Conjugate Hopf-Galois Structures

Paul Truman

Keele University, UK

Hopf algebras and Galois module theory

Wednesday 27th May, 2020

Most of this material is joint work with Alan Koch.

Overview

We study a method of partitioning the set of Hopf-Galois on a finite Galois extension, and show that Hopf-Galois structures in the same class share many properties.

- Definition and examples
- Interaction with some existing constructions
- Isomorphism problems and brace equivalence
- Hopf algebra actions and integral module structure
- A non-normal generalization

Conjugate Hopf-Galois structures

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

Let $\lambda, \rho : G \hookrightarrow \mathrm{Perm}(G)$ be the left and right regular representations of G.

Then G acts on $\mathrm{Perm}(G)$ by ${}^{\sigma}\pi = \lambda(\sigma)\pi\lambda(\sigma)^{-1}$.

The Hopf-Galois structures on L/K correspond bijectively with regular G-stable subgroups of $\mathrm{Perm}(G)$.

The Hopf-Galois structure corresponding to N is given by $L[N]^G$, with a prescribed action on L.

Definition

For N a regular G-stable subgroup of $\mathrm{Perm}(G)$, and $\sigma \in G$, let $N_\sigma = \rho(\sigma)N\rho(\sigma)^{-1}$.

We have $N_\sigma = N_\tau$ if and only if $\rho(\sigma^{-1}\tau) \in \mathrm{Norm}_{\mathrm{Perm}(G)}(N)$.

Only an interesting construction if G is nonabelian.

Conjugate Hopf-Galois structures

Each N_σ is a regular subgroup of $\mathrm{Perm}(G)$.

Proposition

For $\sigma \in G$, the subgroup N_σ is G-stable

Proof.

The elements of $\rho(G)$ and $\lambda(G)$ commute inside $\mathrm{Perm}(G)$, so for $\tau \in G$ we have

$$\begin{aligned} \lambda(\tau)\left(\rho(\sigma)N\rho(\sigma)^{-1}\right)\lambda(\tau)^{-1} &= \rho(\sigma)\lambda(\tau)N\lambda(\tau)^{-1}\rho(\sigma)^{-1} \\ &= \rho(\sigma)N\rho(\sigma)^{-1}. \end{aligned}$$

□

Hence $L[N_\sigma]^G$ gives a Hopf-Galois structure on L/K.

Call Hopf-Galois structures obtained in this way

Conjugate (or ρ-**Conjugate**).

Examples

Example

Let p, q be prime numbers with $p \equiv 1 \pmod{q}$, and L/K be a Galois extension with Galois group $G = \langle s, t \rangle \cong M_{pq}$.

- L/K admits p Hopf-Galois structures of cyclic type.
  The corresponding subgroups are generated by $\lambda(s)\rho(s^c t)$ for $c = 0, \ldots, p-1$.
  These Hopf-Galois structures are all conjugate.
- L/K admits $2 + 2p(q-2)$ Hopf-Galois structures of nonabelian type.
  The subgroups $\rho(G)$ and $\lambda(G)$ are normalized by $\rho(G)$.
  The remaining subgroups fall into $2(q-2)$ classes of size p.

Examples

Example

L/K be a Galois extension with Galois group $G = \langle s, t \rangle \cong D_{2n}$.

- A family of Hopf-Galois structures of dihedral type correspond to the subgroups generated by

$$\lambda(s)\rho(s^i t) \text{ and } \lambda(t)\rho(s^i t) \text{ for odd } i,$$

  and these are all conjugate.

- A family of Hopf-Galois structures of dihedral type correspond to the subgroups generated by

$$\lambda(s)\rho(s^i t) \text{ and } \lambda(t) \text{ for even } i,$$

  and these are all conjugate.

Interactions with existing constructions

Proposition

If N arises from a fixed-point-free abelian endomorphism $G \to G$, then so does each N_σ.

Proof.

Write $N = \alpha(G)$ where $\alpha(\tau) = \lambda(\tau)\rho(\psi(\tau))$ for some fixed point free abelian endomorphism ψ of G. Then

$$\rho(\sigma)\alpha(\tau)\rho(\sigma)^{-1} = \lambda(\tau)\rho(\sigma\psi(\tau)\sigma^{-1}),$$

and the map ψ' defined by $\psi'(\tau) = \sigma\psi(\tau)\sigma^{-1}$ is a fixed point free abelian endomorphism. $\square$

Interactions with existing constructions

Proposition

If $N^{op} = \mathrm{Cent}_{\mathrm{Perm}(G)}(N)$ is the opposite subgroup to N then $(N_\sigma)^{op} = (N^{op})_\sigma$.

Proof.

Every element of $(N^{op})_\sigma = \rho(\sigma)N^{op}\rho(\sigma)^{-1}$, commutes with every element of $N_\sigma = \rho(\sigma)N\rho(\sigma)^{-1}$.

Hence $(N^{op})_\sigma \subseteq (N_\sigma)^{op}$.

But these groups have equal order, so they are equal. $\square$

An earlier example again

Example

Return to the case in which p, q are prime numbers with $p \equiv 1 \pmod{q}$ and L/K is a Galois extension with Galois group $G = \langle s, t \rangle \cong M_{pq}$.

For $i = 0$ and $i = 2, \ldots, q-1$ define $\psi_i : G \to G$ by

$$\psi(s) = 1 \text{ and } \psi_i(t) = t^i.$$

Then each ψ_i is abelian and fixed point free.

Starting with the regular subgroups arising from the ψ_i and taking conjugates and opposites yields all of the regular G-stable subgroups of $\mathrm{Perm}(G)$ that are isomorphic to G.

Caveat: we need Byott's classification to be the sure that we have captured **all** such subgroups.

Hopf algebra isomorphisms

Proposition

The Hopf algebras $L[N]^G$ and $L[N_\sigma]^G$ are isomorphic.

Proof.

The isomorphism $N \xrightarrow{\sim} N_\sigma$ defined by $\eta \mapsto \rho(\sigma)\eta\rho(\sigma)^{-1}$ is a G-isomorphism: for $\eta \in N$ and $\tau \in G$ we have

$$\lambda(\tau)\rho(\sigma)\eta\rho(\sigma)^{-1}\lambda(\tau)^{-1} = \rho(\sigma)\lambda(\tau)\eta\lambda(\tau)^{-1}\rho(\sigma)^{-1}.$$

Hence the isomorphism of L-Hopf algebras $\theta : L[N] \to L[N_\sigma]$ defined by

$$\theta\left(\sum_{\eta \in N} c_\eta \eta\right) = \sum_{\eta \in N} c_\eta \rho(\sigma)\eta\rho(\sigma)^{-1}$$

descends to an isomorphism of K-Hopf algebras $L[N]^G \xrightarrow{\sim} L[N_\sigma]^G$. $\square$

Skew brace equivalence

Proposition

The regular subgroups N and N_σ correspond to the same skew brace.

Proof.

A regular G-stable subgroup M of $\mathrm{Perm}(G)$ corresponds to the same skew brace as N if and only if $M = \varphi N \varphi^{-1}$ for some $\varphi \in \mathrm{Aut}(G)$.

Write the inner automorphism corresponding to σ as $\varphi_\sigma = \rho(\sigma)\lambda(\sigma)$.

Then:

$$\begin{aligned} N_\sigma &= \rho(\sigma) N \rho(\sigma)^{-1} \\ &= \rho(\sigma)\lambda(\sigma) N \lambda(\sigma)^{-1}\rho(\sigma)^{-1} \\ &= \varphi_\sigma N \varphi_\sigma^{-1}. \end{aligned}$$

□

Hopf-Galois actions

Proposition

For $z \in L[N]^G$ and $x \in L$ we have

$$\theta(z) \cdot x = \sigma(z \cdot \sigma^{-1}(x)).$$

Proof.

Recall that the action of $L[N]^G$ on L is obtained by descent from the action of $L[N]$ on $\mathrm{Map}(G, L)$: we have $L \cong \mathrm{Map}(G, L)^G$ via the map

$$x \mapsto f_x = \sum_{\tau \in G} \tau(x) u_\tau \quad (\text{where } u_\tau(\upsilon) = \delta_{\tau,\upsilon}).$$

From the definition of N_σ we have $\theta(z) \cdot f = \rho(\sigma)(z \cdot \rho(\sigma)^{-1}(f))$ for all $z \in L[N]$ and all $f \in \mathrm{Map}(G, L)$, so this certainly holds for all $z \in L[N]^G$ and all $f \in \mathrm{Map}(G, L)^G$. $\square$

Alternatively...

Proof.

Explicitly, the Hopf algebra $L[N]^G$ acts on L by

$$z \cdot x = \left(\sum_{\eta \in N} c_\eta \eta \right) \cdot x = \sum_{\eta \in N} c_\eta \eta^{-1}(1_G)[x].$$

Note that $z = {}^\sigma z$, so

$$\begin{aligned} \theta(z) \cdot x &= \theta({}^\sigma z) \cdot x \\ &= \sum_{\eta \in N} \sigma(c_\eta) \rho(\sigma) \lambda(\sigma) \eta^{-1} \lambda(\sigma)^{-1} \rho(\sigma)^{-1} (1_G)[x] \\ &= \sum_{\eta \in N} \sigma(c_\eta) \sigma \eta^{-1} (1_G)[\sigma^{-1} x] \end{aligned}$$

$\square$

Hopf-Galois actions: Consequences

The Hopf-Galois normal basis theorem: L is a free $L[N]^G$-module of rank 1.

Recall: For $z \in L[N]^G$ and $x \in L$ we have $\theta(z) \cdot x = \sigma(z \cdot \sigma^{-1}(x))$.

Proposition

An element $x \in L$ generates L as an $L[N]^G$-module if and only if $\sigma(x)$ generates L as an $L[N_\sigma]^G$-module.

Hopf-Galois actions: Consequences

Hopf-Galois theory allows us to generalize classical Galois module theory.

If L/K is an extension of local or global fields and $L[N]^G$ gives a Hopf-Galois structure on L/K then can study each fractional ideal $\mathfrak{B}$ of L over its **associated order** in $L[N]^G$:

$$\mathfrak{A}(\mathfrak{B}) = \{z \in L[N]^G \mid z \cdot x \in \mathfrak{B} \text{ for all } x \in \mathfrak{B}\}.$$

It can be interesting to make comparisons between different structures. Recall: For $z \in L[N]^G$ and $x \in L$ we have $\theta(z) \cdot x = \sigma(z \cdot \sigma^{-1}(x))$.

Theorem

If $\mathfrak{B}$ is an ambiguous ideal of L then $\mathfrak{B}$ is free over its associated order in $L[N]^G$ if and only if it is free over its associated order in $L[N_\sigma]^G$.

Brace equivalence and/or Hopf algebra isomorphism?

Idea (At most, half-baked)

Conjugate Hopf-Galois structures involve isomorphic Hopf algebras and correspond to the same skew brace.

Could one, or the combination, of these properties lie behind the "uniform" integral module structure, or is it just a quirk of this particular construction?

Example (Skew brace equivalence isn't sufficient)

Let L/K be a Galois extension of number fields with Galois group $G \cong C_2 \times C_2$.

Then L/K admits 3 Hopf-Galois structures corresponding to cyclic $N \leq \mathrm{Perm}(G)$.

These all correspond to the same skew brace.

But it is possible for them to give "different" descriptions of $\mathfrak{O}_L$.

A tiny consolation

Proposition

Let N, M be regular G-stable subgroups of $\mathrm{Perm}(G)$, and suppose that they correspond to the same skew brace.

Then an element $x \in L$ generates L as an $L[N]^G$-module if and only if it generates L as an $L[M]^G$-module.

Proof.

We have $M = \varphi N \varphi^{-1}$ for some $\varphi \in \mathrm{Aut}(G)$.

An element $x \in L$ generates L as an $L[N]^G$-module if and only if the matrix $(\eta(\sigma)[x])_{\eta \in N,\, \sigma \in G}$ is nonsingular.

Similarly, x generates L as an $L[M]^G$-module if and only if the matrix $\left(\varphi\eta(\varphi^{-1}(\sigma))[x]\right)_{\eta \in N,\, \sigma \in G}$ is nonsingular. $\square$

Is Hopf algebra isomorphism sufficient?

I can't believe that this could be true, but I haven't been able to cook up an explicit counterexample.

To study this question, we need a Galois extension of local or global fields L/K and Hopf-Galois structures, given by $L[N]^G$ and $L[M]^G$, say, such that

- The Hopf algebras $L[N]^G$ and $L[M]^G$ are isomorphic, but not conjugate;
- We understand the integral module structure of L with respect to $L[N]^G$ and $L[M]^G$ very well.

One candidate: $G \cong C_3 \times C_3$. There are 8 nonclassical Hopf-Galois structures, which fall into 4 pairs under Hopf algebra isomorphism. These isomorphisms can't arise from conjugation.

A non-normal version of conjugate structures?

Let L/K be a separable, but non-normal extension, with Galois closure E.

Let $G = \mathsf{Gal}(E/K)$, $G' = \mathsf{Gal}(E/L)$, and $X = G/G'$, and let $\lambda : G \to \mathrm{Perm}(X)$ be the left translation map.

Then G acts on $\mathrm{Perm}(X)$ by ${}^{\sigma}\pi = \lambda(\sigma)\pi\lambda(\sigma)^{-1}$.

The Hopf-Galois structures on L/K correspond bijectively with regular G-stable subgroups of $\mathrm{Perm}(X)$.

Proposition

Let N be a regular G-stable subgroup of $\mathrm{Perm}(X)$, and let $\pi \in \mathrm{Cent}_{\mathrm{Perm}(X)}(\lambda(G))$. Then $N_\pi = \pi N \pi^{-1}$ is a regular G-stable subgroup of $\mathrm{Perm}(X)$.

Question

What does $\mathrm{Cent}_{\mathrm{Perm}(X)}(\lambda(G))$ look like?

A non-normal version of conjugate structures?

Let $\pi \in \mathrm{Cent}_{\mathrm{Perm}(X)}(\lambda(G))$

Proposition

The Hopf algebras $E[N]^G$ and $E[N_\pi]^G$ are isomorphic.

Proposition

An element $x \in L$ generates L as an $E[N]^G$ module if and only if it generates L as an $E[N_\pi]^G$-module.

However: I can't get such a tight grip on the Hopf algebra actions as in the Galois case, so I can't say anything about integral module structure in this case.

Thank you for your attention.