre K, luego E/K es algebraica.
Recíprocamente, supongamos que E/K y L/E son algebraicas y sea $\alpha \in L$. Entonces α es

algebraico sobre E. Sea $p = \mathrm{Min}_E(\alpha)$ y sean $p_0, p_1, \ldots, p_n$ los coeficientes de p

$$p = p_0 + p_1 X + p_2 X^2 + \cdots + p_n X^n.$$

Por hipótesis $p_0, p_1, \ldots, p_n$ son algebraicos sobre K, lo que implica que la extensión

$$F = K(p_0, p_1, \ldots, p_n)/K$$

es finita, por el Corolario 1.42. Además, α es algebraico sobre F, ya que $p \in F[X]$, y por tanto $F(\alpha)/F$ es finita. Entonces,

$$[K(\alpha) : K] \leq [K(\alpha, p_0, p_1, \ldots, p_n) : K] = [F(\alpha) : F][F : K] < \infty.$$

De la Proposición 1.37 deducimos que α es algebraico sobre K.

Corolario 1.44: Clausura algebraica

Si L/K es una extensión de cuerpos, entonces el conjunto C de los elementos de L que son algebraicos sobre K es un subcuerpo de L que contiene a K, llamado clausura algebraica de L/K, o clausura algebraica de K en L.
En particular, si S es un subconjunto de L formado por elementos algebraicos sobre K, entonces $K(S)$ es algebraico sobre K.

Demostración

Obviamente $K \subseteq C$. Si $\alpha, \beta \in C$, entonces β es algebraico sobre $K(\alpha)$, ya que el polinomio $p \in K[X]$ que anula a β se puede ver como polinomio en $K(\alpha)[X]$.
Por tanto, $K(\alpha)/K$ y $K(\alpha, \beta)/K(\alpha)$ son algebraicas, lo que implica que $K(\alpha, \beta)/K$ es también algebraica por el Corolario 1.43.
Finalmente, todo elemento de $K(\alpha, \beta)$ es algebraico sobre K y en particular $\alpha + \beta, \alpha - \beta, \alpha\beta \in C$ y, si $\beta \neq 0$, entonces $\beta^{-1} \in C$. Esto prueba que C es un subcuerpo de L.

Ejemplo 1.45

Sea $L = \mathbb{C}$ y $K = \mathbb{Q}$. Entonces la clausura algebraica de $\mathbb{Q}$ en $\mathbb{C}$ se denota $\bar{\mathbb{Q}}$ y es trivialmente una extensión algebraica de $\mathbb{Q}$.

Decimos que una clase C de extensiones de cuerpos es cerrada para levantamientos si para cada dos extensiones admisibles L_1/K y L_2/K tales que L_1/K esté en C se verifica que L_1L_2/L_2 también esta en C.

Proposición 1.46: Cierre para levantamientos

Cada una de las clases de extensiones finitas, algebraicas, finitamente generadas y simples, son cerradas para levantamientos.

Demostración

Sean L_1/K y L_2/K dos extensiones admisibles. Esta claro que si $L_1 = K(\alpha_1, \ldots, \alpha_n)$, entonces $L_2L_1 = L_2(L_1) = L_2(\alpha_1, \ldots, \alpha_n)$, lo que muestra que las clases de extensiones finitamente generadas y de extensiones simples son ambas cerradas para extensiones. Por otro lado si L_1/K es algebraica, entonces todo elemento de L_1 es algebraico sobre K y por

tanto también sobre L_2, lo que implica que $L_1L_2 = L_2(L_1)$ es algebraico sobre K, por el Corolario 1.44. Esto prueba que la clase de extensiones algebraicas es cerrada para levantamientos. Como una extensión es finita si y solo si es algebraica y finitamente generada (Proposición 1.37) deducimos que la clase de extensiones finitas también es cerrada para levantamientos.

Recuérdese que todo endomorfismo de una extensión finita ha de ser un automorfismo (Proposición 1.16). Esta propiedad se verifica de hecho para toda extensión algebraica.

Proposición 1.47: Endomorfismos de extensiones algebraicas

Si L/K es una extensión algebraica, entonces todo K-endomorfismo de L es un automorfismo.

Demostración

Sea σ un K-endomorfismo de L. Como todo homomorfismo de cuerpos es inyectivo, solo hay que probar que σ es suprayectivo. Sea $\alpha \in L$ y sea $p = \mathrm{Min}_K(\alpha)$, $\alpha_1, \alpha_2, \ldots, \alpha_n$ las raíces de p en L, donde podemos suponer sin perder generalidad que $\alpha_1 = \alpha$. Del Lema 1.22 se deduce que σ permuta $\{\alpha_1, \ldots, \alpha_n\}$ y por tanto $\alpha = \sigma(\alpha_i)$ para algún i.

Capítulo 2

Cuerpos algebraicamente cerrados y extensiones normales

2.1. Cuerpos algebraicamente cerrados

Una propiedad muy importante que distingue a los números complejos de los números reales es que todo polinomio no constante con coeficientes complejos tiene al menos una raíz compleja. Partiendo de esta observación, cabe preguntarse si existen otros cuerpos que compartan esta propiedad. La respuesta es afirmativa y nos lleva a la siguiente definición. Pero antes, veamos que, como consecuencia del Teorema de Kronecker, hay varias condiciones equivalentes al hecho de que todo polinomio no constante tenga una raíz en el cuerpo.

Proposición 2.1: Caracterización de cuerpos algebraicamente cerrados

Las siguientes condiciones son equivalentes para un cuerpo K:

(1) Todo polinomio no constante de $K[X]$ tiene una raíz en K.

(2) Los polinomios irreducibles de $K[X]$ son precisamente los de grado 1.

(3) Todo polinomio no constante de $K[X]$ es completamente factorizable sobre K.

(4) K contiene un subcuerpo K_0 tal que K/K_0 es algebraica y todo polinomio de $K_0[X]$ es completamente factorizable sobre K.

(5) Si L/K es una extensión algebraica, entonces $L = K$.

(6) Si L/K es una extensión finita, entonces $L = K$.

Demostración

(1) $\Rightarrow$ (2). Supongamos que p es un polinomio irreducible de $K[X]$ de grado $n \geq 1$. Por hipótesis, p tiene una raíz α en K. Entonces $X - \alpha$ divide a p y como p es irreducible, se tiene que $p = a(X - \alpha)$ para algún $a \in K^*$.
(2) $\Rightarrow$ (3). Sea $p \in K[X]$ un polinomio no constante de grado $n \geq 1$. Razonaremos por inducción, si $n = 1$ entonces p ya está completamente factorizado. Suponiendolo cierto para n, si p tiene grado $n+1$, por hipótesis p tiene una raíz α en K. Entonces $X - \alpha$ divide a p y podemos escribir $p(X) = (X - \alpha)q(X)$ con $q \in K[X]$ de grado n. Por hipótesis de inducción, q es completamente factorizable sobre K y por tanto lo es también p.
(3) $\Rightarrow$ (4). Basta tomar $K_0 = K$, que es algebraica puesto que cada elemento α de K es algebraico sobre K (anula al polinomio de grado 1 $X - \alpha \in K[X]$).

(4) $\Rightarrow$ (5). Supongamos que K contiene un subcuerpo K_0 satisfaciendo la propiedad (4). Si L/K es una extensión algebraica, como K/K_0 también es algebraica, entonces L/K_0 es también algebraica, ya que las extensiones algebraicas son multiplicativas (Corolario 1.43). Si $\alpha \in L$, entonces por hipótesis $p = \mathrm{Min}_{K_0}(\alpha)$ es completamente factorizable sobre K, con lo cual todas las raíces de p pertenecen a K. En particular $\alpha \in K$ y esto prueba que $L = K$.
(5) $\Rightarrow$ (6). Si L/K es una extensión finita, por el Corolario 1.42, L/K es algebraica y por tanto $L = K$ por hipótesis.
(6) $\Rightarrow$ (1). Sea $p \in K[X]$ un polinomio no constante. Por el Teorema de Kronecker, existe una extensión L de K que contiene una raíz α de p, y de hecho $K(\alpha)$ es la menor extensión que contiene a esta raíz. Pero como α es raíz de p, por tanto un elemento algebraico, la extensión $K(\alpha)/K$ debe ser finita (Proposición 1.37). Entonces, por hipótesis, $L = K$ y por tanto $\alpha \in K$, es decir, p tiene una raíz en K.

Definición 2.2: Cuerpo algebraicamente cerrado

Se dice que un cuerpo K es algebraicamente cerrado cuando verifica las condiciones equivalentes de la Proposición 2.1.

Ejemplo 2.3: Cuerpos no algebraicamente cerrados

Es fácil encontrar ejemplos de cuerpos que no son algebraicamente cerrados. Por ejemplo, $\mathbb{Q}$ y $\mathbb{R}$ no lo son porque el polinomio X^2+1 no tiene raíces reales y $\mathbb{Z}_2$ tampoco lo es porque $X^2 + X + 1$ no tiene raíces en $\mathbb{Z}_2$.

Ejemplo 2.4

Si $p \geq 3$ es un entero primo entonces $\mathbb{Z}_p$ no es algebraicamente cerrado, pues $X^{p-1} + 1$ no tiene raíces en $\mathbb{Z}_p$ por el Teorema Pequeño de Fermat.

Demostración

Recordemos el Teorema Pequeño de Fermat: si p es un número primo y a es un entero no divisible por p, entonces $a^{p-1} \equiv 1 \mod p$.
En particular, si $\alpha \in \mathbb{Z}_p$ entonces $\alpha^{p-1} = 1$ en $\mathbb{Z}_p$. Por tanto, si α es una raíz de $X^{p-1} + 1$ en $\mathbb{Z}_p$, entonces $\alpha^{p-1} = -1 = p - 1$ en $\mathbb{Z}_p$, y por Teorema Pequeño de Fermat debe ser $p - 1 = 1 \implies p = 2$, una contradicción.

Ejemplo 2.5

Más generalmente, ningún cuerpo finito es algebraicamente cerrado.

Demostración

Supongamos K es un cuerpo finito y algebraicamente cerrado. Como K es finito, tendrá un número finito de elementos, digamos n, sea pues

$$K = \{a_1, a_2, \ldots, a_n\}$$

Entonces, el polinomio

$$p(X) = (X - a_1)(X - a_2) \cdots (X - a_n) + 1$$

es no constante (de hecho es de grado n) y no tiene raíces en K, ya que para cada $a_i \in K$ se tiene que $p(a_i) = 1$. Esto contradice la hipótesis de que K es algebraicamente cerrado.

Observación. En el ejemplo anterior el polinomio $p(X)$ solo toma el valor 1 al evaluarlo, pero no es constante puesto que el término general (el de mayor grado) es X^n, distinto de cero.

Un caso particularmente importante de cuerpo algebraicamente cerrado es el de los números complejos. Veamos la demostración del Teorema Fundamental del Álgebra (se demuestra usando análisis, por supuesto):

Teorema 2.6: Teorema Fundamental del Álgebra

$\mathbb{C}$ es algebraicamente cerrado.

Demostración

Se trata de ver que, dado un polinomio

$$p(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

de grado $n \geq 1$ ($a_n \neq 0$) con coeficientes complejos ($a_i \in \mathbb{C}$ para cada $i = 0, 1, \ldots, n$), existe un número complejo z tal que $p(z) = 0$.
Usaremos propiedades elementales de los números complejos, como las desigualdades entre módulos

$$|z_1| - |z_2| \leq |z_1 + z_2| \leq |z_1| + |z_2|$$

o el hecho de que todos ellos tienen raíces m-ésimas para cualquier entero $m \geq 1$. Para demostrar esto, dado un número complejo z cualquiera, podemos expresar $z = |z|e^{i\theta}$, aplicando el Teorema de Bolzano al polinomio $X^m - |z|$ en el intervalo $[0, |z| + 1]$ se demuestra que el número real $|z|$ tiene una raíz m-ésima, a partir de esta raíz $\sqrt[m]{|z|}$ podemos construir las raíces m-ésimas de z:

$$\sqrt[m]{|z|}e^{i(\theta+2k\pi)/m}, \quad k = 0, 1, \ldots, m-1.$$

También emplearemos los conceptos de límite y continuidad. En particular, el hecho de que toda función continua $\mathbb{C} \to \mathbb{R}$, y en concreto

$$z \mapsto |p(z)| = +\sqrt{p(z)\overline{p(z)}},$$

alcanza su mínimo en cualquier subconjunto cerrado y acotado de $\mathbb{C}$, y por tanto en cualquier bola $\{z \in \mathbb{C} : |z| \leq r\}$, donde r es un número real positivo (Teorema de Weierstrass). El esquema de la demostración es el siguiente

1. Demostrar $z \mapsto |p(z)|$ alcanza su mínimo absoluto en $\mathbb{C}$; para ello, se demuestra que $|p(z)|$ se hace grande fuera de cierta bola $\{z \in \mathbb{C} : |z| \leq r\}$, y entonces el mínimo que alcanza $|p(z)|$ en esa bola es de hecho un mínimo absoluto en $\mathbb{C}$.

2. Ver que ese mínimo es 0, esto lo hacemos por reducción al absurdo: si el mínimo no es 0, construimos una función $\mathbb{C} \to \mathbb{R}$ cuyo mínimo absoluto vale 1, y sin embargo encontramos un punto en el que la misma función vale menos de 1.

Veamos, por inducción en el grado n, que $|p(z)|$ se hace más grande que cualquier número real positivo fuera de cierta bola. Sea $k > 0$ un número real cualquiera.
Si $n = 1$ entonces $p(X) = a_0 + a_1X$ con $a_1 \neq 0$ y basta tomar $r = (k + |a_0|)/|a_1|$ para que cuando $|z| > r$

$$|p(z)| \geq |a_1||z| - |a_0| > |a_1|\frac{k + |a_0|}{|a_1|} - |a_0| = k.$$

Si $n > 1$ entonces la expresión de $p(X)$ se reescribe como

$$p(X) = a_0 + Xq(X), \quad \text{donde} \quad q(X) = a_1 + a_2X + \cdots + a_nX^{n-1},$$

y aplicando la hipótesis de inducción al polinomio q obtenemos un radio r a partir del cual $|q(z)|$ se hace más grande que $k + |a_0|$, por lo que si $|z| > \max\{s, 1\}$ entonces

$$|p(z)| = |zq(z) + a_0| \geq |z||q(z)| - |a_0| > |z|(k + |a_0|) - |a_0| > (k + |a_0|) - |a_0| = k.$$

Para el segundo paso, como la función $|p(z)|$ es continua, alcanza un mínimo en la bola $B = \{z \in \mathbb{C} : |z| \leq r\}$; es decir, existe $z_0 \in B$ tal que $|p(z_0)| \leq |p(z)|$ para cada $z \in B$. La misma desigualdad se tiene cuando $z \notin B$, pues entonces $|z| > r$ y así $|p(z)| > |a_0| = |p(0)| \geq |p(z_0)|$. En consecuencia, $|p(z)|$ alcanza un mínimo absoluto en z_0; es decir, $|p(z_0)| \leq |p(z)|$ para cada $z \in \mathbb{C}$.
Es claro que $p(X)$ tiene una raíz si y solo si la tiene $p(X + z_0)$, y éste tiene la ventaja de que su módulo alcanza un mínimo absoluto en el 0. Por tanto, sustituyendo $p(X)$ por $p(X+z_0)$, podemos suponer que $z_0 = 0$, y por tanto que $|p(z)| \geq |p(0)| = |a_0|$ para cada $z \in \mathbb{C}$. Si $a_0 = 0$ hemos terminado, así que se trata de ver que la condición $a_0 \neq 0$ nos lleva a una contradicción.
En este caso, dividir p por a_0 no va a cambiar el punto en el que se alcanza el mínimo, por lo que podemos suponer que $a_0 = 1$. Excluyendo monomios con coeficiente nulo, podemos escribir

$$p(X) = 1 + a_mX^m + a_{m+1}X^{m+1} + \cdots + a_nX^n \qquad (\text{con } a_m \neq 0)$$

para cierto entero m con $1 \leq m \leq n$. Sea ahora ω una raíz m-ésima de $-a_m^{-1}$ (es decir, $\omega \in \mathbb{C}$ verifica $\omega^m = -a_m^{-1}$). Entonces $p(\omega X) = 1 - X^m +$ (términos de grado mayor que m); es decir,

$$p(\omega X) = 1 - X^m + X^m h(X),$$

donde $h(X)$ es cierto polinomio con $h(0) = 0$.
Finalmente, vamos a encontrar un número real t tal que $|p(\omega t)| < 1$, lo que nos dará la contradicción buscada puesto que 1 es el mínimo absoluto de $|p(z)|$. Consideremos la función $\mathbb{R} \to \mathbb{R}$ dada por $t \mapsto |h(t)|$. Considerando su límite en $x = 0$ (que vale 0 por continuidad) encontramos un número t en el intervalo $(0, 1)$ tal que $|h(t)| < 1$ (haciendo $\epsilon = 1$ en la formulación usual del límite). Entonces también t^m y $1 - t^m$ están en el intervalo $(0, 1)$, por lo que

$$|p(\omega t)| \leq |1 - t^m| + |t^m h(t)| < 1 - t^m + t^m \cdot 1 = 1,$$

como queríamos ver.

Observación. Animamos al lector a consultar la demostración del Teorema Fundamental del Álgebra usando el Teorema de Liouville en análisis complejo, que es más sencilla que la aquí mostrada (a costa de emplear un resultado muy potente).

2.2. Clausura algebraica

Por el Teorema Fundamental del Álgebra, $\mathbb{C}$ es un cuerpo que contiene las raíces de todos los polinomios no constantes de $K[X]$ para cualquier subcuerpo K de $\mathbb{C}$. Por otro lado el Corolario 1.26 muestra que para un cuerpo arbitrario K y un polinomio cualquiera p de $K[X]$, se puede encontrar una extensión L de K en la que el polinomio p factoriza completamente, es decir, en lo que atañe al polinomio p, L se comporta como si fuera algebraicamente cerrado, aunque para que lo fuera todos los polinomios con coeficientes en L tendrían que ser completamente factorizables sobre L, lo que no tiene por qué ser cierto.

En vista de esto es natural preguntarse si todo cuerpo K tiene una extensión algebraicamente cerrada. Por otro lado tenemos la siguiente proposición, que va a garantizar que si K es subcuerpo de un cuerpo algebraicamente cerrado entonces también va a poderse incluir en un cuerpo que además de ser algebraicamente cerrado es algebraico sobre K.

Proposición 2.7: Clausura algebraica en un cuerpo algebraicamente cerrado

Sea L/K una extensión con L algebraicamente cerrado y sea C la clausura algebraica de K en L. Entonces C/K es algebraica y C es algebraicamente cerrado.

Demostración

Que C/K es algebraica es consecuencia de la definición de clausura algebraica de K en L. Por otro lado, si $p \in C[X]$, entonces p tiene una raíz α en L puesto que es algebraicamente cerrado. Eso implica que $C(\alpha)/C$ es finita y, por tanto, algebraica. Como la clase de extensiones algebraicas es multiplicativa, se tiene que $C(\alpha)/K$ es algebraica, lo que implica que $\alpha \in C$. Esto prueba que C es algebraicamente cerrado.

Definición 2.8: Clausura algebraica de un cuerpo

Una clausura algebraica de un cuerpo K es una extensión algebraica L de K formada por un cuerpo algebraicamente cerrado.

Obsérvese la diferencia entre una clausura algebraica de un cuerpo K y la clausura algebraica de una extensión L/K. La primera es una extensión de K que ha de ser algebraica sobre K y algebraicamente cerrada y la segunda es el mayor subcuerpo de L que es algebraico sobre K, pero no tiene que ser algebraicamente cerrado, a no ser que L sea algebraicamente cerrado (Proposición 2.7).

Teorema 2.9: Existencia de clausura algebraica

Todo cuerpo tiene una clausura algebraica.

Demostración

Por la Proposición 2.7, basta demostrar que todo cuerpo está contenido en un cuerpo algebraicamente cerrado. En primer lugar vamos a ver que si K es un cuerpo, entonces existe otro cuerpo E tal que todo polinomio no constante de $K[X]$ tiene una raíz en E. Para eso tenemos que considerar anillos con infinitas indeterminadas.
Si A es un anillo y S es un conjunto de símbolos, entonces se define el anillo de polinomios en S con coeficientes en A como la unión

$$A[S] = \bigcup_{T \in \mathcal{F}} A[T]$$

donde $\mathcal{F}$ es el conjunto de todos los subconjuntos finitos de S y para cada $T \in \mathcal{F}$, $A[T]$ es el anillo de polinomios con coeficientes en A, con indeterminadas los elementos de T. Si $T_1, T_2 \in \mathcal{F}$, entonces $A[T_1]$ y $A[T_2]$ son dos subanillos de $A[T_1 \cup T_2]$. Por tanto cada subconjunto finito de $A[S]$ está dentro de $A[T]$ para algún $T \in \mathcal{F}$, lo que nos permite sumar y multiplicar elementos de $A[S]$ simplemente sumándolos o multiplicándolos en el anillo en un número finito de indeterminadas que los contenga.
Para construir el cuerpo E que contiene raíces de todos los polinomios no constantes de $K[X]$ razonamos de la siguiente forma. A cada polinomio no constante $p \in K[X]$ le asociamos un símbolo X_p y construimos el anillo $K[S]$ donde $S = \{X_p : p \in K[X] \setminus K\}$. Sea I el ideal de $K[S]$ generado por todos los elementos de la forma $p(X_p)$.
Vamos a empezar mostrando que I es un ideal propio de $K[S]$. En caso contrario, $1 \in I$, por lo que existirían $g_1, \ldots, g_n \in K[S]$ y $p_1, \ldots, p_n \in K[X] \setminus K$ tales que $g_1 p_1(X_{p_1}) + \cdots + g_n p_n(X_{p_n}) = 1$. Para simplificar la notación vamos a poner X_i en lugar de X_{p_i}, con lo que tenemos

$$g_1 p_1(X_1) + \cdots + g_n p_n(X_n) = 1. \tag{2.1}$$

Aplicando el Teorema de Kronecker repetidamente deducimos que existe una extensión F de K en la que cada uno de los polinomios $p_1, \ldots, p_n$ tiene una raíz α_i. Sustituyendo X_i por α_i en la ecuación (2.1) obtenemos $0 = 1$, una contradicción.
Una vez que sabemos que I es un ideal propio de $K[S]$ deducimos que I está contenido en un ideal maximal M de $K[S]$. Entonces $E = K(S)/M$ es un cuerpo y la composición de la inclusión $K \to K(S)$ con la proyección $K(S) \to K(S)/M$ proporciona un homomorfismo de cuerpos, con lo que podemos considerar E como una extensión de K. Ahora observamos que $p(X_p + M) = p(X_p) + M = 0$, pues $p(X_p) \in M$, con lo que $X_p + M$ es una raíz de p en E para todo $p \in K[X] \setminus K$.
Utilizando que para cada cuerpo K existe una extensión E de K que contiene raíces de todos los polinomios no nulos de $K[X]$ construimos de forma recursiva una sucesión de extensiones

$$K = E_1 \subseteq E_2 \subseteq E_3 \ldots$$

tal que todo polinomio no constante de $E_i[X]$ tiene una raíz en E_{i+1}. Entonces $E = \bigcup_{i \geq 1} E_i$ tiene una estructura de cuerpo en el que la suma y el producto de cada dos elementos se calcula en un E_i que contiene a ambos. Si f es un polinomio no constante de $E[X]$, entonces $f \in E_i[X]$ para algún i y por tanto f tiene una raíz en E_{i+1} que, por supuesto, pertenece a E. Esto prueba que E es algebraicamente cerrado.

Teorema 2.10: Extensión de homomorfismos a extensiones algebraicas

Si $\sigma : K \to L$ es un homomorfismo de cuerpos con L algebraicamente cerrado y F/K una extensión algebraica, entonces existe otro homomorfismo de cuerpos $F \to L$ que extiende σ.

Demostración

Sea

$$\Omega = \left\{ (E, \tau) : \begin{array}{l} E/K \text{ es una subextensión de } F/K \text{ y} \\ \tau : E \to L \text{ es un homomorfismo que extiende } \sigma \end{array} \right\}$$

y consideremos el siguiente orden en Ω:

$$(E_1, \tau_1) \leq (E_2, \tau_2) \iff E_1 \subseteq E_2 \text{ y } \tau_2|_{E_1} = \tau_1.$$

Es fácil ver que $(\Omega, \leq)$ es un conjunto ordenado inductivo y, por el Lema de Zorn, tiene un elemento maximal (E, τ).
Basta con demostrar que $F \subseteq E$. Sean $\alpha \in F$ y $p = \mathrm{Min}_E(\alpha)$. Como L es algebraicamente cerrado, el polinomio $\tau(p)$ tiene una raíz β en L. Del Lema 1.30 deducimos que existe un

homomorfismo $\tau' : E(\alpha) \to L$ que extiende τ y tal que $\tau'(\alpha) = \beta$. Entonces $(E(\alpha), \tau') \in \Omega$ y $(E, \tau) \leq (E(\alpha), \tau')$. De la maximalidad de (E, τ) deducimos que $E = E(\alpha)$, es decir $\alpha \in E$. Esto prueba que $F \subseteq E$.

El siguiente corolario del Teorema 2.10 muestra que la clausura algebraica de un cuerpo es única salvo isomorfismos, por lo que a partir de ahora utilizaremos el artículo definido para hablar de *la* clausura algebraica de un cuerpo.

Corolario 2.11: Unicidad de la clausura algebraica

Si $\sigma : K_1 \to K_2$ es un isomorfismo de cuerpos y L_1 y L_2 son clausuras algebraicas de K_1 y K_2, respectivamente, entonces existe un isomorfismo $L_1 \to L_2$ que extiende σ.

Demostración

Por el Teorema 2.10 hay un homomorfismo $\tilde{\sigma} : L_1 \to L_2$ que extiende σ. Como L_1 es algebraicamente cerrado y $\tilde{\sigma}$ induce un isomorfismo entre L_1 y $\tilde{\sigma}(L_1)$, este último también es algebraicamente cerrado. Como L_2/K_2 es algebraica, $L_2/\tilde{\sigma}(L_1)$ es algebraica y por tanto $L_2 = \tilde{\sigma}(L_1)$, lo que muestra que $\tilde{\sigma}$ es un isomorfismo.

Apéndice A

Polinomios

Recogemos en este apéndice algunas nociones básicas sobre anillos de polinomios que se utilizan en el texto principal.

A.1. Anillos de polinomios

Definición A.1

Sea A un anillo, definimos el anillo de polinomios en una variable X con coeficientes en A, denotado por $A[X]$, como el conjunto de todas las expresiones formales de la forma

$$p = p_0 + p_1 X + p_2 X^2 + \cdots + p_n X^n$$

con n un número entero no negativo y $p_i \in A$ para todo $0 \leq i \leq n$. La suma y el producto de dos polinomios $p, q \in A[X]$ se definen de la manera usual.

Definición A.2

El grado de un polinomio $p \in A[X]$, denotado por $\mathrm{gr}(p)$, es el mayor entero n tal que el coeficiente p_n de X^n es no nulo. Si $p = 0$, se define $\mathrm{gr}(p) = -\infty$.

Definición A.3

Un polinomio $p \in A[X]$ es mónico si su coeficiente principal (el de mayor grado) es la unidad del anillo $1 \in A$.

A.2. Propiedades de anillos de polinomios

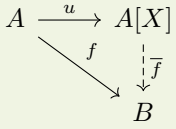
Lema A.4

Un anillo de polinomios $A[X]$ es un dominio si y sólo si A es un dominio. En ese caso se tiene $A[X]^* = A^*$.

En particular, los polinomios invertibles en un cuerpo K son únicamente los polinomios constantes no nulos. Además, $A[X]$ nunca es un cuerpo, pues el polinomio X no es invertible.

Teorema A.5

Sean A un anillo, $A[X]$ el anillo de polinomios con coeficientes en A en la indeterminada X y $u : A \to A[X]$ el homomorfismo de inclusión. Para todo homomorfismo de anillos $f : A \to B$ y todo elemento b de B existe un único homomorfismo de anillos $\overline{f} : A[X] \to B$ tal que $\overline{f}(X) = b$ y $\overline{f} \circ u = f$. Para expresar la última igualdad dice que $\overline{f}$ completa de modo único el diagrama



A.3. Divisibilidad en anillos de polinomios

Por simplicidad, consideraremos a partir de ahora un cuerpo K y su anillo de polinomios $K[X]$.

Definición A.6

Un polinomio $p \in K[X]$ divide a otro polinomio $q \in K[X]$ si existe un polinomio $r \in K[X]$ tal que $q = pr$. En ese caso se escribe $p \mid q$.

Definición A.7

Se dice que dos polinomios $p, q \in K[X]$ son asociados si existen unidades $u, v \in K[X]^* = K^*$ tales que $p = uq$ y $q = vp$.

Definición A.8

Un polinomio $p \in K[X]$ es irreducible si no es constante y sus únicos divisores son los elementos de K^* y los polinomios asociados a p.

Definición A.9

Un polinomio $p \in K[X]$ es primo si siempre que p divide a un producto qr de polinomios $q, r \in K[X]$, entonces p divide a q o a r.

Ejemplo A.10

El polinomio $p = X^2 + 1 \in \mathbb{R}[X]$ es irreducible, pues sus únicos divisores son las unidades y los polinomios asociados a $X^2 + 1$. Notemos que si $\alpha \in \mathbb{R} \setminus \{0\}$ entonces $\alpha(X^2 + 1)$ divide a $X^2 + 1$, ya que ambos polinomios son asociados. Sin embargo, es fácil ver que podemos escoger un único polinomio de entre todos los asociados a $X^2 + 1$ que sea mónico, que es precisamente $X^2 + 1$.
Por el contrario, en $\mathbb{C}[X]$, p se factoriza como $(X + i)(X - i)$ y por tanto no es irreducible.

Proposición A.11

Para un anillo A, las condiciones siguientes son equivalentes:

1. $A[X]$ es un dominio euclídeo con el grado como función euclídea.
2. $A[X]$ es un dominio de ideales principales.
3. A es un cuerpo.

En este caso, un polinomio $p \in A[X]$ es irreducible si y sólo si es primo.

En el caso que nos ocupa, vemos que para un cuerpo K, el anillo de polinomios $K[X]$ es un dominio euclídeo, y por tanto un dominio de ideales principales. Además, en $K[X]$ los polinomios irreducibles son exactamente los primos.

A.4. Polinomios sobre $\mathbb{Q}$

En esta sección estudiamos los anillos de polinomios con coeficientes en los números enteros y racionales, $\mathbb{Z}[x]$ y $\mathbb{Q}[X]$.

Definición A.12

Dado un polinomio $p \in \mathbb{Z}[X]$, se define su contenido, denotado por $c(p)$, como el máximo común divisor de sus coeficientes.

Observación. El contenido de un polinomio $p \in \mathbb{Z}[X]$ está bien definido salvo por signo, pero normalmente lo tomaremos como positivo.

Notemos también que siempre se puede transformar un polinomio $p \in \mathbb{Q}[X]$ en un polinomio $p' \in \mathbb{Z}[X]$ multiplicando por el mínimo común múltiplo de los denominadores de sus coeficientes.

Definición A.13

Un polinomio $p \in \mathbb{Z}[X]$ se dice que es primitivo si su contenido es 1 (es decir, el máximo común divisor de sus coeficientes es 1).

Observación. Cuando hablamos de un polinomio $p \in \mathbb{Q}[X]$ primitivo nos referimos a que los coeficientes de p son enteros y que p es primitivo como polinomio en $\mathbb{Z}[X]$.

Lema A.14: Gauss

Sea $p \in \mathbb{Z}[X]$ un polinomio. Entonces p es irreducible en $\mathbb{Q}[X]$ si y sólo si p es primitivo e irreducible en $\mathbb{Z}[X]$.

En concreto, si un polinomio $p \in \mathbb{Z}[X]$ es mónico, entonces es primitivo (como el coeficiente principal es 1, el contenido es 1), y por tanto p es irreducible en $\mathbb{Q}[X]$ si y sólo si es irreducible en $\mathbb{Z}[X]$.

Ejemplo A.15

Consideremos el polinomio $p(X) = 5X^4 + 3X^3 + 6X + 2$. El contenido de p es 1, luego p es primitivo. Si p fuera reducible en $\mathbb{Z}[X]$, entonces existirían polinomios $q, r \in \mathbb{Z}[X]$ tales que $p = qr$. Observando los grados, las únicas posibilidades son que q y r tengan grados 1 y 3 o ambos grado 2. En cualquier caso, al comparar los coeficientes se llega a una contradicción, luego p es irreducible en $\mathbb{Z}[X]$ y por tanto en $\mathbb{Q}[X]$.

Teorema A.16: Criterio de Eisenstein

Sea

$$p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$$

un polinomio. Si existe un número primo p tal que

1. p divide a a_i para todo $0 \leq i \leq n-1$,
2. p no divide a a_n,
3. p^2 no divide a a_0,

entonces $p(X)$ es irreducible en $\mathbb{Q}[X]$.

Ejemplo A.17

Consideremos el polinomio $p(X) = 3X^4 + 15X^2 + 10$. Aplicando el criterio de Eisenstein con el primo $p = 5$ vemos que p divide a 15 y a 10, pero no a 3, y además $5^2 = 25$ no divide a 10. Por tanto, $p(X)$ es irreducible en $\mathbb{Q}[X]$.

Bibliografía

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