# Integral Hopf-Galois Structures for Tame Extensions

Paul Truman

Keele University, UK

# Hopf-Galois Structures

- Nonclassical Hopf-Galois structures can provide a variety of viewpoints on a given finite separable extension of fields $L/K$. We will focus on Galois extensions of $p$-adic fields.

**Definition**

If $H$ is a $K$-Hopf algebra then we say that $H$ gives a *Hopf-Galois Structure* on the extension $L/K$, or that $L$ is an $H$-Galois extension of $K$, if:

- $L$ is an $H$-module algebra
- The $K$ linear map:

$$j : L \otimes H \to \mathrm{End}_K(L)$$

defined by

$$j(s \otimes h)(t) = s(h \cdot t)$$

is an isomorphism.

- The group algebra $K[G]$ gives a Hopf-Galois structure on $L/K$. (The Classical Structure)

# Greither-Pareigis Theory

Let Perm($G$) be the group of permutations of $G$. Define an embedding $\lambda : G \to \text{Perm}(G)$ by left translation:

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

## Theorem (Greither and Pareigis)

- *There is a bijection between regular subgroups $N$ of Perm($G$) normalised by $\lambda(G)$ and Hopf-Galois structures on $L/K$.*
- *If $N$ is such a subgroup, then $G$ acts on the group algebra $L[N]$ by acting on $L$ as Galois automorphisms and on $N$ by conjugation via $\lambda$:*

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

- *The Hopf algebra giving the Hopf-Galois structure corresponding to the subgroup $N$ is*

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

# Hopf-Galois Module Theory

**Definition**

If $L/K$ is $H$-Galois, 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 $\mathfrak{O}_L$.
- In the classical structure ($H = K[G]$):
  - If $L/K$ is at most tamely ramified then $\mathfrak{A}_{K[G]} = \mathfrak{O}_K[G]$ and $\mathfrak{O}_L$ is a free $\mathfrak{O}_K[G]$-module of rank one (Noether's Theorem).
  - If $L/K$ is wildly ramified then $\mathfrak{O}_K[G] \subsetneq \mathfrak{A}_{K[G]}$.
- There exist wildly ramified extensions $L/K$ 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 Hopf-Galois structure on $L/K$.

# Hopf-Galois Module Theory

## Definition

We call an $\mathfrak{O}_K$-order $A$ in $H$ a *Hopf Order* if it is an $\mathfrak{O}_K$-Hopf algebra with structure maps induced from those on $H$.

## Definition

Suppose that $A$ is a Hopf order in $H$.

- Recall that an element $\theta \in A$ is called a *left integral* of $A$ if $\theta a = \varepsilon(a)\theta$ for all $a \in A$.
- We say that $\mathfrak{O}_L$ is an *A-tame extension* of $\mathfrak{O}_K$ if there exists a left integral $\theta$ of $A$ satisfying $\theta\mathfrak{O}_L = \mathfrak{O}_K$.

## Theorem (Childs)

*Suppose that $A$ is a Hopf order in $H$ and that $\mathfrak{O}_L$ is an A-tame extension of $\mathfrak{O}_K$. Then $\mathfrak{O}_L$ is a free A-module of rank one.*

# Two Results on Tame Extensions

- If $L/K$ is at most tamely ramified then $\mathfrak{A}_{K[G]} = \mathfrak{O}_K[G]$ and $\mathfrak{O}_L$ is free over $\mathfrak{A}_{K[G]}$.
- Can we say anything about the structure of $\mathfrak{O}_L$ as a module over its associated order in any of the nonclassical Hopf-Galois structures admitted by the extension?
- If $H = L[N]^G$ is a Hopf algebra giving a Hopf-Galois structure on the extension, write $\Lambda = \mathfrak{O}_L[N]$.

**Theorem (PT)**

*Suppose that $H$ is commutative and $p \nmid [L:K]$. Then $\Lambda^G$ is the unique maximal order in $H$, $\mathfrak{A}_H = \Lambda^G$ and $\mathfrak{O}_L$ is a free $\Lambda^G$-module.*

**Theorem (PT)**

*Suppose that $L/K$ is unramified. Then $\Lambda^G$ is a Hopf order in $H$, $\mathfrak{A}_H = \Lambda^G$ and $\mathfrak{O}_L$ is a free $\Lambda^G$-module.*

# Describing $\Lambda^G$

- Recall that $G$ acts on $N$ by conjugation via the embedding $\lambda$.
- Let $N_1, \dots, N_r$ be the orbits of $G$ in $N$.
- For each $i = 1, \dots, r$, let $n_i \in N_i$ be a generator of the orbit $N_i$, and let $S_i = \mathrm{Stab}_G(n_i)$.
- Now let $L_i = L^{S_i}$, and let $\{x_{i,j} \mid j = 1, \dots, [L_i : K]\}$ be an integral basis of $L_i$ over $K$. For each $i = 1, \dots, r$ and $j = 1, \dots, [L_i : K]$, define

$$a_{i,j} = \sum_{g \in G/S_i} g(x_{i,j})\, {}^g n_i,$$

  where the sum is taken over a set of left coset representatives of $S_i$ in $G$ (in general $S_i$ need not be normal in $G$).
- Then the set

$$\{a_{i,j} \mid i = 1, \dots, r, \;\; j = 1, \dots, [L_i : K]\}$$

  is an $\mathfrak{O}_K$-basis of $\Lambda^G$.

# When is $\Lambda^G$ a Hopf order?

**Theorem**

*The following are equivalent:*

1. *The $\mathfrak{O}_K$-order $\Lambda^G$ is a Hopf order in $H$,*
2. *For each $i = 1, \ldots, r$, the extension $L_i/K$ is unramified,*
3. *The kernel of the action of $G$ on $N$ contains the inertia group of $L/K$.*

**Theorem**

*Suppose that $L/K$ is at most tamely ramified and that $\Lambda^G$ is a Hopf order in $H$. Then $\mathfrak{A}_H = \Lambda^G$ and $\mathfrak{O}_L$ is a free $\Lambda^G$-module.*

**Proof.**

- The element $\theta = \sum_{n \in N} n$ is a left integral of $\Lambda^G$, and there exists $x \in \mathfrak{O}_L$ such that $\theta \cdot x = \mathrm{tr}_{L/K}(x) = 1$.
- So $\mathfrak{O}_L$ is a $\Lambda^G$-tame extension of $\mathfrak{O}_K$, and so $\mathfrak{O}_L$ is a free $\Lambda^G$-module by Childs's theorem. Thus $\mathfrak{A}_H = \Lambda^G$. $\square$

# Duality for $\Lambda^G$

- The dual algebra $H^*$ is separable and commutative.
- It therefore has a unique maximal order $\Gamma$.
- In the notation used to describe $\Lambda^G$, there is an isomorphism of $\mathfrak{O}_K$-algebras:

$$\Gamma \cong \prod_{i=1}^{r} \mathfrak{O}_{L_i}.$$

- In particular, we have

$$\mathfrak{d}(\Gamma) = \prod_{i=1}^{r} \mathfrak{d}(\mathfrak{O}_{L_i}).$$

- We also have

$$(\Lambda^G)^* = \Gamma \Leftrightarrow \Lambda^G \text{ is a Hopf order in } H.$$

# Integral Hopf-Galois Structures

## Theorem (Greither)

*Suppose that $A$ is a Hopf order in $H$ such that $\mathfrak{O}_L$ is an $A$-module algebra. Then $\mathfrak{O}_L$ is an $A$-Galois extension of $\mathfrak{O}_K$ if and only if*

$$\mathfrak{d}(\mathfrak{O}_L) = \mathfrak{d}(A^*).$$

## Theorem

*The valuation ring $\mathfrak{O}_L$ is a $\Lambda^G$-Galois extension of $\mathfrak{O}_K$ if and only if $L/K$ is unramified.*

## Proof.

- $\Lambda^G$ is a Hopf order if and only if each $L_i$ is unramified over $K$.
- But in this case $\mathfrak{d}((\Lambda^G)^*) = \prod_{i=1}^{r} \mathfrak{d}(\mathfrak{O}_{L_i}) = \mathfrak{O}_K$
- So $\mathfrak{O}_L$ is a $\Lambda^G$-Galois extension of $\mathfrak{O}_K$ if and only if $\mathfrak{d}(\mathfrak{O}_L) = \mathfrak{O}_K$.

□

# Applications: Tame Extensions of Degree $pq$

- Let $p$ and $q$ be distinct primes.
- Write $\ell$ for the residue characteristic of $K$ from now on.
- Consider commutative Hopf-Galois structures on Galois extensions $L/K$ of degree $pq$ which are at most tamely ramified.
- Two possibilities for the structure of $G = \mathrm{Gal}(L/K)$: $G \cong C_{pq}$ or $G \cong M_{pq}$.

**Theorem (Byott)**

*If $p \not\equiv 1 \pmod{q}$ then $G \cong C_{pq}$ and $L/K$ admits only the classical Hopf-Galois structure, with $H = K[G]$.*

- In this case $\Lambda^G = \mathfrak{O}_K[G]$, and $\mathfrak{O}_L$ is a free $\mathfrak{O}_K[G]$-module by Noether's theorem.
- $\mathfrak{O}_L$ is an $\mathfrak{O}_K[G]$-Galois extension of $\mathfrak{O}_K$ if and only if $L/K$ is unramified.

# Applications: Tame Extensions of Degree $pq$

- Suppose that $p \equiv 1 \pmod{q}$ from now on.

**Theorem (Byott)**

- *If $L/K$ is cyclic then it admits precisely $2q-1$ Hopf-Galois structures. The classical structure is of cyclic type, and the other $2(q-1)$ structures are of metacyclic type.*
- *If $L/K$ is metacyclic then it admits precisely $2+p(2q-3)$ Hopf-Galois structures. Of these, $p$ are of cyclic type and the remainder are of metacyclic type.*

- We can deal with the classical structure on a cyclic extension as before.
- Since cyclic extensions do not admit any commutative nonclassical structures, we shall say nothing more about them.

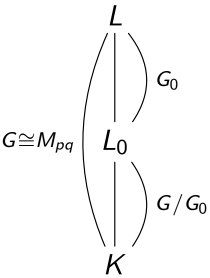
# Applications: Tame Extensions of Degree $pq$

- Summary: $p, q$ prime numbers, $p \equiv 1 \pmod{q}$. $L/K$ tamely ramified Galois extension of $\ell$-adic fields with group $M_{pq}$.
- $L/K$ admits $p$ commutative nonclassical Hopf-Galois structures.

**Theorem**

*Suppose that $\ell \nmid pq$. For each commutative Hopf algebra $H = L[N]^G$ giving a Hopf-Galois structure on the extension, $\mathfrak{A}_H = \Lambda^G$ and $\mathfrak{O}_L$ is a free $\mathfrak{O}_L$-module.*

- The case $\ell = p$ cannot occur:
- Let $L_0$ be the maximal unramified subextension of $L/K$. Then $\mathrm{Gal}(L/L_0) = G_0 \triangleleft G$.
- Since $L/K$ is tamely ramified we require $\ell \nmid |G_0|$, so if $\ell = p$ then $|G_0| = q$.
- But $M_{pq}$ does not have any normal subgroups of order $q$, so this is impossible.

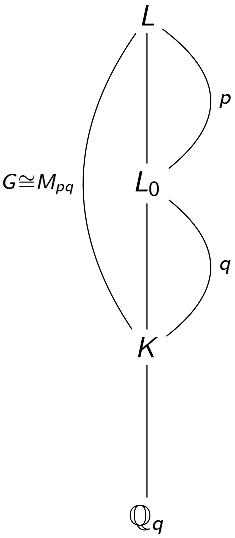


# Applications: Tame Extensions of Degree $pq$

- The remaining case is $\ell = q$.
- We may present $G \cong M_{pq}$ as

$$G = \langle \sigma, \tau \mid \sigma^p = \tau^q = 1, \tau\sigma\tau^{-1} = \sigma^d \rangle,$$

  where $d$ is a fixed natural number whose order modulo $p$ is $q$.
- We must have $|G_0| = p$, and $G_0 = \langle \sigma \rangle$, the unique normal subgroup of order $p$ in $G$.



# Applications: Tame Extensions of Degree $pq$

- A result of Byott describes explicitly the $p$ regular subgroups of $\mathrm{Perm}(G)$ which correspond to the commutative nonclassical Hopf-Galois structures on $L/K$.
  Denote them by $N_c$, for $0 \leq c \leq p-1$.
- Recall that $G$ acts on each $N_c$ by conjugation via the embedding $\lambda$:

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

- Using the explicit description of each $N_c$, it is easy to show that for each $c$, we have $^{\sigma^r}n = n$ for all $r \in \mathbb{Z}$ and $n \in N_c$, so $\langle \sigma \rangle = G_0$ is contained in the kernel of the action of $G$ on $N_c$.
- Therefore by a previous theorem $\Lambda_c^G = \mathfrak{O}_L[N_c]^G$ is a Hopf order in $H_c = L[N_c]^G$, and since $L/K$ is tamely ramified $\mathfrak{A}_H = \Lambda_c^G$ and $\mathfrak{O}_L$ is a free $\Lambda_c^G$-module.

# Applications: Tame Extensions of Degree $pq$

## Theorem

*Let $p, q$ and $\ell$ be prime numbers, and let $L/K$ be a Galois extension of $\ell$-adic fields which has degree $pq$ and is at most tamely ramified. Let $H = L[N]^G$ be a commutative Hopf algebra giving a Hopf-Galois structure on the extension. Then:*

- $\mathfrak{A}_H = \mathfrak{O}_L[N]^G$*, and* $\mathfrak{O}_L$ *is a free* $\mathfrak{O}_L[N]^G$*-module,*
- $\mathfrak{O}_L$ *is a* $\mathfrak{O}_L[N]^G$*-Galois extension of* $\mathfrak{O}_K$ *if and only if* $L/K$ *is unramified and* $H = K[G]$*, giving the classical structure on* $L/K$*.*

# Further Work

- I had wondered whether tameness of the extension $L/K$ might imply that $\mathfrak{A}_H = \Lambda^G$ and $\mathfrak{O}_L$ is a free $\Lambda^G$-module in each of the Hopf algebras $H$ giving Hopf-Galois structures on the extension.
- This is not true; one of the nonclassical structures of metacyclic type on a metacyclic extension of degree $pq$ does not behave like this.
- But clearly it happens under some circumstances, so the questions have become: under what circumstances do we have this kind of behaviour, and can we explain what happens in other cases?
- An obvious class of extensions to study first are those where the residue characteristic does not divide the degree of the extension. See my second talk!