Canonical Nonclassical Hopf-Galois Module Structure of Nonabelian Galois Extensions

Paul Truman

Keele University, UK

Hopf-Galois Structures on Galois Extensions

- Let L/K denote a finite Galois extension of fields with group G.
- The group algebra $K[G]$, with its usual action on L, gives a Hopf-Galois structure on the extension L/K.
- There may be other Hopf algebras giving Hopf-Galois structures on the extension.
- It might be interesting to make comparisons between them.
- Let $\mathrm{Perm}(G)$ be the group of permutations of G. Define an embedding $\lambda : G \to \mathrm{Perm}(G)$ by left translation:

$$\lambda(g)(h) = gh \text{ for } g, h \in G,$$

and an action of G on $\mathrm{Perm}(G)$ by conjugation via λ:

$$^{g}n = \lambda(g)n\lambda(g^{-1}) \text{ for } g \in G, n \in \mathrm{Perm}(G).$$

Greither-Pareigis Theory

Theorem (Greither and Pareigis)

- *There is a bijection between regular subgroups N of $Perm(G)$ normalized by $\lambda(G)$ and Hopf-Galois structures on L/K.*
- *The Hopf algebra giving the Hopf-Galois structure corresponding to the subgroup N is*

$$H = L[N]^G = \left\{ z \in L[N] \mid {}^g z = z \text{ for all } g \in G \right\}.$$

- *The action of an element of such a Hopf algebra on an element $t \in L$ is given by*

$$\left(\sum_{n \in N} c_n n \right) \cdot t = \sum_{n \in N} c_n n^{-1}(1_G)[t].$$

The Canonical Nonclassical Structure

- We can also define another embedding $\rho : G \to \mathrm{Perm}(G)$ by right translation:
$$\rho(g)(h) = hg^{-1} \text{ for } g, h \in G.$$
- The groups $\lambda(G)$ and $\rho(G)$ are regular subgroups of $\mathrm{Perm}(G)$ and are normalized by $\lambda(G)$, so they correspond to Hopf-Galois structures on L/K.
- The action of $\lambda(G)$ on $\rho(G)$ by conjugation is trivial, so we have:
$$L[\rho(G)]^G = L^G[\rho(G)] = K[\rho(G)],$$
and this subgroup corresponds to the classical structure.
- If G is abelian then $\lambda(G) = \rho(G)$, but if G is nonabelian then the subgroup $\lambda(G)$ corresponds to a canonical nonclassical Hopf-Galois structure on L/K. In this case the action of $\lambda(G)$ on itself by conjugation is not trivial, so we have
$$L[\lambda(G)]^G \neq K[\lambda(G)].$$

Hopf-Galois Module Theory

- Now suppose that L/K is an extension of local or global fields.

Definition

If L/K is H-Galois for some Hopf algebra H then we define the *Associated Order* of $\mathfrak{O}_L$ in H by

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

- What can we say about the structure of $\mathfrak{O}_L$ as an $\mathfrak{A}_H$-module?
- Each Hopf algebra that gives a Hopf-Galois structure on L/K provides a different description of $\mathfrak{O}_L$.
- There exist wildly ramified extensions of p-adic fields L/K for which $\mathfrak{O}_L$ is not free over $\mathfrak{A}_{K[G]}$ but is free over $\mathfrak{A}_H$ for some other Hopf algebra H giving a nonclassical Hopf-Galois structure on L/K.

Hopf-Galois Module Theory

- Suppose that L/K is H-Galois for $H = L[N]^G$.
- The $\mathfrak{O}_K$-order $\mathfrak{O}_L[N]^G$ is contained in the associated order $\mathfrak{A}_H$ of $\mathfrak{O}_L$.
- If L/K is wildly ramified then $\mathfrak{O}_L[N]^G \subsetneq \mathfrak{A}_H$, but if L/K is at most tamely ramified then it is possible that $\mathfrak{O}_L[N]^G = \mathfrak{A}_H$:

Theorem (PT)

Suppose that L/K is a finite Galois extension of p-adic fields with group G, that $p \nmid [L : K]$, and that N is abelian. Then $\mathfrak{O}_L[N]^G$ is the unique maximal order in $H = L[N]^G$ and $\mathfrak{O}_L$ is a free $\mathfrak{O}_L[N]^G$-module.

- At this conference last year I asked: Can we remove the hypothesis that N is abelian?

Hopf-Galois Module Theory

Conjecture

Suppose that L/K is a finite Galois extension of p-adic fields with group G and that $p \nmid [L:K]$. Then $\mathfrak{O}_L[N]^G$ is **a** maximal order in $H = L[N]^G$ and $\mathfrak{O}_L$ is a free $\mathfrak{O}_L[N]^G$-module.

Counterexample

- Let p be a prime that is congruent to 2 modulo 3, so that the field $\mathbb{Q}_p$ does not contain a primitive cube root of unity.
- Let L be the splitting field of $x^3 - p$ over $\mathbb{Q}_p$. Then $L/\mathbb{Q}_p$ is tamely ramified and Galois with group $G \cong D_3$.
- Since G is nonabelian, $L/\mathbb{Q}_p$ has a canonical nonclassical Hopf-Galois structure, corresponding to the regular subgroup $\lambda(G)$ of $\mathrm{Perm}(G)$. Let $H_\lambda = L[\lambda(G)]^G$ denote the corresponding Hopf algebra.
- Then $\mathfrak{O}_L$ is free over its associated order $\mathfrak{A}_\lambda$ in H_λ, but $\mathfrak{O}_L[N]^G \subsetneq \mathfrak{A}_\lambda$.

Main Results

- Let L/K be a finite Galois extension of local or global fields in characteristic 0 or p with nonabelian Galois group G.
- Denote by H_λ the Hopf algebra giving the canonical nonclassical Hopf-Galois structure on L/K.

Theorem

A G-stable fractional ideal of L is free over its associated order in $K[G]$ if and only if it is free over its associated order in H_λ.

Theorem

An element $x \in L$ generates L as $K[G]$-module if and only if it generates L as an H_λ-module.

Consequences of the main results

Corollary

If L/K is a tame nonabelian Galois extension of local fields then any fractional ideal of L is free over its associated order in H_λ.

Corollary

If L/K is a tame nonabelian Galois extension of global fields then $\mathfrak{O}_L$ is locally free over its associated order in H_λ.

Corollary

If $L/\mathbb{Q}$ is a tame nonabelian Galois extension whose degree is not divisible by 4 then $\mathfrak{O}_L$ is free over its associated order in H_λ.

Consequences of the main results

Corollary

If L/K is a nonabelian Galois extension of p-adic fields which is weakly ramified then $\mathfrak{O}_L$ is free over its associated order in H_λ.

Corollary

If L/K has has simple nonabelian Galois group then the extension admits only the classical and the canonical nonclassical Hopf-Galois structures, and a G-stable fractional ideal $\mathfrak{B}$ is either free over its associated order in both of these or in neither of them.

Corollary

If L/K is a nonabelian extension of local fields which has a valuation criterion for normal basis generators then it also has a valuation criterion for H_λ-generators.

Sketch of the Proof in one direction

- Suppose that $\mathfrak{O}_L$ is free over $\mathfrak{A}_{K[G]}$, with generator $x \in \mathfrak{O}_L$.
- Let $a_1, \ldots, a_n$ be an $\mathfrak{O}_K$-basis of $\mathfrak{A}_{K[G]}$.
- For each i, write $x_i = a_i(x)$. Then the x_i are an $\mathfrak{O}_K$-basis of $\mathfrak{O}_L$.
- Note that x also generates L as a $K[G]$-module, so the set $\{\sigma(x) \mid \sigma \in G\}$ is a K-basis of L.
- Let $\{\widehat{\sigma(x)} \mid \sigma \in G\}$ be the dual basis with respect to the trace form.

$$\widehat{\sigma(x)} = \sigma(\widehat{x})$$

for each $\sigma \in G$. So

$$\mathrm{Tr}_{L/K}(\sigma(\widehat{x})\tau(x)) = \delta_{\sigma,\tau}$$

for $\sigma, \tau \in G$.

Sketch of the Proof in one direction

- For each i, define an element $h_i \in L[\lambda(G)]$ by

$$h_i = \sum_{g \in G} \left(\sum_{\rho \in G} \rho(x_i) g^{-1} \rho(\widehat{x}) \right) \lambda(g).$$

- It turns out that each $h_i \in L[\lambda(G)]^G$, so it makes sense to let each h_i act on elements of L according to the formula

$$\begin{aligned} \left(\sum_{g \in G} c_g \lambda(g) \right) \cdot t &= \sum_{g \in G} c_g \lambda(g)^{-1}(1_G)(t) \\ &= \sum_{g \in G} c_g g^{-1}(t). \end{aligned}$$

- We will show that $h_i \cdot x = x_i$ and that each $h_i \in \mathfrak{A}_\lambda$, the associated order of $\mathfrak{O}_L$ in H_λ.

Sketch of the Proof in one direction

$$
\begin{aligned}
h_i \cdot x &= \left(\sum_{g \in G} \left(\sum_{\rho \in G} \rho(x_i) g^{-1} \rho(\widehat{x}) \right) \lambda(g) \right) \cdot x \\
&= \sum_{g \in G} \left(\sum_{\rho \in G} \rho(x_i) g^{-1} \rho(\widehat{x}) \right) g^{-1}(x) \\
&= \sum_{\rho \in G} \rho(x_i) \left(\sum_{g \in G} g^{-1} \rho(\widehat{x}) g^{-1}(x) \right) \\
&= \sum_{\rho \in G} \rho(x_i) \mathrm{Tr}_{L/K}(\rho(\widehat{x}) x) \\
&= \sum_{\rho \in G} \rho(x_i) \delta_{\rho,1} \\
&= x_i.
\end{aligned}
$$

Sketch of the Proof in one direction

- We still need to show that each h_i is in $\mathfrak{A}_\lambda$.
- It is sufficient to show that $h_i \cdot x_j$ for any i and j.
- It turns out that for $z \in H_\lambda$ and $\sigma \in G$ we have

$$z \cdot \sigma(t) = \sigma(z \cdot t) \text{ for all } t \in L,$$

so for any i and j we have

$$\begin{aligned} h_i \cdot x_j &= h_i \cdot a_j(x) \\ &= a_j(h_i \cdot x) \\ &= a_j(x_i), \end{aligned}$$

and this lies in $\mathfrak{O}_L$ since $x_i \in \mathfrak{O}_L$ and $a_j \in \mathfrak{A}_{K[G]}$.

- So each $h_i \in \mathfrak{A}_\lambda$ and the set $\{h_i \cdot x \mid i = 1, \ldots, n\}$ is an $\mathfrak{O}_K$-basis of $\mathfrak{O}_L$. Therefore $\mathfrak{O}_L$ is a free $\mathfrak{A}_\lambda$-module.

What about the Converse?

- We can use the same ideas to show that if $\mathfrak{O}_L$ is a free $\mathfrak{A}_\lambda$-module then it is a free $\mathfrak{A}_{K[G]}$-module.
- In this case we need to know that if and element $x \in L$ is an H_λ-generator of L then it is a $K[G]$-generator of L, so that we can consider the dual basis with respect to the trace form.
- For this, we need the second of the main theorems.

Further Questions

- Does assuming that one of $\mathfrak{A}_{K[G]}$ or $\mathfrak{A}_\lambda$ is a Hopf order imply that the other is too? This might be particularly interesting for tame extensions, where $\mathfrak{A}_{K[G]} = \mathfrak{O}_K[G]$ which is certainly a Hopf order.
- Does assuming that one of $\mathfrak{A}_{K[G]}$ or $\mathfrak{A}_\lambda$ is a Maximal order imply that the other is too?
- In the tame case, can we find a criterion for $\mathfrak{A}_\lambda = \mathfrak{O}_L[\lambda(G)]^G$?