Hopf Galois module structure of quartic Galois extensions of $\mathbb{Q}$

Daniel Gil Muñoz

Universitat Politècnica de Catalunya
Departament de Matemàtiques

Hopf Algebras & Galois Module Theory
Omaha (virtually), May 2021

Joint work with Anna Rio

$$\begin{tikzcd}[arrows=dash]
L \arrow[r] \arrow[d, "4"', "H"] & \mathcal{O}_L \arrow[d, "\mathfrak{A}_H"] \\
\mathbb{Q} \arrow[r] & \mathbb{Z}
\end{tikzcd}$$

$L/\mathbb{Q}$ quartic Galois extension of $\mathbb{Q}$.

H Hopf Galois structure of $L/\mathbb{Q}$.

$$\begin{tikzcd}
L \arrow[r, dash] \arrow[d, dash, "4"', "H"] & \mathcal{O}_L \arrow[d, dash, "\mathfrak{A}_H"] \\
\mathbb{Q} \arrow[r, dash] & \mathbb{Z}
\end{tikzcd}$$

$L/\mathbb{Q}$ quartic Galois extension of $\mathbb{Q}$.

H Hopf Galois structure of $L/\mathbb{Q}$.

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

$$\begin{tikzcd}
L \arrow[r, dash] \arrow[d, dash, "4"', "H"] & \mathcal{O}_L \arrow[d, dash, "\mathfrak{A}_H"] \\
\mathbb{Q} \arrow[r, dash] & \mathbb{Z}
\end{tikzcd}$$

$L/\mathbb{Q}$ quartic Galois extension of $\mathbb{Q}$.

H Hopf Galois structure of $L/\mathbb{Q}$.

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

Theorem (Leopoldt)

If $N/\mathbb{Q}$ is an abelian extension with group G, $\mathcal{O}_N$ is $\mathfrak{A}_{N/\mathbb{Q}}$-free.

$$\begin{array}{ccc} L & \text{———} & \mathcal{O}_L \\ {\scriptstyle 4}\Big| {\scriptstyle H} & & \Big| {\scriptstyle \mathfrak{A}_H} \\ \mathbb{Q} & \text{———} & \mathbb{Z} \end{array}$$

$L/\mathbb{Q}$ quartic Galois extension of $\mathbb{Q}$.

H Hopf Galois structure of $L/\mathbb{Q}$.

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

Theorem (Leopoldt)

If $N/\mathbb{Q}$ is an abelian extension with group G, $\mathcal{O}_N$ is $\mathfrak{A}_{N/\mathbb{Q}}$-free.

Classical Galois structure ✓

$$\begin{array}{ccc} L & \text{———} & \mathcal{O}_L \\ 4 \Big| H & & \Big| \mathfrak{A}_H \\ \mathbb{Q} & \text{———} & \mathbb{Z} \end{array}$$

$L/\mathbb{Q}$ quartic Galois extension of $\mathbb{Q}$.

H Hopf Galois structure of $L/\mathbb{Q}$.

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

Theorem (Leopoldt)

If $N/\mathbb{Q}$ is an abelian extension with group G, $\mathcal{O}_N$ is $\mathfrak{A}_{N/\mathbb{Q}}$-free.

Classical Galois structure ✓

What about the non-classical Hopf Galois structures?

Table of contents

Table of contents

$$\begin{array}{c} L \\ \Big| \, H \\ K \end{array}$$

L/K H-Galois extension of number fields.

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

L/K H-Galois extension of number fields.

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

L/K H-Galois extension of number fields.

Assume that $\mathcal{O}_K$ is a PID.

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

L/K H-Galois extension of number fields.

Assume that $\mathcal{O}_K$ is a PID.

Normal basis theorem (HG version): L is H-free of rank one.

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

L/K H-Galois extension of number fields.

Assume that $\mathcal{O}_K$ is a PID.

Normal basis theorem (HG version): L is H-free of rank one.

Associated order of $\mathcal{O}_L$ in H:

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

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

L/K H-Galois extension of number fields.

Assume that $\mathcal{O}_K$ is a PID.

Normal basis theorem (HG version): L is H-free of rank one.

Associated order of $\mathcal{O}_L$ in H:

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

If $\mathcal{O}_L$ is $\mathfrak{H}$-free, then $\mathfrak{H} = \mathfrak{A}_H$.

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

L/K H-Galois extension of number fields.

Assume that $\mathcal{O}_K$ is a PID.

Normal basis theorem (HG version): L is H-free of rank one.

Associated order of $\mathcal{O}_L$ in H:

$$\mathfrak{A}_H := \{h \in H \,|\, h \cdot \mathcal{O}_L \subseteq \mathcal{O}_L\}.$$

If $\mathcal{O}_L$ is $\mathfrak{H}$-free, then $\mathfrak{H} = \mathfrak{A}_H$.

Two kind of problems:

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

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

L/K H-Galois extension of number fields.

Assume that $\mathcal{O}_K$ is a PID.

Normal basis theorem (HG version): L is H-free of rank one.

Associated order of $\mathcal{O}_L$ in H:

$$\mathfrak{A}_H := \{h \in H \,|\, h \cdot \mathcal{O}_L \subseteq \mathcal{O}_L\}.$$

If $\mathcal{O}_L$ is $\mathfrak{H}$-free, then $\mathfrak{H} = \mathfrak{A}_H$.

Two kind of problems:

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

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

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

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

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

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

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

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

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

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

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

It is the matrix of the linear map

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

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

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

It is the matrix of the linear map

$$\begin{array}{rccll} \rho_H\colon & H & \longrightarrow & \mathrm{End}_K(L) & \cong \mathcal{M}_n(K) \\ & h & \longmapsto & x \mapsto h \cdot x & \end{array}$$

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

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

It is the matrix of the linear map

$$\begin{array}{rccccl} \rho_H\colon & H & \longrightarrow & \mathrm{End}_K(L) & \cong \mathcal{M}_n(K) \\ & h & \longmapsto & x \mapsto h \cdot x & \end{array}$$

In $\mathrm{End}_K(L)$ we fix the canonical basis (with respect to B).

Assume that B is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

Assume that B is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

Key idea: We reduce integrally $M(H, L)$ to an $n \times n$ matrix.

Assume that B is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

Key idea: We reduce integrally $M(H, L)$ to an $n \times n$ matrix.

Theorem

There is a matrix $D \in \mathcal{M}_n(K)$ and a unimodular matrix $U \in \mathrm{GL}_{n^2}(\mathcal{O}_K)$ with the property that

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

We say that D is a ***reduced matrix*** *of $M(H, L)$.*

Assume that B is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

Key idea: We reduce integrally $M(H,L)$ to an $n \times n$ matrix.

Theorem

There is a matrix $D \in \mathcal{M}_n(K)$ and a unimodular matrix $U \in \mathrm{GL}_{n^2}(\mathcal{O}_K)$ with the property that

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

We say that D is a ***reduced matrix*** *of $M(H,L)$.*

D is a change basis matrix from a basis of $\mathfrak{A}_H$ to W.

Assume that B is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

Key idea: We reduce integrally $M(H,L)$ to an $n \times n$ matrix.

Theorem

There is a matrix $D \in \mathcal{M}_n(K)$ and a unimodular matrix $U \in \mathrm{GL}_{n^2}(\mathcal{O}_K)$ with the property that

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

We say that D is a ***reduced matrix*** *of $M(H,L)$.*

D is a change basis matrix from a basis of $\mathfrak{A}_H$ to W.

The columns of D^{-1} form a basis of the associated order $\mathfrak{A}_H$.

- Is $\mathcal{O}_L$ $\mathfrak{A}_H$-free?

- Is $\mathcal{O}_L$ $\mathfrak{A}_H$-free?

Let $\beta=\sum_{j=1}^{n}\beta_j\gamma_j\in\mathcal{O}_L$ be a potential $\mathfrak{A}_H$-generator of $\mathcal{O}_L$.

- Is $\mathcal{O}_L$ $\mathfrak{A}_H$-free?

Let $\beta = \sum_{j=1}^{n} \beta_j \gamma_j \in \mathcal{O}_L$ be a potential $\mathfrak{A}_H$-generator of $\mathcal{O}_L$.

We define $M_\beta(H, L) := \sum_{j=1}^{n} \beta_j M_j(H, L)$.

- Is $\mathcal{O}_L$ $\mathfrak{A}_H$-free?

Let $\beta = \sum_{j=1}^{n} \beta_j \gamma_j \in \mathcal{O}_L$ be a potential $\mathfrak{A}_H$-generator of $\mathcal{O}_L$.

We define $M_\beta(H, L) := \sum_{j=1}^{n} \beta_j M_j(H, L)$.

Then,

$$\begin{aligned} M_\beta(H, L) &= \sum_{j=1}^{n} \beta_j M_j(H, L) \\ &= \begin{pmatrix} | & | & \cdots & | \\ (w_1 \cdot \beta)_B & (w_2 \cdot \beta)_B & \cdots & (w_n \cdot \beta)_B \\ | & | & \cdots & | \end{pmatrix} \end{aligned}$$

- Is $\mathcal{O}_L$ $\mathfrak{A}_H$-free?

Let $\beta = \sum_{j=1}^{n} \beta_j \gamma_j \in \mathcal{O}_L$ be a potential $\mathfrak{A}_H$-generator of $\mathcal{O}_L$.

We define $M_\beta(H, L) := \sum_{j=1}^{n} \beta_j M_j(H, L)$.

Then,

$$M_\beta(H, L) = \sum_{j=1}^{n} \beta_j M_j(H, L)$$
$$= \begin{pmatrix} | & | & \cdots & | \\ (w_1 \cdot \beta)_B & (w_2 \cdot \beta)_B & \cdots & (w_n \cdot \beta)_B \\ | & | & \cdots & | \end{pmatrix}$$

If $\mathfrak{H} := \langle w_1, \dots, w_n \rangle_{\mathcal{O}_K}$,

$$D_\beta(H, L) := \det(M_\beta(H, L)) = [\mathcal{O}_L : \mathfrak{H} \cdot \beta]_{\mathcal{O}_K}.$$

Now, D is the change basis matrix from a basis of $\mathfrak{A}_H$ to a basis of $\mathfrak{H}$.

Now, D is the change basis matrix from a basis of $\mathfrak{A}_H$ to a basis of $\mathfrak{H}$.

$\Longrightarrow I_W(H,L) := [\mathfrak{A}_H : \mathfrak{H}]_{\mathcal{O}_K} = \det(D)$.

Now, D is the change basis matrix from a basis of $\mathfrak{A}_H$ to a basis of $\mathfrak{H}$.

$\Longrightarrow I_W(H,L) := [\mathfrak{A}_H : \mathfrak{H}]_{\mathcal{O}_K} = \det(D)$.

$$[\mathcal{O}_L : \mathfrak{H}\cdot\beta]_{\mathcal{O}_K} = [\mathcal{O}_L : \mathfrak{A}_H\cdot\beta]_{\mathcal{O}_K}\,[\mathfrak{A}_H\cdot\beta : \mathfrak{H}\cdot\beta]_{\mathcal{O}_K}$$

Now, D is the change basis matrix from a basis of $\mathfrak{A}_H$ to a basis of $\mathfrak{H}$.

$\implies I_W(H,L) := [\mathfrak{A}_H : \mathfrak{H}]_{\mathcal{O}_K} = \det(D)$.

$$[\mathcal{O}_L : \mathfrak{H} \cdot \beta]_{\mathcal{O}_K} = [\mathcal{O}_L : \mathfrak{A}_H \cdot \beta]_{\mathcal{O}_K} [\mathfrak{A}_H : \mathfrak{H}]_{\mathcal{O}_K}$$

Now, D is the change basis matrix from a basis of $\mathfrak{A}_H$ to a basis of $\mathfrak{H}$.

$\Longrightarrow I_W(H,L) := [\mathfrak{A}_H : \mathfrak{H}]_{\mathcal{O}_K} = \det(D)$.

$$D_\beta(H,L) = [\mathcal{O}_L : \mathfrak{A}_H \cdot \beta]_{\mathcal{O}_K} \, I_W(H,L)$$

Now, D is the change basis matrix from a basis of $\mathfrak{A}_H$ to a basis of $\mathfrak{H}$.

$\Longrightarrow I_W(H,L) := [\mathfrak{A}_H : \mathfrak{H}]_{\mathcal{O}_K} = \det(D)$.

$$D_\beta(H,L) = [\mathcal{O}_L : \mathfrak{A}_H \cdot \beta]_{\mathcal{O}_K} I_W(H,L)$$

Corollary

$\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator β if and only if $I_W(H,L) = D_\beta(H,L)$ up to multiplication by a unit of $\mathcal{O}_K$.

Procedure:

Procedure:

1. We find the entries of $M(H, L)$, where in L we fix an integral basis B.

Procedure:

1. We find the entries of $M(H,L)$, where in L we fix an integral basis B.
2. We compute a reduced matrix of $M(H,L)$ and $I_W(H,L)$.

Procedure:

1. We find the entries of $M(H, L)$, where in L we fix an integral basis B.
2. We compute a reduced matrix of $M(H, L)$ and $I_W(H, L)$.
3. For a given $\beta \in \mathcal{O}_L$, we find the determinant $D_\beta(H, L)$ of the matrix $M_\beta(H, L)$.

Procedure:

1. We find the entries of $M(H,L)$, where in L we fix an integral basis B.
2. We compute a reduced matrix of $M(H,L)$ and $I_W(H,L)$.
3. For a given $\beta \in \mathcal{O}_L$, we find the determinant $D_\beta(H,L)$ of the matrix $M_\beta(H,L)$.
4. If $D_\beta(H,L) = I_W(H,L)$ (up to multiplication by unit), then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator β.

Procedure:

1. We find the entries of $M(H,L)$, where in L we fix an integral basis B.
2. We compute a reduced matrix of $M(H,L)$ and $I_W(H,L)$.
3. For a given $\beta\in\mathcal{O}_L$, we find the determinant $D_\beta(H,L)$ of the matrix $M_\beta(H,L)$.
4. If $D_\beta(H,L)=I_W(H,L)$ (up to multiplication by unit), then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator β.

If $K=\mathbb{Q}$, we need $D_\beta(H,L)=I_W(H,L)$ up to sign.

Procedure:

1. **We find the entries of $M(H, L)$, where in L we fix an integral basis B.**
2. We compute a reduced matrix of $M(H, L)$ and $I_W(H, L)$.
3. For a given $\beta \in \mathcal{O}_L$, we find the determinant $D_\beta(H, L)$ of the matrix $M_\beta(H, L)$.
4. If $D_\beta(H, L) = I_W(H, L)$ (up to multiplication by unit), then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator β.

If $K = \mathbb{Q}$, we need $D_\beta(H, L) = I_W(H, L)$ up to sign.

Assume L/K is Galois with group G.

Assume L/K is Galois with group G.

Suppose that we know how G acts on some K-basis of L.

Assume L/K is Galois with group G.

Suppose that we know how G acts on some K-basis of L.

Let H be a Hopf Galois structure of L/K.

Assume L/K is Galois with group G.

Suppose that we know how G acts on some K-basis of L.

Let H be a Hopf Galois structure of L/K.

- Since H acts as linear combinations of elements of G, we know how H acts on that K-basis of L.

Assume L/K is Galois with group G.

Suppose that we know how G acts on some K-basis of L.

Let H be a Hopf Galois structure of L/K.

- Since H acts as linear combinations of elements of G, we know how H acts on that K-basis of L.
- The action of H on any other K-basis of L is computed using the linearity (change basis of L).

Assume L/K is Galois with group G.

Suppose that we know how G acts on some K-basis of L.

Let H be a Hopf Galois structure of L/K.

- Since H acts as linear combinations of elements of G, we know how H acts on that K-basis of L.
- The action of H on any other K-basis of L is computed using the linearity (change basis of L).

Shortcut

In order to determine the action of H on any K-basis of L, it is enough to know the action of G on some K-basis of L.

Table of contents

Let L/K be a cyclic quartic extension with $G = \mathrm{Gal}(L/K) = \langle\sigma\rangle$.

Let L/K be a cyclic quartic extension with $G = \mathrm{Gal}(L/K) = \langle\sigma\rangle$.

Greither-Pareigis: Hopf Galois structures of L/K correspond to regular G-stable subgroups of $\mathrm{Perm}(G)$.

Let L/K be a cyclic quartic extension with $G = \mathrm{Gal}(L/K) = \langle\sigma\rangle$.

Greither-Pareigis: Hopf Galois structures of L/K correspond to regular G-stable subgroups of $\mathrm{Perm}(G)$.

There are two: $\lambda(G)$ and the one generated by the premutations

$$\mu = (1_G, \sigma^2)(\sigma, \sigma^3),\ \eta = (1_G, \sigma)(\sigma^2, \sigma^3).$$

Let L/K be a cyclic quartic extension with $G = \mathrm{Gal}(L/K) = \langle \sigma \rangle$.

Greither-Pareigis: Hopf Galois structures of L/K correspond to regular G-stable subgroups of $\mathrm{Perm}(G)$.

There are two: $\lambda(G)$ and the one generated by the premutations

$$\mu = (1_G, \sigma^2)(\sigma, \sigma^3),\ \eta = (1_G, \sigma)(\sigma^2, \sigma^3).$$

Proposition

L/K has a unique non-classical Hopf Galois structure, which has K-basis

$$\{\mathrm{Id}, \mu, \eta + \mu\eta, z(\eta - \mu\eta)\},$$

where z is the square root of a non-square element in K.

Let $L/\mathbb{Q}$ be a cyclic quartic extension of number fields.

Let $L/\mathbb{Q}$ be a cyclic quartic extension of number fields.
We need:

Let $L/\mathbb{Q}$ be a cyclic quartic extension of number fields.
We need:

1. A $\mathbb{Z}$-basis of $\mathcal{O}_L$.

Let $L/\mathbb{Q}$ be a cyclic quartic extension of number fields.
We need:

1. A $\mathbb{Z}$-basis of $\mathcal{O}_L$.
2. The action of H on that basis.

Let $L/\mathbb{Q}$ be a cyclic quartic extension of number fields.
We need:

1. A $\mathbb{Z}$-basis of $\mathcal{O}_L$.
2. The action of H on that basis.

Proposition

$L = \mathbb{Q}(\sqrt{a(d+b\sqrt{d})})$, *where:*

- $a \in \mathbb{Z}$ *is odd square-free and* $b \in \mathbb{Z}_{>0}$.
- $d = b^2 + c^2$ *for some* $c \in \mathbb{Z}_{>0}$ *and* d *is square-free.*
- $\gcd(a, d) = 1$.

Let $z = \sqrt{a(d+b\sqrt{d})}$.

Let $z = \sqrt{a(d + b\sqrt{d})}$. The minimal polynomial of z is

$$f(x) = x^4 - 2adx^2 + a^2c^2d.$$

Let $z=\sqrt{a(d+b\sqrt{d})}$. The minimal polynomial of z is

$$f(x)=x^4-2adx^2+a^2c^2d.$$

Let $w=\sqrt{a(d-b\sqrt{d})}$

Let $z = \sqrt{a(d + b\sqrt{d})}$. The minimal polynomial of z is

$$f(x) = x^4 - 2adx^2 + a^2c^2d.$$

Let $w = \sqrt{a(d - b\sqrt{d})} \implies$ the roots of f are z, w and their negatives.

Let $z = \sqrt{a(d + b\sqrt{d})}$. The minimal polynomial of z is

$$f(x) = x^4 - 2adx^2 + a^2c^2d.$$

Let $w = \sqrt{a(d - b\sqrt{d})} \implies$ the roots of f are z, w and their negatives.

Elements of G are permutations of $\{z, w, -z, -w\}$.

Let $z = \sqrt{a(d+b\sqrt{d})}$. The minimal polynomial of z is

$$f(x) = x^4 - 2adx^2 + a^2c^2d.$$

Let $w = \sqrt{a(d-b\sqrt{d})} \Longrightarrow$ the roots of f are z, w and their negatives.

Elements of G are permutations of $\{z, w, -z, -w\}$. We can assume that $\sigma = (z, w, -z, -w)$.

Let $z = \sqrt{a(d + b\sqrt{d})}$. The minimal polynomial of z is

$$f(x) = x^4 - 2adx^2 + a^2c^2d.$$

Let $w = \sqrt{a(d - b\sqrt{d})} \implies$ the roots of f are z, w and their negatives.

Elements of G are permutations of $\{z, w, -z, -w\}$. We can assume that $\sigma = (z, w, -z, -w)$.

Then, we know how G acts on the K-basis $\{1, \sqrt{d}, z, w\}$ of L:

Let $z = \sqrt{a(d+b\sqrt{d})}$. The minimal polynomial of z is

$$f(x) = x^4 - 2adx^2 + a^2c^2d.$$

Let $w = \sqrt{a(d-b\sqrt{d})} \Longrightarrow$ the roots of f are z, w and their negatives.

Elements of G are permutations of $\{z, w, -z, -w\}$. We can assume that $\sigma = (z, w, -z, -w)$.

Then, we know how G acts on the K-basis $\{1, \sqrt{d}, z, w\}$ of L:

$$\begin{array}{lll}
\sigma(\sqrt{d}) = -\sqrt{d}, & \sigma(z) = w, & \sigma(w) = -z, \\
\sigma^2(\sqrt{d}) = \sqrt{d}, & \sigma^2(z) = -z, & \sigma^2(w) = -w, \\
\sigma^3(\sqrt{d}) = -\sqrt{d}, & \sigma^3(z) = -w, & \sigma^3(w) = z.
\end{array}$$

We are able to determine the action of a Hopf Galois structure on any K-basis of L.

We are able to determine the action of a Hopf Galois structure on any K-basis of L.

In particular, on the integral ones.

We are able to determine the action of a Hopf Galois structure on any K-basis of L.

In particular, on the integral ones.

Case	Integral basis
1	$\{1, \sqrt{d}, z, w\}$
2	$\left\{1, \frac{1+\sqrt{d}}{2}, z, w\right\}$
3	$\left\{1, \frac{1+\sqrt{d}}{2}, \frac{z+w}{2}, \frac{z-w}{2}\right\}$
4	$\left\{1, \frac{1+\sqrt{d}}{2}, \frac{1+\sqrt{d}+z+w}{4}, \frac{1-\sqrt{d}+z-w}{4}\right\}$
5	$\left\{1, \frac{1+\sqrt{d}}{2}, \frac{1+\sqrt{d}+z-w}{4}, \frac{1-\sqrt{d}+z+w}{4}\right\}$

We are able to determine the action of a Hopf Galois structure on any K-basis of L.

In particular, on the integral ones.

Case	Integral basis
1	$\{1, \sqrt{d}, z, w\}$
2	$\left\{1, \frac{1+\sqrt{d}}{2}, z, w\right\}$
3	$\left\{1, \frac{1+\sqrt{d}}{2}, \frac{z+w}{2}, \frac{z-w}{2}\right\}$
4	$\left\{1, \frac{1+\sqrt{d}}{2}, \frac{1+\sqrt{d}+z+w}{4}, \frac{1-\sqrt{d}+z-w}{4}\right\}$
5	$\left\{1, \frac{1+\sqrt{d}}{2}, \frac{1+\sqrt{d}+z-w}{4}, \frac{1-\sqrt{d}+z+w}{4}\right\}$

We call $\{\gamma_1, \gamma_2, \gamma_3, \gamma_4\}$ the integral basis of L.

Case 1:

$$D = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & -2c \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2b \end{pmatrix}$$

$$I_W(H, L) = 16b$$
$$D_\beta(H, L) = 16b\beta_1\beta_2(\beta_3^2 + \beta_4^2)$$

Case 1:

$$D = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & -2c \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2b \end{pmatrix} \qquad \begin{array}{l} I_W(H,L) = 16b \\ D_\beta(H,L) = 16b\beta_1\beta_2(\beta_3^2+\beta_4^2) \end{array}$$

$\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator $\beta = \gamma_1 + \gamma_2 + \gamma_3$.

Case 1:

$$D = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & -2c \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2b \end{pmatrix} \qquad \begin{array}{l} I_W(H,L) = 16b \\ D_\beta(H,L) = 16b\beta_1\beta_2(\beta_3^2+\beta_4^2) \end{array}$$

$\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator $\beta = \gamma_1 + \gamma_2 + \gamma_3$.

Cases 2 and 3:

$$D = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & -2c \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2b \end{pmatrix} \qquad \begin{array}{l} I_W(H,L) = 8b \\ D_\beta(H,L) = \pm 8b\beta_2(\beta_3^2+\beta_4^2)(2\beta_1+\beta_2) \end{array}$$

Case 1:

$$D = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & -2c \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2b \end{pmatrix}$$

$$I_W(H,L) = 16b$$
$$D_\beta(H,L) = 16b\beta_1\beta_2(\beta_3^2+\beta_4^2)$$

$\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator $\beta = \gamma_1 + \gamma_2 + \gamma_3$.

Cases 2 and 3:

$$D = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & -2c \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2b \end{pmatrix}$$

$$I_W(H,L) = 8b$$
$$D_\beta(H,L) = \pm 8b\beta_2(\beta_3^2+\beta_4^2)(2\beta_1+\beta_2)$$

$\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator $\beta = \gamma_2 + \gamma_3$.

Cases 4 and 5:

$$D = \begin{pmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & -c \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 2b \end{pmatrix}$$

$$I_W(H, L) = 2b$$
$$D_\beta(H, L) = \mp 2b(\beta_3^2 + \beta_4^2)(2\beta_2 + \beta_3 - \beta_4)(4\beta_1 + 2\beta_2 + \beta_3 + \beta_4)$$

Cases 4 and 5:

$$D = \begin{pmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & -c \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 2b \end{pmatrix}$$

$$I_W(H,L) = 2b$$
$$D_\beta(H,L) = \mp 2b(\beta_3^2 + \beta_4^2)(2\beta_2 + \beta_3 - \beta_4)(4\beta_1 + 2\beta_2 + \beta_3 + \beta_4)$$

$\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator $\beta = \gamma_2 - \gamma_3$.

Cases 4 and 5:

$$D = \begin{pmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & -c \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 2b \end{pmatrix}$$

$$I_W(H, L) = 2b$$
$$D_\beta(H, L) = \mp 2b(\beta_3^2 + \beta_4^2)(2\beta_2 + \beta_3 - \beta_4)(4\beta_1 + 2\beta_2 + \beta_3 + \beta_4)$$

$\mathcal{O}_L$ is $\mathfrak{A}_H$-free with generator $\beta = \gamma_2 - \gamma_3$.

Theorem

Let $L/\mathbb{Q}$ is a cyclic quartic extension. Then $\mathcal{O}_L$ is free over its associated order at every Hopf Galois structure of $L/\mathbb{Q}$.

Table of contents

Let L/K be a biquadratic extension with $G = \mathrm{Gal}(L/K) = \langle\sigma, \tau\rangle$.

Let L/K be a biquadratic extension with $G = \mathrm{Gal}(L/K) = \langle \sigma, \tau \rangle$.

There are three non-classical Hopf Galois structures, given by the subgroups generated by:

- $\eta_1 = (1_G, \sigma\tau, \tau, \sigma)$.
- $\eta_2 = (1_G, \sigma\tau, \sigma, \tau)$.
- $\eta_3 = (1_G, \tau, \sigma\tau, \sigma)$.

Let L/K be a biquadratic extension with $G = \mathrm{Gal}(L/K) = \langle \sigma, \tau \rangle$.

There are three non-classical Hopf Galois structures, given by the subgroups generated by:

- $\eta_1 = (1_G, \sigma\tau, \tau, \sigma)$.
- $\eta_2 = (1_G, \sigma\tau, \sigma, \tau)$.
- $\eta_3 = (1_G, \tau, \sigma\tau, \sigma)$.

Proposition

The non-classical Hopf Galois structures $\{H_i\}_{i=1}^3$ have K-bases

$$\left\{ \mathrm{Id}, \eta_i^2, \eta_i + \eta_i^3, z_i(\eta_i - \eta_i^3) \right\},$$

where:

Let L/K be a biquadratic extension with $G = \mathrm{Gal}(L/K) = \langle \sigma, \tau \rangle$.

There are three non-classical Hopf Galois structures, given by the subgroups generated by:

- $\eta_1 = (1_G, \sigma\tau, \tau, \sigma)$.
- $\eta_2 = (1_G, \sigma\tau, \sigma, \tau)$.
- $\eta_3 = (1_G, \tau, \sigma\tau, \sigma)$.

Proposition

The non-classical Hopf Galois structures $\{H_i\}_{i=1}^{3}$ have K-bases

$$\left\{\mathrm{Id}, \eta_i^2, \eta_i + \eta_i^3, z_i(\eta_i - \eta_i^3)\right\},$$

where:

- $E_1 = L^{\langle\tau\rangle}$, $E_2 = L^{\langle\sigma\rangle}$, $E_3 = L^{\langle\sigma\tau\rangle}$.
- *For each* $i \in \{1, 2, 3\}$, $z_i \in E_i - K$ *and* $z_i^2 \in K$.

Let $L/\mathbb{Q}$ be a biquadratic extension with $G = \mathrm{Gal}(L/\mathbb{Q}) = \langle\sigma, \tau\rangle$.

Let $L/\mathbb{Q}$ be a biquadratic extension with $G = \mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle$.

$L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ with:

Let $L/\mathbb{Q}$ be a biquadratic extension with $G = \mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle$.

$L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ with:

- $m, n \in \mathbb{Z}$ square-free.

Let $L/\mathbb{Q}$ be a biquadratic extension with $G = \mathrm{Gal}(L/\mathbb{Q}) = \langle\sigma, \tau\rangle$.

$L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ with:

- $m, n \in \mathbb{Z}$ square-free.
- $k = \frac{mn}{d^2}$, $d = \gcd(m, n)$.

Let $L/\mathbb{Q}$ be a biquadratic extension with $G = \mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle$.

$L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ with:

- $m, n \in \mathbb{Z}$ square-free.
- $k = \frac{mn}{d^2}$, $d = \gcd(m, n)$.
- m, n and k are exchangeable.

Let $L/\mathbb{Q}$ be a biquadratic extension with $G = \mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle$.

$L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ with:

- $m, n \in \mathbb{Z}$ square-free.
- $k = \frac{mn}{d^2}$, $d = \gcd(m, n)$.
- m, n and k are exchangeable.

Lattice of intermediate fields:

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{m}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{n}) \arrow[d, dash] & \mathbb{Q}(\sqrt{k}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Let $L/\mathbb{Q}$ be a biquadratic extension with $G = \mathrm{Gal}(L/\mathbb{Q}) = \langle\sigma,\tau\rangle$.

$L = \mathbb{Q}(\sqrt{m},\sqrt{n})$ with:

- $m, n \in \mathbb{Z}$ square-free.
- $k = \frac{mn}{d^2}$, $d = \gcd(m,n)$.
- m, n and k are exchangeable.

Lattice of intermediate fields:

$$
\begin{tikzcd}
 & L \arrow[dl, dash, "\langle\tau\rangle"'] \arrow[d, dash, "\langle\sigma\rangle"'] \arrow[dr, dash, "\langle\sigma\tau\rangle"] & \\
\mathbb{Q}(\sqrt{m}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{n}) \arrow[d, dash] & \mathbb{Q}(\sqrt{k}) \arrow[dl, dash] \\
 & K &
\end{tikzcd}
$$

Action of G on the K-basis $\{1, \sqrt{m}, \sqrt{n}, \sqrt{k}\}$ of L:

$$\sigma(\sqrt{m}) = -\sqrt{m}, \quad \sigma(\sqrt{n}) = \sqrt{n}, \quad \sigma(\sqrt{k}) = -\sqrt{k},$$
$$\tau(\sqrt{m}) = \sqrt{m}, \quad \tau(\sqrt{n}) = -\sqrt{n}, \quad \tau(\sqrt{k}) = -\sqrt{k},$$
$$\sigma\tau(\sqrt{m}) = -\sqrt{m}, \quad \sigma\tau(\sqrt{n}) = -\sqrt{n}, \quad \sigma\tau(\sqrt{k}) = \sqrt{k}$$

Action of G on the K-basis $\{1, \sqrt{m}, \sqrt{n}, \sqrt{k}\}$ of L:

$$\sigma(\sqrt{m}) = -\sqrt{m}, \quad \sigma(\sqrt{n}) = \sqrt{n}, \quad \sigma(\sqrt{k}) = -\sqrt{k},$$
$$\tau(\sqrt{m}) = \sqrt{m}, \quad \tau(\sqrt{n}) = -\sqrt{n}, \quad \tau(\sqrt{k}) = -\sqrt{k},$$
$$\sigma\tau(\sqrt{m}) = -\sqrt{m}, \quad \sigma\tau(\sqrt{n}) = -\sqrt{n}, \quad \sigma\tau(\sqrt{k}) = \sqrt{k}$$

Case	Integral basis
$m, n, k \equiv 1\,(4)$	$\left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)\right\}$
$m \equiv 3\,(4)$, $n, k \equiv 2\,(4)$	$\left\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right\}$
$m \equiv 1\,(4)$, $n, k \not\equiv 1\,(4)$	$\left\{1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right\}$

Action of G on the K-basis $\{1, \sqrt{m}, \sqrt{n}, \sqrt{k}\}$ of L:

$$\sigma(\sqrt{m}) = -\sqrt{m}, \quad \sigma(\sqrt{n}) = \sqrt{n}, \quad \sigma(\sqrt{k}) = -\sqrt{k},$$
$$\tau(\sqrt{m}) = \sqrt{m}, \quad \tau(\sqrt{n}) = -\sqrt{n}, \quad \tau(\sqrt{k}) = -\sqrt{k},$$
$$\sigma\tau(\sqrt{m}) = -\sqrt{m}, \quad \sigma\tau(\sqrt{n}) = -\sqrt{n}, \quad \sigma\tau(\sqrt{k}) = \sqrt{k}$$

Case	Integral basis
$m, n, k \equiv 1\,(4)$	$\left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{k}}{2}\right)\right\}$
$m \equiv 3\,(4),\, n, k \equiv 2\,(4)$	$\left\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right\}$
$m \equiv 1\,(4),\, n, k \not\equiv 1\,(4)$	$\left\{1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right\}$

L/K is tamely ramified if and only if $m, n \equiv 1 \pmod 4$

Case 1: $m, n, k \equiv 1 \pmod 4$

Proposition (Truman)

Let $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ with $a, b \equiv 1 \pmod 4$, and let $g = \gcd(a, b)$. If H is the non-classical Hopf Galois structure of $L/\mathbb{Q}$ given by $\sqrt{a}$, $\mathcal{O}_L$ is $\mathfrak{A}_H$-free if and only if there are $x, y \in \mathbb{Z}$ such that

$$x^2 + ay^2 = \pm 2g.$$

Case 1: $m, n, k \equiv 1 \pmod 4$

Proposition (Truman)

Let $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ with $a, b \equiv 1 \pmod 4$, and let $g = \gcd(a, b)$. If H is the non-classical Hopf Galois structure of $L/\mathbb{Q}$ given by $\sqrt{a}$, $\mathcal{O}_L$ is $\mathfrak{A}_H$-free if and only if there are $x, y \in \mathbb{Z}$ such that

$$x^2 + ay^2 = \pm 2g.$$

His proof uses the theory of idèles.

Case 1: $m, n, k \equiv 1 \pmod 4$

Proposition (Truman)

Let $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ with $a, b \equiv 1 \pmod 4$, and let $g = \gcd(a, b)$. If H is the non-classical Hopf Galois structure of $L/\mathbb{Q}$ given by $\sqrt{a}$, $\mathcal{O}_L$ is $\mathfrak{A}_H$-free if and only if there are $x, y \in \mathbb{Z}$ such that

$$x^2 + ay^2 = \pm 2g.$$

His proof uses the theory of idèles.

$x^2 + ay^2 = \pm 2g$ are **generalized Pell equations.**

Case 1: $m, n, k \equiv 1 \pmod 4$

Proposition (Truman)

Let $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ with $a, b \equiv 1 \pmod 4$, and let $g = \gcd(a, b)$. If H is the non-classical Hopf Galois structure of $L/\mathbb{Q}$ given by $\sqrt{a}$, $\mathcal{O}_L$ is $\mathfrak{A}_H$-free if and only if there are $x, y \in \mathbb{Z}$ such that

$$x^2 + ay^2 = \pm 2g.$$

His proof uses the theory of idèles.

$x^2 + ay^2 = \pm 2g$ are **generalized Pell equations.**

- If $a > 0$, they have a finite number of solutions.

Case 1: $m, n, k \equiv 1 \pmod 4$

Proposition (Truman)

Let $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ with $a, b \equiv 1 \pmod 4$, and let $g = \gcd(a, b)$. If H is the non-classical Hopf Galois structure of $L/\mathbb{Q}$ given by $\sqrt{a}$, $\mathcal{O}_L$ is $\mathfrak{A}_H$-free if and only if there are $x, y \in \mathbb{Z}$ such that

$$x^2 + ay^2 = \pm 2g.$$

His proof uses the theory of idèles.

$x^2 + ay^2 = \pm 2g$ are **generalized Pell equations.**

- If $a > 0$, they have a finite number of solutions.
- If $a < 0$, there could be infinitely many and there are algorithms of computation.

Case 1: $m, n, k \equiv 1 \pmod 4$

Proposition (Truman)

Let $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ with $a, b \equiv 1 \pmod 4$, and let $g = \gcd(a, b)$. If H is the non-classical Hopf Galois structure of $L/\mathbb{Q}$ given by $\sqrt{a}$, $\mathcal{O}_L$ is $\mathfrak{A}_H$-free if and only if there are $x, y \in \mathbb{Z}$ such that

$$x^2 + ay^2 = \pm 2g.$$

His proof uses the theory of idèles.

$x^2 + ay^2 = \pm 2g$ are **generalized Pell equations.**

- If $a > 0$, they have a finite number of solutions.
- If $a < 0$, there could be infinitely many and there are algorithms of computation.

What if we use the reduction method?

Case 1: $m, n, k \equiv 1 \pmod{4}$

Reduced matrix of $M(H_i, L)$, $i \in \{1, 2, 3\}$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Case 1: $m, n, k \equiv 1 \pmod 4$

Reduced matrix of $M(H_i, L)$, $i \in \{1, 2, 3\}$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

For $\beta \in \mathcal{O}_L$,

$$D_\beta(H_1, L) = -2(2\beta_2 + \beta_4)(4\beta_1 + 2\beta_2 + 2\beta_3 + \beta_4)$$
$$\left(2d\beta_3^2 + 2m\beta_3\beta_4 + \frac{m}{d}\frac{m+1}{2}\beta_4^2\right).$$

Case 1: $m, n, k \equiv 1 \pmod 4$

Reduced matrix of $M(H_i, L)$, $i \in \{1, 2, 3\}$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

For $\beta \in \mathcal{O}_L$,

$$D_\beta(H_1, L) = -2(2\beta_2 + \beta_4)(4\beta_1 + 2\beta_2 + 2\beta_3 + \beta_4) \left(2d\beta_3^2 + 2m\beta_3\beta_4 + \frac{m}{d}\frac{m+1}{2}\beta_4^2\right).$$

If we want β to be a free generator, we must have

$$2d\beta_3^2 + 2m\beta_3\beta_4 + \frac{m}{d}\frac{m+1}{2}\beta_4^2 = \pm 1.$$

Case 1: $m, n, k \equiv 1 \pmod{4}$

If we want β to be a free generator, we must have

$$2d\beta_3^2 + 2m\beta_3\beta_4 + \frac{m}{d}\frac{m+1}{2}\beta_4^2 = \pm 1.$$

Case 1: $m, n, k \equiv 1 \pmod 4$

If we want β to be a free generator, we must have

$$2d\beta_3^2 + 2m\beta_3\beta_4 + \frac{m}{d}\frac{m+1}{2}\beta_4^2 = \pm 1.$$

Let $f(\beta_3) = 2d\beta_3^2 + 2m\beta_3\beta_4 + \frac{m}{d}\frac{m+1}{2}\beta_4^2 - s$, $s \in \{-1, 1\}$.

Case 1: $m, n, k \equiv 1 \pmod 4$

If we want β to be a free generator, we must have

$$2d\beta_3^2 + 2m\beta_3\beta_4 + \frac{m}{d}\frac{m+1}{2}\beta_4^2 = \pm 1.$$

Let $f(\beta_3) = 2d\beta_3^2 + 2m\beta_3\beta_4 + \frac{m}{d}\frac{m+1}{2}\beta_4^2 - s$, $s \in \{-1, 1\}$. It has discriminant

$$\Delta = 4(-m\beta_4^2 + 2ds).$$

Case 1: $m, n, k \equiv 1 \pmod 4$

If we want β to be a free generator, we must have

$$2d\beta_3^2 + 2m\beta_3\beta_4 + \frac{m}{d}\frac{m+1}{2}\beta_4^2 = \pm 1.$$

Let $f(\beta_3) = 2d\beta_3^2 + 2m\beta_3\beta_4 + \frac{m}{d}\frac{m+1}{2}\beta_4^2 - s$, $s \in \{-1, 1\}$. It has discriminant

$$\Delta = 4(-m\beta_4^2 + 2ds).$$

This is a square if and only if there are $x, y \in \mathbb{Z}$ if and only if

$$x^2 = -my^2 + 2ds.$$

Case 1: $m, n, k \equiv 1 \pmod 4$

If we want β to be a free generator, we must have

$$2d\beta_3^2 + 2m\beta_3\beta_4 + \frac{m}{d}\frac{m+1}{2}\beta_4^2 = \pm 1.$$

Let $f(\beta_3) = 2d\beta_3^2 + 2m\beta_3\beta_4 + \frac{m}{d}\frac{m+1}{2}\beta_4^2 - s$, $s \in \{-1, 1\}$. It has discriminant

$$\Delta = 4(-m\beta_4^2 + 2ds).$$

This is a square if and only if there are $x, y \in \mathbb{Z}$ if and only if

$$x^2 + my^2 = 2ds.$$

Case 1: $m, n, k \equiv 1 \pmod 4$

Proposition

For $i \in \{1, 2, 3\}$, $\mathcal{O}_L$ is $\mathfrak{A}_{H_i}$-free if and only if there exist integers $x, y \in \mathbb{Z}$ such that:

1. $x^2 + my^2 = \pm 2d$, *if* $i = 1$.
2. $x^2 + ny^2 = \pm 2d$, *if* $i = 2$.
3. $x^2 + ky^2 = \pm 2\frac{n}{d}$, *if* $i = 3$.

Case 1: $m, n, k \equiv 1 \pmod 4$

Proposition

For $i \in \{1,2,3\}$, $\mathcal{O}_L$ is $\mathfrak{A}_{H_i}$-free if and only if there exist integers $x, y \in \mathbb{Z}$ such that:

1. $x^2 + my^2 = \pm 2d$, *if* $i = 1$.
2. $x^2 + ny^2 = \pm 2d$, *if* $i = 2$.
3. $x^2 + ky^2 = \pm 2\frac{n}{d}$, *if* $i = 3$.

This matches with Truman's result because $\frac{n}{d} = \gcd(k, n)$.

Case 2: $m \equiv 3 \pmod{4}$, $n, k \equiv 2 \pmod{4}$

Case 2: $m \equiv 3 \pmod 4$, $n, k \equiv 2 \pmod 4$

Reduced matrices of $M(H_i, L)$, $i \in \{1, 2, 3\}$:

$$\begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Case 2: $m \equiv 3 \pmod 4$, $n, k \equiv 2 \pmod 4$

Reduced matrices of $M(H_i, L)$, $i \in \{1, 2, 3\}$:

$$\begin{pmatrix} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Given $\beta \in \mathcal{O}_L$,

$$D_\beta(H_1, L) = -32\beta_1\beta_2 \left(d\beta_3^2 + d\beta_3\beta_4 + \frac{1}{4}\left(d + \frac{m}{d}\right)\beta_4^2 \right),$$

$$D_\beta(H_2, L) = 8\beta_1(2\beta_3 + \beta_4)\left(2d\beta_2^2 + \frac{n}{2d}\beta_4^2\right),$$

$$D_\beta(H_3, L) = 8\beta_1\beta_4 \left(2\frac{m}{d}\beta_2^2 + 2\frac{n}{d}\beta_3^2 + 2\frac{n}{d}\beta_3\beta_4 + \frac{n}{2d}\beta_4^2\right).$$

Case 2: $m \equiv 3 \pmod 4$, $n, k \equiv 2 \pmod 4$

Proposition

For $i \in \{1, 2, 3\}$, $\mathcal{O}_L$ is $\mathfrak{A}_{H_i}$-free if and only if there exist integers $x, y \in \mathbb{Z}$ such that:

1. $x^2 + my^2 = \pm 4d$, *if* $i = 1$.
2. $x^2 + ny^2 = \pm 2d$, *if* $i = 2$.
3. $x^2 + ky^2 = \pm 2\frac{n}{d}$, *if* $i = 3$.

Case 2: $m \equiv 3 \pmod 4$, $n, k \equiv 2 \pmod 4$

Proposition

For $i \in \{1,2,3\}$, $\mathcal{O}_L$ is $\mathfrak{A}_{H_i}$-free if and only if there exist integers $x, y \in \mathbb{Z}$ such that:

1. $x^2 + my^2 = \pm 4d$, *if* $i = 1$.
2. $x^2 + ny^2 = \pm 2d$, *if* $i = 2$.
3. $x^2 + ky^2 = \pm 2\frac{n}{d}$, *if* $i = 3$.

n and k play exactly the same role.

Case 2: $m \equiv 3 \pmod 4$, $n, k \equiv 2 \pmod 4$

Proposition

For $i \in \{1,2,3\}$, $\mathcal{O}_L$ is $\mathfrak{A}_{H_i}$-free if and only if there exist integers $x, y \in \mathbb{Z}$ such that:

1. $x^2 + my^2 = \pm 4d$, *if* $i = 1$.
2. $x^2 + ny^2 = \pm 2d$, *if* $i = 2$.
3. $x^2 + ky^2 = \pm 2\frac{n}{d}$, *if* $i = 3$.

n and k play exactly the same role.

Corollary

The Pell equation $x^2 + ny^2 = \pm 2d$ has solutions if and only if so has $x^2 + ny^2 = \pm 2\frac{n}{d}$.

Case 2: $m \equiv 3 \pmod 4$, $n, k \equiv 2 \pmod 4$

Proposition

1. *If $m > 0$, $\mathcal{O}_L$ is not $\mathfrak{A}_{H_1}$-free unless m and n are coprime or m divides n.*
2. *If $n > 0$ (resp. $k > 0$), then $\mathcal{O}_L$ is not $\mathfrak{A}_{H_2}$-free (resp. not $\mathfrak{A}_{H_3}$-free) unless $n = 2d$.*

Case 2: $m \equiv 3 \pmod 4$, $n, k \equiv 2 \pmod 4$

Proposition

1. *If $m > 0$, $\mathcal{O}_L$ is not $\mathfrak{A}_{H_1}$-free unless m and n are coprime or m divides n.*
2. *If $n > 0$ (resp. $k > 0$), then $\mathcal{O}_L$ is not $\mathfrak{A}_{H_2}$-free (resp. not $\mathfrak{A}_{H_3}$-free) unless $n = 2d$.*

Corollary

The unique totally real biquadratic extensions $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ of $\mathbb{Q}$ with $m \equiv 3 \pmod 4$ and $n \equiv 2 \pmod 4$ for which $\mathcal{O}_L$ is $\mathfrak{A}_{H_i}$-free for all $i \in \{1, 2, 3\}$ are of the form $L = \mathbb{Q}(\sqrt{m}, \sqrt{2})$.

Case 3: $m \equiv 1 \pmod 4$, $n, k \not\equiv 1 \pmod 4$

Case 3: $m \equiv 1 \pmod 4$, $n, k \not\equiv 1 \pmod 4$

Reduced matrices of $M(H_i, L)$, $i \in \{1, 2, 3\}$:

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Case 3: $m \equiv 1 \pmod 4$, $n, k \not\equiv 1 \pmod 4$

Reduced matrices of $M(H_i, L)$, $i \in \{1,2,3\}$:

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Given $\beta \in \mathcal{O}_L$,

$$D_\beta(H_1, L) = -8\beta_2(2\beta_1+\beta_2)\left(2d\beta_3^2 + 2d\beta_3\beta_4 + \frac{1}{2}\left(d + \frac{m}{d}\right)\beta_4^2\right),$$

$$D_\beta(H_2, L) = 4(2\beta_1 + \beta_2)(2\beta_3 + \beta_4)\left(d\beta_2^2 + \frac{n}{d}\beta_4^2\right),$$

$$D_\beta(H_3, L) = 4\beta_4(2\beta_1 + \beta_2)\left(\frac{m}{d}\beta_2^2 + 4\frac{n}{d}\beta_3^2 + 4\frac{n}{d}\beta_3\beta_4 + \frac{n}{d}\beta_4^2\right).$$

Case 3: $m \equiv 1 \pmod 4$, $n, k \not\equiv 1 \pmod 4$

Proposition

- $\mathcal{O}_L$ *is* $\mathfrak{A}_{H_1}$*-free if and only if there exist integers* $x, y \in \mathbb{Z}$ *such that* $x^2 + my^2 = \pm 2d$*.*
- $\mathcal{O}_L$ *is not* $\mathfrak{A}_{H_2}$*-free nor* $\mathfrak{A}_{H_3}$*-free.*

Case 3: $m \equiv 1 \pmod 4$, $n, k \not\equiv 1 \pmod 4$

Proposition

- *$\mathcal{O}_L$ is $\mathfrak{A}_{H_1}$-free if and only if there exist integers $x, y \in \mathbb{Z}$ such that $x^2 + my^2 = \pm 2d$.*
- *$\mathcal{O}_L$ is not $\mathfrak{A}_{H_2}$-free nor $\mathfrak{A}_{H_3}$-free.*

Corollary

If $m > 0$, $\mathcal{O}_L$ is not $\mathfrak{A}_{H_1}$-free.

- F. Ferri, I. del Corso, D. Lombardo; *How far is an extension of p-adic fields from having a normal integral basis?,* Preprint
- D. Gil-Muñoz, A. Rio; *On Induced Hopf Galois structures and their Local Hopf Galois modules,* To appear in Publications Matemàtiques
- R.H. Hudson, K. S. Williams; *The integers of a cyclic quartic field,* Rocky Mountain Journal of Mathematics, No. 1 Vol. 20 (1990), 145-150
- P.J. Truman; *Hopf-Galois module structure of tame biquadratic extensions,* Journal de Théorie des Nombres de Bordeaux, No. 1 Vol. 24 (2012), 173-199
- D.A. Marcus; *Number fields,* Universitext, Springer, 1977

Thank you for your attention