The Hopf-Galois module structure of integers in tame radical extensions of number fields

Paul Truman

Keele University, UK

Hopf algebras and Galois module structure
University of Nebraska at Omaha
May, 2024

Idea...

Could these ideas be used to develop analogues of the Del Corso / Rossi results for tame non-normal radical extensions of number fields?

More precisely: let L/K be a tame radical extension of number fields and suppose H gives a Hopf-Galois structure on L/K.

- Is $\mathfrak{O}_L$ locally free over $\mathfrak{A}_H$?
  (Unlike classical case, not known to be automatic.)
- Can we find criteria for $\mathfrak{O}_L$ to be free over $\mathfrak{A}_H$?

In this talk we survey the results in this area and give a glimpse of the methods used to prove them.

Outline

A family of tame non-normal extensions

Let K be a number field. Fix $m, r \in \mathbb{N}$.

Let $a_1, \ldots, a_r \in \mathfrak{O}_K$ be such that $x^m - a_i$ is irreducible for each i.

For each i let α_i be a root of $x^m - a_i$.

Let $L = K(\alpha_1, \ldots, \alpha_r)$.

Suppose that:

- $n = [L : K] = m^r$;
- $L \cap K(\zeta_m) = K$ (and $\zeta_m \notin K$);
- L/K **is tame.**

A family of tame non-normal extensions

$$
\begin{tikzcd}
& E = LK(\zeta_m) \arrow[dl, dash, "S"'] \arrow[dr, dash, "T"] \arrow[dd, dash, dashed, "G"', "dm^r"] & \\
K(\zeta_m) \arrow[dr, dash, "d|\varphi(m)"'] & & L = K(\alpha_1, \dots, \alpha_r) \arrow[dl, dash, "n=m^r"] \\
& K &
\end{tikzcd}
$$

The Galois closure of L/K is $E = LK(\zeta_m)$;

$S = \mathrm{Gal}(E/K(\zeta_m)) \cong C_m^r$;

$T = \mathrm{Gal}(E/L)$ isomorphic to a subgroup of $\mathbb{Z}_m^\times$;

$G = \mathrm{Gal}(E/K) = S \rtimes T$.

An almost classical Hopf-Galois structure

Recall: $\mathrm{Gal}(E/K) = S \rtimes T$ with
$S = \mathrm{Gal}(E/K(\zeta_m)) \cong C_m^r$ and $T = \mathrm{Gal}(E/L)$.

- The Hopf-Galois structures on L/K correspond with regular subgroups of $\mathrm{Perm}(G/T)$ normalized by the image of the left translation map $\lambda : G \to \mathrm{Perm}(G/T)$.
- Since S is normal in G, one candidate is $\lambda(S)$; the corresponding Hopf algebra is $H = E[\lambda(S)]^G$.
- We have $E[\lambda(S)] \cong E^n$ as E-algebras; it turns out that $H \cong K^n$ as K-algebras.
- Within H we have a unique maximal $\mathfrak{O}_K$-order $\mathfrak{M} \cong \mathfrak{O}_K^n$, and the associated order of $\mathfrak{O}_L$:

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

What kind of result do we expect?

Definition

For $\mathbf{i} = (i_1, \ldots, i_r) \in \mathbb{Z}_m^r$ define $\mathbf{a}^{\mathbf{i}} = a_1^{i_1} \ldots a_r^{i_r}$ and

$$\mathfrak{b}_{\mathbf{i}} = \prod_{\mathfrak{p} \subset \mathfrak{O}_K} \mathfrak{p}^{\left\lfloor \frac{v_{\mathfrak{p}}(\mathbf{a}^{\mathbf{i}})}{m} \right\rfloor}.$$

Let H give the Hopf-Galois structure corresponding to $\lambda(S)$.

Conjecture

1. The ring of integers $\mathfrak{O}_L$ is locally free over $\mathfrak{A}$.
2. It is free if and only if each $\mathfrak{b}_{\mathbf{i}}$ is principal with generators $b_{\mathbf{i}}$ such that

$$\frac{1}{n} \sum_{\mathbf{i}} \frac{\alpha^{\mathbf{i}}}{b_{\mathbf{i}}} \in \mathfrak{O}_L.$$

Some families where the conjecture holds

Theorem (T. (2020))

Suppose that $m = p$ (an odd prime) and $r = 1$, so that $L = K(\alpha)$ with $\alpha^p \in \mathfrak{O}_K$. Suppose that p is unramified in K. Then (1) and (2) hold.

Theorem (Prestidge (Thesis, 2024))

Suppose that $m = p$ (an odd prime), so that $L = K(\alpha_1, \ldots, \alpha_r)$ with $\alpha_i^p \in \mathfrak{O}_K$ for each i. Suppose that p is unramified in K. Then (1) and (2) hold.

Theorem (Prestidge (Thesis, 2024))

Suppose that m is odd and squarefree and $r = 1$, so that $L = K(\alpha)$ with $\alpha^m \in \mathfrak{O}_K$. Suppose that each prime dividing m is unramified in K. Then (1) and (2) hold.

Examples

Example

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\alpha, \beta, \gamma)$ with $\alpha^3 = 10$ and $\beta^3 = 19$, $\gamma^3 = -17$. Then $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module.

Example

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\alpha)$ with $\alpha^{15} = 226$. Then $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module.

Example

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\alpha, \beta)$ with $\alpha^3 = 10$ and $\beta^3 = 28$. Then $\mathfrak{O}_L$ is a locally free $\mathfrak{A}$-module, but not a free $\mathfrak{A}$-module. The ideals $\mathfrak{b}_\mathbf{i}$ are all principal, but there is no family of generators of the required form.

Outline

Tools for establishing local freeness

Henceforth, suppose that $m = p$, or that m is squarefree and $r = 1$.

Since $H = E[\lambda(S)]^G$ is commutative we have:

Proposition (T. 2011)

If $\mathfrak{p} \nmid n$ then $\mathfrak{A}_\mathfrak{p} = \mathfrak{M}_\mathfrak{p}$ and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_\mathfrak{p}$-module.

What about $\mathfrak{p} \mid n$?

In the known cases m is squarefree, so $E = L(\zeta_m)$ is a tame Galois extension of L.

$$\begin{tikzcd}
 & E = LK(\zeta_m) \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, dashed, "dm^r"] & \\
K(\zeta_m) \arrow[dr, dash, "d|\varphi(m)"'] & & L = K(\alpha_1, \ldots, \alpha_r) \arrow[dl, dash, "n=m^r"] \\
 & K &
\end{tikzcd}$$

Tools for establishing local freeness: $\mathfrak{p} \mid n$

$$\begin{tikzcd}[arrows=dash]
 & E = LK(\zeta_m) \arrow[dl] \arrow[dr] \arrow[dd, dashed, "dm^r"] & \\
K(\zeta_m) \arrow[dr, "d|\varphi(m)"'] & & L = K(\alpha_1, \ldots, \alpha_r) \arrow[dl, "n=m^r"] \\
 & K &
\end{tikzcd}$$

- E/L is a tame Galois extension, so $\mathrm{Tr}_{E/L}(\mathfrak{O}_E) = \mathfrak{O}_L$.
- $E/K(\zeta_m)$ is a tame Kummer extension.
- We determine an explicit $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{L,\mathfrak{p}}$ by taking traces of an $\mathfrak{O}_{K,\mathfrak{p}}$-basis of $\mathfrak{O}_{E,\mathfrak{p}}$ and resolving linear dependencies.
- Using a few more tricks, we find that $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{\mathfrak{p}}$-module.

This establishes (1): $\mathfrak{O}_L$ is locally free over $\mathfrak{A}$.

Local-to-global techniques

Theorem (Bley and Johnston, 2007)

The ring of integers $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module if and only if

- *$\mathfrak{O}_L$ is a locally free $\mathfrak{A}$-module;*
- *$\mathfrak{M}\mathfrak{O}_L$ is a free $\mathfrak{M}$-module, with a generator $x \in \mathfrak{O}_L$.*

Since H is commutative, $\mathfrak{M}\mathfrak{O}_L$ is a free $\mathfrak{M}$-module if and only if it has trivial class in the locally free class group $\mathrm{Cl}(\mathfrak{M})$.

Since $H \cong K^n$ and $\mathfrak{M} \cong \mathfrak{O}_K^n$ we have

$$\mathrm{Cl}(\mathfrak{M}) \cong \frac{\mathbb{J}(H)}{H^\times \mathbb{U}(\mathfrak{M})} \cong \left(\frac{\mathbb{J}(K)}{K^\times \mathbb{U}(\mathfrak{O}_K)} \right)^n \cong \mathrm{Cl}(K)^n.$$

Local-to-global techniques

Recall: Given that $\mathfrak{O}_L$ is a locally free $\mathfrak{A}$-module, it is free if and only if $\mathfrak{M}\mathfrak{O}_L$ is a free $\mathfrak{M}$-module with a generator in $x \in \mathfrak{O}_L$.

We study the class of $\mathfrak{M}\mathfrak{O}_L$ in $\mathrm{Cl}(\mathfrak{M}) \cong \mathrm{Cl}(K)^n$.

- $\mathfrak{M}\mathfrak{O}_L$ is a free $\mathfrak{M}$-module if and only if the ideals $\mathfrak{b}_{\mathbf{i}}$ are principal;

$$\mathfrak{b}_{\mathbf{i}} = \prod_{\mathfrak{p} \subset \mathfrak{O}_K} \mathfrak{p}^{\lfloor \frac{v_{\mathfrak{p}}(\mathbf{a}^{\mathbf{i}})}{m} \rfloor}$$

- $\mathfrak{M}\mathfrak{O}_L$ has a free generator $x \in \mathfrak{O}_L$ if and only if the $\mathfrak{b}_{\mathbf{i}}$ have generators $b_{\mathbf{i}}$ such that

$$\frac{1}{n} \sum_{\mathbf{i}} \frac{\alpha^{\mathbf{i}}}{b_{\mathbf{i}}} \in \mathfrak{O}_L.$$

This establishes the criteria for freeness expressed in (2).

Outline

Almost tame extensions?

Many of the arguments exploit the fact that $\mathrm{Tr}_{L/K}(\mathfrak{O}_L) = \mathfrak{O}_K$, rather than tameness per se.

In the Galois case the trace condition is equivalent to tameness; in the non-normal case it is weaker.

Example

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\alpha)$ with $\alpha^9 = 163$. Then

$$\frac{1 + \alpha + \cdots + \alpha^8}{9}$$

is an integral element of trace 1.

But $3\mathfrak{O}_L = \mathfrak{P}_1\mathfrak{P}_2^2\mathfrak{P}_3^6$, so 3 ramifies wildly.

Possibly the conjecture could also hold in cases such as these.

Thank you for your attention.