Hopf-Galois module structure of dihedral local extensions

Anna Rio   Daniel Gil

Math Department

UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

16 March 2019

Galois modules

L/k finite Galois field extension with group $G \implies L$ is a $k[G]-$module

Normal Basis Theorem L is a free $k[G]-$module of rank one

L/k local fields with integer rings $\mathcal{O}_L, \mathcal{O}_k$

Theorem (E. Noether, Normal Integral Basis)

$\mathcal{O}_L$ free $\mathcal{O}_k[G]-$ module $\iff L/k$ at most tamely ramified

What for wildly ramified L/k ?
Idea: replace

$$\mathcal{O}_k[G] \longleftarrow \mathfrak{A} = \{h \in k[G] \mid h \cdot x \in \mathcal{O}_L \ \forall x \in \mathcal{O}_L\}$$

the associated order   Is $\mathcal{O}_L$ a free $\mathfrak{A}-$module?

Examples

- $k = \mathbb{Q}$ and G abelian (Leopoldt)
- $k = \mathbb{Q}$ and $G = D_{2p}$ (Bergé)
- If $k = \mathbb{Q}_p$(or finite extension) and $Gal(L/k) = C_p$

  t $(\neq -1)$ the ramification number. We have $1 \leq t \leq \dfrac{pe}{p-1}$

  $a = t \ mod \ p$

  - $a = 0 \implies \mathcal{O}_L$ free $\mathfrak{A}-$module
  - $a \neq 0$ and $t < \frac{pe}{p-1} - 1$

  $$\mathcal{O}_L \text{ free } \mathfrak{A} - \text{module} \iff a \mid p-1$$

  - *presque maximal* $\quad \frac{pe}{p-1} - 1 \leq t \leq \frac{pe}{p-1}$

  $$\frac{t}{p} = [a_0, a_1 \ldots, a_n] \text{ continued fraction}$$

  $\mathcal{O}_L$ free $\mathfrak{A}-$module $\iff n \leq 4$ (Bertrandias, Bertrandias, Ferton)

Examples

- (Byott) L/k abelian extension of $p-$adic fields, wildly and weakly ($G_2 = 1$) ramified

$$\mathcal{O}_L \text{ free } \mathfrak{A} - \text{module}$$

- (Johnston) L/k wildly and weakly ramified finite Galois extension of complete local fields with finite residue fields

$$\mathcal{O}_L \text{ free } \mathfrak{A} - \text{module}$$

Hopf Galois-module structures

K/k finite

K/k Hopf-Galois

$\Updownarrow$

There exist

- a $k-$Hopf algebra H of finite dimension
- a Hopf action $\mu : H \to End_k(K)$ (K *is* H*-module*)

such that

$$(1, \mu) : K \otimes_k H \to End_k(K) \text{ isomorphism}$$

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

Separable Hopf Galois Extensions

K/k separable

- $\widetilde{K}/k$ normal closure K/k
- $G = Gal(\widetilde{K}/k) \qquad G' = Gal(\widetilde{K}/K)$

Provide the information on the Hopf Galois character of K/k

Greither-Pareigis

K/k Hopf Galois $\Leftrightarrow \exists$ regular subgroup $N \subseteq Sym(G/G')$ normalized by $\lambda(G)$

$\lambda(G), \rho(G)$ image of G under left,right regular reperesentation

Separable Hopf Galois Extensions

Let K/k be a separable field extension, then there is a one-to-one correspondence between

1. Hopf-Galois structures on K/k
2. regular subgroups $N \subseteq Sym(G/G')$ normalized by $\lambda(G)$

L/k Galois non abelian, at least two different structures:
classical $N = \rho(G)$ and non classical $N = \lambda(G)$

Separable Hopf Galois Extensions

Hopf algebra attached (twist of a group algebra)

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

G acts on $\widetilde{K}$ as automorphism group
$\lambda(G)$ acts on N via conjugation

Hopf action $\mu : H \longrightarrow End_k(K)$

$$\left(\sum_{n \in N} c_n n\right) \cdot x = \sum_{n \in N} c_n \; n^{-1}(\,\overline{1}_G\,)(x)$$

Associated orders

L/k Galois extension of local fields with integer rings $\mathcal{O}_L, \mathcal{O}_k$
L/k Hopf Galois with algebra H

$$\mathfrak{A}_H = \{h \in H \mid h\mathcal{O}_L \subseteq \mathcal{O}_L\}$$

the associated order. Is $\mathcal{O}_L$ a free $\mathfrak{A}-$module?

- Classical Galois structure: $H = k[G]$
- Structure corresponding to regular group N: $H = L[N]^G$

Induced Hopf Galois structures

L/k Galois
$G = Gal(L/k)$
$G' = Gal(L/F)$

$$\begin{array}{c} L \\ | \\ F \\ | \\ k \end{array}$$

Assume G' has normal complement in G

If N_1 gives a Hopf Galois structure for F/k and N_2 gives a Hopf Galois structure for L/F, then

$$N_1 \times N_2 \subseteq Sym(G/G') \times Sym(G') \subseteq Sym(G)$$

gives a Hopf Galois structure for L/k Induced

Crespo, T; Rio, A; Vela, M: Induced Hopf Galois structures. J. Algebra 457 (2016) 312-322.

Induced Hopf Galois structures

A Galois extension L/k with Galois group $G = G_1 \rtimes G'$ has at least one split Hopf Galois structure of type $G_1 \times G'$

$$\lambda(G_1) \times \rho(G') \subset Sym(G)$$

For Galois groups of order $2p$, split structures are induced

Local extensions with dihedral Galois group D_{2p}

p odd prime
$K/\mathbb{Q}_p$ degree p, normal closure $L/\mathbb{Q}_p$ with Galois group $G \simeq D_{2p}$

1. $p = 3$ six non-isomorphic cubic extensions of $\mathbb{Q}_3$

$$\begin{array}{ll} x^3+3 & x^3+6x+3 \\ x^3+21 & x^3+3x+3 \\ x^3+12 & x^3+3x^2+3 \end{array}$$

   Inertia group D_6 except for the last one, which has inertia group C_3

2. $p > 3$ three non-isomorphic degree p extensions of $\mathbb{Q}_p$

$$\begin{array}{l} x^p + px^{p-1} + p \\ x^p + 2px^{\frac{p-1}{2}} + p \\ x^p + (p-2)px^{\frac{p-1}{2}} + p \end{array}$$

   Inertia group of the first is C_p. The other two have inertia D_{2p}

(Awtrey, Edwards)(Amano polynomials)

Ramification

Ore's conditions on totally ramified extensions and Eisenstein polynomials

	Polynomial	$d_{K/\mathbb{Q}_p}$	$d_{L/\mathbb{Q}_p}$	$G_0 \supseteq G_1 \supseteq \dots$
$p = 3$	$x^3 + 3$	3^5	3^{11}	$S_3 \supseteq C_3 \supseteq C_3 \supseteq C_3 \supseteq 1$
	$x^3 + 12$	3^5	3^{11}	$S_3 \supseteq C_3 \supseteq C_3 \supseteq C_3 \supseteq 1$
	$x^3 + 21$	3^5	3^{11}	$S_3 \supseteq C_3 \supseteq C_3 \supseteq C_3 \supseteq 1$
	$x^3 + 3x^2 + 3$	3^4	3^8	$C_3 \supseteq C_3 \supseteq 1$
	$x^3 + 3x + 3$	3^3	3^7	$S_3 \supseteq C_3 \supseteq 1$
	$x^3 + 6x + 3$	3^3	3^7	$S_3 \supseteq C_3 \supseteq 1$
$p > 3$	$x^p + px^{p-1} + p$	$p^{2(p-1)}$	$p^{4(p-1)}$	$C_p \supseteq C_p \supseteq 1$
	$x^p + 2px^{\frac{p-1}{2}} + p$	$p^{\frac{3(p-1)}{2}}$	p^{3p-2}	$D_{2p} \supseteq C_p \supseteq 1$
	$x^p + (p-2)px^{\frac{p-1}{2}} + p$	$p^{\frac{3(p-1)}{2}}$	p^{3p-2}	$D_{2p} \supseteq C_p \supseteq 1$

All but first three are wildly and weakly ramified

Hopf Galois structures

- Dihedral type D_{2p}
  2 structures corresponding to $\rho(G)$ (classical) and $\lambda(G)$
- Cyclic type $C_{2p} = C_p \times C_2$
  p split induced from intermediate fields

$$\mathbb{Q}_p(\alpha_i) = L^{D_i} \qquad D_i = \langle r^i s \rangle \quad i = 0 \dots p-1$$

Attached regular subgroups are $\lambda(\langle r \rangle) \times \rho(D_i)$

Dihedral type

Truman

$\mathcal{O}_L$ free over $\mathfrak{A}_{\mathbb{Q}_p[G]}$ if and only if it is free over $\mathfrak{A}_{H_\lambda}$, the Hopf algebra corresponding to the canonical nonclassical structure, that is, the nonclassical Hopf Galois structure of dihedral type

Johnston

For weakly ramified $\mathcal{O}_L$ free over $\mathfrak{A}_{\mathbb{Q}_p[G]}$

We are left with three cases where $p = 3$ and have to check only the classical Galois action

$x^3 + a$ Classical structure

$L = \mathbb{Q}_3(\alpha, \zeta) = \mathbb{Q}_3(\alpha, \omega)$ with $\omega^2 = -3$
Galois action on L

	1	α	α^2	ω	$\omega\alpha$	$\omega\alpha^2$
id	1	α	α^2	ω	$\omega\alpha$	$\omega\alpha^2$
r	1	$-\frac{1}{2}\alpha + \frac{1}{2}\omega\alpha$	$-\frac{1}{2}\alpha^2 - \frac{1}{2}\omega\alpha^2$	ω	$-\frac{3}{2}\alpha - \frac{1}{2}\omega\alpha$	$\frac{3}{2}\alpha^2 - \frac{1}{2}\omega\alpha^2$
r^2	1	$-\frac{1}{2}\alpha - \frac{1}{2}\omega\alpha$	$-\frac{1}{2}\alpha^2 + \frac{1}{2}\omega\alpha^2$	ω	$\frac{3}{2}\alpha - \frac{1}{2}\omega\alpha$	$-\frac{3}{2}\alpha^2 - \frac{1}{2}\omega\alpha^2$
s	1	α	α^2	$-\omega$	$-\omega\alpha$	$-\omega\alpha^2$
rs	1	$-\frac{1}{2}\alpha + \frac{1}{2}\omega\alpha$	$-\frac{1}{2}\alpha^2 - \frac{1}{2}\omega\alpha^2$	$-\omega$	$\frac{3}{2}\alpha + \frac{1}{2}\omega\alpha$	$-\frac{3}{2}\alpha^2 + \frac{1}{2}\omega\alpha^2$
r^2s	1	$-\frac{1}{2}\alpha - \frac{1}{2}\omega\alpha$	$-\frac{1}{2}\alpha^2 + \frac{1}{2}\omega\alpha^2$	$-\omega$	$-\frac{3}{2}\alpha + \frac{1}{2}\omega\alpha$	$\frac{3}{2}\alpha^2 + \frac{1}{2}\omega\alpha^2$

$h = h_0 id + h_1 r + h_2 r^2 + h_3 s + h_4 rs + h_5 r^2 s \in \mathbb{Q}_3[G]$ such that $h \cdot \mathcal{O}_L \subseteq \mathcal{O}_L$

$x^3 + a$ Classical structure

$$\mathcal{O}_L = \mathcal{O}_K[\omega] = \mathbb{Z}_3[\alpha, \omega]$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1/2 & -1/2 & 1 & -1/2 & -1/2 \\ 0 & 1/2 & -1/2 & 0 & 1/2 & -1/2 \\ 1 & -1/2 & -1/2 & 1 & -1/2 & -1/2 \\ 0 & -1/2 & 1/2 & 0 & -1/2 & 1/2 \\ 1 & 1 & 1 & -1 & -1 & -1 \\ 0 & -3/2 & 3/2 & 0 & 3/2 & -3/2 \\ 1 & -1/2 & -1/2 & -1 & 1/2 & 1/2 \\ 0 & 3/2 & -3/2 & 0 & -3/2 & 3/2 \\ 1 & -1/2 & -1/2 & -1 & 1/2 & 1/2 \end{bmatrix} \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ h_4 \\ h_5 \end{bmatrix}$$

should be a vector of integers.

$x^3 + a$ Classical structure

$\mathbb{Z}_3$ basis for the associated order $\mathfrak{A}_{\mathbb{Q}_3[D_6]}$

$$g_1 = \frac{1+r+r^2+s+rs+r^2s}{6}$$
$$g_2 = \frac{2-r-r^2+2s-rs-r^2s}{6}$$
$$g_3 = \frac{r-r^2+rs-r^2s}{2}$$
$$g_4 = \frac{1+r+r^2-s-rs-r^2s}{6}$$
$$g_5 = \frac{-r+r^2+rs-r^2s}{6}$$
$$g_6 = \frac{2-r-r^2-2s+rs+r^2s}{6}$$

	1	α	α^2	ω	$\omega\alpha$	$\omega\alpha^2$
g_1	1	0	0	0	0	0
g_2	0	α	α^2	0	0	0
g_3	0	$\omega\alpha$	$-\omega\alpha^2$	0	0	0
g_4	0	0	0	ω	0	0
g_5	0	0	0	0	α	$-\alpha^2$
g_6	0	0	0	0	$\omega\alpha$	$\omega\alpha^2$

$\beta = 1 + \alpha + \alpha^2 + \omega + \omega\alpha + \omega\alpha^2$

$g_1\beta = 1$ $\quad$ $g_4\beta = \omega$

$(g_2+g_5)\beta = 2\alpha$ $\quad$ $(g_2-g_5)\beta = 2\alpha^2$

$(g_3+g_6)\beta = 2\omega\alpha$ $\quad$ $(-g_3+g_6)\beta = 2\omega\alpha^2$

$2 \in \mathbb{Z}_3^* \implies \mathcal{O}_L$ free over $\mathfrak{A}_{\mathbb{Q}_3[D_6]}$ generated by β

Freeness over the associated order for all the Hopf-Galois structures of dihedral type.

$x^3 + a$ Induced split structure

Cyclic types: regular subgroups of $Sym(G)$ normalized by G

$$\begin{aligned} N &= \langle\lambda(r),\rho(s)\rangle \simeq C_6 \simeq C_3 \times C_2 \simeq \langle\lambda(r)\rangle \times \langle\rho(s)\rangle \\ N_1 &= \langle\lambda(r),\rho(rs)\rangle \\ N_2 &= \langle\lambda(r),\rho(r^2s)\rangle \end{aligned}$$

Work with $N = \langle g = (1, rs, r^2, s, r, r^2s)\rangle$

- $\lambda(G)$ action on N: $\lambda(r)g\lambda(r)^{-1} = g \qquad \lambda(s)g\lambda(s)^{-1} = g^{-1}$
- $\mathbb{Q}_p$−basis of Hopf algebra $H = L[N]^{\lambda(G)}$:

  $$id, \quad (g+g^{-1}), \quad \omega(g-g^{-1}), \quad g^3, \quad (g^2+g^{-2}), \quad \omega(g^{-2}-g^2)$$

- is tensor product of basis:

  $$H = L[\langle\lambda(r)\rangle \times \langle\rho(s)\rangle]^{\lambda(G)} = L[\langle\lambda(r)\rangle]^{\lambda(G)} \otimes \mathbb{Q}_3[\langle\rho(s)\rangle] = H_1 \otimes H_2$$

  $\mathbb{Q}_3$−basis for H_1: $id, (\lambda(r)+\lambda(r)^{-1}), \omega(\lambda(r)-\lambda(r)^{-1})$
  $\mathbb{Q}_3$−basis for H_2: $id, \rho(s)$

$x^3 + a$ Induced split structure

Hopf action

$$\left(\sum c_i g^i\right) \cdot x = \sum c_i (g^i)^{-1}(1_G)(x)$$

	1	α	α^2	ω	$\omega\alpha$	$\omega\alpha^2$
id	1	α	α^2	ω	$\omega\alpha$	$\omega\alpha^2$
$(g^2 + g^{-2})$	2	$-\alpha$	$-\alpha^2$	2ω	$-\omega\alpha$	$-\omega\alpha^2$
$\omega(g^{-2} - g^2)$	0	3α	$-3\alpha^2$	0	$3\omega\alpha$	$-3\omega\alpha^2$
g^3	1	α	α^2	$-\omega$	$-\omega\alpha$	$-\omega\alpha^2$
$(g + g^{-1})$	2	$-\alpha$	$-\alpha^2$	-2ω	$\omega\alpha$	$\omega\alpha^2$
$\omega(g - g^{-1})$	0	3α	$-3\alpha^2$	0	$-3\omega\alpha$	$3\omega\alpha^2$

See the induced action in the structure

Box	ωBox
Box	$-\omega$Box

$x^3 + a$ Induced split structure

H_1 is the Hopf algebra corresponding to the unique (almost classical) Hopf Galois extension $\mathbb{Q}_3(\alpha)/\mathbb{Q}_3$

Hopf action

	1	α	α^2
id	1	α	α^2
$\lambda(r)+\lambda(r)^{-1}$	2	$-\alpha$	$-\alpha^2$
$\omega(\lambda(r)-\lambda(r)^{-1})$	0	3α	$-3\alpha^2$

H_2 is the Hopf algebra corresponding to the unique (classical) Hopf Galois extension $\mathbb{Q}_3(\omega)/\mathbb{Q}_3$

Hopf action

	1	ω
id	1	ω
$\rho(s)$	1	$-\omega$

$x^3 + a$ Induced split structure

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 1 & -1 & 3 \\ 1 & -1 & -3 \end{pmatrix} \qquad A^{-1} = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & -\frac{1}{6} & -\frac{1}{6} \\ 0 & \frac{1}{6} & -\frac{1}{6} \end{pmatrix}$$

$\mathbb{Z}_3$—basis for the associated order $\mathfrak{A}_{H_1}$

$$h = \frac{id}{3} + \frac{\lambda(r) + \lambda(r)^{-1}}{3}$$
$$h' = \frac{id}{3} - \frac{\lambda(r) + \lambda(r)^{-1}}{6} + \frac{\omega(\lambda(r) - \lambda(r)^{-1})}{6}$$
$$h'' = \frac{id}{3} - \frac{\lambda(r) + \lambda(r)^{-1}}{6} - \frac{\omega(\lambda(r) - \lambda(r)^{-1})}{6}$$

	1	α	α^2
h	1	0	0
h'	0	α	0
h''	0	0	α^2

$\mathcal{O}_K$ is free over the associated order $\mathfrak{A}_{H_1}$ and $\beta = 1 + \alpha + \alpha^2$ is a generator

$x^3 + a$ Induced split structure

In order to do the same for a basis of the associated order $\mathfrak{A}_H$ we have to deal with the block matrix

$$B = \begin{pmatrix} A & A \\ A & -A \end{pmatrix}$$

We have $detB = det(-2A^2)$ and

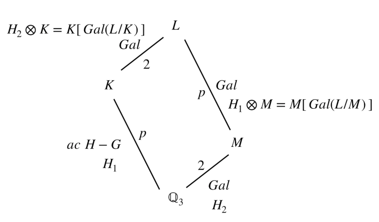
$$B^{-1} = \frac{1}{2} \begin{pmatrix} A^{-1} & A^{-1} \\ A^{-1} & -A^{-1} \end{pmatrix}$$

The same procedure gives a $\mathbb{Z}_3-$basis for $\mathfrak{A}_H$, freeness of $\mathcal{O}_L$ over $\mathfrak{A}_H$ and generator

$$\gamma = 1 + \alpha + \alpha^2 + \omega + \omega\alpha + \omega\alpha^2$$

Induced split structures

$H = H_1 \otimes H_2$



- Associated order $\mathfrak{A}_H$
  obtained from $\mathfrak{A}_{H_1}$ and $\mathfrak{A}_{H_2}$
  obtained from $\mathfrak{A}_{L/K}$ and $\mathfrak{A}_{L/M}$
- Freeness: $\mathcal{O}_L$ free over $\mathfrak{A}_H$
  $\iff$ free over $\mathfrak{A}_{L/K}$ and $\mathfrak{A}_{L/M}$
  $\iff$ $\mathcal{O}_K$ free over $\mathfrak{A}_{H_1}$ and $\mathcal{O}_M$ free over $\mathfrak{A}_{H_2}$

Dihedral Induced split structures

- $\mathfrak{A}_{H_2} = \mathbb{Z}_p[\,Gal(M/\mathbb{Q}_p)\,]$ and $\mathcal{O}_M$ free over $\mathfrak{A}_{H_2}$ (Noether)

	Polynomial	$G_0 \supseteq G_1 \supseteq \dots$	$t_{L/M}$
$p=3$	x^3+3	$S_3 \supseteq C_3 \supseteq C_3 \supseteq C_3 \supseteq 1$	3
	x^3+12	$S_3 \supseteq C_3 \supseteq C_3 \supseteq C_3 \supseteq 1$	3
	x^3+21	$S_3 \supseteq C_3 \supseteq C_3 \supseteq C_3 \supseteq 1$	3
	x^3+3x^2+3	$C_3 \supseteq C_3 \supseteq 1$	1
	x^3+3x+3	$S_3 \supseteq C_3 \supseteq 1$	1
	x^3+6x+3	$S_3 \supseteq C_3 \supseteq 1$	1
$p>3$	$x^p+px^{p-1}+p.$	$C_p \supseteq C_p \supseteq 1$	1
	$x^p+2px^{\frac{p-1}{2}}+p$	$D_{2p} \supseteq C_p \supseteq 1$	1
	$x^p+(p-2)px^{\frac{p-1}{2}}+p$	$D_{2p} \supseteq C_p \supseteq 1$	1

C_p-extension L/M has either $a=0$ or $a=1(\mid p-1)$

- $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/M}$ (Bertrandias, Bertrandias, Ferton)

$L/\mathbb{Q}_p$ a D_{2p}—Galois extension with induced Hopf Galois structure with Hopf algebra H

$\mathcal{O}_L$ is free over $\mathfrak{A}_H$