Hopf-Galois module structure of tame radical extensions of prime degree

Paul Truman

Keele University, UK

AMS Spring Southeastern Sectional Meeting

Auburn, Alabama

Saturday 16$^{\text{th}}$ March, 2019

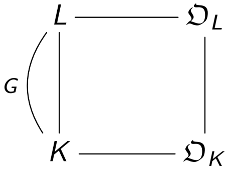
Overview

This talk is about the application of Hopf algebras to questions of integral Galois module structure in finite extensions of number fields.

- Integral Galois module structure
- Tame Kummer extensions of prime degree
- Hopf-Galois structures on field extensions
- Tame radical extensions of prime degree

Integral Galois module structure

Let L/K be a finite Galois extension of number fields with group G.
Write $\mathfrak{O}_L, \mathfrak{O}_K$ for the rings of algebraic integers of L, K.



L is a free $K[G]$-module of rank one.
Study $\mathfrak{O}_L$ as a module over its *associated order* in $K[G]$

$$\mathfrak{A}_{K[G]} = \{z \in K[G] \mid z \cdot \mathfrak{O}_L \subseteq \mathfrak{O}_L\}.$$

We have $\mathfrak{O}_K[G] \subseteq \mathfrak{A}_{K[G]}$, with equality if and only if $\mathrm{Tr}_{L/K}(\mathfrak{O}_L) = \mathfrak{O}_K$.
(That is: if and only if L/K is *tame*.)

Integral Galois module structure

Theorem (Noether, 1932)

If L/K is tame then $\mathfrak{O}_L$ is a locally free *$\mathfrak{O}_K[G]$-module (of rank one).*

That is: $\mathfrak{O}_{K,\mathfrak{p}} \otimes \mathfrak{O}_L$ is a free $\mathfrak{O}_{K,\mathfrak{p}}[G]$-module for each prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$.

Theorem (Hilbert-Speiser, 1897, 1916)

If $L/\mathbb{Q}$ is tame and abelian then $\mathfrak{O}_L$ is a free $\mathbb{Z}[G]$-module.

Integral Galois module structure

Theorem (Noether, 1932)

If L/K is tame then $\mathfrak{O}_L$ is a locally free *$\mathfrak{O}_K[G]$-module (of rank one).*

That is: $\mathfrak{O}_{K,\mathfrak{p}} \otimes \mathfrak{O}_L$ is a free $\mathfrak{O}_{K,\mathfrak{p}}[G]$-module for each prime ideal $\mathfrak{p}$ of $\mathfrak{O}_K$.

Theorem (Hilbert-Speiser, 1897, 1916)

If $L/\mathbb{Q}$ is tame and abelian then $\mathfrak{O}_L$ is a free $\mathbb{Z}[G]$-module.

For base fields different from $\mathbb{Q}$ the problem is more delicate.

Theorem (Greither et al, 1999)

If $K \neq \mathbb{Q}$ then there exists a prime number p and a tame Galois extension L/K of degree p such that $\mathfrak{O}_L$ is not a free $\mathfrak{O}_K[G]$-module.

Tame Kummer extensions of degree p

Theorem (Gómez Ayala, 1994)

Let K be a number field and p be a prime number. Suppose that $\zeta_p \in K$ and that L/K is a tame Galois extension of prime degree p with group G. Then $\mathfrak{O}_L$ is a free $\mathfrak{O}_K[G]$-module if and only if there exists an element $\beta \in \mathfrak{O}_L$ such that

1. $L = K(\beta)$,
2. $b = \beta^p \in \mathfrak{O}_K$,
3. *the ideals $\mathfrak{b}_j$ defined by $\mathfrak{b}_j = \prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor v_{\mathfrak{p}}(b^j)/p \rfloor}$ for $j = 0, 1, \ldots, p-1$ are principal, with generators b_j such that $\displaystyle\sum_{j=0}^{p-1} \frac{\beta^j}{b_j} \equiv 0 \pmod{p\mathfrak{O}_L}$.*

A new proof of Gómez Ayala's result

Theorem (Bley and Johnston, 2007)

Let L/K be a finite Galois extension of number fields with group G, and let $\mathfrak{M}$ be a maximal order in $K[G]$ that contains $\mathfrak{A}_{K[G]}$. Then $\mathfrak{O}_L$ is a free $\mathfrak{A}_{K[G]}$-module if and only if

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

A new proof of Gómez Ayala's result

Theorem (Bley and Johnston, 2007)

Let L/K be a finite Galois extension of number fields with group G, and let $\mathfrak{M}$ be a maximal order in $K[G]$ that contains $\mathfrak{A}_{K[G]}$. Then $\mathfrak{O}_L$ is a free $\mathfrak{A}_{K[G]}$-module if and only if

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

Now suppose L/K is a tame Kummer extension of prime degree p.

- $\mathfrak{O}_L$ is a locally free $\mathfrak{O}_K[G]$-module by Noether's theorem.
- We have $K[G] \cong K^p$ via orthogonal idempotents.
- $K[G]$ contains a unique maximal order $\mathfrak{M} \cong \mathfrak{O}_K^p$.
- $\mathfrak{M}\mathfrak{O}_L$ is a free $\mathfrak{M}$-module if and only if the ideals $\mathfrak{b}_j$ are principal.
- $\mathfrak{M}\mathfrak{O}_L$ has a generator in $\mathfrak{O}_L$ if and only if the congruence in point (3) of the theorem is satisfied.

Hopf-Galois structures

Let L/K be a finite Galois extension of fields with group G.

The action of $K[G]$ on L is an example of a *Hopf-Galois structure* on the extension; there may be others.

If H is a Hopf algebra giving a Hopf-Galois structure on L/K then define

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

and study the structure of $\mathfrak{O}_L$ as a module over the various $\mathfrak{A}_H$.

Hopf-Galois structures

Let L/K be a finite Galois extension of fields with group G.

The action of $K[G]$ on L is an example of a *Hopf-Galois structure* on the extension; there may be others.

If H is a Hopf algebra giving a Hopf-Galois structure on L/K then define

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

and study the structure of $\mathfrak{O}_L$ as a module over the various $\mathfrak{A}_H$.

Proposition (Childs, 1989/Kohl, 1998/Byott, 1996)

If L/K is a Galois extension of prime degree p then the Hopf-Galois structure given by $K[G]$ is the only Hopf-Galois structure on L/K.

Hopf-Galois structures

Non-normal extensions of number fields may also admit Hopf-Galois structures. These allow us to study rings of integers in these extensions.

Idea

Let K be a number field, suppose that $\zeta_p \notin K$, and let L/K be a radical extension of degree p (that is: $L = K(\alpha)$ with $\alpha^p \in K - K^p$).
Can we use Hopf-Galois structures to study $\mathfrak{O}_L$?

Hopf-Galois structures

Non-normal extensions of number fields may also admit Hopf-Galois structures. These allow us to study rings of integers in these extensions.

Idea

Let K be a number field, suppose that $\zeta_p \notin K$, and let L/K be a radical extension of degree p (that is: $L = K(\alpha)$ with $\alpha^p \in K - K^p$).
Can we use Hopf-Galois structures to study $\mathfrak{O}_L$?

Proposition (Childs, 1989/Kohl, 1998/Byott, 1996)

The extension L/K admits a unique Hopf-Galois structure.

Main Result

Theorem

Let K be a number field and p be a prime number. Suppose that p is unramified in K and that L/K is a tame radical extension of degree p. Let H give the unique Hopf-Galois structure on L/K. Then

- $\mathfrak{O}_L$ *is a locally free* $\mathfrak{A}_H$*-module;*
- $\mathfrak{O}_L$ *is a free* $\mathfrak{A}_H$*-module if and only if there exists* $\beta \in \mathfrak{O}_L$ *such that*
  1. $L = K(\beta)$,
  2. $b = \beta^p \in \mathfrak{O}_K$,
  3. *the ideals* $\mathfrak{b}_j$ *defined by* $\mathfrak{b}_j = \prod_{\mathfrak{p}} \mathfrak{p}^{\lfloor v_{\mathfrak{p}}(b^j)/p \rfloor}$ *for* $j = 0, 1, \ldots, p-1$ *are principal, with generators* b_j *such that* $\sum_{j=0}^{p-1} \frac{\beta^j}{b_j} \equiv 0 \pmod{p\mathfrak{O}_L}$.

Sketch of the proof

- We have $H \cong K^p$ via orthogonal idempotents.
- H contains a unique maximal order $\mathfrak{M} \cong \mathfrak{O}_K^p$.
- Bley and Johnston: $\mathfrak{O}_L$ is a free $\mathfrak{A}_H$-module if and only if it is a locally free $\mathfrak{A}_H$-module and $\mathfrak{M}\mathfrak{O}_L$ is free on an element of $\mathfrak{O}_L$.
- $\mathfrak{O}_L$ is a locally free $\mathfrak{A}_H$-module:
  - If $\mathfrak{p} \nmid p\mathfrak{O}_K$ then $\mathfrak{A}_{H,\mathfrak{p}} = \mathfrak{M}_{\mathfrak{p}}$, so $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.
  - If $\mathfrak{p} \mid p\mathfrak{O}_K$ then compute explicit $\mathfrak{O}_{K,\mathfrak{p}}$ bases of $\mathfrak{O}_{L,\mathfrak{p}}$ and $\mathfrak{A}_{H,\mathfrak{p}}$, and show that $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.
- $\mathfrak{M}\mathfrak{O}_L$ is a free $\mathfrak{M}$-module if and only if the ideals $\mathfrak{b}_j$ are principal.
- $\mathfrak{M}\mathfrak{O}_L$ has a generator in $\mathfrak{O}_L$ if and only if the congruence in point (3) of the theorem is satisfied.

Where next?

- Tame extensions of degree p^2:
  - Radical: $L = K(\alpha)$ with $\alpha^{p^2} \in K - K^{p^2}$.
    Harder to characterize tame versions of these.
  - Biradical: $L = K(\alpha, \beta)$ with $\alpha^p, \beta^p \in K - K^p$.
    Hopf-Galois structures not known in this case.
- Wild extensions of degree p:
  - There is a unique Hopf-Galois structure.
  - If $\mathfrak{p} \nmid p\mathfrak{O}_K$ then $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_{H,\mathfrak{p}}$-module.
  - What about for $\mathfrak{p} \mid p\mathfrak{O}_K$?
    Elder has analysed the Hopf-Galois module structure of wild non-normal extensions of local fields of degree p. Perhaps his results could be used to complete the local picture.
  - Then use result of Bley and Johnston to get global results.

Thank you for your attention.