Hopf-Galois module structure of some non-normal extensions of number fields

George Prestidge

School of Computing and Mathematics
Keele University
Research supervised by Dr. Paul Truman

Hopf algebras and Galois module theory conference
26^{th} May 2021

Some historical results

Theorem (Noether, 1932)

If L/K is a tamely ramified Galois extension of number fields with Galois group G, then $\mathcal{O}_L$ is a locally free $\mathcal{O}_K G$-module (of rank one).

Remark

In general, criteria for global freeness are more delicate.

- Del Corso and Rossi (2013) determined criteria for global freeness for L/K a tame Kummer extension (see the following slide)
- Truman (2020) studied a non-normal analogue of the result of Del Corso and Rossi for tamely ramified extensions of prime degree using Hopf-Galois theory

Aim

Our main aim is to generalise the work of Truman to certain families of tamely ramified extensions of prime-power degree which have a unique almost classical Hopf-Galois structure.

The result of Del Corso and Rossi

Let L/K be a tamely ramified Kummer extension of exponent m and degree N.

Definition

For $\alpha_1, ..., \alpha_r$ a set of Kummer generators for L/K, define $a_i = \alpha_i^m$, and write $\boldsymbol{\alpha}$ for $(\alpha_1, ..., \alpha_r)$ and $\boldsymbol{a}$ for $(a_1, ..., a_r)$. Similarly if $i_1, ..., i_r \in \mathbb{N}$ write $\boldsymbol{i}$ for $(i_1, ..., i_r)$.

Theorem

The extension L/K has a normal integral basis iff there exists a set of integral Kummer generators $\boldsymbol{\alpha}$ such that the following conditions hold.

- *The ideals $\mathcal{B}_{\boldsymbol{i}} = \prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor \frac{v_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{i}})}{m} \rfloor}$ are principal for all $\boldsymbol{i}$.*
- *The congruence $\sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{x_{\boldsymbol{i}}} \equiv 0 \pmod{N}$ holds for some $x_{\boldsymbol{i}} \in \mathcal{O}_K$ with $\mathcal{B}_{\boldsymbol{i}} = x_{\boldsymbol{i}} \mathcal{O}_K$.*

Further, when this is the case, the integer $\omega = \frac{1}{N} \sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{x_{\boldsymbol{i}}}$ generates $\mathcal{O}_L$ over $\mathcal{O}_K G$.

Hopf-Galois module theory

Now let L/K be a finite extension of number fields and suppose L/K is Hopf-Galois for some Hopf algebra H. Using Hopf-Galois module theory, we have a Hopf-Galois analogue of the normal basis theorem.

Theorem

L is a free H-module (of rank one).

Definition

We can define the *associated order* of $\mathcal{O}_L$ in H as $\mathcal{A}_H := \{h \in H | h.x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}$.

Hopf-Galois module theory is concerned with the following properties of $\mathcal{A}_H$.

- The structure of $\mathcal{A}_H$ as a ring
- The structure of $\mathcal{O}_L$ as an $\mathcal{A}_H$-module
    - i.e. whether $\mathcal{O}_L$ is locally or globally free as an $\mathcal{A}_H$-module

Setup for the extension

- Let K be a number field
- Let p be an odd prime
- Let ζ be a primitive p^{th} root of unity
- Assume that p is *unramified* in K
  - Note that this implies that $\zeta \notin K$
- Let $L = K(\alpha_1, ..., \alpha_r)$ where each $a_i := \alpha_i^p \in K$
- To ensure that the extension has degree p^r we require that
  - $a_i \in K \backslash K^p$ for all i
  - $\alpha_i \notin K(\alpha_j)$ for $i \neq j$
- Let E be the Galois closure of L/K
- It can be shown that $E = L(\zeta)$

Properties of the Galois group

- Let $G = Gal(E/K)$ and let $T = Gal(E/L)$
- We have $G = \langle \sigma_1, ..., \sigma_r, \tau \rangle$ and $T = \langle \tau \rangle$ where $\sigma_i(\alpha_i) = \zeta\alpha_i$, $\sigma_i(\alpha_j) = \alpha_j$, $\sigma_i(\zeta) = \zeta$, $\tau(\alpha_i) = \alpha_i$ and $\tau(\zeta) = \zeta^d$ for d some primitive root modulo p
- $G \cong S \rtimes T$ with $S := \langle \sigma_1, ..., \sigma_r \rangle$ the unique Sylow p-subgroup of G

Lemma

Since $Gal(E/L)$ (the group T) has a normal complement in G (namely S), the extension L/K is almost classically Galois.

Remark

Since S is the unique Sylow p-subgroup of G, the extension L/K has a unique almost classical Hopf-Galois structure.

Remark

For $r = 2$, this is the only Hopf-Galois structure admitted by the extension.

Properties of the Hopf-Galois structure

- The subgroup of $Perm(G/T)$ which gives rise to the unique almost classical Hopf-Galois structure is $\lambda(S)$
- The corresponding Hopf algebra is $H = E[\lambda(S)]^G$
- H has a K-basis consisting of mutually orthogonal idempotents

$$e_{\boldsymbol{i}} = \frac{1}{p^r} \prod_{k=1}^{r} \sum_{n=0}^{p-1} \zeta^{-i_k n} \lambda(\sigma_k)^n$$

- These give rise to an isomorphism of K-algebras, $H \cong K^{p^r}$
- H acts on L in the following way

$$e_{\boldsymbol{i}}(\boldsymbol{\alpha}^{\boldsymbol{j}}) = \begin{cases} \boldsymbol{\alpha}^{\boldsymbol{j}} & \text{if } \boldsymbol{i} = \boldsymbol{j} \\ 0 & \text{otherwise} \end{cases}$$

Determining criteria for the extension to be tamely ramified

Lemma

L/K is tame iff all α_i can be chosen to satisfy $a_i := \alpha_i^p \equiv 1 \pmod{p^2\mathcal{O}_K}$.

Proof.

- Firstly, we apply the standard result that L/K is tame iff the sub-extensions $K(\alpha_i)/K$ are tame for all i.
- Secondly, we apply a result of Truman (2020) that $K(\alpha_i)/K$ is tame iff α_i can be chosen to satisfy $a_i := \alpha_i^p \equiv 1 \pmod{p^2\mathcal{O}_K}$.

$\square$

Remark

Henceforth, we will assume that these congruences hold.

Determining local integral bases

For prime ideals $\mathfrak{p} \nmid p\mathcal{O}_K$ we study each sub-extension and use properties of arithmetic disjointness and obtain that a local integral basis is given by

$$\left\{ \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{\pi_{\mathfrak{p}}^{\lfloor \frac{v_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{i}})}{p} \rfloor}} \right\}$$

For prime ideals $\mathfrak{p} | p\mathcal{O}_K$ we use a different approach

- Define $F := K(\zeta)$
- E/F is a Galois extension and has local integral basis $\{\prod_{k=1}^{r}(\frac{\alpha_k - 1}{\zeta - 1})^{i_k} | 0 \leq i_k \leq p-1\}$
- F/K is a cyclotomic extension and has local integral basis $\{1, \zeta, ..., \zeta^{p-2}\}$
- It follows that an $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{E,\mathfrak{p}}$ is

$$\left\{ \prod_{k=1}^{r}(\frac{\alpha_k - 1}{\zeta - 1})^{i_k} \zeta^j | 0 \leq i_k \leq p-1, 0 \leq j \leq p-2 \right\}$$

Determining local integral bases

- Since the extension E/L is tamely ramified, the trace map is surjective at the level of rings of integers i.e. $Tr_{E/L}(\mathcal{O}_{E,\mathfrak{p}}) = \mathcal{O}_{L,\mathfrak{p}}$
- Hence $\mathcal{O}_{L,\mathfrak{p}}$ is spanned over $\mathcal{O}_{K,\mathfrak{p}}$ by the traces of the integral basis elements
- To simplify calculations when taking the trace, we remove the powers of $\zeta - 1$ from the denominator as follows. We use the division algorithm to write $i_1 + ... + i_r = Q(p-1) + R$ with $0 \leq R < p-1$. Since $(\zeta-1)^{p-1} \sim p$, the $\mathcal{O}_{K,\mathfrak{p}}$-basis of $\mathcal{O}_{E,\mathfrak{p}}$ becomes (up to units)

$$\left\{ \frac{(\alpha_1 - 1)^{i_1} ... (\alpha_r - 1)^{i_r}}{p^{Q+1}} (1-\zeta)^{p-1-R} \zeta^j | 0 \leq i_k \leq p-1, 0 \leq j \leq p-2 \right\}$$

- After taking the trace and resolving linear dependencies we find that a local integral basis is given by

$$\left\{ \frac{(\alpha_1 - 1)^{i_1} ... (\alpha_r - 1)^{i_r}}{p^{Q}} | 0 \leq i_k \leq p-1 \right\}$$

Determining the associated order

Definition

Let $\mathcal{M}$ denote the unique *maximal order* in H.
For $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$, let $\mathcal{M}_{\mathfrak{p}}$ denote the unique *maximal order* in $H_{\mathfrak{p}}$.

Proposition (Truman, 2011)

For prime ideals $\mathfrak{p} \nmid p\mathcal{O}_K$, we have $\mathcal{A}_{H,\mathfrak{p}} = \mathcal{M}_{\mathfrak{p}}$ and $\mathcal{O}_{L,\mathfrak{p}}$ is free over $\mathcal{A}_{H,\mathfrak{p}}$.

In our case $\mathcal{M}_{\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}}\langle(e_{\boldsymbol{i}})\rangle$.

Proposition

For prime ideals $\mathfrak{p}|p\mathcal{O}_K$, $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{A}_{H,\mathfrak{p}}$-module (of rank one).

For prime ideals $\mathfrak{p}|p\mathcal{O}_K$ we determine the associated order and prove freeness "all in one". We will sketch the proof of freeness for prime ideals $\mathfrak{p}|p\mathcal{O}_K$ on the following slide.

Determining the associated order

- We take the element $x_{\boldsymbol{p-1}} = \frac{(1+\alpha_1+...+\alpha_1^{p-1})...(1+\alpha_r+...+\alpha_r^{p-1})}{p^r}$ as a "candidate generator"
- Note that we choose this particular element because it has the largest power of p in the denominator
- We determine elements $a_{\boldsymbol{i}} \in H_{\mathfrak{p}}$ such that $a_{\boldsymbol{i}}.x_{\boldsymbol{p-1}} = x_{\boldsymbol{i}}$ for all basis elements $x_{\boldsymbol{i}}$
- Note that these elements exist because our "candidate generator" generates $L_{\mathfrak{p}}$ as an $H_{\mathfrak{p}}$-module
- To determine whether $a_{\boldsymbol{i}} \in \mathcal{A}_{H,\mathfrak{p}}$ we need to evaluate $a_{\boldsymbol{i}}.x_{\boldsymbol{j}}$ for all basis elements $x_{\boldsymbol{j}}$
- $a_{\boldsymbol{i}} \in \mathcal{A}_{H,\mathfrak{p}}$ iff $a_{\boldsymbol{i}}.x_{\boldsymbol{j}} \in \mathcal{O}_{L,\mathfrak{p}}$ for all basis elements $x_{\boldsymbol{j}}$
- It turns out that the elements $a_{\boldsymbol{i}}$ are actually in the associated order as claimed
- Hence the elements $a_{\boldsymbol{i}}$ form an $\mathcal{O}_{K,\mathfrak{p}}$-basis of the associated order and $\mathcal{O}_{L,\mathfrak{p}} = \mathcal{A}_{H,\mathfrak{p}}.x_{\boldsymbol{p-1}}$

Using idèlic theory to derive conditions for global freeness

The main result that we will use to derive conditions for global freeness is the following.

Theorem (Bley and Johnston, 2008)

$\mathcal{O}_L$ is a free $\mathcal{A}_H$-module iff

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

We have shown that $\mathcal{O}_L$ is a *locally* free $\mathcal{A}_H$-module.
To determine when $\mathcal{M}\mathcal{O}_L$ is free $\mathcal{M}$-module with a generator $x \in \mathcal{O}_L$, we use the idèlic description of $Cl(\mathcal{M})$ (the locally free class group of $\mathcal{M}$).

- $\mathcal{M}\mathcal{O}_L$ is a free $\mathcal{M}$-module iff $\mathcal{M}\mathcal{O}_L$ has trivial class in $Cl(\mathcal{M})$
- The isomorphism $H \cong K^{p^r}$ gives rise to an isomorphism of class groups
- $Cl(\mathcal{M}) \cong \frac{\mathbb{J}(H)}{H^\times \mathbb{U}(\mathcal{M})} \cong Cl(\mathcal{O}_K)^{p^r}$

Using idèlic theory to derive conditions for global freeness

- The class of $\mathcal{M}\mathcal{O}_L$ corresponds to the tuple $(\mathcal{B}_{\boldsymbol{i}})$ where

$$\mathcal{B}_{\boldsymbol{i}} = \prod_{\mathfrak{p}} \mathfrak{p}^{\left\lfloor \frac{v_{\mathfrak{p}}(\boldsymbol{a}^{\boldsymbol{i}})}{p} \right\rfloor}$$

- $\mathcal{M}\mathcal{O}_L$ is a free $\mathcal{M}$-module with a generator $x \in \mathcal{O}_L$ iff the ideals $\mathcal{B}_{\boldsymbol{i}}$ are principal with generators $x_{\boldsymbol{i}}$ such that $\sum_{i=0}^{p-1} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{x_{\boldsymbol{i}}} \equiv 0 \pmod{p^r \mathcal{O}_L}$

Our conclusion is the following.

Theorem

$\mathcal{O}_L$ is a free $\mathcal{A}_H$-module iff there exist $\alpha_1, ..., \alpha_r \in \mathcal{O}_L$ such that

- $L = K(\alpha_1, ..., \alpha_r)$
- $a_i := \alpha_i^p \in \mathcal{O}_K$ *for all* $1 \leq i \leq r$
- *The ideals $\mathcal{B}_{\boldsymbol{i}}$ as defined above are principal with generators $x_{\boldsymbol{i}}$ such that* $\sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{x_{\boldsymbol{i}}} \equiv 0 \pmod{p^r \mathcal{O}_L}$

Furthermore, in this case the element $\frac{1}{p^r} \sum_{\boldsymbol{i}} \frac{\boldsymbol{\alpha}^{\boldsymbol{i}}}{x_{\boldsymbol{i}}}$ is a free generator of $\mathcal{O}_L$ as an $\mathcal{A}_H$-module

Further work

- Mix primes
  - i.e. study extensions of the form $L = K(\alpha, \beta)$ where α^p, $\beta^q \in K$
- Single p^r root
  - i.e. study extensions of the form $L = K(\alpha)$ where $\alpha^{p^r} \in K$
- Work towards a complete analogue of the Del Corso and Rossi result

Thank you for your attention.