A method to compute the associated order in Hopf Galois structures of extensions of p-adic fields

Daniel Gil Muñoz

Universitat Politècnica de Catalunya
Departament de Matemàtiques

Hopf Algebras & Galois Module Theory
Omaha, May 2020

Joint work with Anna Rio Doval

Table of contents

L/K finite extension of fields, H K-algebra acting on L.

L/K finite extension of fields, H K-algebra acting on L.

$$\begin{array}{rccc} \rho_H\colon & H & \longrightarrow & \mathrm{End}_K(L) \\ & h & \longmapsto & x \mapsto h \cdot x \end{array}$$

L/K finite extension of fields, H K-algebra acting on L.

$$\begin{array}{rccc} \rho_H\colon & H & \longrightarrow & \mathrm{End}_K(L) \\ & h & \longmapsto & x \mapsto h \cdot x \end{array}$$

Definition

A Hopf Galois structure in L/K is a pair $(H, \cdot)$ where H is a K-Hopf algebra and $\cdot$ is a K-linear action of H over L such that:

1. *The action $\cdot$ endows L with H-module algebra structure.*
2. *The canonical map $j = (1, \rho_H)\colon L \otimes_K H \longrightarrow \mathrm{End}_K(L)$ is a K-linear isomorphism.*

We also say that L/K is H-Galois.

L/K finite separable extension, $\widetilde{L}$ Galois closure.

$G = \mathrm{Gal}(\widetilde{L}/K)$, $G' = \mathrm{Gal}(\widetilde{L}/L)$, $X = G/G'$.

$$\begin{array}{rccc} \lambda\colon & G & \longrightarrow & \mathrm{Perm}(X) \\ & \sigma & \longmapsto & \overline{\tau} \mapsto \overline{\sigma\tau} \end{array}$$

L/K finite separable extension, $\widetilde{L}$ Galois closure.

$G = \mathrm{Gal}(\widetilde{L}/K)$, $G' = \mathrm{Gal}(\widetilde{L}/L)$, $X = G/G'$.

$$\begin{array}{rccc} \lambda\colon & G & \longrightarrow & \mathrm{Perm}(X) \\ & \sigma & \longmapsto & \overline{\tau} \mapsto \overline{\sigma\tau} \end{array}$$

Theorem (Greither-Pareigis)

The Hopf Galois structures of L/K are in one-to-one correspondence with regular subgroups of $\mathrm{Perm}(X)$ normalized by $\lambda(G)$.

L/K finite separable extension, $\widetilde{L}$ Galois closure.

$G = \mathrm{Gal}(\widetilde{L}/K)$, $G' = \mathrm{Gal}(\widetilde{L}/L)$, $X = G/G'$.

$$\begin{array}{rccc} \lambda\colon & G & \longrightarrow & \mathrm{Perm}(X) \\ & \sigma & \longmapsto & \overline{\tau} \mapsto \overline{\sigma\tau} \end{array}$$

Theorem (Greither-Pareigis)

The Hopf Galois structures of L/K are in one-to-one correspondence with regular subgroups of $\mathrm{Perm}(X)$ normalized by $\lambda(G)$.

If N is such a subgroup, the Hopf algebra of the corresponding Hopf Galois structure is

$$H = \widetilde{L}[N]^G = \{x \in \widetilde{L}[N] \mid \sigma(x) = x \text{ for all } \sigma \in G\}.$$

$$\begin{array}{c} L \\ | \\ K \\ | \\ \mathbb{Q}_p \end{array}$$

L/K extension of p-adic fields.

$$\begin{tikzcd} L \arrow[d, dash, "H"] \\ K \arrow[d, dash] \\ \mathbb{Q}_p \end{tikzcd}$$

L/K extension of p-adic fields.

(H, μ) Hopf Galois structure of L/K.

$$\begin{tikzcd} L \arrow[d, dash, "H"] \\ K \arrow[d, dash] \\ \mathbb{Q}_p \end{tikzcd}$$

L/K extension of p-adic fields.

(H, μ) Hopf Galois structure of L/K.

L is H-free of rank one:
$\exists \alpha \in L : \{w \cdot \alpha : w \in W\}$ K-basis of L,
W K-basis of H.

$$\begin{tikzcd}
L \arrow[r, dash] \arrow[d, dash, "H"] & \mathcal{O}_L \arrow[d, dash] \\
K \arrow[r, dash] \arrow[d, dash] & \mathcal{O}_K \arrow[d, dash] \\
\mathbb{Q}_p \arrow[r, dash] & \mathbb{Z}_p
\end{tikzcd}$$

L/K extension of p-adic fields.

(H, μ) Hopf Galois structure of L/K.

L is H-free of rank one:
$\exists \alpha \in L: \ \{w \cdot \alpha : \ w \in W\}$ K-basis of L,
W K-basis of H.

$\mathcal{O}_L/\mathcal{O}_K$ extension of integer rings.

$$\begin{tikzcd}
L \arrow[r, dash] \arrow[d, dash, "H"] & \mathcal{O}_L \arrow[d, dash, "\mathfrak{A}_H"] \\
K \arrow[r, dash] \arrow[d, dash] & \mathcal{O}_K \arrow[d, dash] \\
\mathbb{Q}_p \arrow[r, dash] & \mathbb{Z}_p
\end{tikzcd}$$

L/K extension of p-adic fields.

(H, μ) Hopf Galois structure of L/K.

L is H-free of rank one:
$\exists \alpha \in L : \{w \cdot \alpha : w \in W\}$ K-basis of L,
W K-basis of H.

$\mathcal{O}_L/\mathcal{O}_K$ extension of integer rings.

The **associated order** of $\mathcal{O}_L$ in H is

$$\mathfrak{A}_H := \{h \in H \mid h \cdot \mathcal{O}_L \subset \mathcal{O}_L\}.$$

$$\begin{tikzcd}
L \arrow[r, dash] \arrow[d, dash, "H"] & \mathcal{O}_L \arrow[d, dash, "\mathfrak{A}_H"] \\
K \arrow[r, dash] \arrow[d, dash] & \mathcal{O}_K \arrow[d, dash] \\
\mathbb{Q}_p \arrow[r, dash] & \mathbb{Z}_p
\end{tikzcd}$$

L/K extension of p-adic fields.

(H, μ) Hopf Galois structure of L/K.

L is H-free of rank one:
$\exists \alpha \in L : \{w \cdot \alpha : w \in W\}$ K-basis of L,
W K-basis of H.

$\mathcal{O}_L/\mathcal{O}_K$ extension of integer rings.

The **associated order** of $\mathcal{O}_L$ in H is

$$\mathfrak{A}_H := \{h \in H \mid h \cdot \mathcal{O}_L \subset \mathcal{O}_L\}.$$

Two kind of problems:

- Compute an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$.
- Is $\mathcal{O}_L$ $\mathfrak{A}_H$-free?

$$\begin{array}{ccc} L & \text{———} & \mathcal{O}_L \\ \Big| H & & \Big| \mathfrak{A}_H \\ K & \text{———} & \mathcal{O}_K \\ \Big| & & \Big| \\ \mathbb{Q}_p & \text{———} & \mathbb{Z}_p \end{array}$$

L/K extension of p-adic fields.

(H,μ) Hopf Galois structure of L/K.

L is H-free of rank one:
$\exists \alpha \in L: \ \{w \cdot \alpha : \ w \in W\}$ K-basis of L,
W K-basis of H.

$\mathcal{O}_L/\mathcal{O}_K$ extension of integer rings.

The **associated order** of $\mathcal{O}_L$ in H is

$$\mathfrak{A}_H := \{h \in H \mid h \cdot \mathcal{O}_L \subset \mathcal{O}_L\}.$$

Two kind of problems:

- **Compute an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$.**
- Is $\mathcal{O}_L$ $\mathfrak{A}_H$-free?

Table of contents

$L = \mathbb{Q}_3(\alpha)$, α root of $f(x) = x^3 + 3x^2 + 3$ in $\overline{\mathbb{Q}_3}$.

$L=\mathbb{Q}_3(\alpha)$, α root of $f(x)=x^3+3x^2+3$ in $\overline{\mathbb{Q}_3}$.

Unique Hopf Galois structure of $L/\mathbb{Q}_3$: H with $\mathbb{Q}_3$-basis

$$w_1=\mathrm{Id} \qquad w_2=(\sigma-\sigma^{-1})z \qquad w_3=\sigma+\sigma^{-1}$$

where $\sigma\in\mathrm{Gal}(\widetilde{L}/\mathbb{Q}_3)$ is a 3-cycle and $z\in L-\mathbb{Q}_3$, $z^2\in\mathbb{Q}_3$.

$L = \mathbb{Q}_3(\alpha)$, α root of $f(x) = x^3 + 3x^2 + 3$ in $\overline{\mathbb{Q}_3}$.

Unique Hopf Galois structure of $L/\mathbb{Q}_3$: H with $\mathbb{Q}_3$-basis

$$w_1 = \mathrm{Id} \qquad w_2 = (\sigma - \sigma^{-1})z \qquad w_3 = \sigma + \sigma^{-1}$$

where $\sigma \in \mathrm{Gal}(\widetilde{L}/\mathbb{Q}_3)$ is a 3-cycle and $z \in L - \mathbb{Q}_3$, $z^2 \in \mathbb{Q}_3$.

$\mathcal{O}_L = \mathbb{Z}_3[\alpha] \implies \{1, \alpha, \alpha^2\}$ $\mathbb{Z}_3$-basis of $\mathcal{O}_L$.

$L=\mathbb{Q}_3(\alpha)$, α root of $f(x)=x^3+3x^2+3$ in $\overline{\mathbb{Q}_3}$.

Unique Hopf Galois structure of $L/\mathbb{Q}_3$: H with $\mathbb{Q}_3$-basis

$$w_1=\mathrm{Id} \qquad w_2=(\sigma-\sigma^{-1})z \qquad w_3=\sigma+\sigma^{-1}$$

where $\sigma\in\mathrm{Gal}(\widetilde{L}/\mathbb{Q}_3)$ is a 3-cycle and $z\in L-\mathbb{Q}_3$, $z^2\in\mathbb{Q}_3$.

$\mathcal{O}_L=\mathbb{Z}_3[\alpha]\implies\{1,\alpha,\alpha^2\}$ $\mathbb{Z}_3$-basis of $\mathcal{O}_L$.

$$\begin{array}{c|ccc} & 1 & \alpha & \alpha^2 \\ \hline w_1 & 1 & \alpha & \alpha^2 \\ w_2 & 0 & 27+81\alpha+18\alpha^2 & -27-270\alpha-81\alpha^2 \\ w_3 & 2 & -3-\alpha & 9-\alpha^2 \end{array},$$

$$\mathfrak{A}_H = \{h \in H \mid h \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}.$$

$\mathfrak{A}_H = \{h \in H \,|\, h \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}$.

For $h = \sum_{i=1}^{3} h_i w_i \in H$ and $x = \sum_{j=1}^{3} x_j \alpha^{j-1} \in \mathcal{O}_L$,

$\mathfrak{A}_H = \{h \in H \,|\, h \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}$.

For $h = \sum_{i=1}^{3} h_i w_i \in H$ and $x = \sum_{j=1}^{3} x_j \alpha^{j-1} \in \mathcal{O}_L$,

$$\begin{aligned} h \cdot x = {} & [x_1(h_1 + 2h_3) + x_2(27h_2 - 3h_3) + x_3(-27h_2 + 9h_3)] \\ & + [x_2(h_1 + 81h_2 - h_3) + x_3(-270h_2)]\,\alpha \\ & + [x_2(18h_2) + x_3(h_1 - 81h_2 - h_3)]\,\alpha^2. \end{aligned}$$

$\mathfrak{A}_H = \{h \in H \mid h \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}$.

For $h = \sum_{i=1}^{3} h_i w_i \in H$ and $x = \sum_{j=1}^{3} x_j \alpha^{j-1} \in \mathcal{O}_L$,

$$\begin{aligned} h \cdot x = & \, [x_1(h_1 + 2h_3) + x_2(27h_2 - 3h_3) + x_3(-27h_2 + 9h_3)] \\ & + [x_2(h_1 + 81h_2 - h_3) + x_3(-270h_2)]\,\alpha \\ & + [x_2(18h_2) + x_3(h_1 - 81h_2 - h_3)]\,\alpha^2. \end{aligned}$$

$\mathfrak{A}_H = \{h \in H \mid h \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}$.

For $h = \sum_{i=1}^{3} h_i w_i \in H$ and $x = \sum_{j=1}^{3} x_j \alpha^{j-1} \in \mathcal{O}_L$,

$$\begin{aligned} h \cdot x = {} & [x_1(h_1 + 2h_3) + x_2(27h_2 - 3h_3) + x_3(-27h_2 + 9h_3)] \\ & + [x_2(h_1 + 81h_2 - h_3) + x_3(-270h_2)]\,\alpha \\ & + [x_2(18h_2) + x_3(h_1 - 81h_2 - h_3)]\,\alpha^2. \end{aligned}$$

$h \in \mathfrak{A}_H$ if and only if

$$h_1 + 2h_3,$$

$$27h_2 - 3h_3,\ h_1 + 81h_2 - h_3,\ 18h_2,$$

$$-27h_2 + 9h_3,\ -270h_2,\ h_1 - 81h_2 - h_3$$

are 3-adic integers.

$h \in \mathfrak{A}_H$ if and only if

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 27 & -3 \\ 1 & 81 & -1 \\ 0 & 18 & 0 \\ 0 & -27 & 9 \\ 0 & -270 & 0 \\ 1 & -81 & -1 \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} \in \mathbb{Z}_3^9$$

$h \in \mathfrak{A}_H$ if and only if

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 9 & 3 \\ 0 & 0 & 6 \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} \in \mathbb{Z}_3^3$$

$h \in \mathfrak{A}_H$ if and only if

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 9 & 3 \\ 0 & 0 & 6 \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} \in \mathbb{Z}_3^3$$

if and only if

$$\begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} = \frac{1}{18} \begin{pmatrix} 18 & 0 & -6 \\ 0 & 2 & -1 \\ 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}$$

for some $c_1, c_2, c_3 \in \mathbb{Z}_3$.

$h \in \mathfrak{A}_H$ if and only if

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 9 & 3 \\ 0 & 0 & 6 \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} \in \mathbb{Z}_3^3$$

if and only if

$$\begin{pmatrix} h_1 \\ h_2 \\ h_3 \end{pmatrix} = \frac{1}{18} \begin{pmatrix} 18 & 0 & -6 \\ 0 & 2 & -1 \\ 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}$$

for some $c_1, c_2, c_3 \in \mathbb{Z}_3$.

$\Longrightarrow \{w_1, \frac{w_2}{9}, \frac{-6w_1 - w_2 + 3w_3}{18}\}$ $\mathbb{Z}_3$-basis of $\mathfrak{A}_H$.

L/K H-Galois of degree n.

L/K H-Galois of degree n.

$W=\{w_i\}_{i=1}^n$ K-basis of H, $B=\{\gamma_j\}_{j=1}^n$ K-basis of L.

L/K H-Galois of degree n.

$W=\{w_i\}_{i=1}^n$ K-basis of H, $B=\{\gamma_j\}_{j=1}^n$ K-basis of L.

For $1\leq j\leq n$, set

$$M_j(H,L)\colon=\begin{pmatrix} | & | & \cdots & | \\ (w_1\cdot\gamma_j)_B & (w_2\cdot\gamma_j)_B & \cdots & (w_n\cdot\gamma_j)_B \\ | & | & \cdots & | \end{pmatrix}\in\mathcal{M}_n(K),$$

L/K H-Galois of degree n.

$W = \{w_i\}_{i=1}^n$ K-basis of H, $B = \{\gamma_j\}_{j=1}^n$ K-basis of L.

For $1 \leq j \leq n$, set

$$M_j(H,L) := \begin{pmatrix} | & | & \cdots & | \\ (w_1 \cdot \gamma_j)_B & (w_2 \cdot \gamma_j)_B & \cdots & (w_n \cdot \gamma_j)_B \\ | & | & \cdots & | \end{pmatrix} \in \mathcal{M}_n(K),$$

Definition

*The **matrix of the action** of H over L is defined as*

$$M(H,L) = \begin{pmatrix} M_1(H,L) \\ \hline \cdots \\ \hline M_n(H,L) \end{pmatrix} \in \mathcal{M}_{n^2 \times n}(K).$$

Alternative definition of $M(H, L)$:

Alternative definition of $M(H, L)$:

Let $\varphi\colon \mathcal{M}_n(K) \longrightarrow K^{n^2}$ the map that carries matrices to columns of vectors.

Alternative definition of $M(H,L)$:

Let $\varphi\colon \mathcal{M}_n(K) \longrightarrow K^{n^2}$ the map that carries matrices to columns of vectors.

If $n=2$, $\varphi\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\right) = \begin{pmatrix} a_{11} \\ a_{21} \\ a_{12} \\ a_{22} \end{pmatrix}$.

Alternative definition of $M(H, L)$:

Let $\varphi\colon \mathcal{M}_n(K) \longrightarrow K^{n^2}$ the map that carries matrices to columns of vectors.

If $n = 2$, $\varphi\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\right) = \begin{pmatrix} a_{11} \\ a_{21} \\ a_{12} \\ a_{22} \end{pmatrix}$.

$\rho_H\colon H \longrightarrow \mathcal{M}_n(K)$ linear representation, $\rho_H(w_i) \equiv w_i$.

Alternative definition of $M(H,L)$:

Let $\varphi\colon \mathcal{M}_n(K) \longrightarrow K^{n^2}$ the map that carries matrices to columns of vectors.

If $n=2$, $\varphi\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\right) = \begin{pmatrix} a_{11} \\ a_{21} \\ a_{12} \\ a_{22} \end{pmatrix}$.

$\rho_H\colon H \longrightarrow \mathcal{M}_n(K)$ linear representation, $\rho_H(w_i) \equiv w_i$.

Then, the matrix of the action is defined as:

$$M(H,L) := \begin{pmatrix} | & | & \cdots & | \\ \varphi(w_1) & \varphi(w_2) & \cdots & \varphi(w_n) \\ | & | & \cdots & | \end{pmatrix} \in \mathcal{M}_n(K),$$

Example

In the motivating example,

Example

In the motivating example,

$$M_1(H,L) = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$M_2(H,L) = \begin{pmatrix} 0 & 27 & -3 \\ 1 & 81 & -1 \\ 0 & 18 & 0 \end{pmatrix}$$

$$M_3(H,L) = \begin{pmatrix} 0 & -27 & 9 \\ 0 & -270 & 0 \\ 1 & -81 & -1 \end{pmatrix}$$

Example

In the motivating example,

$$M_1(H,L) = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$M_2(H,L) = \begin{pmatrix} 0 & 27 & -3 \\ 1 & 81 & -1 \\ 0 & 18 & 0 \end{pmatrix}$$

$$M(H,L) = \begin{pmatrix} M_1(H,L) \\ \hline M_2(H,L) \\ \hline M_3(H,L) \end{pmatrix}$$

$$M_3(H,L) = \begin{pmatrix} 0 & -27 & 9 \\ 0 & -270 & 0 \\ 1 & -81 & -1 \end{pmatrix}$$

Proposition

Suppose that $B = \{\gamma_j\}_{j=1}^{n}$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. Given $h \in H$,

$$h \in \mathfrak{A}_H \Longleftrightarrow M(H,L)h \in \mathcal{O}_K^{n^2}$$

Proposition

Suppose that $B = \{\gamma_j\}_{j=1}^n$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. Given $h \in H$,

$$h \in \mathfrak{A}_H \iff M(H,L)h \in \mathcal{O}_K^{n^2}$$

Definition

*A **reduced matrix** of $M(H,L)$ is a matrix D such that there is some unimodular matrix $U \in \mathcal{M}_n(\mathcal{O}_K)$ such that*

$$UM(H,L) = \left(\frac{D}{O}\right)$$

Definition

*A **reduced matrix** of $M(H,L)$ is a matrix D such that there is some unimodular matrix $U \in \mathcal{M}_n(\mathcal{O}_K)$ such that*

$$UM(H,L) = \left(\frac{D}{O}\right)$$

Definition

A ***reduced matrix*** *of $M(H,L)$ is a matrix D such that there is some unimodular matrix $U \in \mathcal{M}_n(\mathcal{O}_K)$ such that*

$$UM(H,L) = \left(\frac{D}{O}\right)$$

Equivalently, if

$$M(H,L) = dM,\ d \in K,\ M \in \mathcal{M}_n(\mathcal{O}_K),$$

then $D = d\Phi$ with $UM = \left(\frac{\Phi}{O}\right)$

Proposition

The reduced matrix of $M(H, L)$ always exists.

Proposition

The reduced matrix of $M(H,L)$ always exists.

Corollary

Let D be a reduced matrix of $M(H,L)$. Given $h \in H$,

$$h \in \mathfrak{A}_H \text{ if and only if } Dh \in \mathcal{O}_K^n.$$

Proposition

The reduced matrix of $M(H, L)$ always exists.

Corollary

Let D be a reduced matrix of $M(H, L)$. Given $h \in H$,

$$h \in \mathfrak{A}_H \text{ if and only if } Dh \in \mathcal{O}_K^n.$$

Theorem (G., Rio)

Let D be a reduced matrix of $M(H, L)$ and call $D^{-1} = (d_{ij})_{i,j=1}^n$. The elements

$$v_i = \sum_{l=1}^{n} d_{li} w_l, \; 1 \leq i \leq n$$

form an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$.

Example

In the motivating example:

- $D = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 9 & 3 \\ 0 & 0 & 6 \end{pmatrix}$ is a reduced matrix of $M(H, L)$.
- The inverse is $D^{-1} = \frac{1}{18}\begin{pmatrix} 18 & 0 & -6 \\ 0 & 2 & -1 \\ 0 & 0 & 3 \end{pmatrix}$.
- $\mathfrak{A}_H$ has a basis formed by

$$v_1 = w_1 \qquad v_2 = \frac{w_2}{9} \qquad v_3 = \frac{-6w_1 - w_2 + 3w_3}{18}$$

L/K H-Galois extension of p-adic fields.

L/K H-Galois extension of p-adic fields.

Reduction method

W K-basis of H, B $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

L/K H-Galois extension of p-adic fields.

Reduction method

W K-basis of H, B $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

1. Determine the matrix of the action $M(H,L)$.

L/K H-Galois extension of p-adic fields.

Reduction method

W K-basis of H, B $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

1. Determine the matrix of the action $M(H,L)$.
2. Decompose $M(H,L) = dM$, $d \in K$, $M \in \mathcal{M}_n(\mathcal{O}_K)$.

L/K H-Galois extension of p-adic fields.

Reduction method

W K-basis of H, B $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

1. Determine the matrix of the action $M(H, L)$.
2. Decompose $M(H, L) = dM$, $d \in K$, $M \in \mathcal{M}_n(\mathcal{O}_K)$.
3. Find an unimodular matrix U such that UM is a square matrix Φ and zero rows (for instance, Hermite normal form).

L/K H-Galois extension of p-adic fields.

Reduction method

W K-basis of H, B $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

1. Determine the matrix of the action $M(H,L)$.
2. Decompose $M(H,L) = dM$, $d \in K$, $M \in \mathcal{M}_n(\mathcal{O}_K)$.
3. Find an unimodular matrix U such that UM is a square matrix Φ and zero rows (for instance, Hermite normal form).
4. Compute the inverse of $D = d\Phi$. Its columns form an $\mathcal{O}_K$-basis of $\mathfrak{A}_H$.

Some remarks:

Some remarks:

- If D is a reduced matrix of $M(H, L)$, D is a change basis matrix from a basis of $\mathfrak{A}_H$.

Some remarks:

- If D is a reduced matrix of $M(H, L)$, D is a change basis matrix from a basis of $\mathfrak{A}_H$.
- Consequently, D^{-1} is also a change basis matrix that provides the desired basis.

Some remarks:

- If D is a reduced matrix of $M(H, L)$, D is a change basis matrix from a basis of $\mathfrak{A}_H$.
- Consequently, D^{-1} is also a change basis matrix that provides the desired basis.
- The reduction method provides a basis of $\mathfrak{A}_H$ from a basis of $\mathcal{O}_L$.

Some remarks:

- If D is a reduced matrix of $M(H, L)$, D is a change basis matrix from a basis of $\mathfrak{A}_H$.
- Consequently, D^{-1} is also a change basis matrix that provides the desired basis.
- The reduction method provides a basis of $\mathfrak{A}_H$ from a basis of $\mathcal{O}_L$.
- If we perform the reduction method with a basis of $\mathfrak{A}_H$, we obtain as reduced matrix the identity.

Table of contents

L/K Galois extension with group of the form

$$G = J \rtimes G',$$

$J \trianglelefteq G$, $G' \leq G$. Let $L_1 = L^{G'}$, $L_2 = L^J$.

L/K Galois extension with group of the form

$$G = J \rtimes G',$$

$J \trianglelefteq G$, $G' \leq G$. Let $L_1 = L^{G'}$, $L_2 = L^J$.

$$\begin{tikzcd}[column sep=small]
 & L \arrow[dl, dash] \arrow[dr, dash] & \\
L_1 \arrow[dr, dash] & & L_2 \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

L/K Galois extension with group of the form

$$G = J \rtimes G',$$

$J \trianglelefteq G$, $G' \leq G$. Let $L_1 = L^{G'}$, $L_2 = L^J$.

$$r := [L_1 : K],\ s := [L : L_1].$$

$$\begin{tikzcd}
 & L \arrow[dl, dash, "s"'] \arrow[dr, dash] & \\
L_1 \arrow[dr, dash, "r"'] & & L_2 \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

L/K Galois extension with group of the form

$$G = J \rtimes G',$$

$J \trianglelefteq G$, $G' \leq G$. Let $L_1 = L^{G'}$, $L_2 = L^J$.

$$r := [L_1 : K],\ s := [L : L_1].$$

$$\begin{tikzcd}[column sep=small] & L \arrow[dl, dash] \arrow[dr, dash] & \\ L_1 \arrow[dr, dash, "N_1"'] & & L_2 \arrow[dl, dash] \\ & K & \end{tikzcd}$$

Theorem (Crespo, Rio, Vela)

If $N_1 \leq S_r$ gives L_1/K a H-G structure and $N_2 \leq S_s$ gives L/L_1 a H-G structure, then $N := N_1 \times N_2 \leq S_n$ gives L/K a H-G structure.

L/K Galois extension with group of the form

$$G = J \rtimes G',$$

$J \trianglelefteq G$, $G' \leq G$. Let $L_1 = L^{G'}$, $L_2 = L^J$.

$$r := [L_1 : K],\ s := [L : L_1].$$

$$\begin{tikzcd} & L \arrow[dl, dash, "N_2"'] \arrow[dr, dash] & \\ L_1 \arrow[dr, dash, "N_1"'] & & L_2 \arrow[dl, dash] \\ & K & \end{tikzcd}$$

Theorem (Crespo, Rio, Vela)

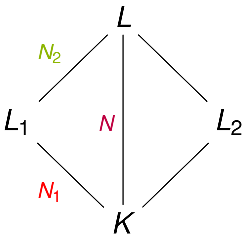
If $N_1 \leq S_r$ gives L_1/K a H-G structure and $N_2 \leq S_s$ gives L/L_1 a H-G structure, then $N := N_1 \times N_2 \leq S_n$ gives L/K a H-G structure.

L/K Galois extension with group of the form

$$G = J \rtimes G',$$

$J \trianglelefteq G$, $G' \leq G$. Let $L_1 = L^{G'}$, $L_2 = L^J$.

$$r := [L_1 : K],\ s := [L : L_1].$$



Theorem (Crespo, Rio, Vela)

If $N_1 \leq S_r$ gives L_1/K a H-G structure and $N_2 \leq S_s$ gives L/L_1 a H-G structure, then $N := N_1 \times N_2 \leq S_n$ gives L/K a H-G structure.

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[dr, dash] & \\
L_1 \arrow[dr, dash] & & L_2 \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

Lemma

There is a one-to-one correspondence between the Hopf Galois structures of L/L_1 and the Hopf Galois structures of L_2/K.

$$\begin{tikzcd} & L \arrow[dl, dash] \arrow[dr, dash] & \\ L_1 \arrow[dr, dash] & & L_2 \arrow[dl, dash] \\ & K & \end{tikzcd}$$

Lemma

There is a one-to-one correspondence between the Hopf Galois structures of L/L_1 and the Hopf Galois structures of L_2/K.

$$G' \cong G/J \Longrightarrow \mathrm{Perm}(G') \cong \mathrm{Perm}(G/J)$$

$$\begin{tikzcd}
 & L \arrow[dl, dash, "N_2"'] \arrow[dr, dash] & \\
L_1 \arrow[dr, dash] & & L_2 \arrow[dl, dash, "N_2"] \\
 & K &
\end{tikzcd}$$

Lemma

There is a one-to-one correspondence between the Hopf Galois structures of L/L_1 and the Hopf Galois structures of L_2/K.

$$G' \cong G/J \Longrightarrow \mathrm{Perm}(G') \cong \mathrm{Perm}(G/J)$$

$$N_2 \leq \mathrm{Perm}(G') \longleftrightarrow N_2 \leq \mathrm{Perm}(G/J)$$

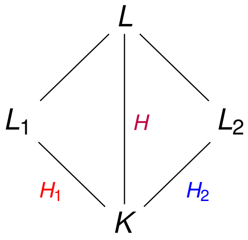
$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[dr, dash] & \\
L_1 \arrow[dr, dash] & & L_2 \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

Lemma

There is a one-to-one correspondence between the Hopf Galois structures of L/L_1 and the Hopf Galois structures of L_2/K.

$$G' \cong G/J \Longrightarrow \mathrm{Perm}(G') \cong \mathrm{Perm}(G/J)$$

$$N_2 \leq \mathrm{Perm}(G') \longleftrightarrow N_2 \leq \mathrm{Perm}(G/J)$$



Lemma

There is a one-to-one correspondence between the Hopf Galois structures of L/L_1 and the Hopf Galois structures of L_2/K.

$$G' \cong G/J \Longrightarrow \mathrm{Perm}(G') \cong \mathrm{Perm}(G/J)$$

$$N_2 \leq \mathrm{Perm}(G') \longleftrightarrow N_2 \leq \mathrm{Perm}(G/J)$$

Proposition (G., Rio)

H is an induced Hopf Galois structure of L/K if and only if

$$H = H_1 \otimes_K H_2,$$

where H_1 is a Hopf Galois structure of L_1/K and H_2 is a Hopf Galois structure of L_2/K.

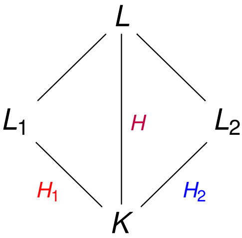
$$\begin{tikzcd}
& L \arrow[dl, dash] \arrow[dr, dash] & \\
L_1 \arrow[dr, dash] & & L_2 \arrow[dl, dash] \\
& K &
\end{tikzcd}$$

L/K H-Galois extension of fields.

$$\begin{tikzcd}
& L \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "H"] & \\
L_1 \arrow[dr, dash, "H_1"'] & & L_2 \arrow[dl, dash, "H_2"] \\
& K &
\end{tikzcd}$$

L/K H-Galois extension of fields.

$H = H_1 \otimes_K H_2$ induced.



L/K H-Galois extension of fields.

$H = H_1 \otimes_K H_2$ induced.

- What is the relation between $M(H, L)$, $M(H_1, L_1)$ and $M(H_2, L_2)$?

$$\begin{tikzcd} & L \arrow[dl, dash] \arrow[dd, dash, "H"] \arrow[dr, dash] & \\ L_1 \arrow[dr, dash, "H_1"'] & & L_2 \arrow[dl, dash, "H_2"] \\ & K & \end{tikzcd}$$

L/K H-Galois extension of p-adic fields.

$H = H_1 \otimes_K H_2$ induced.

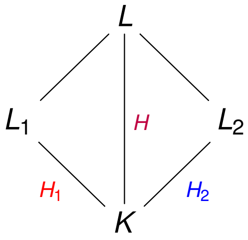
- What is the relation between $M(H, L)$, $M(H_1, L_1)$ and $M(H_2, L_2)$?

$$\begin{tikzcd}
& L \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "H"] & \\
L_1 \arrow[dr, dash, "H_1"'] & & L_2 \arrow[dl, dash, "H_2"] \\
& K &
\end{tikzcd}$$

L/K H-Galois extension of p-adic fields.

$H = H_1 \otimes_K H_2$ induced.

- What is the relation between $M(H, L)$, $M(H_1, L_1)$ and $M(H_2, L_2)$?
- Is it true that $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}$?



L/K H-Galois extension of p-adic fields.

$H = H_1 \otimes_K H_2$ induced.

- What is the relation between $M(H, L)$, $M(H_1, L_1)$ and $M(H_2, L_2)$?
- Is it true that $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}$?

Definition

The Kronecker product of two matrices $A = (a_{ij})$ and B is the matrix defined by blocks as

$$A \otimes B = (a_{ij}B).$$

Theorem (G., Rio)

When in L we consider the product of the bases of L_1 and L_2, there is a permutation matrix (hence unimodular) $P \in \mathrm{GL}_{n^2}(\mathcal{O}_K)$ such that

$$PM(H,L) = M(H_1,L_1) \otimes M(H_2,L_2).$$

Theorem (G., Rio)

When in L we consider the product of the bases of L_1 and L_2, there is a permutation matrix (hence unimodular) $P \in \mathrm{GL}_{n^2}(\mathcal{O}_K)$ such that

$$PM(H, L) = M(H_1, L_1) \otimes M(H_2, L_2).$$

Definition

*A K-basis of L with the property of the previous result is called **induced**.*

Theorem (G., Rio)

When in L we consider the product of the bases of L_1 and L_2, there is a permutation matrix (hence unimodular) $P \in \mathrm{GL}_{n^2}(\mathcal{O}_K)$ such that

$$PM(H,L) = M(H_1,L_1) \otimes M(H_2,L_2).$$

Definition

*A K-basis of L with the property of the previous result is called **induced**.*

- The product of the fixed K-bases of L_1 and L_2 is induced.

Theorem (G., Rio)

When in L we consider the product of the bases of L_1 and L_2, there is a permutation matrix (hence unimodular) $P \in \mathrm{GL}_{n^2}(\mathcal{O}_K)$ such that

$$PM(H,L) = M(H_1,L_1) \otimes M(H_2,L_2).$$

Definition

A K-basis of L with the property of the previous result is called ***induced****.*

- The product of the fixed K-bases of L_1 and L_2 is induced.
- If L_1/K and L_2/K are arithmetically disjoint, the product of their fixed integral bases is an integral induced basis.

Theorem (G., Rio)

If L/K has some integral induced basis, then

$$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}.$$

Theorem (G., Rio)

If L/K has some integral induced basis, then

$$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}.$$

Corollary

If L_1/K and L_2/K are arithmetically disjoint, then

$$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}.$$

Theorem (G., Rio)

If L/K has some integral induced basis, then

$$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}.$$

Theorem (G., Rio)

If L/K has some integral induced basis, then

$$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}.$$

Sketch of proof:

Theorem (G., Rio)

If L/K has some integral induced basis, then

$$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}.$$

Sketch of proof:

$PM(H,L) = M(H_1, L_1) \otimes M(H_2, L_2)$ for some unimodular P.

Theorem (G., Rio)

If L/K has some integral induced basis, then

$$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}.$$

Sketch of proof:

$PM(H,L) = M(H_1,L_1) \otimes M(H_2,L_2)$ for some unimodular P.

D is a reduced matrix of $M(H,L) \Longleftrightarrow$
D is a reduced matrix of $M(H_1,L_1) \otimes M(H_2,L_2)$.

Theorem (G., Rio)

If L/K has some integral induced basis, then

$$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}.$$

Sketch of proof:

$PM(H,L) = M(H_1,L_1) \otimes M(H_2,L_2)$ for some unimodular P.

D is a reduced matrix of $M(H,L) \iff$
D is a reduced matrix of $M(H_1,L_1) \otimes M(H_2,L_2)$.

D_i reduced matrix of $M(H_i,L_i)$, $i \in \{1,2\} \Longrightarrow$
$D_1 \otimes D_2$ reduced matrix of $M(H_1,L_1) \otimes M(H_2,L_2)$.

Theorem (G., Rio)

If L/K has some integral induced basis, then

$$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}.$$

Sketch of proof:

$PM(H,L) = M(H_1,L_1) \otimes M(H_2,L_2)$ for some unimodular P.

D is a reduced matrix of $M(H,L) \Longleftrightarrow$
D is a reduced matrix of $M(H_1,L_1) \otimes M(H_2,L_2)$.

D_i reduced matrix of $M(H_i,L_i)$, $i \in \{1,2\} \Longrightarrow$
$D_1 \otimes D_2$ reduced matrix of $M(H,L)$

Theorem (G., Rio)

If L/K has some integral induced basis, then

$$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}.$$

Sketch of proof:

$PM(H, L) = M(H_1, L_1) \otimes M(H_2, L_2)$ for some unimodular P.

D is a reduced matrix of $M(H, L) \iff$
D is a reduced matrix of $M(H_1, L_1) \otimes M(H_2, L_2)$.

D_i reduced matrix of $M(H_i, L_i)$, $i \in \{1, 2\} \implies$
$D_1 \otimes D_2$ reduced matrix of $M(H, L)$

$(D_1 \otimes D_2)^{-1} = {D_1}^{-1} \otimes {D_2}^{-1}$

Theorem (G., Rio)

If L/K has some integral induced basis, then

$$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}.$$

Sketch of proof:

$PM(H,L) = M(H_1,L_1) \otimes M(H_2,L_2)$ for some unimodular P.

D is a reduced matrix of $M(H,L) \Longleftrightarrow$
D is a reduced matrix of $M(H_1,L_1) \otimes M(H_2,L_2)$.

D_i reduced matrix of $M(H_i,L_i)$, $i \in \{1,2\} \Longrightarrow$
$D_1 \otimes D_2$ reduced matrix of $M(H,L)$

$(D_1 \otimes D_2)^{-1} = {D_1}^{-1} \otimes {D_2}^{-1} \Longrightarrow \mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{H_2}$.

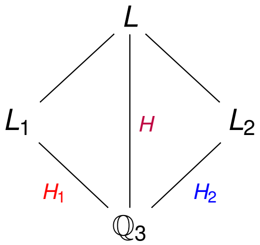
$L/\mathbb{Q}_3$ dihedral extension of degree 6.

$L/\mathbb{Q}_3$ dihedral extension of degree 6.

The induced Hopf Galois structures of $L/\mathbb{Q}_3$ are the ones of type C_6.

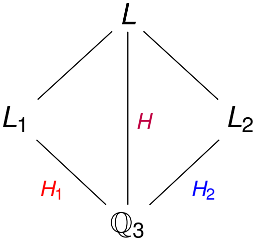
$L/\mathbb{Q}_3$ dihedral extension of degree 6.

The induced Hopf Galois structures of $L/\mathbb{Q}_3$ are the ones of type C_6.



$L/\mathbb{Q}_3$ dihedral extension of degree 6.

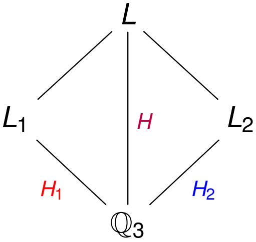
The induced Hopf Galois structures of $L/\mathbb{Q}_3$ are the ones of type C_6.



$L_1/\mathbb{Q}_3$ totally ramified degree 3
$L_2/\mathbb{Q}_3$ tamely ramified degree 2

$L/\mathbb{Q}_3$ dihedral extension of degree 6.

The induced Hopf Galois structures of $L/\mathbb{Q}_3$ are the ones of type C_6.



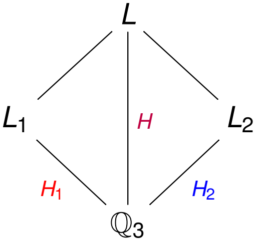
$L_1/\mathbb{Q}_3$ totally ramified degree 3
$L_2/\mathbb{Q}_3$ tamely ramified degree 2

L is the splitting field over $\mathbb{Q}_3$ of one of the polynomials:

- x^3+3
- x^3+12
- x^3+21
- x^3+3x^2+3
- x^3+3x+3
- x^3+6x+3

$L/\mathbb{Q}_3$ dihedral extension of degree 6.

The induced Hopf Galois structures of $L/\mathbb{Q}_3$ are the ones of type C_6.



$L_1/\mathbb{Q}_3$ totally ramified degree 3
$L_2/\mathbb{Q}_3$ tamely ramified degree 2

L is the splitting field over $\mathbb{Q}_3$ of one of the polynomials:

- x^3+3
- x^3+12
- x^3+21
- x^3+3x^2+3
- x^3+3x+3
- x^3+6x+3

f splitting polynomial of $L/\mathbb{Q}_3$.

f splitting polynomial of $L/\mathbb{Q}_3$.

1. If $f(x) = x^3 + a$, $a \in \{3, 12, 21\}$, then $L/\mathbb{Q}_3$ has an integral induced basis and $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_3} \mathfrak{A}_{H_2}$.

f splitting polynomial of $L/\mathbb{Q}_3$.

1. If $f(x) = x^3 + a$, $a \in \{3, 12, 21\}$, then $L/\mathbb{Q}_3$ has an integral induced basis and $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_3} \mathfrak{A}_{H_2}$.
2. If $f(x) = x^3 + 3x^2 + 3$, then $L_1/\mathbb{Q}_3$ and $L_2/\mathbb{Q}_3$ are arithmetically disjoint and $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_3} \mathfrak{A}_{H_2}$.

f splitting polynomial of $L/\mathbb{Q}_3$.

1. If $f(x) = x^3 + a$, $a \in \{3, 12, 21\}$, then $L/\mathbb{Q}_3$ has an integral induced basis and $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_3} \mathfrak{A}_{H_2}$.
2. If $f(x) = x^3 + 3x^2 + 3$, then $L_1/\mathbb{Q}_3$ and $L_2/\mathbb{Q}_3$ are arithmetically disjoint and $\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_3} \mathfrak{A}_{H_2}$.
3. If $f(x) = x^3 + ax + 3$, $a \in \{3, 6\}$, then $\mathfrak{A}_H \neq \mathfrak{A}_{H_1} \otimes_{\mathbb{Z}_3} \mathfrak{A}_{H_2}$ (it is not even a tensor product).

- S.U. Chase, M.E. Sweedler; *Hopf Algebras and Galois Theory*, Lecture Notes in Mathematics, Springer, 1969.
- L.N. Childs; *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory,* Mathematical Surveys and Monographs 80, American Mathematical Society, 1986
- T. Crespo, A. Rio, M. Vela; *Induced Hopf Galois structures,* Journal of Algebra **457** (2016), 312-322.
- C. Awtrey, T. Edwards; *Dihedral p-adic fields of prime degree,* International Journal of Pure and Applied Mathematics Vol. 75 **2** (2012), 185-194

Thank you for your attention