

EXTENSIONES ALGEBRAICAS DE CUERPOS

Cuerpo de ruptura, clausura algebraica y extensiones normales

00. Introducción

00.1. Cuerpos y extensión de un cuerpo

Un conjunto k se dice que tiene estructura de cuerpo con respecto a dos leyes, que llamaremos "+" (ley aditiva) y "." (ley multiplicativa) si se verifica que:

- A) $(k, +)$ es grupo conmutativo con respecto a la ley aditiva, cuyo elemento neutro representaremos por 0.
- B) $(k - \{0\}, \cdot)$ es grupo con respecto a la ley multiplicativa. Si fuera grupo conmutativo diremos que el cuerpo es conmutativo. Podemos representar por e el elemento neutro de esta ley.
- C) La ley multiplicativa distribuye a la ley aditiva.

Podemos utilizar la notación $(k, +, \cdot)$ para representar al cuerpo cuyo conjunto de elementos es k y las leyes internas son las ya indicadas. Cuando se sobreentienden tales leyes utilizaremos simplemente la notación k .

Si dos cuerpos, k y L , tienen las mismas leyes de composición interna, diremos que el cuerpo k es subcuerpo de L si k está contenido en L . También podemos decir que L es supercuerpo de k , o que L es una extensión de k .

Si L se obtiene adjuntando a k un número finito de elementos, $a_1, \dots, a_n$, se dice que L se obtiene por adjunción desde k : $L = k(a_1, \dots, a_n)$ y que L es una extensión finita de k .

Si la extensión L de k se obtiene adjuntándole a k un solo elemento $a \in L$ diremos que $L = k(a)$ es una extensión simple de k .

La extensión $L = k(a_1, \dots, a_n)$ se dice que es algebraica sobre k si todo elemento $a_i, i=1, \dots, n$ es algebraico sobre k , es decir, si para cada $a_i, i=1, \dots, n$ siempre existe algún polinomio $p(x) \in k[x]$ con coeficientes en k tal que $p(a_i) = 0$.

Si algún $a_i \in L(a_1, \dots, a_n)$ no es algebraico sobre k , entonces la extensión L se dice que es una extensión trascendente sobre k .

Si L es extensión de k , entonces L es espacio vectorial sobre k . La dimensión de este espacio vectorial se denomina *grado de la extensión*. Si tal grado es finito se dice que L es extensión finita de k . En otro caso se dirá que es extensión infinita. Representaremos por $(L : k)$ al grado de la extensión de L sobre k .

Sea L una extensión de k . Diremos que el cuerpo k' es un cuerpo intermedio, si k' es supercuerpo de k y subcuerpo de L . O sea, cumpliendo: $k \subseteq k' \subseteq L$.

Dados dos cuerpos, $(k, +, \cdot)$ y $(k', \Delta, \times)$, una aplicación f de k en k' se dice que es homomorfismo de cuerpos si respeta las dos leyes internas de ambos cuerpos, es decir:

$$\begin{aligned}\forall a, b \in k, f(a+b) &= f(a) \Delta f(b) \in k' \\ \forall a, b \in k, f(a \cdot b) &= f(a) \times f(b) \in k'\end{aligned}$$

Si el homomorfismo f es aplicación inyectiva se denomina monomorfismo, y si f es biyectiva, isomorfismo.

Si los cuerpos k y k' son el mismo cuerpo, entonces el homomorfismo se denomina endomorfismo. Un automorfismo en k es un endomorfismo biyectivo, esto es, un isomorfismo de k en k .

Un automorfismo de cuerpos es, en definitiva, una aplicación biyectiva de un cuerpo en si mismo que respeta sus las leyes internas.

00.2. K-automorfismos y Grupo de Galois

Un conjunto importante de resultados de la teoría de cuerpos puede establecerse desde propiedades simples de la teoría de grupos. Esta conexión de la teoría de cuerpos con la teoría de grupos es lo que conocemos como Teoría de Galois.

En el breve artículo [Los automorfismos de cuerpos y el Grupo de Galois](#) tratamos los automorfismos definidos en un cuerpo L (los endomorfismos biyectivos definidos sobre L) que dejan invariantes los elementos de un subcuerpo k del mismo. Tales automorfismos los denominamos k -automorfismos de L y presentan la interesante propiedad de que constituyen un grupo, que denominamos *Grupo de Galois de la extensión de L sobre k* .

Nos encontramos, además, que todo subgrupo del Grupo de Galois de los k -automorfismos de L sobre k es, a su vez, un conjunto de k -automorfismos que dejan invariante a los elementos de un cuerpo intermedio entre k y L , y, recíprocamente, para todo cuerpo intermedio existe también el correspondiente grupo de Galois constituido por aquellos k -automorfismos de L que dejan invariantes a sus elementos, y que es subgrupo del Grupo de Galois de los k -automorfismos de la extensión de L sobre k .

Los conceptos clave que manejamos son:

Por una parte, el subconjunto del cuerpo L que queda invariante para un conjunto H dado de automorfismos de L . Vemos que tal subconjunto tiene estructura de cuerpo y se denomina *cuerpo fijo* o *cuerpo invariante* del conjunto de automorfismos H .

El cuerpo fijo o invariante del Grupo de Galois de la extensión de L sobre k no tiene porqué coincidir con el cuerpo k . Puede ser un cuerpo intermedio (cuerpo que contiene a k y es subcuerpo de L).

Asimismo, el Grupo de Galois del cuerpo fijo de un conjunto H de automorfismos no ha de coincidir obviamente con el conjunto H . Vemos también en este artículo la condición que debe cumplirse para que esta situación ocurra.

00.3. Cuerpo algebraicamente cerrado

Un cuerpo k se dice que es algebraicamente cerrado si todo polinomio con coeficientes en k y grado mayor o igual que la unidad tiene un cero en k . Por ejemplo, el cuerpo R de los números reales no es algebraicamente cerrado, pues existe un polinomio, $p(x) = x^2 + 1$, que no tiene un cero en R . En cambio, el cuerpo C de los números complejos sí es algebraicamente cerrado.

Una extensión del cuerpo k que sea algebraicamente cerrada se llama clausura algebraica de k . Por ejemplo, el cuerpo C de los números complejos es la clausura algebraica de R , cuerpo de los números reales.

En lo que sigue vamos a tratar de mostrar la idea de cuerpo de ruptura y la existencia de la clausura algebraica de un cuerpo, al objeto de que podamos definir las extensiones normales, extensiones que, cuando también son separables se denominan extensiones galoisianas.

01. Cuerpo de ruptura

Teorema 01: Sea k un cuerpo y sea $p(x) \in k[x]$ un polinomio irreducible en k . Existe siempre una extensión simple L/k tal que $L = k(a)$, determinada salvo isomorfismo y denominada *cuerpo de ruptura del polinomio $p(x)$* , tal que en ella dicho polinomio admite como cero a a .

Demostración:

Si $p(x) \in k[x]$ es irreducible en k , entonces el ideal $(p(x))$ es maximal, por lo que:

$$\left. \begin{array}{l} (p(x)) \text{ ideal maximal} \\ k[x] \text{ anillo con el unidad} \end{array} \right\} \rightarrow k[x]/(p(x)) \text{ cuerpo}$$

Por ser $k \subseteq k[x]$, el epimorfismo canónico $n: k[x] \rightarrow k[x]/(p(x))$ transforma a k en un cuerpo isomorfo a k' , subcuerpo de $k[x]/(p(x))$. En adelante identificamos

los cuerpos isomorfos k y k' y consideramos $L = k[x]/(p(x))$ como un

supercuerpo de k . Sea, para $x \in k[x]$, $n(x) = \varepsilon \in k[x]/(p(x))$,

y para $f(x) \in k[x]$ tal que $f(x) = r_0 + r_1x + \dots + r_nx^n$, $n(f(x)) = r_0 + r_1\varepsilon + \dots + r_n\varepsilon^n$

Es decir, los elementos del cuerpo $L = k[x]/(p(x))$ son expresiones polinómicas en

ε . Entonces: $L \subseteq k[\varepsilon] \subseteq k(\varepsilon)$. Ahora bien, como L es cuerpo, será $k(\varepsilon) \subseteq L$, por tanto:

$$\left. \begin{array}{l} L \subseteq k(\varepsilon) \\ k(\varepsilon) \subseteq L \end{array} \right\} \rightarrow L = k(\varepsilon)$$

El polinomio $p(x) = a_0 + a_1x + \dots + a_sx^s$ pertenece a la clase 0 de L (por pertenecer al

ideal $(p(x))$). Es decir, se tiene por una parte que $n(p(x))=0$, y por otra parte se tiene que $n(p(x))=a_0 + a_1\varepsilon + \dots + a_s\varepsilon^s$. Por tanto: $a_0 + a_1\varepsilon + \dots + a_s\varepsilon^s = 0$, de lo cual deducimos que $\varepsilon \in L$ es algebraico sobre k y además admite a ε como cero lo que implica que L es el cuerpo de ruptura de $p(x)$.

Si existieran dos cuerpos de ruptura, $k(a)$ y $k(b)$, ambos, por ser isomorfos a $k[x]/(p(x))$ serían isomorfos entre sí. Son, efectivamente, k -isomorfos en el k -isomorfismo g tal que $g(c_0 + c_1a + \dots + c_r a^r) = c_0 + c_1b + \dots + c_r b^r$.

Corolario 01: Dado un polinomio $p(x) \in k[x]$ irreducible en k , existe siempre una extensión L/k , obtenida mediante una sucesión de extensiones algebraicas simples, sobre la que $p(x)$ se descompone totalmente en factores lineales.

Demostración:

a) Si sobre un primer cuerpo de ruptura $L_1(\varepsilon_1)$, el polinomio $p(x)$ se descompone en factores lineales irreducibles ya está resuelta la cuestión. $\square$

b) En caso contrario, sea $L_2 = L_1(\varepsilon_2)$ el cuerpo de ruptura de uno de los factores irreducibles no lineales, $p_1(x)$, y realizamos la descomposición de $p_1(x)$ en factores irreducibles sobre L_2 . Ahora aparecerán más factores lineales que en la descomposición sobre L_1 .

La reiteración de este procedimiento conduce, al cabo de un número finito de operaciones a una extensión finita L/k sobre la que $p(x)$ se descompone totalmente en factores lineales.

02. La clausura algebraica

Teorema 02: Consideremos un cuerpo k y su anillo de polinomios $k[x]$. Existe una extensión algebraica $\bar{k}$ del cuerpo k en la que cualquier polinomio de dicho anillo se descompone en factores lineales, minimal para esta propiedad y algebraicamente cerrada.

Demostración:

Sea el polinomio $P(x) = a_0 + a_1x + \dots + a_nx^n$ y llamemos

$$p(x) = \frac{P(x)}{a_n} = \frac{a_0}{a_n} + \frac{a_1}{a_n}x + \dots + x^n = b_0 + b_1x + \dots + b_nx^n$$

por tanto. $p(x) = b_0 + b_1x + \dots + b_nx^n$.

Llamemos $K' = K(x)$ al cuerpo de las funciones racionales con coeficientes en K .

Introduzcamos el conjunto $\{y_{ij}\}$ de indeterminadas de dos índices, i y j , de los cuales el primero recorre todo $K[x]: p_i(x) \in K[x]$, y el segundo recorre el conjunto $\{1, 2, \dots, n_i\}$ donde $n_i = \text{grad } p_i(x)$.

Así, por ejemplo, al polinomio $p_s(x)$ le corresponden las indeterminadas

$$\{y_{s1}, y_{s2}, \dots, y_{sn_s}\}$$

Si es $\text{grad } p_2(x) = 4$, le corresponderán

$$\{y_{21}, y_{22}, y_{23}, y_{24}\}$$

Lo que se ha hecho, realmente, es construir una indeterminada por cada raíz de cada polinomio de $K[x]$.

Sea $D = K[y_{ij}]$ el anillo de polinomios con coeficientes en K' , con respecto a las indeterminadas y_{ij} , y consideremos el ideal A de D engendrado por los polinomios $f_i(x)$ de expresión:

$$f_i(x) = p_i(x) - (x - y_{i1}) \cdot (x - y_{i2}) \dots (x - y_{in_i})$$

El elemento neutro e de K no pertenece al ideal A , pues si $e \in A$, sería e combinación lineal de un número r de polinomios $f_i(x)$ de A :

$$e = \sum_{i=1}^r \mu_i f_i(x) = \mu_1 f_1(x) + \mu_2 f_2(x) + \dots + \mu_r f_r(x)$$

si damos a y_{ij} los valores de las j raíces de $f_i(x)$, se tiene que $f_i(x) = 0$ y, por tanto, es

$$e = \sum_{i=1}^r \mu_i f_i(x) = 0$$

lo cual es falso, pues sabemos que en todo cuerpo es $e \neq 0$.

De esto se deduce que e no es elemento del ideal A y, por tanto, es $A \neq D$.

Como la familia $I(D)$ de los ideales de D es U-inductiva, existirá, por el Lema de Zorn, un ideal maximal:

$$\exists m \in I(D) / \forall A \in I(D), A \subseteq m$$

Y, puesto que D tiene elemento unidad, $E = D/m$ es un cuerpo. Es el cuerpo de las clases (módulo m) de elementos de D .

Se tiene, además, que $\forall h_1, h_2 \in K / h_1 - h_2 = z \neq 0$, entonces h_1, h_2 pertenecen a clases diferentes pues, caso contrario, será

$$h_1 - h_2 = z \in E, z z^{-1} = e \in m$$

de lo cual $D = m$, contra la hipótesis de ser D distinto de m .

Luego, elementos diferentes de K pertenecen a clases diferentes de $E = D/m$ lo que implica que E contiene un subcuerpo isomorfo a K , es decir, se trata de una extensión de K .

Sea ahora q_{ij} la clase de E que contiene a y_{ij} y sea L el cuerpo de adjunción $K(q_{ij})$.

Si $f_i(x) \in m$, entonces $f_i(x)$ pertenece a la clase cero del cuerpo E:

$$p_i(x) = (x - q_{i1})(x - q_{i2}) \dots (x - q_{in_i})$$

Al ser $\{q_{ij}\}$ algebraicos sobre K y $L = K(q_{ij})$, será L extensión algebraica de K.

También L es elemento minimal de la clase de las extensiones algebraicas de K tales que en ellas se descompone en factores lineales todo elemento de $K[x]$, pues al haber sido construido L como cuerpo de adjunción $K(q_{ij})$ se tiene que cualquier cuerpo K' intermedio, $K \subseteq K' \subseteq L$, no contiene a todos los q_{ij} , lo que implica que existen polinomios de $K[x]$ que no se descomponen en factores lineales sobre el cuerpo K' .

Luego, es L extensión algebraica de K en la que todo polinomio de $K[x]$ se descompone en factores lineales y es además minimal entre las que tienen esta propiedad.

Veamos que el cuerpo $L = K(q_{ij})$ es también algebraicamente cerrado. Sea $f(x) \in K[x]$ un polinomio irreducible en L tal que $\text{grado } f(x) > 1$ y comprobemos que esto es contradictorio.

Sea $z \in H$ un cero de $f(x)$ en un cuerpo de ruptura H de $f(x)$: $K \subseteq L \subseteq H$.

Es decir, $z \in H$ es algebraico sobre L y, por tanto, es algebraico sobre K. Esto implica que z verifica una ecuación $g(x) = 0$ irreducible en el cuerpo K, y, por consiguiente, $f(x)$ divide a $g(x)$. Pero, por la construcción del cuerpo L ($L = K(q_{ij})$) sabemos que $g(x)$ se descompone en L en factores lineales. Luego es contradictorio.

Por tanto, no existe un polinomio $f(x) \in K[x]$ de grado mayor que 1 que sea irreducible en L, lo que implica que L es algebraicamente cerrado.

Y recíprocamente, una extensión de L que sea algebraicamente cerrada es extensión minimal del cuerpo K entre las que son algebraicas y verifican que en ellas se descompone en factores lineales todo polinomio de $K[x]$. Para comprobarlo, consideremos una de tales extensiones H/K tal que $K \subseteq H \subseteq L$. Debe ser necesariamente $H=L$, pues, caso contrario, sea $d \in L-H$ y $f(x)$ el polinomio irreducible de $K[x]$ anulado por d. Este polinomio no puede descomponerse en H en factores lineales, luego $H=L$. Con esto termina la demostración.

Teorema 03: Sea E/K una extensión algebraica y sea $g: K \rightarrow L$ una inmersión de K en un cuerpo algebraicamente cerrado L. Existe entonces una prolongación de g a una inmersión de E en L. Además, si E es algebraicamente cerrado y L es algebraico sobre gK , entonces toda prolongación de este tipo de g es un isomorfismo de E en L.

Demostración:

Sea S el conjunto de todos los pares (F, T) , donde $F \subseteq E$ es un subcuerpo de E , que contiene a K , y T es una extensión de g a una inmersión de F en L . $\square$

Si $(F, T), (F', T')$ son dos de tales pares, podemos definir la relación de orden:

$$(F, T) \leq (F', T') \leftrightarrow \begin{cases} 1^\circ) F \subseteq F' \\ 2^\circ) \text{Restricción de } T' \text{ a } F = T \end{cases}$$

El conjunto S es no vacío, pues contiene a (K, g) y, además, es inductivo:

Si $\{(F_i, T_i)\}$ es una cadena de S , bastará hacer $F = \bigcup F_i$ y definiremos $T: F \rightarrow L$ tal que la restricción de T a F_i coincida con T_i .

$\square$ El par (F, T) , construido de este modo, es, pues, mayorante mínimo de la cadena $\{(F_i, T_i)\}$, por lo que S es U-inductivo. $\square$

Aplicando a S el Lema de Zorn, existe al menos un elemento maximal $(H, \lambda) \in S$, donde λ es una prolongación a H de la inmersión g y, como veremos a continuación, es $H = E$. Pues, caso contrario, sería:

Si $H \neq E \rightarrow \exists d \in E / d \notin H$ y d anula a un polinomio irreducible $f(x) \in K[x]$.

Entonces: $g(f(x)) = f'(x) \in L[x]$

Y sea $q \in L$ tal que $f'(q) = 0$ (q existe siempre en L , pues L es algebraicamente cerrado).

Prolonguemos λ a λ' siendo $\lambda': H(d) \rightarrow L$ de modo que

$$g(c_0 + c_1 d + \dots + c_n d^n) = c_0' + c_1' q + \dots + c_n' q^n$$

Es claro, entonces, que

$$a) (H(d), \lambda') \in S$$

$$b) (H, \lambda) < (H(d), \lambda')$$

Pero esto se contradice con el hecho de que (H, λ) es elemento maximal de S . Luego, efectivamente, es $H = E$.

Es decir, (E, λ) es elemento maximal de S , y queda probada la primera parte de la proposición.

Para probar la segunda parte supongamos que E es algebraicamente cerrado; en este caso tanto λE como L son algebraicamente cerrados (λE lo es por ser isomorfo a E , y L lo es por hipótesis).

Pero sabemos que tiene carácter minimal toda extensión algebraica de K que sea algebraicamente cerrada, entre todas las extensiones algebraicas de K que

descompongan en factores lineales todo polinomio de $K[X]$. Por tanto es $\lambda E = L$ y los cuerpos E y L resultan ser isomorfos.

Corolario 02: Sea el cuerpo k y dos extensiones algebraicas de k , F y F' . Si tales extensiones son algebraicamente cerradas, entonces existe un isomorfismo $h: F \rightarrow F'$ que induce la identidad sobre k , es decir, existe un k -isomorfismo.

Demostración:

Es inmediato de la proposición anterior.

De este corolario se deduce que toda extensión algebraica de K que sea algebraicamente cerrada es única, salvo isomorfismo. Ese carácter de unicidad da sentido a la definición de clausura algebraica como una extensión algebraica de K que sea algebraicamente cerrada.

03. Cuerpo de descomposición. Extensiones normales

Sea k un cuerpo y sea $k[X]$ su anillo de polinomios. Sea asimismo L un supercuerpo de k , esto es, un cuerpo del cual k es subcuerpo. Llamaremos a L *cuerpo de descomposición* del polinomio $p(x) \in k[X]$ si se verifican las dos condiciones siguientes:

- El polinomio $p(x)$ se descompone en $L[X]$ en factores lineales.
- Si k' es un cuerpo intermedio, $k \subseteq k' \subseteq L$, $p(x)$ no se descompone en $k'[X]$ en factores todos lineales.

Si consideramos una familia de polinomios de $k[X]$, $\{p_i(x)\}_{i \in I}$, todos de grado mayor o igual que la unidad, y donde I es un conjunto de índices, llamaremos cuerpo de descomposición de tal familia a un cuerpo L , extensión de k , tal que cada polinomio $p_i(x)$ se descompone en $L[X]$ en factores lineales, sin que tal propiedad la tenga ningún otro cuerpo intermedio k' , $k \subseteq k' \subseteq L$.

Un cuerpo N , extensión de k , N/k , se dice que es *extensión normal* de k , si N es cuerpo de descomposición de una familia de polinomios de $k[X]$.

Obviamente, si $p(x) \in k[X]$ se descompone en factores lineales en $k[X]$, entonces el mismo k es cuerpo de descomposición de $p(x)$. Y caso de que no se descomponga en factores lineales en $k[X]$, siempre se descompondrá en factores lineales en $\bar{k}[X]$, donde es $\bar{k}$ la clausura algebraica de k .

En el siguiente teorema veremos que el cuerpo de descomposición de una familia de polinomios se obtiene adjuntando las raíces al cuerpo de los coeficientes.

Teorema 04: Sea L/k una extensión en la que el polinomio $p(x) \in k[X]$ se descompone totalmente en factores lineales. Si las raíces de dicho polinomio son $\{r_1, \dots, r_n\}$ entonces su cuerpo de descomposición es $D = k(r_1, \dots, r_n)$.

Si $\{r_j\}_{j \in J}$ es la familia de las raíces de la colección $\{p_i(x)\}_{i \in I}$ de polinomios de $k[x]$, raíces que obviamente están en la clausura algebraica $\bar{k}$, entonces su cuerpo de descomposición es $D = k(r_j)$, $j \in J$.

Demostración:

Es obvio que si $D = k(r_1, \dots, r_n)$ entonces $p(x) \in k[x]$ se descompone en D en factores lineales, ya que D contiene por adjunción todas sus raíces.

Veamos que no existe otro cuerpo k' intermedio, $k \subseteq k' \subseteq D = k(r_1, \dots, r_n)$, tal que en $k'[x]$ el polinomio $p(x)$ se descompone también en factores lineales.

Supongamos que esto fuera posible. Como $L[x]$ es anillo de factorización única, coincidirán las factorizaciones de $p(x)$ en $k'[x]$ y en $L[x]$. Por tanto, tendría que ser $\{r_1, \dots, r_n\} \subset k'$, con lo que $k(r_1, \dots, r_n) \subseteq k'$, y como por hipótesis del teorema se da la inclusión contraria, $k \subseteq k' \subseteq D = k(r_1, \dots, r_n)$, será $k' = k(r_1, \dots, r_n) \rightarrow k' = D$ y $D = k(r_1, \dots, r_n)$ es, por consiguiente, cuerpo de descomposición del polinomio.

De forma análoga probamos que $D = k(r_j)$, $j \in J$ es el cuerpo de descomposición de la familia de polinomios $\{p_i(x)\}_{i \in I}$.

La consecuencia inmediata es que el cuerpo de descomposición de una familia de polinomios, y, en particular, toda extensión normal, es una extensión algebraica.

En cuanto a la posibilidad de que dos cuerpos distintos, L y L' , sean cuerpos de descomposición de un mismo polinomio, veamos que existe un isomorfismo de cuerpos, que concretamos en el siguiente teorema.

Teorema 05: Si son L y L' cuerpos de descomposición del polinomio $p(x) \in k[x]$ existen un k -isomorfismo $\varphi: L \rightarrow L'$.

Si es $k \subseteq L \subseteq \bar{k}$, donde es $\bar{k}$ la clausura algebraica de k , entonces toda k -inmersión de L' en $\bar{k}$ es un k -isomorfismo $\varphi': L' \rightarrow L$.

Demostración:

Sea $\bar{L}$ clausura algebraica de L , lo que implica que $\bar{L}$ es extensión algebraica de k y clausura algebraica de L . Existe, por tanto, una k -inmersión $\varphi: L' \rightarrow \bar{L}$, teniéndose en $L'[x]$ la factorización

$$p(x) = c(x - a_1) \dots (x - a_n), \quad c \in k, a_i \in L'$$

y como es $\varphi(p(x)) = p(x)$ será:

$$\varphi(p(x)) = p(x) = c(x - \varphi(a_1)) \dots (x - \varphi(a_n)) = c(x - a_1) \dots (x - a_n)$$

con lo que los conjuntos $\{a_1, \dots, a_n\}$ y $\{\varphi(a_1), \dots, \varphi(a_n)\}$ coinciden, salvo permutación, por lo que $\varphi L' = k(\varphi(a_1), \dots, \varphi(a_n)) = k(a_1, \dots, a_n) = L$.

Esto permite enunciar un corolario inmediato.

Corolario 03: Sea la familia $\{p_i(x)\}_{i \in I}$ de polinomios de $k[x]$. Si son L y L' cuerpos de descomposición de esta familia, entonces, toda k -inmersión $\gamma: L' \rightarrow \bar{L}$ es un k -isomorfismo de L' en L .

En efecto, pues si L' y L son cuerpos de descomposición de la familia entonces L' contiene un único cuerpo L'_i de descomposición del polinomio $p_i(x)$, y, asimismo,

L contiene también un único cuerpo de descomposición, L_i , para el mismo polinomio $p_i(x)$.

Por el anterior teorema, toda k -inmersión de L'_i en la clausura algebraica de k aplica L'_i en L_i y por tanto aplica L' en L , y tal aplicación es sobreyectiva, pues L es el compuesto de los L_i , por lo que la inmersión $\gamma: L' \rightarrow \bar{L}$ es un k -isomorfismo de L' en L .

El siguiente teorema relaciona las extensiones normales con los automorfismos del grupo de Galois y también con la descomposición de un polinomio en factores lineales.

Teorema 06: Sea L/k un extensión algebraica contenida en la clausura algebraica, $\bar{k}$, del cuerpo k . Los siguientes enunciados son equivalentes:

- L/k es una extensión normal.
- Toda k -inmersión, $\varphi: L \rightarrow \bar{k}$, de L en la clausura algebraica de k es un automorfismo de k .
- Todo polinomio irreducible de $k[x]$ que tiene una raíz en L se descompone en factores lineales en $L[x]$.

Demostración:

a) $\rightarrow$ b): Sea la extensión L/k tal que está contenida en la clausura algebraica $\bar{k}$ de k . O sea, $L \subseteq \bar{k}$.

Sea $\{p_i(x)\}_{i \in I}$ una familia de polinomios con coeficientes en k , $p_i(x) \in k[x]$, $i \in I$, tales que es L el cuerpo de descomposición de los $p_i(x)$, $i \in I$.

Consideremos la k -inmersión $\varphi: L \rightarrow \bar{k}$, esto es, una aplicación inyectiva que deja invariantes los elementos de k ,

$$\forall a \in L, \varphi(a) \in \bar{k}, \text{ tal que si } \beta \in k \subseteq L, \varphi(\beta) = \beta \in \bar{k}$$

Esto quiere decir que si $p_i(x) \in k[x]$, $\varphi(p_i(x)) = p_i(x)$.

Si $\alpha \in L$ es raíz de $p_i(x)$, entonces $\varphi(\alpha)$ es raíz de $\varphi(p_i(x)) = p_i(x)$, y como $p_i(x)$ se descompone en factores lineales en $L[x]$, entonces $\varphi(\alpha) \in L$.

Ahora bien, L está engendrado por la adjunción a k de las raíces $\{d_j\}_{j \in J}$ de la familia de polinomios $\{p_i(x)\}_{i \in I}$, luego φ aplica L en sí mismo, por lo que es un k -automorfismo de L .

b) $\rightarrow$ c): Sea $p(x) \in k[x]$ un polinomio irreducible en k , y sean a y b dos raíces de $p(x)$ en L .

Si consideramos las extensiones simples $k(a)$ y $k(b)$, vemos que existe isomorfismo $\varphi: k(a) \approx k(b)$ tal que deja invariante a k y aplica a en b :

$$\begin{aligned} \forall c \in k, \varphi(c) &= c \\ \varphi(a) &= \varphi(b) \end{aligned}$$

Tal isomorfismo puede extenderse a una inmersión de L en $\bar{k}$

$$\varphi: L \rightarrow \bar{k}$$

que será k -automorfismo de L y $\varphi(a) = b \in L$, con lo que toda raíz de $p(x)$ está en L . Esto es, $p(x)$ se descompone en factores lineales en $L[x]$.

c) $\rightarrow$ a): Sea $p_a(x) \in k[x]$ un polinomio irreducible en k que tiene la raíz $a \in L$. Por c) sabemos que $p_a(x)$ se descomponen en $L[x]$ en factores lineales. Por consiguiente es L el cuerpo de descomposición de la familia $\{p_a(x)\}_{a \in k}$ de polinomios de $L[x]$, lo que implica que L/k es extensión normal.

04. Bibliografía

01. Artin, E., "Teoría de Galois". Vicens-Vives, 1970.
02. Atiyah, M.F., Macdonald, I.G., "Introducción al Álgebra conmutativa". Ed. Reverté.
03. Carrega, J.C., "Théorie des corps. La règle et le compas". Hermann, Paris, 1981.
04. Childs, L.N., "A Concrete Introduction to Higher Algebra". Springer UTM, New York, 1979.
05. Dorronsoro, J. y Hernández, E., "Números, grupos y anillos". Addison-Wesley./Universidad Autónoma de Madrid, 1996.
06. Garling, D.J.H., "A course in Galois Theory". Cambridge University Press.
07. Herstein, I. N., "Álgebra moderna : grupos, anillos, campos, teoría de Galois". Ed. Trillas, México, 1973.
08. Kostrikin, A. I., "Introducción al álgebra". McGraw-Hill, Madrid, 1992.
09. Lang, S., "Álgebra". Ed. Aguilar, Madrid, 1971.
10. Milne, J.S., "Fields and Galois Theory",
<http://www.jmilne.org/math/CourseNotes/math594f.html>
11. S. Chinae, C., "Extensiones Algebraicas",
http://casanchi.com/mat/ext_algebraicas.pdf
12. Stewart, I., "Galois Theory". Chapman and Hall, London, 1973.
13. Van der Waerden, B.L., "Modern Algebra" Vol I. Frederick Ungar, New York, 1964.
14. Xambó Descamps, S., Delgado de la Mata, F. y Fuertes, C., "Introducción al Álgebra: anillos, factorización y teoría de cuerpos". Universidad de Valladolid. Manuales y Textos Universitarios. Ciencias nº 29, 1998.