

Cuartas Jornadas de Teoría de Números

Universidad Euskal Herriko
del País Vasco Unibertsitatea

13 de julio de 2011

Teoría de Galois de extensiones no normales

Teresa Crespo, Universitat de Barcelona

Un ejemplo previo.

La extensión de cuerpos $\mathbb{Q}(\alpha)|\mathbb{Q}$, para $\alpha = \sqrt[3]{2}$, no es normal, $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \{\text{Id}_{\mathbb{Q}(\alpha)}\}$.

Podemos definir dos endomorfismos c, s del \mathbb{Q} -espacio vectorial $\mathbb{Q}(\alpha)$ por

$$c(1) = 1, \quad c(\alpha) = -\frac{1}{2}\alpha, \quad c(\alpha^2) = -\frac{1}{2}\alpha^2$$

$$s(1) = 0, \quad s(\alpha) = \frac{1}{2}\alpha, \quad s(\alpha^2) = -\frac{1}{2}\alpha^2.$$

Para $x \in \mathbb{Q}(\alpha)$, tenemos $x \in \mathbb{Q} \Leftrightarrow c(x) = x$ y $s(x) = 0$.

Además c y s están relacionados con la estructura de anillo de $\mathbb{Q}(\alpha)$ por

$$\begin{aligned} c(xy) &= c(x) \cdot c(y) - 3 \cdot s(x) \cdot s(y), \\ s(xy) &= c(x) \cdot s(y) + s(x) \cdot c(y) \end{aligned}$$

para $x, y \in \mathbb{Q}(\alpha)$.

El álgebra de grupo.

$$K[G] = \left\{ \sum_{\sigma \in G} \lambda_{\sigma} \sigma, \lambda_{\sigma} \in K \right\} \text{ álgebra de grupo}$$

$$\text{suma: } \sum_{\sigma \in G} \lambda_{\sigma} \sigma + \sum_{\sigma \in G} \mu_{\sigma} \sigma = \sum_{\sigma \in G} (\lambda_{\sigma} + \mu_{\sigma}) \sigma$$

$$\text{producto externo: } \mu \left(\sum_{\sigma \in G} \lambda_{\sigma} \sigma \right) = \sum_{\sigma \in G} \mu \lambda_{\sigma} \sigma$$

$$\text{producto interno: } \sum_{\sigma \in G} \lambda_{\sigma} \sigma \cdot \sum_{\tau \in G} \mu_{\tau} \tau = \sum_{\rho \in G} \left(\sum_{\sigma \tau = \rho} \lambda_{\sigma} \mu_{\tau} \right) \rho$$

Si $L|K$ es extensión de Galois con grupo G , el isomorfismo $G \xrightarrow{\varphi} \text{Aut}(L|K)$ induce una acción de $K[G]$ sobre L , dada por

$$\begin{aligned} \mu : K[G] &\rightarrow \text{End}_K(L) \\ \sum_{\sigma \in G} \lambda_{\sigma} \sigma &\mapsto \sum_{\sigma \in G} \lambda_{\sigma} \varphi(\sigma) \end{aligned}$$

y se tiene un isomorfismo

$$I \otimes \mu : L \otimes_K K[G] \rightarrow \text{End}_K(L).$$

$K[G]$ tiene también una estructura de K -coálgebra y de K -álgebra de Hopf.

Álgebras y coálgebras.

Una K -álgebra es una terna (A, m, u) , donde A es un K -espacio vectorial, $m : A \otimes A \rightarrow A$ y $u : K \rightarrow A$ son morfismos de K -espacios vectoriales tales que los diagramas siguientes conmutan

$$\begin{array}{ccc}
 A \otimes A \otimes A & \xrightarrow{Id \otimes m} & A \otimes A \\
 \downarrow m \otimes Id & & \downarrow m \\
 A \otimes A & \xrightarrow{m} & A
 \end{array}$$

$$\begin{array}{ccc}
 & A \otimes A & \\
 u \otimes Id \nearrow & & \nwarrow Id \otimes u \\
 K \otimes A & & A \otimes K \\
 \searrow \cong & \downarrow m & \nearrow \cong \\
 & A &
 \end{array}$$

Una K -coálgebra es una terna (C, Δ, ε) , donde C es un K -espacio vectorial, $\Delta : C \rightarrow C \otimes C$ y $\varepsilon : C \rightarrow K$ son morfismos de K -espacios vectoriales tales que los diagramas siguientes conmutan

$$\begin{array}{ccc}
 C \otimes C \otimes C & \xleftarrow{Id \otimes \Delta} & C \otimes C \\
 \uparrow \Delta \otimes Id & & \uparrow \Delta \\
 C \otimes C & \xleftarrow{\Delta} & C
 \end{array}$$

$$\begin{array}{ccc}
 & C \otimes C & \\
 \varepsilon \otimes Id \swarrow & & \searrow Id \otimes \varepsilon \\
 K \otimes C & & C \otimes K \\
 \searrow \cong & \uparrow \Delta & \nearrow \cong \\
 & C &
 \end{array}$$

Álgebras de Hopf.

Una K -biálgebra es un K -espacio vectorial H , dotado de estructura de K -álgebra (H, m, u) i de estructura de K -coálgebra (H, Δ, ε) tal que m i u son morfismos de K -coálgebras (equivalentemente Δ i ε son morfismos de K -álgebras).

Si H es K -biálgebra, una aplicación lineal $S : H \rightarrow H$ se llama **antípoda de H** si cumple

$$m \circ (S \otimes Id) \circ \Delta = u\varepsilon = m \circ (Id \otimes S) \circ \Delta.$$

Una K -álgebra de Hopf es una K -biálgebra con antípoda.

La K -álgebra $K[G]$ es álgebra de Hopf con coproducto Δ definido por $\Delta(g) = g \otimes g$, counidad definida por $\varepsilon(g) = 1$, antípoda definida por $S(g) = g^{-1}$, para $g \in G$.

Notación. Si C es K -coálgebra, para $c \in C$, escribimos $\Delta(c) = \sum c_1 \otimes c_2$.

Extensiones Hopf-Galois.

Sean $L|K$ una extensión finita de cuerpos, H una K -álgebra de Hopf finita. Decimos que $L|K$ es **H -Galois** si existe un morfismo de K -álgebras

$$\mu : H \rightarrow \text{End}_K(L)$$

tal que $I \otimes \mu : L \otimes H \rightarrow \text{End}_K(L)$ es isomorfismo y se cumple

$$\mu(h)(xy) = \sum \mu(h_1)(x) \cdot \mu(h_2)(y), \quad (1)$$

$$\mu(h)(1) = \varepsilon(h) \cdot 1, \quad (2)$$

para $h \in H, x, y \in L$.

Ejemplo 1. Si $L|K$ es extensión de Galois con grupo G , tenemos

$$\begin{aligned} \mu : K[G] &\rightarrow \text{End}_K(L) \\ \sum_{\sigma \in G} \lambda_{\sigma} \sigma &\mapsto \sum_{\sigma \in G} \lambda_{\sigma} \varphi(\sigma) \end{aligned}$$

inducido por $G \stackrel{\varphi}{\simeq} \text{Aut}(L|K)$ e $I \otimes \mu$ es isomorfismo. Además

$$\varphi(\sigma)(xy) = \varphi(\sigma)(x)\varphi(\sigma)(y) \text{ implica (1),}$$

$$\varphi(\sigma)(1) = 1 = \varepsilon(\sigma) \cdot 1 \text{ implica (2).}$$

Ejemplo 2. Consideramos la extensión $\mathbb{Q}(\alpha)|\mathbb{Q}$, con $\alpha = \sqrt[3]{2}$ i el álgebra $H = \mathbb{Q}[c, s]/(3s^2 + c^2 - 1, (2c + 1)s, (2c + 1)(c - 1))$ con la estructura de álgebra de Hopf dada por

$$\begin{aligned}\Delta(c) &= c \otimes c - 3s \otimes s, \quad \varepsilon(c) = 1, \quad S(c) = c, \\ \Delta(s) &= c \otimes s + s \otimes c, \quad \varepsilon(s) = 0, \quad S(s) = -s.\end{aligned}$$

El morfismo $\mu : H \rightarrow \text{End}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ viene dado por

$$c(1) = 1, \quad c(\alpha) = -\frac{1}{2}\alpha, \quad c(\alpha^2) = -\frac{1}{2}\alpha^2$$

$$s(1) = 0, \quad s(\alpha) = \frac{1}{2}\alpha, \quad s(\alpha^2) = -\frac{1}{2}\alpha^2$$

y las relaciones

$$\begin{aligned}c(xy) &= c(x) \cdot c(y) - 3 \cdot s(x) \cdot s(y), \\ s(xy) &= c(x) \cdot s(y) + s(x) \cdot c(y)\end{aligned}$$

son exactamente la condición

$$\mu(h)(xy) = \sum \mu(h_1)(x) \cdot \mu(h_2)(y).$$

Si una K -álgebra de Hopf H opera sobre un cuerpo L extensión de K , definimos el subcuerpo de L fijo por la acción como

$$L^H := \{x \in L : \mu(h)(x) = \varepsilon(h) \cdot x, \forall h \in H\}.$$

En este ejemplo, tenemos

$$(\mathbb{Q}(\alpha))^H = \{x \in \mathbb{Q}(\alpha) : c(x) = \varepsilon(c) \cdot x = x, s(x) = \varepsilon(s) \cdot x = 0\} = \mathbb{Q}.$$

Ejemplo 3. Consideramos la extensión $L = \mathbb{Q}(\sqrt[4]{2})|\mathbb{Q} = K$. La extensión $L(i)|\mathbb{Q}(i)$ es Galois con grupo $N = C_4$. Por tanto es H_0 -Galois con $H_0 = \mathbb{Q}(i)[N]$. Si e es generador de N , tenemos $H_0 = \{\lambda_0 + \lambda_1 e + \lambda_2 e^2 + \lambda_3 e^3\}$. La sub-álgebra de Hopf de H_0

$$H = \mathbb{Q} \left[\frac{e + e^{-1}}{2}, \frac{e - e^{-1}}{2i} \right]$$

cumple $H_0 = H[i]$ y $L|\mathbb{Q}$ es H -Galois.

Formulación en términos de grupos.

Para una extensión finita y separable $L|K$, denotamos por

$$\begin{array}{c}
 \tilde{L} \\
 | \\
 G' \\
 | \\
 L \\
 | \\
 K
 \end{array}
 \begin{array}{l}
 \tilde{L} \text{ clausura normal de } L|K, \\
 G = \text{Gal}(\tilde{L}|K), \\
 G' = \text{Gal}(\tilde{L}|L), \\
 S = G/G' \text{ (clases laterales por la izquierda),} \\
 B = \text{Perm}(S).
 \end{array}$$

La acción de G sobre $S = G/G'$ da un monomorfismo $G \hookrightarrow \text{Perm}(S) = B$.

Son equivalentes las dos condiciones siguientes

1. Existe una K -álgebra de Hopf H tal que $L|K$ es H -Galois.
2. Existe un subgrupo regular $N \subset B$ (i.e. N opera transitivamente y con estabilizadores triviales sobre S) tal que el subgrupo G de B normaliza N .

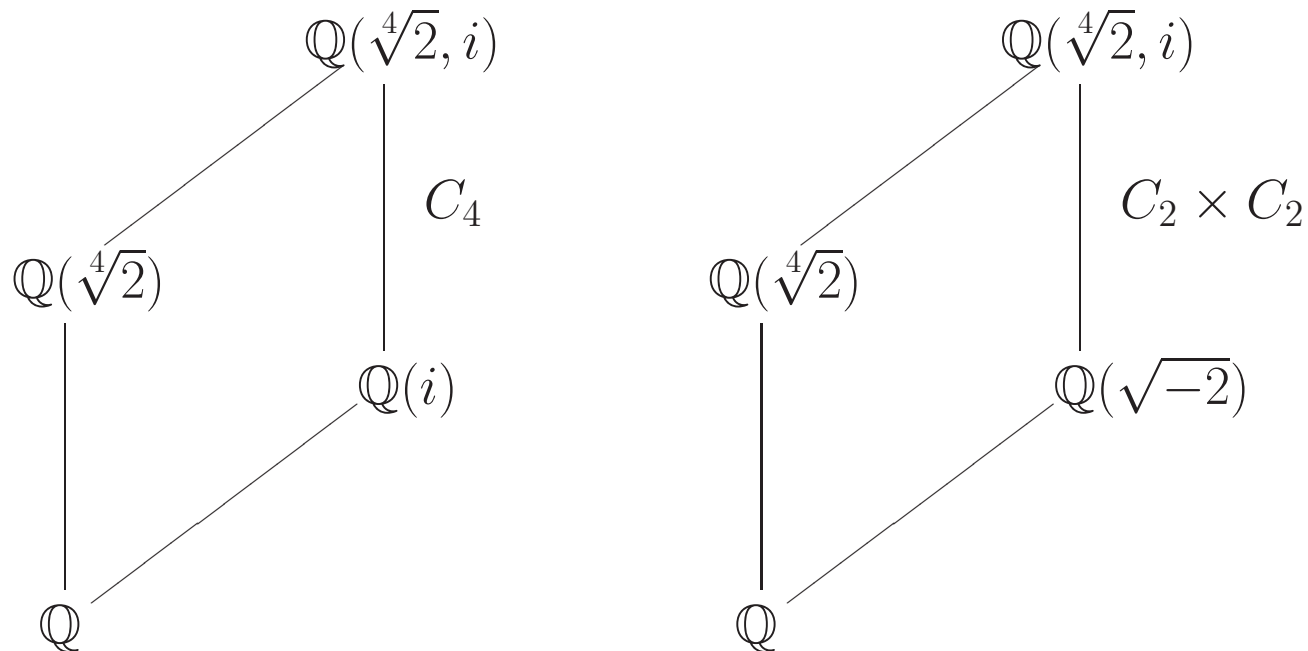
Además $H \otimes \tilde{L} \simeq K[N] \otimes \tilde{L} \simeq \tilde{L}[N]$.

Ejemplo 3'. Consideramos la extensión $L = \mathbb{Q}(\sqrt[4]{2})|\mathbb{Q} = K$.

Sabemos $G = D_4 = \{\rho, \sigma\}$, $\rho = (1234)$, $\sigma = (13)$. Si tomamos $N = \langle \rho^2, \sigma \rangle \simeq C_2 \times C_2$, tenemos N regular y obtenemos una K -álgebra de Hopf H' , no isomorfa a la K -álgebra de Hopf considerada anteriormente. Poniendo $N = \langle s, t | s^2 = t^2 = 1, st = ts \rangle$, tenemos

$$H' = \mathbb{Q}[st, s + t, \sqrt{-2}(t - s)] \subset \mathbb{Q}(\sqrt{-2})[N].$$

Las dos estructuras Hopf-Galois de esta extensión corresponden a dos diagramas de extensiones de cuerpos.



Extensiones cuasigaloisianas.

\tilde{L} clausura normal de $L|K$, $G = \text{Gal}(\tilde{L}|K)$, $G' = \text{Gal}(\tilde{L}|L)$, $S = G/G'$, $B = \text{Perm}(S)$.

Las condiciones siguientes son equivalentes:

1. Existe una extensión de Galois $E|K$ tal que $L \otimes E$ es un cuerpo que contiene \tilde{L} .
2. Existe una extensión de Galois $E|K$ tal que $L \otimes E = \tilde{L}$.
3. G' tiene un complemento normal en G .
4. Existe un subgrupo regular N de B normalizado por G y contenido en G .

Decimos que $L|K$ es **cuasigaloisiana** si cumple las condiciones anteriores.

Proposición. Sea $L|K$ extensión separable de grado n , $G = \text{Gal}(\tilde{L}|K)$.

1. Si $n = 2$, $L|K$ es galoisiana,
2. Si $n = 3$ o 4 , $L|K$ es cuasigaloisiana,
3. Si $n = 5$, $L|K$ es Hopf-Galois si y sólo si $G \neq A_5$ y $G \neq S_5$,
4. Si $n \geq 5$ y $G = A_n$ o S_n , entonces $L|K$ no es Hopf-Galois,
5. Si $n \leq 7$, $L|K$ es Hopf-Galois si y sólo si es cuasigaloisiana.

Ejemplo. Consideramos la extensión $L = \mathbb{Q}(\sqrt[5]{2})|\mathbb{Q}$. Entonces $\tilde{L} = \mathbb{Q}(\sqrt[5]{2}, \zeta_5)$. La extensión $L|\mathbb{Q}$ es cuasigaloisiana.

Ahora consideramos la extensión $E = \mathbb{Q}(\sqrt[5]{2}, \zeta_5 + \zeta_5^4)|\mathbb{Q}$. Esta extensión es Hopf-Galois pero no cuasigaloisiana. Tenemos $\tilde{E} = \tilde{L} = \mathbb{Q}(\sqrt[5]{2}, \zeta_5)$, $[E : \mathbb{Q}] = 10$ y $G = \text{Gal}(\tilde{L}|\mathbb{Q})$ está generado por los automorfismos

$$\begin{array}{ccc} \sigma : \sqrt[5]{2} \mapsto \zeta_5 \sqrt[5]{2} & \tau : \sqrt[5]{2} \mapsto \sqrt[5]{2} \\ \zeta_5 \mapsto \zeta_5 & \zeta_5 \mapsto \zeta_5^3 \end{array}$$

que cumplen las relaciones $\sigma^5 = Id, \tau^4 = Id, \tau\sigma\tau^{-1} = \sigma^3$. Vemos que $\langle\sigma\rangle$ es complemento normal de $\text{Gal}(\tilde{L}|L) = \langle\tau\rangle$ en G ; por tanto $L|\mathbb{Q}$ es cuasigaloisiana. En cambio $G' = \text{Gal}(\tilde{L}|E) = \langle\tau^2\rangle$ no tiene complemento normal en G . En efecto, el único subgrupo normal de orden 10 de G es $\langle\sigma, \tau^2\rangle$. Las clases laterales de G/G' son

$$\begin{array}{l} C_1 = \{I, \tau^2\}, \quad C_2 = \{\sigma, \sigma\tau^2\}, \quad C_3 = \{\sigma^2, \sigma^2\tau^2\}, \quad C_4 = \{\sigma^3, \sigma^3\tau^2\}, \quad C_5 = \{\sigma^4, \sigma^4\tau^2\} \\ C_6 = \{\tau, \tau^3\}, \quad C_7 = \{\sigma\tau, \sigma\tau^3\}, \quad C_8 = \{\sigma^2\tau, \sigma^2\tau^3\}, \quad C_9 = \{\sigma^3\tau, \sigma^3\tau^3\}, \quad C_{10} = \{\sigma^4\tau, \sigma^4\tau^3\} \end{array}$$

La inclusión de G en $B = \text{Perm}(S)$ viene dada por

$$\sigma \mapsto (1, 2, 3, 4, 5)(6, 7, 8, 9, 10), \tau \mapsto (1, 6)(2, 9, 5, 8)(3, 7, 4, 10).$$

El subgrupo cíclico $N = \langle(1, 9, 2, 10, 3, 6, 4, 7, 5, 8)\rangle$ es regular y normalizado por G .

Extensiones de grado 6.

Consideramos $L|K$ de grado 6, $G = Gal(\tilde{L}|K)$.

G	$ G $	$L K$
$C(6)$	6	Galois
$D6(6)$	6	Galois
$D(6)$	12	cuasigaloisiana
$A4(6)$	12	no Hopf-Galois
$F18(6)$	18	cuasigaloisiana
$2A4(6)$	24	no Hopf-Galois
$S4(6d)$	24	no Hopf-Galois
$S4(6c)$	24	no Hopf-Galois
$F18(6) : 2$	36	cuasigaloisiana
$F36(6)$	36	no Hopf-Galois
$2S4(6)$	48	no Hopf-Galois
$A5(6)$	60	no Hopf-Galois
$F36(6) : 2$	72	no Hopf-Galois
$L(6) : 2$	120	no Hopf-Galois
$A6$	360	no Hopf-Galois
$S6$	720	no Hopf-Galois

Extensiones de grado 7.

Consideramos $L|K$ de grado 7, $G = Gal(\tilde{L}|K)$.

G	$ G $	$L K$
$C(7)$	7	Galois
$D(7)$	14	cuasigaloisiana
$F_{21}(7)$	21	cuasigaloisiana
$F_{42}(7)$	42	cuasigaloisiana
$L(7)$	168	no Hopf-Galois
A_7	2520	no Hopf-Galois
S_7	5040	no Hopf-Galois

Teorema fundamental.

1. Sea $L|K$ una extensión Hopf-Galois con K -álgebra de Hopf H . Entonces la aplicación

$$f : \left\{ \begin{array}{l} H' : H' \text{ es sub-álgebra de Hopf de } H \\ H' \end{array} \right\} \rightarrow \left\{ \begin{array}{l} E : K \subset E \subset L, K \text{ cuerpo} \\ L^{H'} \end{array} \right\},$$

donde $L^{H'} := \{x \in L : \mu(h)(x) = \varepsilon(h) \cdot x, \forall h \in H'\}$, es inyectiva e invierte las inclusiones.

2. Si $L|K$ es cuasigaloisiana, existe una K -álgebra de Hopf H tal que $L|K$ es H -Galois y f es también exhaustiva.

Proposición. Sean $L|K$, $F|L$ separables, tales $L \subset F \subset \tilde{L}$, para \tilde{L} la clausura galoisiana de $L|K$. Entonces

$$\left. \begin{array}{l} F|L \text{ Hopf-Galois} \\ L|K \text{ Hopf-Galois} \end{array} \right\} \Rightarrow F|K \text{ Hopf-Galois.}$$

Idea de la demostración:

$$G \left[\begin{array}{c} \tilde{L} \\ | \\ G'' \\ F \\ | \\ L \\ | \\ K \end{array} \right] G'$$

Ponemos $[L : K] = n$, $[F : L] = r$.

La acción de G sobre G/G' da un morfismo inyectivo $G \rightarrow S_n$ y, por ser $L|K$ Hopf-Galois, existe un subgrupo regular N de S_n normalizado por G .

La acción de G' sobre G'/G'' da un morfismo inyectivo $G' \rightarrow S_r$ y, por ser $F|L$ Hopf-Galois, existe un subgrupo regular N' de S_r normalizado por G' .

Escribiendo un sistema de representantes de G módulo G'' como $\{x_i y_j\}$, para $\{x_i\}_{1 \leq i \leq n}$ sistema de representantes de G/G' , $\{y_j\}_{1 \leq j \leq r}$ sistema de representantes de G'/G'' , obtenemos un morfismo $G \rightarrow Perm(\{1, \dots, n\} \times \{1, \dots, r\}) = S_{nr}$ y la imagen de $N \times N'$ por $S_n \times S_r \hookrightarrow S_{nr}$ es subgrupo regular normalizado por G .

Extensiones inseparables.

Sea K un cuerpo de característica $p > 0$.

Si $L|K$ es extensión puramente inseparable de exponente 1 (i.e. $L^p \subset K$), decimos que los elementos x_1, \dots, x_n de L son p -independientes sobre K si

$$\sum a_{r_1 \dots r_n} x_1^{r_1} \dots x_n^{r_n} = 0, a_{r_1 \dots r_n} \in K, 0 \leq r_i < p \Rightarrow a_{r_1 \dots r_n} = 0, \forall r_1, \dots, r_n.$$

Una p -base de $L|K$ es un conjunto p -independiente maximal.

Sea ahora L una extensión puramente inseparable de exponente m de K (i.e. $L^{p^m} \subset K$). Podemos considerar la torre de cuerpos intermedios

$$K \subset L_1 := K^{p^{-1}} \cap L \subset L_2 := K^{p^{-2}} \cap L \subset \dots \subset L_{m-1} := K^{p^{1-m}} \cap L \subset K^{p^{-m}} \cap L = L,$$

donde cada eslabón es una extensión puramente inseparable de exponente 1. Podemos tomar una p -base $B_{m,m}$ de $L|L_{m-1}$. Tenemos $B_{m,m}^p \subset L_{m-1}$. Tomamos un conjunto maximal $B_{m-1,m}$ de elementos p -independientes de $B_{m,m}^p$ y $B_{m-1,m-1}$ tal que $B_{m-1,m} \cup B_{m-1,m-1}$ es p -base de $L_{m-1}|L_{m-2}$ y procedemos en esta forma hasta obtener una p -base $B_{1,m} \cup \dots \cup B_{1,1}$ de $L_1|K$.

Ponemos $N := B_{1,1} \cup B_{2,2} \cup \dots \cup B_{m,m}$. Si $x \in B_{i,i}$, ponemos $i = h(x)$.

Derivaciones superiores.

Si $L|K$ es extensión de cuerpos, una **K -derivación superior** D de L es una sucesión $D_0 = Id, D_1, \dots, D_n, \dots$ de aplicaciones K -lineales de L en L cumpliendo

$$D_n(ab) = \sum_{i=0}^n D_i(a)D_{n-i}(b), \text{ para todo } a, b \in L.$$

El **cuerpo de constantes** de D es $\{a \in L | D_n(a) = 0, \forall n > 0\}$.

Si K es cuerpo de característica p , se tiene

$$D_n(x^p) = 0 \text{ salvo si } p \mid n$$

y, en este caso

$$D_n(x^p) = D_{n/p}(x)^p.$$

Extensiones modulares.

Sea ahora L una extensión puramente inseparable de K . Decimos que $L|K$ es **modular** si cumple una de las condiciones equivalentes siguientes.

1. L es isomorfo al producto tensorial sobre K de extensiones de K generadas por un elemento.
2. Los monomios $\prod_{x \in N} x^k, 0 \leq k < p^{h(x)}$, forman una K -base de L .
3. Existe una K -derivación superior de L cuyo cuerpo de constantes es K .

Ejemplo 1. Sea $K = \mathbb{F}_p(X^p, Y^p, Z^{p^2})$, $L = K[Z, XZ + Y]$.

La extensión $L|K$ no es modular.

Supongamos que existe una K -derivación superior D de L tal que Z^p no está en el cuerpo de constantes. Entonces, tenemos $D_n(Z^p) \neq 0$ para algún n , por tanto $p \mid n$ y $D_n(Z^p) = (D_{n/p}(Z))^p$. Obtenemos

$$X^p(D_{n/p}(Z))^p = D_n(X^p Z^p) = D_n(X^p Z^p + Y^p) = (D_{n/p}(XZ + Y))^p.$$

Esto implica $X = (D_{n/p}(XZ + Y))/(D_{n/p}(Z))$ que contradice $X \notin L$.

Ejemplo 2. Sea $K = \mathbb{F}_p(X^{p^2}, Y^{p^2}, Z^{p^2})$, $L = K[Z, XZ + Y, X^p, Y^p]$.
Entonces

$$L = K[Z] \otimes K[XZ + Y] \otimes K[Y^p].$$

Por tanto, la extensión $L|K$ es modular.

Tenemos la torre de extensiones de exponente 1

$$K \subset K[Z^p, (XZ + Y)^p] \subset L,$$

$$B_{2,2} = \{Z, XZ + Y\}, B_{1,2} = B_{2,2}^p = \{Z^p, (XZ + Y)^p\}, B_{1,1} = \{Y^p\}.$$

En cambio, L no es modular sobre el cuerpo intermedio $E = K[X^p, Y^p]$.

Si L es una extensión puramente inseparable de K , la existencia de una K -derivación superior de L con cuerpo de constantes K equivale a la existencia de una K -álgebra de Hopf H , generada por elementos D_n que cumplen

$$\Delta(D_n) = \sum_{i=0}^n D_i \otimes D_{n-i},$$

tal que $L|K$ es Hopf-Galois y $L^H = K$.