EXTENSIONES ALGEBRAICAS

1. Introducción:

Conocemos el concepto de cuerpo como una estructura algebraica definida con dos leyes de composición interna, concepto que se expone en otros artículos que figuran en esta misma Web (Ver ***Cuerpos. Extensiones de un cuerpo***, o también, ***Extensiones Trascendentes de un cuerpo***). Conocemos también el concepto de subcuerpo de un cuerpo dado y que la familia $\mathcal{F}_L$ de los subcuerpos de un cuerpo L verifica las condiciones de definición de una familia de Moore:

$$1) \quad L \in F_L$$
$$2) \quad \forall P \subseteq F_L, \bigcap \{H : H \in P\} \in F_L$$

A la familia de Moore $\mathcal{F}_L$ de los subcuerpos de L está asociada, pues, la aplicación llamada *Clausura de Moore M*:

$$\forall X \in L, M(X) \equiv \overline{X} = \bigcap \{H : H \in F_L \ \wedge X \subseteq H\}$$

La Clausura de Moore de una parte X del cuerpo L es, por tanto, el mínimo subcuerpo $\overline{X}$ de L que contiene a X.

Se tiene, además, que, precisamente por ser familia de Moore, es $\mathcal{F}_L$ retículo completo, cuyos elementos mínimos y máximo son, respectivamente, el subcuerpo primo Π_L y el mismo cuerpo L:

$$\min(F_L) = \Pi_L$$
$$\max(F_L) = L$$

Conocemos también, del tema anterior, el concepto de extensión de un cuerpo, junto con la subdivisión de las extensiones en dos clases excluyentes entre sí:

- Extensiones Trascendentes.
- Extensiones Algebraicas.

Se entenderá, pues, en adelante, que un cuerpo L es extensión de un cuerpo K, si L contiene un subcuerpo K' que es isomorfo a K.

Es claro que si L es supercuerpo del cuerpo K, es L extensión de K, pues contiene un subcuerpo (el mismo K) isomorfo a K (isomorfismo identidad).

Además, si L es extensión del cuerpo K, es inmediato que L es espacio vectorial sobre el cuerpo K:

$$(L,+,.K)$$

y la dimensión de este espacio vectorial se llama *grado de la extensión*, que acostumbramos a representar por (L:K) o bien por (L/K):

$$(L\,/\,K) = \dim(L,+,.k)$$

Notación empleada también para indicar, simplemente, que es L extensión de K.

Se dirá que L es extensión infinita de K si $(L/K) = +\infty$. Caso contrario, si $(L/K) \neq +\infty$ diremos que L es *extensión finita* de K.

Si $H \in F_L$ y es *S* una parte de *L*, el mínimo subcuerpo de *L* que contiene a *H* y a *S* se llama extensión de *H* por adjunción de *S* y se representa por *H(S).* Sabemos también que es $H(S_1 \cup S_2) = H(S_1)(S_2)$.

Si la parte S tiene un solo elemento, S={a} la extensión H(S) se llama *extensión simple de H.* De acuerdo con lo afirmado en el anterior párrafo, se tendrá:

$$H(a_1, a_2, \ldots, a_n) = H(a_1)(a_2)\ldots(a_n)$$

Es decir, la extensión de un cuerpo *H* por adjunción de un conjunto finito *A* de *n* elementos, $A=\{a_1,a_2,\ldots,a_n\}$ es la extensión de *H* por sucesivas adjunciones de los *n* elementos de *A*.

Señalemos que la extensión simple *H(a)* es realmente la familia de cocientes

$$H(a) = \{p(a)/q(a) : p(x), q(x) \in H[x] \wedge q(a) \neq 0\}$$

donde *p(x)* y *q(x)* son polinomios del anillo *H[x].*

También, el mínimo subanillo de *L* que contiene a *a*, denotado por *H[a]*, es

$$H[a] = \{p(a) : p(x) \in H[x]\}$$

Naturalmente, siempre es $H[a] \subseteq H(a)$, y, en algunos casos que analizaremos más adelante se da el caso de igualdad: $H[a] = H(a)$.

Dados dos cuerpos, L y H, la adjunción L(H) (o bien H(L)) la representaremos por LH, o sea:

$$LH \equiv L(H) = H(L)$$

Estudiaremos a continuación las extensiones algebraicas de un cuerpo de forma general, tanto las propiedades de los grados de las extensiones componentes de torres de cuerpos, que inmediatamente definiremos, como el carácter de esta clase de extensiones, que también concretaremos mediante definición formalizada.

DEFINICION 1.

Una torre de cuerpos es una sucesión de cuerpos $k_1 \subset k_2 \subset \ldots \subset k_n$ tal que cada k_{i+1} es extensión de k_i. (i=1, ..., n-1).

DEFINICION 2.

Sea T una clase de cuerpos, cada uno de ellos extensión del cuerpo K (es decir, cada uno de ellos conteniendo un subcuerpo K' isomorfo a K):

$$T = \left\{ L_1/k , L_2/k , \ldots , L_n/k , \ldots \right\}$$

Se dice que T es clase distinguida entre todas las clases posibles cuyos elementos son cuerpos extensiones de K, si T cumple las condiciones siguientes:

1) Para la torre $K \subset L_i \subset L_j$ se cumple siempre que

$$L_j/k \in T \Leftrightarrow \begin{cases} L_i/K \in T \\ L_j/L_i \in T \end{cases}$$

2) Dados dos subcuerpos, H y S, de un cuerpo L, ambos extensiones de K, se cumple que

$$H/K \in T \Rightarrow HS/S \in T$$

3) Si son $L_r , L_s \subseteq L$ entonces $L_r/K , L_s/K \in T \Rightarrow L_r L_s/K \in T$

DEFINICION 3:

Una *inmersión* $s : K \to L$ del cuerpo K en L es un monomorfismo de K en L. Si $K \subseteq E$ una aplicación $t : E \to L$ se dice que es una *prolongación o extensión* de s si la restricción de t a K coincide con s .

2. **Extensiones algebraicas:**

DEFINICION 4:

Si el cuerpo L es una extensión de K, se dice que $t \in L$ es *algebraico* sobre K sii existen elementos a_0, ..., a_n de K, no todos nulos $(n \geq 1)$ tales que

$$a_0 + a_1.t + \ldots + a_n.t^n = 0$$

Una extensión *L* de *K* se dice que es *algebraica* si todo elemento de L es algebraico sobre K.

Es claro que $\forall t \in K$, t es algebraico sobre el cuerpo *K*, pues verifica la ecuación polinómica

$$X - t = 0$$

es decir, existen coeficientes, *x, -1* de *K* tales que $x - t = 0$

PROPOSICION 1:

Sea *L* una extensión del cuerpo *K*. Entonces, si $t \in L$ es algebraico sobre K, la familia de los polinomios de *K[x]* que se anulan para $x = t$, es decir, el conjunto $I = \{f(x) / f(x) \in K[x], f(t) = 0\}$, es un ideal principal engendrado por un polinomio p(x) irreducible tal que si $t \in K$, es *grado p(x) = 1*, y si $t \notin K$ entonces es *grado p(x)* ³ *2*. Se verifica también que: $K[x]/(p(x)) \approx K[t] = K(t)$, siendo *K(t)* una extensión finita de K.

En efecto:

a) sean *f(x)* y *g(x)* dos polinomios del anillo *K[x]* que se anulan para $x = t$. Esto quiere decir que $f(t) = 0$ y que $g(t)=0$, por lo cual, si es *I* el conjunto de los polinomios que se anulan para $x = t$:

$$\begin{cases} f(t) - g(t) = 0 \\ f(t).g(t) = 0 \end{cases} \Rightarrow \begin{cases} f(x) - g(x) \in I \\ f(x).g(x) \in I \end{cases} \Rightarrow I \text{ ideal de } K[x]$$

b) Al ser *K[x]* un anillo principal, todos sus ideales son principales, por lo cual el conjunto I de los polinomios que se anulan en $x = t$ es un ideal principal, esto es, está engendrado por un polinomio irreducible *p(x):*

$$\exists p(x) \in K[x] / I = (p(x)),$$

siendo *p(x)* el polinomio de menor grado entre los que se anulan para $x = t$.

Veamos que *p(x)* es irreducible, pues si no lo fuera se tendría que

$$\exists h(x),\ l(x) \in K[x] \,/\, p(x) = h(x).l(x) \Rightarrow p(t) = h(t).l(t) = 0 \Rightarrow$$

$$\Rightarrow h(t) = 0 \wedge l(t) = 0 \wedge grad\ h(x) < grad\ p(x) \wedge grad\ l(x) < grad\ p(x) \Rightarrow$$

$\Rightarrow$ p(x) no es el polinomio de menor grado que se anula para x = t $\Rightarrow$ contradicción.

Luego, p(x) es irreducible.

Si es a_s el coeficiente director del polinomio p(x), llamaremos *polinomio irreducible de t sobre K* al polinomio

$$I_{rr}(t, K, x) = \frac{1}{a_s} p(x)$$

c) Sea la aplicación $F : K[x] \to K[t]$ definida por

$$\forall f(x) \in K[x],\ F(f(x)) = f(t)$$

es inmediato que F es homomorfismo sobreyectivo, y se tiene que

$$Ker\ F = \{m(x) \in K[x] \,/\, m(t) = 0\} = (p(x))$$

y su descomposición canónica:

$$\begin{array}{ccc} K[x] & \xrightarrow{\ F\ } & K[t] \\ n \downarrow & & \uparrow i \\ & b & \\ K[x]/(p(x)) & \approx & K[t] \end{array}$$

por tanto:

$$K[t] \approx K[x]/(p(x))$$

d) Puesto que *p(x)* es irreducible y *K[x]* es anillo principal, el ideal *I=(p(x))* es un ideal maximal. Y puesto que *K[x]* tiene elemento unidad ello implica que

$$\begin{cases} K[x]/(p(x))\ cuerpo \\ K[t] \approx K[x]/(p(x)) \end{cases} \Rightarrow K[t]\ cuerpo$$

Es decir, *K[t]* es un cuerpo que contiene a *K* y a *t* $\Rightarrow K(t) \subseteq K[t]$.

Y como se tiene siempre que $K[t] \subseteq K(t)$, se deduce que es $K[t] = K(t)$.

La igualdad anterior nos indica que todo elemento de la extensión simple *K(t)* es una expresión polinómica con coeficientes en el cuerpo *K.* Veamos que se trata de una extensión finita de K.

$$\forall e \in K(t) \Rightarrow e \in K[t] \Rightarrow e = e(t)$$

Dividiendo $e(x)$ por *p(x)*: $e(x) = p(x).q(x) + r(x)$, y para $x = t$ se tiene:

$$e(t) = p(t).q(t) + r(t) = 0 + r(t) = r(t)$$

Si es *n = grad (p(x)),* entonces $grad\ e(t) = grad\ r(t) \leq n - 1$, o sea, es:

$$e(t) = a_0 + a_1.t + \ldots + a_{n-1}.t^{n-1}$$

por tanto, $\forall e(t) \in K(t)$, $e(t)$ es combinación lineal de los monomios $\{1, t, \ldots, t^{n-1}\}$, que son linealmente independientes y, por tanto, una base del espacio vectorial $(K(t), K, +, .K)$.

En definitiva, $\dim(K(t), +, .K) = (K(t) / K) = n$, por lo cual L es extensión finita de K.

3. Extensiones finitas:

PROPOSICION 2:

Si *L* es extensión finita de *K*, entonces *L* es extensión algebraica de *K*.

En efecto:

L extensión finita de *K* $\Rightarrow (L/K) = n \Rightarrow \{1, t, ..., t^{n-1}\}$ es una base del espacio vectorial dado por $(L, +, \circ K) \Rightarrow \{1, t, ..., t^{n-1}\}\ lineal.\ indep \Rightarrow \forall t \in K, \exists \{a_1, a_2, ..., a_n\} \subseteq K / \sum_{i=1}^{n} a_i t^i = 0$

Y es alguno de los $a_i \neq 0 \Rightarrow$ t es algebraico sobre K $\Rightarrow (L/K)$ algebraica.

PROPOSICIÓN 3:

Sea $K_1 \subset K_2 \subset K_3$ una torre de cuerpos. Se verifica que

$$(K_3 : K_1) = (K_3 : K_2).(K_2 : K_1)$$

En efecto:

1) Sean $\{a_1, a_2, \ldots, a_r\}$ *r* elementos de K_3 linealmente independientes sobre K_2 $(r \leq (K_3 : K_2))$.

   Sean $\{b_1, b_2, \ldots, b_s\}$ s elementos de K_2 linealmente independientes sobre K_1 $(s \leq (K_2 : K_1))$.

Los *r.s* elementos $\{a_i b_j\}$ pertenecen a K_3 y son linealmente independientes sobre k_1:

a) por ser $a_i \in K_3,\ b_j \in K_2 \subseteq K_3 \Rightarrow a_i.b_j \in K_3$

b) de ser $\sum_{i,j} l_{ij} a_i b_j = 0,\ l_{ij} \in K_1 \Rightarrow \sum_{i=1}^{r} \left(\sum_{j=1}^{s} l_{ij} b_j \right) a_i = 0$, y siendo los a_i independientes sobre K_2 y $\sum_{j=1}^{s} l_{ij} b_j \in K_2 \Rightarrow \sum_{j=1}^{s} l_{ij} b_j = 0$ y los bj independientes sobre K1 $\Rightarrow l_{ij} = 0,\ \forall ij$.

Por tanto, al ser los *r.s* elementos $\{a_i b_j\}$ linealmente independientes sobre *K1*, se tiene que:

$$r.s \leq (K_3 : K_1)$$

Lo que hemos probado, por consiguiente, es:

$$\left.\begin{array}{l} r \le (K_3 : K_2) \\ s \le (K_2 : K_1) \end{array}\right\} \Rightarrow r.s \le (K_3 : K_1)$$

2) Si uno al menos de los r o s es infinito, es decir, si es $r = \infty$ o bien $s = \infty$, entonces:

$$r.s = \infty \le (K_3 : K_1) \Rightarrow (K_3 : K_1) = \infty$$

o sea:

$$r.s = (K_3 : K_1)$$

o bien:

$$(K_3 : K_2).(K_2 : K_1) = (K_3 : K_1)$$

y la proposición quedaría probada para este caso.

3) Si ambos r o s son finitos, se tiene:

$$\begin{cases} r = (K_3 : K_2) \neq \infty \\ s = (K_2 : K_1) \neq \infty \end{cases}$$

y de 1):

$$r.s \le (K_3 : K_1)$$

Además, $\forall x \in K_3$, $x = \sum_{i=1}^{r} d_i a_i$, $d_i \in K_2$ ($pues \{a_1, a_2, \ldots, a_r\}$ es una base de K_3).

También, $\forall d_i \in K_2$, $d_i = \sum_{i=1}^{r} l_{ij} b_j$, $l_{ij} \in K_1$ ($pues \{b_1, b_2, \ldots, b_s\}$ es una base de K_2).

Por tanto:

$\forall x \in K_3$, $x = \sum_{i=1}^{r} \left(\sum_{j=1}^{s} l_{ij} b_j \right) a_i = \sum_{i,j=1}^{rs} l_{ij} a_i b_j \Rightarrow \{a_i b_j\}$ son generadores de K_3, y, al ser linealmente independientes $\Rightarrow \{a_i b_j\}$ es base de $(K_3 : K_1)$

Entonces:

$$r.s = (K_3 : K_1)$$

o bien

$$(K_3 : K_2).(K_2 : K_1) = (K_3 : K_1)$$

COROLARIO 1:

1) Para una torre $K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n$ de n cuerpos se tiene:

$$(K_n : K_1) = (K_n : K_{n-1}) \ldots (K_2 : K_1)$$

2) El cuerpo $L = K(a_1, a_2, \ldots, a_n)$ obtenido por adjunción de un número finito n de elementos a_i algebraicos sobre K, es una extensión finita de K.

En efecto:

1) Es inmediato, aplicando recurrencia, del resultado de la proposición 3, pues si

$$(K_{n-1} : K_1) = (K_n : K_{n-1}) \ldots (K_2 : K_1)$$

entonces

$$(K_n : K_{n-1}) = (K_n : K_{n-1}).(K_{n-1} : K_1) = (K_n : K_{n-1}).(K_{n-1} : K_{n-2}) \ldots (K_2 : K_1)$$

2) Llamaremos:

$$K_0, \quad k_1 = K(a_1), \quad K_2 = K(a_1, a_2), \quad \ldots, \quad K_n = K(a_1, \ldots, a_n)$$

y queda la torre:

$$K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$$

Así, pues, se tiene que es: $K_i = K_{i-1}(a_i)$, con a_i algebraico sobre K_{i-1} (por ser algebraico sobre *K*), para *i = 1, 2, ..., n*; por lo tanto, la extensión $(K_i : K_{i-1})$ es finita para *i = 1, 2, ..., n*, de donde se deduce que $K_n = K(a_1, \ldots, a_n)$ es extensión finita de *K*.

PROPOSICION 4:

1) Toda extensión finita *L* de un cuerpo *K* puede obtenerse adjuntando a *K* un número finito de elementos algebraicos.
2) La suma, diferencia, producto y cociente de elementos algebraicos sobre *K* son también algebraicos sobre *K.*
3) Sea la torre $K \subseteq L \subseteq H$ y supongamos *L* extensión algebraica de *K*. Entonces, si $t \in H$ es algebraico sobre L, es también algebraico sobre *K*.

En efecto:

1) Sea L extensión finita de K y $\{q_1, q_2, \ldots, q_n\}$ una base del espacio vectorial $(L, +, \circ K)$, entonces

$$\dim(L, +, \circ K) = (L : K) = n$$

$$\forall e \in L,\ e = a_1 q_1 + \ldots + a_n q_n, \quad a_i \in K \Rightarrow L \subseteq K[q_1, \ldots, q_n] = K(q_1, \ldots, q_n)$$

Ahora bien, por ser $K \subseteq L \quad y \quad q_i \in L, (i = 1, \ldots, n) \Rightarrow K(q_1, \ldots, q_n)$

$$\left.\begin{array}{l} L \subseteq K(q_1, \ldots, q_n) \\ K(q_1, \ldots, q_n) \subseteq L \end{array}\right\} \Rightarrow L = K(q_1, \ldots, q_n)$$

2) Sea L supercuerpo de K y sean $d_1, d_2 \in L$ elementos algebraicos sobre K. Entonces se tiene la torre

$$K \subseteq K(d_1, d_2) \subseteq L$$

donde es $K(d_1, d_2)$ una extensión finita (por corolario 1. 2) y, por tanto, algebraica.

A esta extensión algebraica pertenecen los elementos

$$d_1 + d_2,\ d_1 - d_2,\ d_1.d_2 \ \ y\ d_1 / d_2 \ \ (d_2 \neq 0).$$

que serán, en consecuencia, elementos algebraicos sobre K.

3) $t \in H \ algebraico\ sobre\ K \Rightarrow \exists f(x) \in K[x] / \ f(x) = a_0 + a_1.t + ... + a_n.t^n = 0,\ a_i \in L$

considerando el cuerpo intermedio $N = K(a_1, a_2, ..., a_n)$ será:

$$K \subseteq N \subseteq N(t)$$

Al ser L extensión algebraica de K, los $a_i \in L$ son algebraicos sobre K, *i=0,1, ..., n,* entonces es M extensión finita del cuerpo K, por corolario 1. 2).

Igualmente es *t* algebraico sobre N (puesto que $f(x) \in N[x]$) por lo que es también *N(t)* extensión finita de K, y por la proposición 2, extensión algebraica de K.

PROPOSICIÓN 5:

Toda extensión *L=K(A)* obtenida por la adjunción al cuerpo *k* de un número *A* (finito o infinito) de elementos algebraicos sobre *K*, es una extensión algebraica de *K.*

En efecto:

a) Si A es finito, por proposición 4 es *L=K(A)* una extensión finita de K, y, por proposición 2, una extensión algebraica de K.

b) Si A es infinito, sea *H* un supercuerpo común a *K* y a *A* y sea *L=K(A)* el cuerpo obtenido de *K* por adjunción de *A*.

   Si es $F = \{d_1, d_2, ..., d_n\}$ una parte finita de *A*, se tendrá que $K(F) \subseteq K(A) = L$.

   Llamando *F(A)* a la familia de las partes finitas de *A,* sea su reunión:

$$R = U\{K(F) / F \in F(A)\}$$

   Puesto que $\forall F \in F(A), K(F) \subseteq L \Rightarrow R \subseteq L$

Pero la reunión *R* es, realmente, el conjunto de las expresiones racionales, con coeficientes en *K*, formadas cada una por un número finito de elementos de A.

Es inmediato que se trata de un cuerpo, cuerpo que contiene a *K* y a *A*. Por tanto, *L = R.*

PROPOSICION 6:

1) La clase T_k, de las extensiones finitas de un cuerpo K, es clase distinguida.

2) La clase Z_k, de las extensiones algebraicas de un cuerpo K, es clase distinguida.

En efecto:

1) Veamos la clase T_k de las extensiones finitas.

1.1) Sea la torre $K \subseteq L_i \subseteq L_j \; con \; L_j \; / K \in T_k$. Se Tiene

$$\left.\begin{array}{c}(L_j : K) \; finito \\ (L_j : K) = (L_i : K).(L_j : L_i)\end{array}\right\} \Rightarrow (L_i : K).(L_j : L_i) \; finito \Rightarrow$$

$$\Rightarrow (L_i : K) \; finito \wedge (L_j : L_i) \; finito \Rightarrow {}^{L_i}\!/_{K} \in T_K \; \wedge \; {}^{L_j}\!/_{L_i} \in T_K$$

por tanto:

$${}^{L_j}\!/_{K} \in T_K \Rightarrow \begin{cases} {}^{L_i}\!/_{K} \in T_K \\ {}^{L_j}\!/_{L_i} \in T_K \end{cases}$$

1.2) $L \; / K \in T_K \Rightarrow \exists A = \{d_1, \ldots, d_m\} \; algebraicos \; sobre \; K, \; tales \; que \; L = K(A)$

Sea *H/K*. Se tiene:

$HL = L(H) = H(L) = H(K(A)) = H(A) \Rightarrow HL = H(A)$ y *A* es algebraica sobre *K* y sobre *H* $\Rightarrow {}^{HL}\!/_{H}$ finita.

Por tanto:

$${}^{L}\!/_{K} \in T_K \Rightarrow {}^{HL}\!/_{H} \in T_K$$

1.3) Sean ${}^{L}\!/_{K}, {}^{H}\!/_{K} \in T_K$. Entonces:

L = K(A), con $A = \{d_1, \ldots d_s\}$ algebraicos sobre *K.*
H = K(B), con $B = \{e_1, \ldots e_r\}$ algebraicos sobre *K*

$LH = H(L) = H\big(K(A)\big) = H(A) = K(B)(A) = K(BUA)$

y siendo *BUA* finito y sus elementos algebraicos sobre K $\Rightarrow {}^{HL}\!/_{K}$ *finita*

por tanto:

$$ {}^{L}\!/_{K}, {}^{H}\!/_{K} \in T_K \Rightarrow {}^{HL}\!/_{K} \in T_K $$

2) Veamos la clase Z_k de las extensiones algebraicas.

2.1) Sea la torre $K \subseteq L_i \subseteq L_j$, *con* ${}^{L_j}\!/_{K} \in Z_K$

$$ {}^{L_j}\!/_{K} \text{ algebraica y } L_i \subseteq L_j \Rightarrow {}^{L_i}\!/_{K} \text{ algebraica} $$

por ser $K \subseteq L_i$, todo elemento de L_j algebraico sobre K es también algebraico sobre $L_i \Rightarrow {}^{L_j}\!/_{L_i}$ algebraica

por tanto:

$$ {}^{L_j}\!/_{K} \in Z_K \Rightarrow \begin{cases} {}^{L_i}\!/_{K} \in Z_K \\ {}^{L_j}\!/_{L_i} \in Z_K \end{cases} $$

2.2)

$$ {}^{L}\!/_{K} \in Z_K \wedge {}^{H}\!/_{K} \wedge H, L \text{ subcuerpos de } M \Rightarrow $$

$$ \Rightarrow \begin{cases} HL = H(L) \\ {}^{L}\!/_{K} \in z_k \end{cases} \Rightarrow \text{por propos } 5, \ {}^{H(L)}\!/_{H} \in Z_K \Rightarrow {}^{HL}\!/_{H} \in Z_K $$

por tanto:

$$ {}^{L}\!/_{K} \in Z_K \Rightarrow {}^{HL}\!/_{H} \in Z_K $$

2.3) Sean ${}^{L}\!/_{K}, {}^{H}\!/_{K} \in Z_K \wedge L(H) = H(L) = LH \Rightarrow {}^{LH}\!/_{K} \in Z_K$

por tanto: ${}^{L}\!/_{K}, {}^{H}\!/_{K} \in Z_K \Rightarrow {}^{LH}\!/_{K} \in Z_K$

4. El cuerpo de ruptura:

DEFINICION 5:

Dado un cuerpo *K* y un polinomio irreducible $p(x) \in K[x]$, se llama cuerpo de ruptura de *p(x)* a una extensión simple *L = K(t)* tal que *p(t) = 0*.

PROPOSICION 7:

Dado un cuerpo *K* y un polinomio irreducible $p(x) \in K[x]$, existe siempre el cuerpo de ruptura de *p(x),* determinado salvo isomorfismo.

En efecto:

Si $p(x) \in K[x]$ es irreducible en $K[x] \Rightarrow (p(x))$ es ideal máximo $\Rightarrow$

$$\Rightarrow \begin{cases} (p(x)) \text{ ideal maximal} \\ K[x] \text{ anillo con el. unidad} \end{cases} \Rightarrow K[x]/(p(x)) \text{ cuerpo}$$

Por ser $K \subseteq K[x]$, el epimorfismo canónico $n : K[x] \to K[x]/(p(x))$ 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 subcuerpo de K.

Sea, para $x \in K[x]$, $n(x) = e \in K[x]/(p(x))$.

Y para $f(x) \in K[x] / f(x) = r_0 + r_1 x + \ldots + r_n x^n$ sea:

$$n(f(x)) = \overline{f}(e) = r_0 + r_1 e + \ldots + r_n e^n$$

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

Entonces:

$$L \subseteq K[e] \subseteq K(e)$$

y como L es un cuerpo, será $K(e) \subseteq L$

por tanto:

$$\left.\begin{matrix} L \subseteq K(e) \\ K(e) \subseteq L \end{matrix}\right\} \Rightarrow L = K(e)$$

El polinomio $p(x) = a_0 + a_1 x + \ldots + a_n x^s$ 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 $n(p(x)) = a_0 + a_1 e + \ldots + a_n e^s$

por tanto:

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

De lo cual se deduce que $e \in L$ es algebraico sobre *K* y además es cero de $p(x) \in K[x] \Rightarrow L$ es extensión algebraica simple de *K* y además *p(x)* admite en *L* a e como cero $\Rightarrow L$ es 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 $g(c_0 + c_1 a + \ldots + c_r a^r) = c_0 + c_1 b + \ldots + c_r b^r$

COROLARIO 2:

Dado un polinomio $p(x) \in K[x]$ irreducible sobre *K* existe una extensión *L/K* obtenida por una sucesión de *n* extensiones simples, sobre la que *p(x)* se descompone totalmente en factores lineales.

En efecto:

a) Si sobre un primer cuerpo de ruptura $L_1(e_1)$, el polinomio *p(x)* se descompone en factores lineales irreducibles ya está resuelta la cuestión.

b) En caso contrario, sea $L_2 = L_1(e_2)$ 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 precedimiento conduce, al cabo de un número finito, *n*, de operaciones, a una extensión finita, L/K, sobre la que $p(x)$ se descompone totalmente en factores lineales.

5. Clausura algebraica:

PROPOSICIÓN 8:

Sea *K* un cuerpo y sea *K[x]* su anillo de polinomios. Existe una extensión algebraica de *K* en la que $\forall p(x) \in K[x]$ se descompone en factores lineales, minimal para esta propiedad y algebraicamente cerrada.

En efecto:

Sea $P(x) = a_0 + a_1 x + \ldots + a_n x^n$ y llamemos

$$p(x) = \frac{P(x)}{a_n} = \frac{a_0}{a_n} + \frac{a_1}{a_n} x + \ldots + x^n = b_0 + b_1 x + \ldots + b_n x^n$$

por tanto, $p(x) = b_0 + b_1 x + \ldots + b_{n-1} x^{n-1} + b_n x^n$.

Llamemos $K' = K(x)$, 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 $\{1,2,\ldots,n_i\}$ donde es $n_i = grado\ p_i(x)$.

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

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

Si es $grad\ p_2(x) = 4$, le corresponderán:

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

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:

$$f_i(x) = p_i(x) - (x - y_{i1}).(x - y_{i2})\ldots(x - y_{in_i})$$

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*:

$$e = \sum_{i=1}^{r} g_i f_i(x) = g_1 f_1(x) + g_2 f_2(x) + \ldots + g_r f_r(x)$$

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:

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

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 (modulo *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, es una extensión de *K.*

Sea a hora 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*:

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

Al ser $\{q_{ij}\}$ algebraicos sobre K y $L=K(q_{ij})$ será, por proposición 5, 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 en *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 el *grado de 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 proposición 4 –3º), 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 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 $f(x) \in K[x]$ con 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, en 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.

PROPOSICION 9:

Sea *E/K* una extensión algebraica y $s : K \to L$ una inmersión de K en un cuerpo algebraicamente cerrado *L*. Existe una prolongación de s a una inmersión de *E* en *L*. Si *E* es algebraicamente cerrado y *L* es algebraico sobre *GK,* toda prolongación de este tipo de s es un isomorfismo de *E* en *L.*

En efecto:

Sea *S* el conjunto de todos los pares *(F,T)*, donde *F Í E* es un subcuerpo de *E,* que contiene a *K*, y *T* es una extensión de σ a una inmersión de *F* en *L*.

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

$$(F,T) \le (F'.T') \Leftrightarrow \begin{cases} 1^{o}) \; F \subseteq F' \\ 2^{o}) \; \text{Re}\, stric \; T' \; a \; F = T \end{cases}$$

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

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

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.

Aplicando a *S* el Lema de Zorn, existe al menos un elemento maximal *(H, l) ÎS*, donde es λ una prolongación a *H* de la inmersión s 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:

$$s(f(x)) = f'(x) \in L[x]$$

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

Prolonguemos λ a λ' siendo $l'\colon H(d) \to L$ de modo que

$$s(c_0 + c_1 d + \ldots + c_n d^n) = c'_0 + c'_1 q + \ldots + c'_n q^n$$

Es claro, entonces, que

$$a)\ (H(d),\ l') \in S$$
$$b)\ (H,\ l) < (H(d),\ l')$$

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

Es decir, *(E, l*) 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 λ*E* como *L* son algebraicamente cerrados (λ*E* lo es por ser isomorfo a *E*, y *L* lo es por hipótesis).

Pero en la proposición 8 se probó el carácter minimal de toda extensión algebraica de *K* que fuera algebraicamente cerrada, entre todas las extensiones algebraicas de *K* que descompongan en factores lineales todo polinomio de *K[x]*. Por tanto, es λ*E=L,* y los cuerpos *E* y *L* resultan ser isomorfos.

COROLARIO 3:

Sea *K* un cuerpo y *E, E',* extensiones algebraicas de K, ambas algebraicamente cerradas. Existe un isomorfismo $t : E \to E'$ que induce la identidad sobre K o K-isomorfismo.

En efecto:

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. Este carácter de unicidad de sentido a la definición siguiente:

DEFINICION 6:

Se llama *clausura algebraica de un cuerpo K,* abreviadamente, $\overline{K}$, a una extensión algegraica de *K* que sea algebraicamente cerrada.

6. Bibliografía:

1. **Artin, E**. Galois Theory.
2. **Artin, E**. Geometric Algebra
3. **Birkhoff-Mc Lane**. Algebra moderna.
4. **Birkhoff,G., Bartee, T.C.,** Modern Applied Algebra, Mc Graw-Hill, 1970.
5. **Bourbak**i. Algebre, Ch. II - 3ra. Ed.
6. B**ourbaki**. Algebre, Ch. VII - 2da. Ed.
7. **Bourbaki**, N. Algèbre.
8. **Burton, D.M**., Introduction to Modern Abstract Algebra, Addison-Wesley, 1967.
9. **Caton, G. y Grossman, S. J**., Linear Algebra.,., Ed. Wordsworth Publ. Co. 1980.
10. **Childs, L.**, A Concrete Introduction to Higher Algebra, Springer-Verlag, 1979.
11. **Cignoli, R. O**., Apuntes de la materia Lógica (Computadores): Algebras de Boole. Cálculo proposicional.
12. **Fraleigh, J**. A First Course in Abstract Algebra.
13. **Fraleigh, J.B**., A First Course in Abstract Algebra, Addison-Wesley, 1967.
14. **Friedberg, S, Insel, A, Spence, L**., Linear Algebra, Prentice Hall (1979).
15. **Gamtmacher, F. R.,** The Theory of Mathematics., Vol. I y II., Ed. Chelsea, 1974.
16. **Gentile, E.**, Estructuras algebraicas I. (Public. OEA).
17. **Gentile, E**., Notas de Algebra (EUDEBA).
18. **Gentile, E**., Notas de Algebra II, Editorial Docencia.
19. **Godement, R**., Cours d'algèbre.
20. **Herstein, I. N.,** Algebra Moderna.
21. **Herstein, I. N**., Topics in Algebra.
22. **Hoffman, K y R. Kunze**, Algebra lineal, Prentice Hall.
23. **Hoffman, K, y R. Kunzc,** Linear Algebra, Prentice Hall, 1971.
24. **Hungerford, T.W.,** Álgebra.
25. **Jacobson, N.,** Lecture in Abstract Algebra, Princeton, N.J. Van Nostrand, 1951-1964.
26. **Jacobson, N.** Basic Algebra I.
27. **Kaplansky, I.** Linear Algebra and Geometry
28. **Lang, Serge,** Algebra lineal, Addison Wesley.
29. **Larotonda, A.,** Algebra lineal y Geometría. Eudeba.
30. **Lipschutz, S.,** Algebra lineal, Serie Schaum.
31. **Rotman, J.,** The Theory of Groups.
32. **Strang G.,,** Algebra Lineal con aplicaciones., Ed. Fondo Educativo Interamericano, 1981.
33. **Van der Waerden, B.**L. Moderne Algebra.
34. **Vargas, J.A.** Algebra Abstracta.
35. **Zariski, O. y Samuel, P**. Commutative Algebra I y II.