Teoria de Hopf-Galois

STNB 2012

Extensions Hopf-Galois inseparables.

Exemple. Sigui k un cos de característica $p > 0$ i sigui $K = k(\omega)|k$ una extensió de cossos purament inseparable d'exponent n (i.e. $\omega^{p^n} \in k$ però $\omega^{p^{n-1}} \notin k$).

Definim la k-àlgebra A per $A = k[t]/(t^{p^n})$. Posem x la classe de t a A. Dotem A d'estructura d'àlgebra de Hopf amb coproducte, counitat i antípoda definits per

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

Es pot comprovar que $K|k$ té estructura Hopf-Galois donada per

$$\begin{aligned} \mu'' : K &\to K \otimes_k A \\ \omega &\mapsto \omega \otimes 1 + 1 \otimes x \end{aligned}$$

Condicions de descens galoisià.

$L|k$ extensió de Galois amb grup de Galois G,
A un objecte (espai vectorial, àlgebra, àlgebra de Hopf) sobre k.
Una *L-forma* de A és un k-objecte B tal que $L \otimes_k A \simeq L \otimes_k B$.

Teorema 1. *El conjunt $Form_L(A)$ d'L-formes de A mòdul k-isomorfisme està en bijecció amb $H^1(G, Aut_L(L \otimes A))$.*

Si B és una L-forma de A, $\phi : L \otimes B \to L \otimes A$ un isomorfisme, per a cada $\sigma \in G$, definim $p_\sigma \in Aut_L(L \otimes A)$ com la composició

$$L \otimes A \xrightarrow{\sigma^{-1}} L \otimes A \xrightarrow{\phi^{-1}} L \otimes B \xrightarrow{\sigma} L \otimes B \xrightarrow{\phi} L \otimes A.$$

L'assignació $\sigma \mapsto p_\sigma$ defineix un 1-cocicle de G en $Aut_L(L \otimes A)$ i la correspondència

$$\begin{array}{ccc} Form_L(A) & \to & H^1(G, Aut_L(L \otimes A)) \\ B & \mapsto & p_\sigma \end{array}$$

és bijectiva.

Observació. Siguin $(a_1, \ldots, a_n), (b_1, \ldots, b_m)$ k-bases de A i B, respectivament. Si $\psi : L \otimes A \to L \otimes B$ té matriu (c_{ij}) en les bases $1 \otimes a_j, 1 \otimes b_i$, aleshores $\sigma \circ \psi \circ \sigma^{-1}$ té matriu (c_{ij}^{σ}) en les mateixes bases.

Posem $\psi^{\sigma} := \sigma \circ \psi \circ \sigma^{-1}$. Amb aquesta notació, el cocicle p_{σ} associat a la L-forma B de A amb isomorfisme ϕ de $L \otimes B$ en $L \otimes A$ és $p_{\sigma} = \phi \circ \phi^{-\sigma}$.

Definició 2. *Si A_1, A_2 són k-objectes, un morfisme*

$$f : L \otimes A_1 \to L \otimes A_2$$

es diu descendible *si existeixen L-formes B_i de A_i, amb isomorfismes ϕ_i de $L \otimes B_i$ en $L \otimes A_i$, $i = 1, 2$, i un morfisme g de B_1 en B_2 tals que el diagrama*

$$\begin{array}{ccc} L \otimes B_1 & \xrightarrow{L \otimes g} & L \otimes B_2 \\ \phi_1 \downarrow & & \downarrow \phi_2 \\ L \otimes A_1 & \xrightarrow{f} & L \otimes A_2 \end{array}$$

commuta.

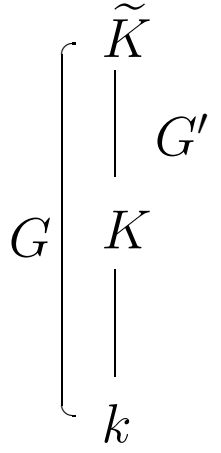
Lema 3. *Un morfisme* $f : L \otimes A_1 \to L \otimes A_2$ *és descendible si i només si existeixen* L*-formes* B_i *de* A_i*, amb isomorfismes* $\phi_i : L \otimes B_i \xrightarrow{\sim} L \otimes A_i, i = 1, 2$*, tals que el diagrama*

$$\begin{array}{ccc} L \otimes A_1 & \xrightarrow{f^\sigma} & L \otimes A_2 \\ p_\sigma^{(1)} \downarrow & & \downarrow p_\sigma^{(2)} \\ L \otimes A_1 & \xrightarrow{f} & L \otimes A_2 \end{array}$$

commuta per a tot $\sigma \in G$*, on* $p_\sigma^{(i)}$ *és l'1-cocicle associat a* $\phi_i, i = 1, 2$*.*

Caracterització d'extensions Hopf-Galois separables.

Per a una extensió finita i separable $K|k$, denotem per



$\widetilde{K}$ clausura normal de $K|k$,
$G = \mathrm{Gal}(\widetilde{K}|k)$,
$G' = \mathrm{Gal}(\widetilde{K}|K)$,
$S = G/G'$ (classes laterals per l'esquerra),
$B = Perm(S)$.

L'acció de G sobre $S = G/G'$ dóna un monomorfisme $G \hookrightarrow Perm(S) = B$.

Sigui $L \supset \widetilde{K}$. El conjunt $L^S = \{S \to L\}$ és L-espai vectorial amb base

$$\{e_{\overline{g}} : \overline{g} \in S\}, \text{ on } e_{\overline{g}}(\overline{h}) = \delta_{\overline{g},\overline{h}}.$$

El grup $\Gamma = Gal(L|k)$ opera sobre L^S per $\gamma(\lambda e_{\overline{h}}) = \gamma(\lambda) e_{\overline{gh}}$, on $\gamma \mapsto g \in G$.

Lema 4. *L'aplicació*

$$\begin{array}{rccc} \varphi : & L \otimes K & \to & L^S \\ & \lambda \otimes x & \mapsto & \sum_{\overline{g} \in G/G'} \lambda g(x) e_{\overline{g}} \end{array}$$

és isomorfisme de L-àlgebres i Γ-morfisme.

Un grup N que opera sobre un conjunt S es diu *regular* si l'acció és transitiva i amb estabilitzadors trivials.

Lema 5. *Sigui $K|k$ separable i H-Galois. Aleshores existeix, per a cada extensió $L \supset \widetilde{K}$, un únic subgrup regular $N \subset B = Perm(S)$ tal que es té un L-isomorfisme $\alpha : L \otimes H \to L[N]$ i un diagrama commutatiu*

$$\begin{array}{ccc} (L \otimes H) \otimes_L (L \otimes K) & \xrightarrow{L \otimes \mu'} & L \otimes K \\ \alpha \otimes \varphi \downarrow & & \downarrow \varphi \\ L[N] \otimes_L L^S & \xrightarrow{\nu'} & L^S \end{array} .$$

Demostració. Com $K|k$ és H-Galois, tenim $\mu'' : K \to K \otimes H^*$ que indueix un isomorfisme $K \otimes K \simeq K \otimes H^*$. Tenim doncs $L \otimes K \simeq L \otimes H^*$, com a L-àlgebres. D'altra banda, pel lema 4, $L \otimes K$ és L-isomorfa a L^S. Per tant l'L-àlgebra de Hopf $L \otimes H^*$ té L^S com a àlgebra subjacent i això implica $L \otimes H^* \simeq L^N$, com a àlgebres de Hopf, per a algun grup N i, per tant, $L \otimes H \simeq L[N]$.
Com $\mu' : H \otimes K \to K$ indueix un isomorfisme $K \otimes H \simeq End_k(K)$, definint ν' que faci commutar el diagrama, obtenim que l'acció de $L[N]$ sobre L^S també és fidel. Ara, donar una acció (fidel) de $L[N]$ sobre L^S equival a donar una acció (regular) de N sobre S. Com ν' està determinat pel diagrama, la inclusió $N \subset B$ també està determinada de forma única.

Teorema 6. *Sigui $K|k$ una extensió separable. Les condicions següents són equivalents.*

a) Existeix una k-àlgebra de Hopf H tal que $K|k$ és H-Galois.

b) Existeix un subgrup regular N de B, normalitzat per G, com a subgrup de B.

A més, l'àlgebra de Hopf H és una $\widetilde{K}$-forma de $k[N]$.

Demostració. b) $\Rightarrow$ a).
Considerem la base canònica $(e_{\overline{g}})_{\overline{g}\in S}$ de $\widetilde{K}^S$. Definim

$$\begin{array}{rccc} \mu' : & \widetilde{K}[N] \otimes_{\widetilde{K}} \widetilde{K}^S & \to & \widetilde{K}^S \\ & \rho \otimes x e_{\overline{g}} & \mapsto & x e_{\rho(\overline{g})} \end{array}$$

on $\rho \in N, g \in G$. Definim, per a $g \in G$, $p_g : N \to N$ per $p_g(n) = gng^{-1}$. Tenim $Aut_{\widetilde{K}-Hopf}(\widetilde{K}[N]) \simeq AutN$, per tant, p_g s'exten a un automorfisme de $\widetilde{K}$-àlgebra de Hopf de $\widetilde{K}[N]$. Com p_g és extès d'un automorfisme de N, l'acció de G sobre p_g via $\widetilde{K}$ és trivial. Tenim $p_g p_h = p_{gh}$; per tant, p_g és 1-cocicle.

El grup G opera sobre $\widetilde{K}^S$ per $h(xe_{\overline{g}}) = h(x)e_{\overline{hg}}, h \in G$. Definim $\mu'^h = h\mu' h^{-1}$.
El diagrama

$$\begin{array}{ccc} \widetilde{K}[N] \otimes_{\widetilde{K}} \widetilde{K}^S & \xrightarrow{\mu'^h} & \widetilde{K}^S \\ p_h \otimes 1 \downarrow & & || \\ \widetilde{K}[N] \otimes_{\widetilde{K}} \widetilde{K}^S & \xrightarrow{\mu'} & \widetilde{K}^S \end{array}$$

commuta.

Pel lema 4, $\widetilde{K}^S = \widetilde{K} \otimes K$ com a $\widetilde{K}$-àlgebres i com a G-conjunts. Obtenim doncs $\widetilde{\mu}$ tal que el diagrama

$$\begin{array}{ccc} \widetilde{K}[N] \otimes_{\widetilde{K}} (\widetilde{K} \otimes K) & \xrightarrow{\widetilde{\mu}^h} & \widetilde{K} \otimes K \\ p_h \otimes 1 \downarrow & & || \\ \widetilde{K}[N] \otimes_{\widetilde{K}} (\widetilde{K} \otimes K) & \xrightarrow{\widetilde{\mu}} & \widetilde{K} \otimes K \end{array}$$

commuta.

Sigui H la $\widetilde{K}$-forma de $k[N]$ definida pel cocicle p_h. Tenim $\widetilde{K} \otimes H \simeq \widetilde{K} \otimes k[N] \simeq \widetilde{K}[N]$ i, per tant

$$\widetilde{K}[N] \otimes_{\widetilde{K}} (\widetilde{K} \otimes K) \simeq (\widetilde{K} \otimes k[N]) \otimes_{\widetilde{K}} (\widetilde{K} \otimes K) \simeq \widetilde{K} \otimes H \otimes K.$$

Com $\widetilde{\mu} \circ p_h = p_1 \circ \widetilde{\mu}^h$, pel lema 3, $\widetilde{\mu}$ és descendible, és a dir, existeix una aplicació k-lineal $\mu_0 : H \otimes K \to K$ tal que $\widetilde{\mu} = \widetilde{K} \otimes \mu_0$.
Per descens fidelment pla, μ_0 defineix una estructura H-Galois ja que $\widetilde{\mu}$ defineix una estructura $\widetilde{K} \otimes H$-Galois.

a) $\Rightarrow$ b).
Pel lema 5, tenim, $\widetilde{K} \otimes H \simeq \widetilde{K}[N]$, per a algun grup N. El grup $G = Aut(\widetilde{K}|k)$ opera sobre $\widetilde{K} \otimes K$ via el factor de l'esquerra i sobre $\widetilde{K}^S$ per

$$g(\lambda e_{\overline{h}}) = g(\lambda) e_{\overline{gh}}.$$

Sigui $\mu_0 : H \otimes K \to K$ l'estructura H-Galois donada. La $\widetilde{K}$-forma H de $k[N]$ correspon a un 1-cocicle $p_g, g \in G$. Ara definim $\widetilde{\mu}$ que faci commutatiu el diagrama

$$\begin{array}{rcccc} \widetilde{K} \otimes (H \otimes K) & \simeq & (\widetilde{K} \otimes H) \otimes_{\widetilde{K}} (\widetilde{K} \otimes K) & \stackrel{\widetilde{K} \otimes \mu_0}{\longrightarrow} & \widetilde{K} \otimes K \\ & & \downarrow \wr & & || \\ \widetilde{K} \otimes \widetilde{K}[N] & \simeq & \widetilde{K}[N] \otimes_{\widetilde{K}} (\widetilde{K} \otimes K) & \stackrel{\widetilde{\mu}}{\longrightarrow} & \widetilde{K} \otimes K \end{array} .$$

Per definició, $\widetilde{\mu}$ és descendible, per tant, pel lema 3, el diagrama següent commuta per a tot $g \in G$.

$$\begin{array}{ccc} \widetilde{K}[N] \otimes_{\widetilde{K}} (\widetilde{K} \otimes K) & \stackrel{\widetilde{\mu}^g}{\longrightarrow} & \widetilde{K} \otimes K \\ p_g \otimes 1 \downarrow & & || \\ \widetilde{K}[N] \otimes_{\widetilde{K}} (\widetilde{K} \otimes K) & \stackrel{\widetilde{\mu}}{\longrightarrow} & \widetilde{K} \otimes K \end{array}$$

Pel lema 4, $\widetilde{K} \otimes K$ i $\widetilde{K}^S$ són isomorfes com a $\widetilde{K}$-àlgebres i com a G-conjunts. Per tant, obtenim un diagrama commutatiu

$$\begin{array}{ccc} \widetilde{K}[N] \otimes_{\widetilde{K}} \widetilde{K}^S & \xrightarrow{\mu'^g} & \widetilde{K}^S \\ p_g \otimes 1 \downarrow & & || \\ \widetilde{K}[N] \otimes_{\widetilde{K}} \widetilde{K}^S & \xrightarrow{\mu'} & \widetilde{K}^S \end{array} . \tag{1}$$

L'automorfisme $p_g \in Aut_{\widetilde{K}-Hopf}(\widetilde{K}[N])$ ve induit per un automorfisme del grup N. Volem veure que la restricció de p_g a N és la conjugació per g. Definim una acció de N per permutació sobre S per

$$\nu(\overline{g}) = \overline{h} \text{ si } \ \mu'(\nu \otimes e_{\overline{g}}) = e_{\overline{h}}, \text{ per a } \ \nu \in N, \overline{g} \in S.$$

Seguim l'element $\nu \otimes e_s, \nu \in N, s \in S$ pel diagrama commutatiu (1). Tenim

$$\mu'^g(\nu \otimes e_s) = g\mu' g^{-1}(\nu \otimes e_s) = g\mu'(\nu \otimes e_{g^{-1}(s)}) = g e_{vug^{-1}(s)} = e_{g\nu g^{-1}(s)} \tag{2}$$

I, d'altra banda,

$$\mu'(p_g \otimes 1)(\nu \otimes e_s) = \mu'(p_g(\nu) \otimes e_s) = e_{p_g(\nu)(s)} \tag{3}$$

Ara (2) i (3) impliquen $p_g(\nu) = g\nu g^{-1}$.En particular, N és normalitzat per G.

Corol·lari 7. *Amb les mateixes notacions del teorema 6, suposem que es compleixen a) i b). Sigui $G_0 \subset G$ el grup dels elements que operen trivialment sobre N i sigui*

$$L_0 = \widetilde{K}^{G_0} \subset \widetilde{K}.$$

Aleshores L_0 és l'extensió de k més petita amb $L_0 \otimes H \simeq L_0[N]$.

Si $N \subset S_n$ és subgrup regular, tenim una bijecció

$$\begin{array}{rcl} \{1, 2, \ldots, n\} & \to & N \\ i & \mapsto & \mu_i \text{ determinat per } \mu_i(1) = i \end{array}$$

Per a cada $\sigma \in N$, definim $\phi_\sigma \in S_n$, per $\phi_\sigma(i) = \mu_i(\sigma(1))$. Tenim

$$Cent_{S_n}(N) = \{\phi_\sigma : \sigma \in N\} \simeq N^{op}.$$

Teorema 8. *Sigui $K|k$ una extensió de cossos separable. Suposem que existeix una extensió galoisiana $E|k$ tal que $K \otimes E$ és un cos que conté una clausura galoisiana $\widetilde{K}$ de $K|k$. Aleshores $K|k$ és H-Galois, on H és una E-forma de $k[N]$ i $N \simeq Aut(K \otimes E|E)$.*

Prova. a) Es pot provar $\widetilde{K} = \widetilde{K} \cap (KE) = K \cdot (\widetilde{K} \cap E) = K \otimes (\widetilde{K} \cap E)$ i posant $E' = \widetilde{K} \cap E$, tenim $E'|k$ Galois amb $K \otimes E' = \widetilde{K}$.
b) Suposem $K \otimes E = \widetilde{K}$. Siguin $N = \mathrm{Gal}(\widetilde{K}|E), G' = \mathrm{Gal}(\widetilde{K}|K)$. Aleshores N és complement normal de G' en G i per tant és regular sobre $S = G/G'$. Ara el grup oposat N^{op} és normalitzat per $G \subset B$ (es compleix $g\phi_\sigma g^{-1} = \phi_{g\sigma g^{-1}}$, per a $g \in G, \sigma \in N$) i centralitzat per $N \subset B$. Tenim doncs la condició b) del teorema 6 i per tant $K|k$ és H-Galois. A més, N opera trivialment sobre N^{op} i, pel corol·lari, l'isomorfisme $\widetilde{K} \otimes H \simeq \widetilde{K}[N]$ ja està definit sobre $\widetilde{K}^N = E$.

Extensions quasigaloisianes.

$\widetilde{K}$ clausura normal de $K|k$, $G = \mathrm{Gal}(\widetilde{K}|k), G' = \mathrm{Gal}(\widetilde{K}|K)$, $S = G/G', B = Perm(S)$.

Les condicions següents són equivalents:

(a) Existeix una extensió de Galois $E|k$ tal que $K \otimes E$ és un cos que conté $\widetilde{K}$.

(b) Existeix una extensió de Galois $E|k$ tal que $K \otimes E = \widetilde{K}$.

(c) G' té un complement normal a G.

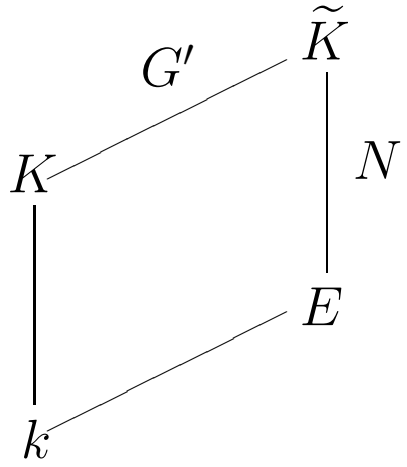
(d) Existeix un subgrup regular N de B normalitzat per G i contingut en G.

Diem que $K|k$ és *quasigaloisiana* si compleix les condicions equivalents anteriors.

Prova. Trivialment (b) $\Rightarrow$ (a)

(a) $\Rightarrow$ (b) com en el teorema 8.

(b) $\Rightarrow$ (c):



Posem $N := \mathrm{Gal}(\widetilde{K}|E)$.
Tenim $K \otimes E = \widetilde{K} \Rightarrow [K : k] \cdot [E : k] = [\widetilde{K} : k]$
$\Rightarrow K \cap E = k$.
Obtenim doncs $N \cap G' = 1, NG' = G$.
Ara $E|k$ Galois $\Rightarrow N \lhd G$.

(c) $\Rightarrow$ (b): Posem $E := \widetilde{K}^N$. Tenim $|N| \cdot |G'| = |G|$ i per tant $KE = \widetilde{K}$ i $K \cap E = k$. L'isomorfisme $KE \simeq K \otimes E$ ve del fet que K i E són linealment disjuntes sobre k, ja que $[K : k] \cdot [E : k] = [KE : k]$

(c) $\Leftrightarrow$ (d): Tenim $G \subset B$, G transitiu sobre S i $G' = Stab_G(\overline{e})$. Per a $N \subset G$, tenim

$$N \cdot G' = G \quad \text{sii} \quad N \text{ és transitiu;}$$
$$N \cap G' = \{e\} \quad \text{sii} \quad Stab_N(\overline{e}) = 1.$$

Proposició 9. *Sigui $K|k$ extensió separable de grau n, $G = Gal(\widetilde{K}|k)$.*

1. *Si $n = 2$, $K|k$ és galoisiana,*
2. *Si $n = 3$ o 4, $K|k$ és quasigaloisiana,*
3. *Si $n = 5$, $K|k$ és Hopf-Galois si i només si $G \neq A_5$ i $G \neq S_5$,*
4. *Si $n \geq 5$ i $G = A_n$ o S_n, aleshores $K|k$ no és Hopf-Galois,*
5. *Si $n \leq 7$, $K|k$ és Hopf-Galois si i només si és quasigaloisiana.*

Exemples.

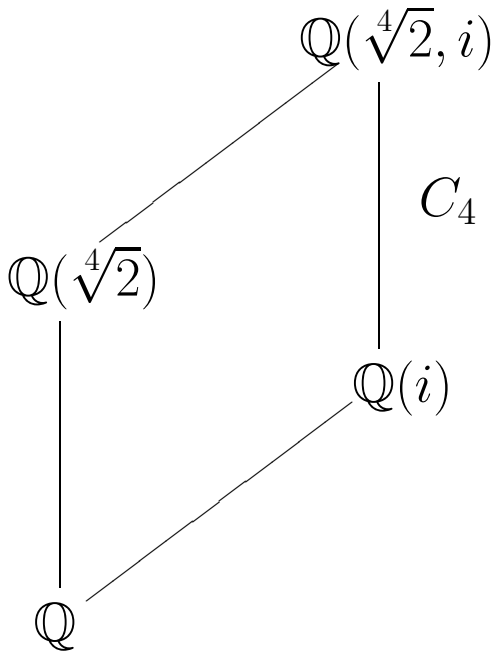
1. Considerem l'extensió $K = \mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$. L'extensió $\mathbb{Q}(i)|\mathbb{Q}$ és Galois i $\widetilde{K} = \mathbb{Q}(i)K$. L'extensió $\widetilde{K}|\mathbb{Q}(i)$ és Galois amb grup de Galois $N = C_4$. Per tant $K|\mathbb{Q}$ és H-Galois amb H una $\mathbb{Q}(i)$-forma de $\mathbb{Q}[N]$. Si e és generador de N, tenim $H_0 = \mathbb{Q}(i)[N] = \{\lambda_0 + \lambda_1 e + \lambda_2 e^2 + \lambda_3 e^3 : \lambda_i \in \mathbb{Q}(i)\}$. L'algebra de Hopf H és

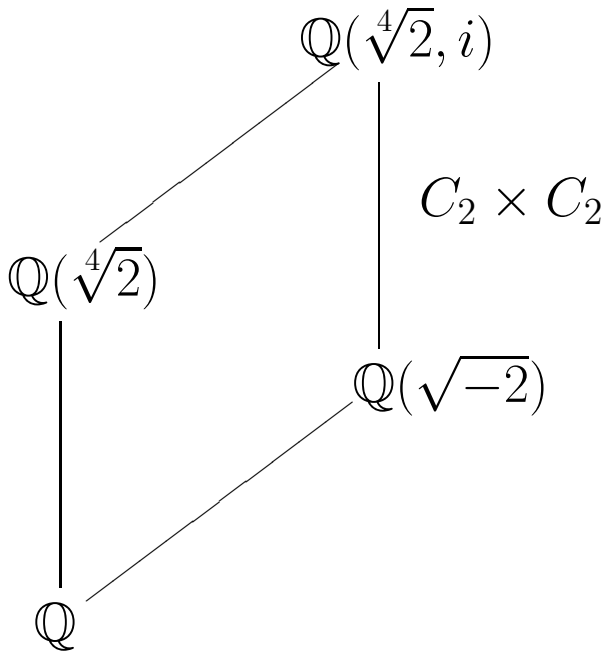
$$H = \mathbb{Q}\left[\frac{e + e^{-1}}{2}, \frac{e - e^{-1}}{2i}\right].$$

Tenim $Gal(\widetilde{K}|\mathbb{Q}) = D_4 = \{\rho, \sigma\}, \rho = (1234), \sigma = (13)$. Si prenem $N' = \langle \rho^2, \sigma \rangle \simeq C_2 \times C_2$, N' és regular i obtenim una $\mathbb{Q}$-álgebra de Hopf H', no isomorfa a la $\mathbb{Q}$-álgebra de Hopf considerada anteriormente. Posant $N' = \langle s, t | s^2 = t^2 = 1, st = ts \rangle$, tenim

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

Les dues estructures Hopf-Galois d'aquesta extensió corresponen als dos diagrames d'extensions de cossos següents.


$\mathbb{Q}(\sqrt[4]{2}, i)$
C_4
$\mathbb{Q}(\sqrt[4]{2})$
$\mathbb{Q}(i)$
$\mathbb{Q}$


$\mathbb{Q}(\sqrt[4]{2}, i)$
$C_2 \times C_2$
$\mathbb{Q}(\sqrt[4]{2})$
$\mathbb{Q}(\sqrt{-2})$
$\mathbb{Q}$

2. Considerem l'extensió $K = \mathbb{Q}(\sqrt[5]{2})|\mathbb{Q}$. Aleshores $\widetilde{K} = \mathbb{Q}(\sqrt[5]{2}, \zeta_5)$, $\mathrm{Gal}(\widetilde{K}|\mathbb{Q}) \simeq C_5 \rtimes C_4$ i l'extensió $K|\mathbb{Q}$ es quasigaloisiana.

Tenim $\widetilde{K} = \mathbb{Q}(\sqrt[5]{2}, \zeta_5)$, $[K : \mathbb{Q}] = 5$ i $G = \mathrm{Gal}(\widetilde{K}|\mathbb{Q})$ està generat pels automorfismes

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

que compleixen les relacions $\sigma^5 = Id, \tau^4 = Id, \tau\sigma\tau^{-1} = \sigma^3$. Veiem que $\langle\sigma\rangle$ és complement normal de $G' = \mathrm{Gal}(\widetilde{K}|K) = \langle\tau\rangle$ a G; per tant $K|\mathbb{Q}$ es quasigaloisiana amb $\mathbb{Q}$-àlgebra de Hopf H tal que

$$H \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta) \simeq \mathbb{Q}(\zeta)[C_5] = \{\lambda_0 + \lambda_1\sigma + \lambda_2\sigma^2 + \lambda_3\sigma^3 + \lambda_4\sigma^4 | \lambda_i \in \mathbb{Q}(\zeta)\}.$$

Calculem H com a subàlgebra d'elements invariants.

$$\tau(\sum_{i=0}^{4} \lambda_i\sigma^i) = \tau(\lambda_0) + \tau(\lambda_1)\sigma^2 + \tau(\lambda_2)\sigma^4 + \tau(\lambda_3)\sigma + \tau(\lambda_4)\sigma^3.$$

Per tant, $\sum_{i=0}^{4} \lambda_i\sigma^i$ és invariant per l'acció de G' si i només si

$$\lambda_0 \in \mathbb{Q}, \tau(\lambda_1) = \lambda_2, \tau(\lambda_2) = \lambda_4, \tau(\lambda_4) = \lambda_3, \tau(\lambda_3) = \lambda_1.$$

Posant $\lambda_1 = a + b\zeta + c\zeta^2 + d\zeta^3$, amb $a, b, c, d \in \mathbb{Q}$, obtenim

$$\begin{aligned}
\lambda_1 &= a + b\zeta + c\zeta^2 + d\zeta^3 \\
\tau(\lambda_1) &= a + b\zeta^2 + c\zeta^4 + d\zeta \\
\tau^2(\lambda_1) &= a + b\zeta^4 + c\zeta^3 + d\zeta^2 \\
\tau^3(\lambda_1) &= a + b\zeta^3 + c\zeta + d\zeta^4.
\end{aligned}$$

Un element de H és doncs de la forma

$$\lambda_0 + \lambda_1\sigma + \tau(\lambda_1)\sigma^2 + \tau^3(\lambda_1)\sigma^3 + \tau^2(\lambda_1)\sigma^4 = \lambda_0 + aA + bB + cC + dD,$$

on

$$\begin{aligned}
A &:= \sigma + \sigma^2 + \sigma^3 + \sigma^4 \\
B &:= \zeta\sigma + \zeta^2\sigma^2 + \zeta^3\sigma^3 + \zeta^4\sigma^4 \\
C &:= \zeta^2\sigma + \zeta^4\sigma^2 + \zeta\sigma^3 + \zeta^3\sigma^4 \\
D &:= \zeta^3\sigma + \zeta\sigma^2 + \zeta^4\sigma^3 + \zeta^2\sigma^4.
\end{aligned}$$

3. Sigui $K|k$ una extensió separable de grau 4 i sigui $\widetilde{K}$ la seva clausura galoisiana. Suposem $Gal(\widetilde{K}|k) = S_4$ i considerem un cos F amb $K \subset F \subset \widetilde{K}$ i $[F : k] = 8$. Aleshores, $F|k$ és Hopf-Galois però no quasigaloisiana.

El cos F és subcòs de $\widetilde{K}$ fix per un subgrup G' d'ordre 3 de G, posem $G' = \langle (1,2,3) \rangle$. Com S_4 no té cap subgrup normal d'ordre 8, G' no té complement normal a G i per tant $F|k$ no és quasigaloisiana.

Veiem ara que $F|k$ és Hopf-Galois per a alguna H. Tenim que $S = G/G'$ té 8 elements i per tant $B = Perm(S) \simeq S_8$. Hem de veure si existeix un subgrup N de B, regular sobre S i normalitzat per G (com a subgrup de B).

Les classes laterals de G/G' són

$$\begin{array}{ll} C_1 = \{Id, (1,2,3), (1,3,2)\}, & C_2 = \{(1,2), (1,3), (2,3)\}, \\ C_3 = \{(1,4), (1,4,2,3), (1,4,3,2)\}, & C_4 = \{(2,4), (1,2,4,3), (1,4,3,2)\}, \\ C_5 = \{(3,4), (1,2,3,4), (1,3,4,2)\}, & C_6 = \{(1,2,4), (1,3)(2,4), (2,43)\}, \\ C_7 = \{(1,3,4), (2,3,4), (1,2)(3,4)\}, & C_8 = \{(1,4,2), (1,4,3), (1,4)(2,3)\}. \end{array}$$

L'acció de G per traslació dóna la seva immersió en S_8:

$$\begin{aligned}(1,2,3,4) &\mapsto (1,5,6,3)(2,7,4,8)\\ (1,2) &\mapsto (1,2)(3,6)(4,8)(5,7)\end{aligned}$$

El subgrup de B

$$N = \langle (1,4)(2,8)(3,6)(5,7), (1,5)(2,6)(3,8)(4,7), (1,6)(2,5)(3,4)(7,8)\rangle$$

és regular i normalitzat per G.

Formes de les àlgebres de grup.

Teorema 10. *Sigui k un cos.*

a) Les àlgebres de Hopf que són k-formes de $k[\mathbb{Z}]$ són

$$H = k[c, s]/(s^2 - asc - bc^2 + u).$$

b) Les àlgebres de Hopf que són k-formes de $k[C_3]$ són

$$H = k[c, s]/(s^2 - asc - bc^2 + u, (c+1)(c-2), (c+1)(s-a)).$$

c) Les àlgebres de Hopf que són k-formes de $k[C_4]$ són

$$H = k[c, s]/(s^2 - asc - bc^2 + u, c(ac - 2s)).$$

d) Les àlgebres de Hopf que són k-formes de $k[C_6]$ són

$$H = k[c, s]/(s^2 - asc - bc^2 + u, (c-2)(c-1)(c+1)(c+2), (c-1)(c+1)(sc - 2a)).$$

En tots els casos, $a, b, u \in k$ compleixen $a^2 + 4b = u \in k^*$. L'estructura d'àlgebra de Hopf està definida per

$$\begin{aligned}
&\Delta(c) = u^{-1}((a^2 + 2b)c \otimes c - a(c \otimes s + s \otimes c) + 2s \otimes s);\\
&\Delta(s) = u^{-1}(-abc \otimes c + 2b(c \otimes s + s \otimes c) + as \otimes s);\\
&\varepsilon(c) = 2; \quad \varepsilon(s) = a; \quad S(c) = c; \quad S(s) = ac - s.
\end{aligned}$$

Teorema fonamental.

Teorema 11. *Sigui $K|k$ una extensió Hopf-Galois amb k-álgebra de Hopf H. Aleshores*

a) l'aplicació

$$\begin{array}{ccc} f : \{H' : H' \text{ es sub-àlgebra de Hopf de } H\} & \to & \{E : k \subset E \subset K, E \text{ cos }\} \\ H' & \mapsto & K^{H'} \end{array},$$

on $K^{H'} := \{x \in K : \mu(h)(x) = \varepsilon(h) \cdot x,\ \forall h \in H'\}$, és injectiva i inverteix les inclusions.

b) Si $E = K^{H'}$, l'extensió $K|E$ és Hopf-Galois amb E-àlgebra de Hopf $E \otimes_k H'$.

La prova de b) es basa en la teoria de Morita.

Teoria de Morita.

Donats un anell R commutatiu i R-àlgebres A, B, volem saber quan són equivalents les categories $\mathcal{M}_A$ d'A-mòduls per l'esquerra i $\mathcal{M}_B$ de B-mòduls per l'esquerra.

Definició 12. *Un* context de Morita *consisteix en les dades següents.*

(a) R-àlgebres A i B;

(b) un (A,B)-bimòdul P i un (B,A)-bimòdul Q, centralitzats per R;

(c) dos morfismes

$$\begin{array}{rcl} P \otimes_B Q & \to & A \\ x \otimes y & \mapsto & \{x,y\} \end{array} \qquad \begin{array}{rcl} Q \otimes_A P & \to & B \\ y \otimes x & \mapsto & [y,x] \end{array}$$

de (A,A)-bimòduls i (B,B)-bimòduls, respectivament,

tals que

$$\begin{aligned} \{x,y\}z &= x[y,z] \\ [y,z]w &= y\{z,w\} \end{aligned}$$

per a $x,z \in P, y,w \in Q$.

A partir d'un context de Morita, podem definir de forma natural morfismes d'àlgebres

$$\begin{array}{cccc} B \to End_A(P) & A \to End_B(P) & A \to End_B(Q) & B \to End_A(Q) \\ b \mapsto (x \mapsto xb)\,' & a \mapsto (x \mapsto ax)\,' & a \mapsto (y \mapsto ya)\,' & b \mapsto (y \mapsto by) \end{array}$$

i morfismes de bimòduls

$$\begin{array}{cccc} Q \to Hom_A(P,A) & P \to Hom_A(Q,A)) & P \to Hom_B(Q,B) & Q \to Hom_B(P,B) \\ y \mapsto (x \mapsto \{x,y\})\,' & x \mapsto (y \mapsto \{x,y\})\,' & x \mapsto (y \mapsto [y,x])\,' & y \mapsto (x \mapsto [y,x]) \end{array}$$

El context de Morita es diu *estricte* si $\{\ \}$ i $[\ ]$ són exhaustius.
Notem que, si P és R-mòdul fidel i $\{\ \}$ és exhaustiva, $[\ ]$ també ho és.

Teorema 13. *Suposem que* $A, B, P, Q, \{\ \}, [\ ]$ *formen un context de Morita estricte. Aleshores*

(a) $\{\ \} : P \otimes_B Q \to A$ *i* $[\ ] : Q \otimes_A P \to B$ *són isomorfismes;*

(b) P *i* Q *són mòduls projectius finitament generats sobre* A *i sobre* B*;*

(c) les aplicacions naturals indueixen isomorfismes d'àlgebres

$$A \simeq End_B(P) \simeq End_B(Q)\ ,\ \ B \simeq End_A(P) \simeq End_A(Q)$$

i isomorfismes de bimòduls

$$Q \simeq Hom_A(P, A) \simeq Hom_B(P, B)\ ,\ \ P \simeq Hom_A(Q, A) \simeq Hom_B(Q, B);$$

(d) els functors

$$Q \otimes_A (-) : \mathcal{M}_A \to \mathcal{M}_B,\ P \otimes_B (-) : \mathcal{M}_B \to \mathcal{M}_A$$

són equivalències de categories, inverses una de l'altra.

Sigui A una R-àlgebra de Hopf. Una R-àlgebra commutativa S es diu *A-objecte* si existeix un morfisme de R-àlgebres

$$\alpha : S \to S \otimes A$$

que indueix una estructura de A-comòdul en S.
Diem que l'A-objecte S és *A-objecte de Galois* si es compleix

1) S és R-mòdul fidelment pla;

2) el morfisme d'àlgebres

$$S \otimes S \overset{Id_S \otimes \alpha}{\longrightarrow} S \otimes S \otimes A \overset{m_S \otimes Id_A}{\longrightarrow} S \otimes A$$

és un isomorfisme.

Si A és R-àlgebra de Hopf finita i S un R-mòdul, tenim

$$Hom_R(S, S \otimes A) \simeq Hom_R(A^* \otimes S, S).$$

Per tant, si S és A-objecte, tenim $\beta : A^* \otimes S \to S$.

Sigui $K|k$ extensió de cossos finita, H una k-àlgebra de Hopf. La condició "$K|k$ és H-Galois" equival a "K és H^*-objecte de Galois amb $\alpha = \mu''$ (i $\beta = \mu'$)".

A partir d'ara prenem $R = k$ cos i A una k-àlgebra de Hopf commutativa.

Si S és A-objecte i $B^* \subset A^*$, posem $S^{B^*} := \{s \in S : us = \varepsilon(u)s,\ \forall u \in B^*\}$.

Si S és A-objecte i $S^{A^*} = k$, li podem associar un context de Morita. Considerem

1) $D := S\#A^*$ (producte creuat). Com a k-mòdul, $S\#A^* = S \otimes A^*$ i el producte està definit per

$$(x\#u)(y\#v) = \sum_{(u)} xu_{(1)}(y)\#u_{(2)}v \quad x, y \in S, v, u \in A^*.$$

Definim una estructura de D-mòdul a S per

$$(x\#u)y = xu(y), \quad x, y \in S, u \in A^*.$$

2) $Q = D^{A^*} := \{w \in D : (1\#u)w = \varepsilon(u)w = u(1)w, \text{per a tot } \ u \in A^*\}$ ideal per la dreta de D.

3) Definim $\{\ \} : S \otimes_k Q \to D, [\ ] : Q \otimes_D S \to S^{A^*} = k$ per les fòrmules

$$\{x, w\} = (x\#1)w, \quad [w, x] = wx, \quad x \in S, w \in Q.$$

Les k-àlgebres D i k; el (D,k)-bimòdul S, el (k,D)-bimòdul Q i els acoplaments $\{\ \}, [\ ]$ formen un context de Morita.

Teorema 14. *Sigui S un A-objecte. Són equivalents*

1. *S és un A-objecte de Galois*
2. *$S^{A^*} = k$ i el context de Morita $(D, k, S, Q, \{\ \}, [\ ])$ és estricte.*

Sigui ara $K|k$ una extensió de cossos H-Galois, H' una k-subàlgebra de Hopf de H. Posem $i^* : H^* \to H'^*$ el morfisme dual de la inclusió de H' en H. A partir de $\mu'' : K \to K \otimes H^*$, obtenim

$$\mu''_{H'} : K \xrightarrow{\mu''} K \otimes H^* \xrightarrow{Id_K \otimes i^*} K \otimes H'^* \simeq K \otimes_E (E \otimes H')^*$$

i, per tant la E-àlgebra K és un $(E \otimes H')^*$-objecte.
Li associem el context de Morita corresponent i es pot provar que és estricte. Obtenim doncs que $K|E$ és $(E \otimes H)$-Galois.

Lema 15. *Sigui A una k-àlgebra de Hopf, commutativa i finita.*

a) $\Delta_A : A \to A \otimes A$ *dota* A *d'estructura d'*A*-objecte.*

b) Siguin H' *una* k*-subàlgebra de Hopf de* $H = A^*$*. Aleshores*

$$H' = \{u \in H : \langle u, I\rangle = 0\},$$

on I *és l'ideal per la dreta de* A *generat pels elements de la forma* $x - \epsilon_A(x)$*, amb* $x \in A^{H'}$*.*

Corol·lari 16. *Sigui A una k-àlgebra de Hopf finita i commutativa i S un A-objecte de Galois. Siguin H_1, H_2 subàlgebres de Hopf de $H = A^*$. Aleshores $H_1 \subset H_2$ si i només si $S^{H_1} \supset S^{H_2}$.*

Idea de la prova. En el cas $S = A$, és conseqüència del lema. Per passar al cas general, usem

$$S \otimes S^{H_i} \simeq (S \otimes S)^{S \otimes H_i}.$$

Obtenim $S \otimes H_1 \subset S \otimes H_2$ que implica $H_1 \subset H_2$.

Teorema 17.

Si $K|k$ és quasigaloisiana, existeix una k-àlgebra de Hopf H tal que $K|k$ és H-Galois i l'aplicació

$$\begin{array}{ccc} f : \{H' : H' \text{ es sub-àlgebra de Hopf de } H\} & \to & \{E : k \subset E \subset K, E \text{ cos}\} \\ H' & \mapsto & K^{H'} \end{array},$$

és també exhaustiva.

Demostració. Si $K|k$ és quasigaloisiana, G' té un complement normal N a G. La forma H de $k[N^{op}]$ correspon a l'1-cocicle p_g, on p_g és la conjugació a B per l'element g de G. Ara el conjunt de sub-àlgebres de Hopf de H està en bijecció amb el conjunt de subgrups U de N^{op} estables per tots els p_g. Com $G = N \rtimes G'$ i N centralitza N^{op}, U és estable per tots els p_g, $g \in G$, si i només si ho és per tots els p_h, amb $h \in G'$. Ara tenim una bijecció

$$\begin{array}{ccc} \{V \text{ grup} : G' \subset V \subset G\} & \leftrightarrow & \{U \text{ subgrup de } N^{op} : U \text{ estable per } G'\} \\ V & \to & V \cap N \\ U \rtimes G' & \leftarrow & U \end{array}$$

Obtenim doncs $\#\{W \subset H : W \text{ sub-àlgebra de Hopf}\} = \#\{V \text{ grup} : G' \subset V \subset G\} = \#\{E \text{ cos} : k \subset E \subset K\}$.

Bases normals d'extensions Hopf-Galois.

Teorema 18 (Teorema de la Base Normal)**.** *Sigui $K|k$ una extensió de cossos, finita i galoisiana amb grup de Galois G. Aleshores, existeix un element $\rho \in K$ tal que*

$$\{\sigma(\rho) : \sigma \in G\}$$

és una k-base del k-espai vectorial K.

La tesi del Teorema de la Base Normal equival a:
"K és un mòdul lliure de rang 1 sobre l'àlgebra de grup $k[G]$ amb generador ρ."

Teorema 19 (Childs, 2000)**.** *Sigui $K|k$ una extensió finita i separable de cossos. Si $K|k$ és H-Galois per a alguna k-àlgebra de Hopf H, aleshores K és H-mòdul lliure de rang 1.*