

Hopf-Galois i Ramificació (salvatge)

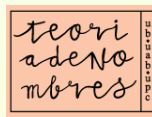
Anna Rio

Departament de Matemàtiques



UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

STNB 2016



30è aniversari

WORKSHOP SOBRE REPRESENTACIONS D'ARTIN I CORBES EL·LÍPTIQUES

29 - 30 de Juny, 1987

PROGRAMA

Dilluns, 29

9 : 30 - 11	J. GONZALEZ	Grups formals
11 : 30 - 13	M. NUÑEZ	El teorema de Hasse-Arf
15 - 16 : 30	A. RIO	Sobre la component salvatge del conductor
17 - 17 : 30	S. COMALADA	Corbes el·líptiques amb conductor trivial sobre cossos quadràtics

Take a walk on the wild side...

TEHA (Doctorat 86187)

Sobre la component salvatge del conductor

Objectiu. Donada una corba el·líptica E/K_F , l'exponent del conductor f_E s'ha definit com una suma,
 $f_E = E_E + \tilde{E}_E$, en la qual:

$$E_E = \dim_{\mathbb{Q}_\ell} V_\ell / V_\ell^{I_E}$$

$$\tilde{E}_E = \sum_{i=1}^{\infty} \frac{e_i}{e_0} \dim_{\mathbb{F}_\ell} E[e] / E[e]^{G_{E,i}}$$

Es tracta de millorar la definició de $\tilde{E}_E$, produint una quantitat (b_E) llegible en el mòdul de Tate.

... de la mà dels grups de ramificació...

K és complet per una valoració discreta v_K

A_K anell de valoració corresponent

m_K maximal de A_K

$k = A_K/m_K$ és residual, que suposarem perfecte

L/K extensió de Galois finita

Local fields $\left. \begin{array}{l} \text{Ch 2 q2 Prop 3} \\ \text{Ch 3 q6 Prop 12} \end{array} \right\} \rightarrow A_L \text{ té una } A_K\text{-base de la} \\ \text{forma } 1, x, \dots, x^{n-1} \text{ amb } x \in A_L \\ \text{i } n = [L:K]$

Lema (L.F. Ch 4 q1 lema 1)

Si $G = \text{Gal}(L/K)$ i $\sigma \in G$, $\forall i \geq -1$ són equivalents

a) σ opera trivialment en l'anell quocient A_L/m_L^{i+1}

b) $v_L(\sigma(a) - a) \geq i+1 \quad \forall a \in A_L$

c) $v_L(\sigma(x) - x) \geq i+1$

Definició de l'i-èsim grup de ramificació de G :

$$G_i = \{ \sigma \in G \mid v_L(\sigma(x) - x) \geq i+1 \} =$$

$$= \{ \sigma \in G \mid v_L(\sigma(a) - a) \geq i+1 \quad \forall a \in A_L \} =$$

$$= \{ \sigma \in G \mid \sigma \text{ opera trivialment en } A_L/m_L^{i+1} \}$$

...passant per la representació de Swan...

$$\underline{sw_G = a_G - \text{Ind}_{G_0}^G(u_{G_0}) = \sum_{i=1}^{\infty} \frac{g_i}{g_0} \text{Ind}_{G_i}^G(u_{G_i})}$$

És el caràcter d'una representació de G
(representació de Swan)

$$\text{Ind}_{G_i}^G(u_{G_i})(\sigma) = \begin{cases} 0 & \text{si } \sigma \notin G_i \quad (G_i \text{ subgrups normals de } G) \\ -\frac{g}{g_i} & \text{si } \sigma \in G_i, \sigma \neq 1 \\ \frac{g(g_i-1)}{g_i} & \text{si } \sigma = 1 \end{cases}$$

$$(g = -fg_0)$$

Ja que $G/G_0 \simeq \text{Gal}(\tilde{L}/k)$ i $f = [\tilde{L}:k]$

$\overline{G_0}$ grup d'inversió de l'extensió

$$a_G = (a_{G_0})^* = \text{Ind}_{G_0}^G(a_{G_0})$$

$\rightarrow$ Podem reduir-nos al cas totalment ramificat ($f=1$)

$$\underline{sw_G = 0} \Leftrightarrow G_4 = \{1\} \Leftrightarrow \underline{L/k \text{ moderadament ramificada.}}$$

...per acabar amb el 2...

J. reine angew. Math. 517 (1999), 1–17

Journal für die reine und
angewandte Mathematik

© Walter de Gruyter
Berlin · New York 1999

Dyadic exercises for octahedral extensions

In memory of Jürgen Neukirch

By *Pilar Bayer* and *Anna Rio* at Barcelona

Abstract. The object of this paper is the description of a family of extensions of dyadic type of the field $\mathbb{Q}_2$ of the 2-adic numbers. Let $\tilde{S}_4$ be the double cover of the symmetric group S_4 that has as matrix model the general linear group $\mathrm{GL}(2, \mathbb{F}_3)$. Modulo isomorphisms, the number of Galois extensions of $\mathbb{Q}_2$ having as Galois group a non-

... el més salvatge de tots els primers!

Table 12

Ramification of 2 in an extension $\tilde{K}/\mathbb{Q}$ with Galois group $\tilde{S}_4$

Condition	$G _0, G_1, G_2, \dots$ in $\tilde{K}/\mathbb{Q}$
$v_2(d_{K_1}) = 0$	$\{1\}$ C_3^A, C_2^A C_2^A, C_2^A, C_2^A
$v_2(d_{K_1}) = 2, v_2(d_M) = 0$	C_3 C_6, C_2^A, C_2^A, C_2^A $C_6, C_2^A, C_2^A, C_2^A, C_2^A, C_2^A, C_2^A, C_2^A$
$v_2(d_{K_1}) = 2 = v_2(d_M)$ and $2 = p_1^2 p_1' p_1''$	C_2^B, C_2^B V_4, V_4, C_2^A, C_2^A
$v_2(d_{K_1}) = 2 = v_2(d_M)$ and $2 = p_1^2 p_2$	V_4, V_4 V_4, V_4, C_2^A, C_2^A
$v_2(d_{K_1}) = 3$	C_2^B, C_2^B, C_2^B V_4, V_4, C_2^B, C_2^B
$v_2(d_{K_1}) = 4$	$\tilde{A}_4, H_8, C_2^A, C_2^A$ $\tilde{A}_4, H_8, C_2^A, C_2^A, C_2^A, C_2^A, C_2^A, C_2^A, C_2^A, C_2^A$ $\tilde{A}_4, H_8, C_2^A, \dots, C_2^A$ 20
$v_2(d_{K_1}) = 5$	$D_8, D_8, V_4, V_4, C_2^A, C_2^A$
$v_2(d_{K_1}) = 6,$ $v_2(d_M) = 0$ and $2 \neq p_1^4$	$C_4, C_4, C_4, C_2^A, C_2^A$
$v_2(d_{K_1}) = 6,$ $v_2(d_M) = 0$ and $2 = p_1^4$	H_8, H_8, C_2^A, C_2^A $H_8, H_8, C_2^A, C_2^A, C_2^A, C_2^A$
$v_2(d_{K_1}) = 6, v_2(d_M) = 2$	$D_8, D_8, C_4, C_4, C_2^A, C_2^A, C_2^A, C_2^A$
$v_2(d_{K_1}) = 8, v_2(d_{L_1}) = 0$	$H_8, H_8, C_4, C_4, C_2^A, C_2^A, C_2^A, C_2^A$
$v_2(d_{K_1}) = 8, v_2(d_{L_1}) = 2$	$\tilde{A}_4, H_8, H_8, H_8, H_8, C_2^A, \dots, C_2^A$ 10
$v_2(d_{K_1}) = 9$	$SD_{16}, SD_{16}, D_8, D_8, C_4, C_4, C_2^A, \dots, C_2^A$ 8
$v_2(d_{K_1}) = 10$	$SD_{16}, SD_{16}, H_8, H_8, C_4, C_4, C_2^A, \dots, C_2^A$ 8
$v_2(d_{K_1}) = 11$	$C_8, C_8, C_8, C_4, C_4, C_2^A, C_2^A, C_2^A, C_2^A$ $SD_{16}, SD_{16}, C_8, C_8, C_4, C_4, C_4, C_4, C_2^A, \dots, C_2^A$ 8

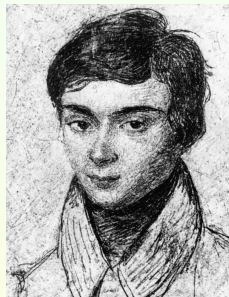
34

2. Exercicis diàdics

- 4) G_1 és el p -subgrup de Sylow de G_0 i G_0/G_1 és cíclic. Si $i \geq 1$, els quocients G_i/G_{i+1} són grups abelians, producte directe de grups cíclics d'ordre p .
- 5) Si $\sigma \in G_i$ i $\tau \in G_j$, amb $i, j \geq 1$, aleshores $\sigma\tau\sigma^{-1}\tau^{-1} \in G_{i+j}$.
- 6) Si G és abelià, per a cada i no divisible per l'ordre de G_0/G_1 es té $G_i = G_{i+1}$.
- 7) Els enters $i \geq 1$ tals que $G_i \neq G_{i+1}$ són tots congruents entre sí mòdul p .

Nombres de ramificació

STNB12: Hopf-Galois



K/k finita

K/k Hopf-Galois



Existeixen

- una k -àlgebra de Hopf H de dimensió finita
- una acció de Hopf $\mu : H \rightarrow \text{End}_k(K)$ (K és H -mòdul)

amb

$(1, \mu) : K \otimes_k H \rightarrow \text{End}_k(K)$ isomorfisme

$$\implies \dim H = [K : k]$$

K/k **Galois**



$(1, \mu) : K \otimes_k k[G] \rightarrow \text{End}_k(K)$ isomorfisme

amb $(1, \mu)(s \otimes h)(t) = s \cdot (\mu(h)(t))$

No unicitat: una extensió Hopf Galois pot tenir diverses estructures Hopf Galois associades

Crespo, T.; Rio, A.; Vela, M.: Non-isomorphic Hopf Galois structures with isomorphic underlying Hopf algebras, J. Algebra 422 (2015), 270-276.

Extensions Hopf Galois separables

K/k **separable** de grau n

- $\tilde{K}/k$ clausura normal de K/k
- $G = \text{Gal}(\tilde{K}/k)$

Contenen la informació sobre el caràcter Hopf Galois de K/k

Greither-Pareigis

K/k Hopf Galois $\Leftrightarrow \exists$ subgrup **regular** $N \subseteq S_n$ normalitzat per G

Enumeració d'estructures Hopf Galois: prob. de teoria de grups.

L/K **Galois no abeliana**, com a mínim **dues** estructures diferents:
clàssica $N = \rho(G)$ i no clàssica $N = \lambda(G)$

Extensions Hopf Galois separables

Álgebra de Hopf associada

(twist d'una àlgebra de grup)

$$H = \tilde{K}[N]^G$$

G opera a $\tilde{K}$ com a grup d'automorfismes

G opera a N per conjugació

H es un $\tilde{K}$ -forma de $\tilde{K}[N]$:

$$H \otimes_{\tilde{K}} \tilde{K} \simeq \tilde{K}[N]$$

Acció de Hopf $\mu : H \rightarrow \text{End}_K(K)$

$$\left(\sum_{n \in N} c_n n \right) x = \sum_{n \in N} c_n n^{-1}(\bar{1}_G)(x)$$

Mòduls galoisians

Un mòdul galoisià és un $\mathbb{Z}[G]$ —mòdul amb G grup de Galois d'una extensió de cossos

Exemples Si $G = \text{Gal}(L/K)$ amb L/K cossos de nombres

- el cos L
- l'anell d'enters $\mathcal{O}_L$
- el grup d'unitats $\mathcal{O}_L^*$
- el grup de classes $\text{Cl}(\mathcal{O}_L)$
- el grup $E(L)$ de punts L —racionals d'una corba el·líptica E/K
- ...

Bases normals enteres

Teorema de la Base Normal

L/K extensió de cossos Galois finita amb grup G

Existeix $\alpha \in L$ tal que $\{\sigma(\alpha) \mid \sigma \in G\}$ és K -base de L .

És a dir, L és $K[G]$ -mòdul lliure de rang 1.

L/K extensió de cossos de nombres o cossos p -àdics, Galois finita amb grup G

té **base normal entera** si existeix un element $\alpha \in \mathcal{O}_L$ tal que els seus conjugats formen una $\mathcal{O}_K$ -base de $\mathcal{O}_L$.

Equivalentment, si $\mathcal{O}_L$ és $\mathcal{O}_K[G]$ -mòdul lliure de rang 1

Teorema de Noether (1931)

Dem Swan 1960

L/K Galois finita de cossos **locals**

Existeix base normal entera $\iff L/K$ moderadament ramificada

Teorema de Hilbert-Speiser

$L/\mathbb{Q}$ **abeliana** finita

Existeix base normal entera $\iff L/\mathbb{Q}$ moderadament ramificada
Equiv. existeix n senar i lliure de quadrats tal que $L \subseteq \mathbb{Q}(\zeta_n)$

Martinet (1971) $L = K(\sqrt{\frac{1+\sqrt{5}}{2} \cdot \frac{1+\sqrt{21}}{2}})$ amb $K = \mathbb{Q}(\sqrt{5}, \sqrt{21})$

$L/\mathbb{Q}$ extensió **H_8 (quaternions)** moderadament ramificada
 $\mathcal{O}_L$ no és $\mathbb{Z}[H_8]$ -lliure (i.e. no existeix base normal entera)

Extensions de cossos de nombres

L/K extensió de cossos de nombres moderadament ramificada

Noether $\implies \mathcal{O}_L$ és $\mathcal{O}_K[G]$ -localment lliure

L'obstrucció per ser lliure és la seva classe al grup de classes localment lliure $Cl(\mathcal{O}_K[G])$

Restricció d'escalars: la classe de $\mathcal{O}_N$ a $Cl(\mathbb{Z}[G])$ està determinada per funcions L d'Artin

Més exemples d'extensions moderadament ramificades de $\mathbb{Q}$ amb base normal entera?

Conjectura de Fröhlich

Classe de OL en el grup $Cl(\mathbb{Z}[G])$

Generalització de la resolvent de Lagrange i de sumes de Gauss

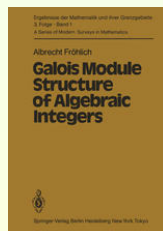
Logaritme en anells de grup locals

Analytic root number class

Artin Root numbers de caràcters simplèctics

Teorema de Taylor (1981)

Taylor, M. J.: *On Fröhlich's conjecture for rings of integers of tame extensions.* Invent. Math. 63 (1981), 41-79



Galois module structure of algebraic integers.

A. Fröhlich, 1983

Cos base diferent de $\mathbb{Q}$?

Greither, Replogle, Rubin, Srivastav (1999) *Swan modules and Hilbert Speiser number fields*

- El cos $\mathbb{Q}$ és l'únic cos base sobre el qual totes les extensions abelianes moderadament ramificades tenen base normal entera
- Per a tot cos de nombres $K \neq \mathbb{Q}$ existeix un primer p i una extensió moderadament ramificada L/K cíclica de grau p que no té base normal entera

Gómez Ayala (1994) *Bases normales d'entiers dans les extensions de Kummer de degré premier*

Criteri explícit per a l'existència de base normal entera en el cas moderadament ramificat

Ordre associat $\mathcal{A}_{L/K} = \{\alpha \in K[G] \mid \alpha \mathcal{O}_L \subseteq \mathcal{O}_L\}$

- és un $\mathcal{O}_K$ -ordre de $K[G]$
- és $\mathcal{O}_K$ -mòdul lliure de rang $[L : K]$
- és l'únic $\mathcal{O}_K$ -ordre de $K[G]$ sobre el qual $\mathcal{O}_L$ pot ser lliure

$$\mathcal{A}_{L/K} = \mathcal{O}_K[G] \iff L/K \text{ moderadament ramificada}$$

Teorema (Leopoldt, 1959)

$L/\mathbb{Q}$ abeliana finita $\implies \mathcal{O}_L$ és $\mathcal{A}_{L/K}$ -mòdul lliure de rang 1

Exemple: $L = \mathbb{Q}(\sqrt{2})$

$$\mathcal{O}_L = \mathbb{Z}[\sqrt{2}]$$

Ramificació salvatge en $p = 2$

$$G = \text{Gal}(L/\mathbb{Q}) = \{1, \sigma\}$$

$$e_1 = \frac{1 + \sigma}{2} \quad e_{-1} = \frac{1 - \sigma}{2}$$

Idempotents centrals de suma 1 $\implies \mathbb{Z}[e_1, e_{-1}]$ és $\mathbb{Z}[G]$ -ordre maximal de $\mathbb{Q}[G]$

$$e_1(a + b\sqrt{2}) = a \quad e_{-1}(a + b\sqrt{2}) = b\sqrt{2}$$

$$\implies \mathbb{Z}[e_1, e_{-1}] \subseteq \mathcal{A}_{L/\mathbb{Q}} \implies \mathbb{Z}[e_1, e_{-1}] = \mathcal{A}_{L/\mathbb{Q}}$$

$\mathbb{Z}[\sqrt{2}]$ és $\mathcal{A}_{L/\mathbb{Q}}$ -lliure amb base $\alpha = 1 + \sqrt{2}$

$$a + b\sqrt{2} = (ae_1 + be_{-1})\alpha$$

O_L és $\mathcal{A}_{L/K}$ -lliure?

- **A.M. Bergé** $L/\mathbb{Q}$ diedral d'ordre $2p$ (p senar)
Diedrals d'ordre $\neq 2p$: O_L no és projectiu sobre l'ordre associat
- **Martinet** $L/\mathbb{Q}$ amb grup de Galois H_8 salvatgement ramificada
- **Byott, Lettl** $L/K/\mathbb{Q}$ tal que $L/\mathbb{Q}$ abeliana i K ciclotòmic

Cap a la teoria de mòduls Hopf Galoisians

Estructures Hopf Galois en extensions d'anells?

R anell commutatiu amb unitat

H una R -biàlgebra

$$\begin{array}{ll} m : H \otimes_R H \rightarrow H & \text{multiplicació} \quad \iota : R \rightarrow H \text{ unitat} \\ \Delta : H \rightarrow H \otimes_R H & \text{comultiplicació} \quad \epsilon : H \rightarrow R \text{ counitat} \end{array}$$

Antípoda $\lambda : H \rightarrow H$

antihomomorfisme de R -àlgebres i de R -coàlgebres

tal que $m(1 \otimes \lambda)\Delta = \iota\epsilon = m(\lambda \otimes 1)\Delta$

R -àlgebra de Hopf

Finita: R -mòdul finitament generat i projectiu

Ordres de Hopf

R Dedekind amb cos de fraccions K , de característica zero
 H una K -àlgebra de Hopf finita

Un R -ordre de H és un **ordre de Hopf** si amb les operacions heretades de H és una R -àlgebra de Hopf

Exemple $R[G]$ és ordre de Hopf de $K[G]$, minimal

Si Λ és un R -ordre de $K[G]$, llavors

$\Delta(\Lambda) \subseteq \Lambda \otimes_R \Lambda \implies \Lambda$ és ordre de Hopf

Anàleg de $R[G]$ en una H qualsevol?

H pot no tenir cap ordre de Hopf

Mòduls Hopf Galoisians

“Teorema de la Base Normal”

L/K finita separable Hopf Galois amb àlgebra H

L és H -mòdul lliure de rang 1

L/K extensió de cossos de nombres o cossos p -àdics, Hopf Galois amb àlgebra H

Ordre associat

$$\mathcal{A}_H = \{h \in H \mid \mu(h) \mathcal{O}_L \subseteq \mathcal{O}_L\}$$

$\mathcal{O}_L$ és $\mathcal{A}_H$ -mòdul

$\mathcal{A}_H$ és l'únic ordre de H sobre el qual $\mathcal{O}_L$ pot ser lliure

Mòduls Hopf Galoisians... on the tame side

Cas local

Si $\mathcal{A}_H$ és un **ordre de Hopf**, $\mathcal{O}_L$ és $\mathcal{A}_H$ -mòdul lliure

Per exemple, quan L/K no ramificada

Cas local

L/K Hopf Galois amb H commutativa i $p \nmid [L : K]$

$\mathcal{A}_H$ és l'únic ordre maximal de H i $\mathcal{O}_L$ és $\mathcal{A}_H$ -mòdul lliure

Cas local moderadament ramificat general (generalització del teorema de Noether) no complet

- $H = L[N]^G$. El $\mathcal{O}_K$ -ordre $\mathcal{O}_L[N]^G$ és **ordre de Hopf** de H si i només si el nucli de l'acció de G en N conté el **grup d'inèrcia** de L/K
- La condició ordre de Hopf no és necessària

Tornem als orígens

K extensió finita de $\mathbb{Q}_p$ $e = e_{K/\mathbb{Q}_p}$ índex de ramificació

L/K extensió de Galois amb grup G

$$G_i = \{\sigma \in G \mid (\sigma - 1)\mathcal{O}_L \subseteq \mathfrak{P}^{i+1}\} \quad \text{grups de ramificació}$$

$$G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots \supseteq \{1\}$$

G_1 és el p -Sylow de G_0

Nombres de ramificació t tals que $G_t \neq G_{t+1}$

p -extensions

Suposem $e_{L/K} = p^n = |G_1|$

$$t_i = \max\{j \mid |G_j| > p^{n-i}\} \quad 1 \leq t_1 \leq t_2 \leq \cdots \leq t_n$$

p -extensions abelianes totalment ramificades

O bé $t_1 = ep/(p-1)$ o bé $p \nmid t_1$ i $1 \leq t_1 < ep/(p-1)$

Problema

Si coneixem els nombres de ramificació (o la cadena sencera de grups de ramificació), què podem dir de l'estructura de $\mathcal{O}_L$ com a mòdul Hopf galoisià?
(O de l'estructura dels ideals fraccionaris)

$$\mathfrak{D}_{L/K}^{-1} = \{x \in L \mid \text{Tr}_{L/K}(x\mathcal{O}_L) \subseteq \mathcal{O}_K\} = \mathfrak{P}^{-\omega}$$

$$\omega = \sum_{j \geq 0} (|G_j| - 1) = (t_1 + 1)(p^n - 1) + \sum_{i=1}^{n-1} (t_{i+1} - t_i)(p^{n-i} - 1)$$

Quan $\mathfrak{D}_{L/K}^{-1}$ és lliure i $\mathfrak{D}_{L/K}^{-1} = c\mathcal{O}_L$ llavors $\mathcal{O}_L$ també és lliure

On the wild side

L/K cíclica de grau p totalment ramificada $G = \text{Gal}(L/K)$

Única estructura Hopf Galois (la clàssica): $H = K[G]$

Noether: $\mathcal{O}_L$ no és $\mathcal{O}_K[G]$ -lliure

$e = e_{K/\mathbb{Q}_p}$ $e' = \frac{e}{p-1}$ t nombre de ramificació: $G_t = C_p$, $G_{t+1} = \{1\}$

Suposem $t < [pe'] - 1$. Sigui $s = t \bmod p$ (rep. entre 0 i $p-1$)

$\mathcal{O}_L$ és lliure sobre l'ordre associat $\mathcal{A}_{K[G]} \iff s \mid p-1$

On the wild side

Childs

L/K p -extensió abeliana amb $e_{L/K} = p^n$

$e = e_{K/\mathbb{Q}_p}$ Suposem $t_n - \left\lfloor \frac{t_n}{p} \right\rfloor < p^{n-1}e$ i $\omega \equiv 0 \pmod{p^n}$

Si $\mathcal{O}_L$ és lliure sobre el seu ordre associat $\mathcal{A}_{K[G]}$, aleshores $t_i \equiv -1 \pmod{p^n}$ per a tot $1 \leq i \leq n$

Investigar nombres de ramificació de p -extensions abelians tals que l'ordre associat és un ordre de Hopf de $K[G]$

Byott

Usant cossos de punts de divisió d'un grup de Lubin-Tate mostra dues estructures Hopf Galois amb diferent comportament a nivell local

On the wild side

Childs

L/K cíclica de grau p^2 (p senar) ($K/\mathbb{Q}_p$ finita, conté $\zeta = \zeta_p$)
 $\text{Gal}(L/K) = \langle \sigma \rangle$

$$M = L^{\langle \sigma^p \rangle} = K(\mathbf{z}) \quad \mathbf{z}^p \in K \quad \sigma(\mathbf{z}) = \zeta \mathbf{z}$$

$$L = M(x) \quad \sigma^p(x) = \zeta x \quad \sigma(x) = \beta x \quad \beta \in \mathcal{O}_M \text{ i } N_{M/K} \beta = \zeta$$

Hi ha p estructures Hopf Galois ($d = 0, 1, \dots, p-1$)

$$N_d = \langle \eta_d \rangle \subset \text{Sym}(G) \quad \eta_d(\sigma^i) = \sigma^{(i-1)(1+pd)} \quad v = z^{-d}$$

$$H_d = K[\eta^p, a_v \eta]$$

$$t_1 = pj - 1 \quad t_2 = p^2 i - 1 \quad 0 \leq i, j \leq e' = \frac{e}{p-1} \quad i' = e' - i$$

$$\beta \equiv v^{-1} \pmod{\pi^{i'+j} \mathcal{O}_M} \iff \mathcal{O}_L \text{ lliure sobre l'ordre associat } \mathcal{A}_{H_d}$$

On the wild side

- En aquest cas cíclic, si $\mathcal{O}_L$ és lliure sobre un $\mathcal{A}_d$, ho és sobre tots ($d = 0, 1, \dots, p-1$)

No hi ha una estructura Hopf Galois millor que una altra

- (Byott) En el cas abelià elemental hi ha p^2 estructures Hopf Galois i es troben casos en què $\mathcal{O}_L$ és lliure sobre l'ordre associat i casos en què no ho és

Casos en què $\mathcal{O}_L$ no és lliure sobre $\mathcal{A}_{K[G]}$ i sí que ho és sobre un altre $\mathcal{A}_H$

Journal of Algebra **248**, 334–365 (2002)

doi:10.1006/jabr.2001.9053, available online at <http://www.idealibrary.com> on 

Integral Hopf–Galois Structures on Degree p^2 Extensions of p -adic Fields

Nigel P. Byott

Altres exemples, altres famílies, extensions no galoisianes...

Explicitar estructures Hopf Galois

Ordres de Hopf $\mathcal{H}$ en les àlgebres de Hopf
corresponents

Criteris per a que $\mathcal{O}_L/\mathcal{O}_K$ sigui $\mathcal{H}$ -Galois

Cas no galoisià: **Candidats a substituir els nombres
de ramificació?**

Estructures Hopf Galois induïdes

Crespo, R., Vela: Induced Hopf Galois structures

Si $\text{Gal}(L/K) = H \rtimes G'$, aleshores L/K té almenys
una estructura Hopf Galois amb $N \simeq H \times G'$

Altres mòduls galoisians

Punts de divisió de corbes el·líptiques, ...

Estudiar **scaffolds** (bastides)

Existeix una valoració (un certificat enter) que garanteixi que qualsevol element amb aquesta valoració és generador d'una base normal?

Challenge (...no cash reward)

Take any instance of Galois action in previous talks (or anything you like) and try the Hopf Galois point of view.

Any new result?