Opposite Hopf-Galois structures and opposite braces

Paul Truman

Braces and Hopf-Galois Theory
Keele University
Wednesday 19th June, 2019

Overview

- This is joint work with Alan Koch (Agnes Scott College, Georgia).
- Each Hopf-Galois structure on a Galois extension of fields has a natural "opposite" Hopf-Galois structure.
- We study the relationship between a Hopf-Galois structure and its opposite.
- In particular, we address certain isomorphism questions for the underlying Hopf algebras.
- Using the connection between Hopf-Galois structures and (skew left) braces, we formulate a notion of an "opposite" brace, and study properties of this construction.

Hopf-Galois structures on Galois field extensions

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

Theorem (Greither and Pareigis, 1987)

- *The Hopf-Galois structures on L/K correspond to regular subgroups of $Perm(G)$ that are normalized by the image of G under the left regular representation $\lambda : G \hookrightarrow Perm(G)$.*
- *The Hopf-Galois structure corresponding to such a subgroup N has Hopf algebra $L[N]^G$, together with a prescribed action on L.*

Example

- $\rho(G)$ corresponds to the *Classical structure*, with Hopf algebra $K[G]$.
- If G is nonabelian then $\lambda(G)$ corresponds to the *Canonical nonclassical structure*, with Hopf algebra $H_\lambda = L[\lambda(G)]^G$.

Opposite Hopf-Galois structures

Proposition (Greither and Pareigis)

If N is a regular subgroup of $\mathsf{Perm}(G)$ that is normalized by $\lambda(G)$, then so is $N' = \mathrm{Cent}_{\mathsf{Perm}(G)}(N)$.

Some properties of this construction:

- $(N')' = N$;
- $N \cong N'$;
- $N = N'$ if and only if N is abelian.

If $H = L[N]^G$, let $H' = H[N']^G$. Call the Hopf-Galois structure given by H' the *Opposite* of the one given by H.

Example

If $N = \rho(G)$ then $N' = \lambda(G)$. The canonical nonclassical structure is the opposite of the classical structure.

Existing results on opposite structures

Let H give a Hopf-Galois structure on L/K.

Lemma

For $h \in H, h' \in H', x \in L$, we have $h' \cdot (h \cdot x) = h \cdot (h' \cdot x)$.

Theorem (T, 2018)

An element $x \in L$ is a free generator of L as an H-module if and only if it is a free generator of H as an H'-module.

Theorem (T, 2018)

Suppose that L/K is an extension of local or global fields, and let $\mathfrak{O}_L$ denote the ring of algebraic integers in L. Let $\mathfrak{A}, \mathfrak{A}'$ denote the associated orders of $\mathfrak{O}_L$ in H, H'. The ring $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module if and only if it is a free $\mathfrak{A}'$-module.

Isomorphism problems

There has recently been interest in the question of when two Hopf algebras H_1, H_2 giving Hopf-Galois structures on L/K are isomorphic, either as K-Hopf algebras or as K-algebras.

Theorem

Write $H_1 = L[N_1]^G$, $H_2 = L[N_2]^G$. Then $H_1 \cong H_2$ as K-Hopf algebras if and only if there is an isomorphism of groups $\phi : N_1 \xrightarrow{\sim} N_2$ that respects the actions of G:

$$\phi(\lambda(g)\eta\lambda(g^{-1})) = \lambda(g)\phi(\eta)\lambda(g^{-1}) \text{ for all } \eta \in N_1, \; g \in G.$$

The question of K-algebra isomorphism is more delicate: no simple criterion is currently known.

For simplicity, assume K has characteristic zero from now on.

Isomorphism problems for $K[G]$ and $L[\lambda(G)]^G$

Theorem

Suppose that G is nonabelian. Then $K[G] \not\cong L[\lambda(G)]^G$ as K-Hopf algebras.

Proof.

For $g, h \in G$ we have

$$\lambda(g)\rho(h)\lambda(g^{-1}) = \lambda(g)\lambda(g^{-1})\rho(h) = \rho(h)$$

and

$$\lambda(g)\lambda(h)\lambda(g^{-1}) = \lambda(ghg^{-1}).$$

Hence $\lambda(G)$ centralizes $\rho(G)$, but does not centralize itself. Therefore there is no isomorphism $\phi : \rho(G) \xrightarrow{\sim} \lambda(G)$ with the required property. □

Isomorphism problems for $K[G]$ and $L[\lambda(G)]^G$

Theorem (Greither)

We have $K[G] \cong L[\lambda(G)]^G$ as K-algebras.

Sketch Proof.

- Let $K[G] = A_1 \times \cdots \times A_r$ be the Wedderburn decomposition of $K[G]$.
- For each i, let $B_i = L \otimes_K A_i$. Then $L[\lambda(G)] \cong B_1 \times \cdots \times B_r$.
- The action of G on $L[\lambda(G)]$ is inner, so respects this decomposition.
- For each i, the K-algebras A such that $L \otimes_K A \cong B_i$ are classified by $H^1(G, \mathrm{Aut}(B_i))$; in fact, in this case, by $H^1(G, \mathrm{Inn}(B_i))$.
- There is a surjection $H^1(G, B_i^\times) \to H^1(G, \mathrm{Inn}(B_i))$, but the domain is trivial by a generalization of Hilbert's theorem 90.

□

Isomorphism problems for H, H' in general

Theorem

In general, $H \cong H'$ as K-algebras.

Proof.

There exists $x \in L$ such that $L = H \cdot x = H' \cdot x$. Define $\varphi : H \to H'$ by $\varphi(a) \cdot x = a \cdot x$ for all $a \in H$. For $a, b \in H$ we have:

$$\begin{aligned}
\varphi(ab) \cdot x &= (ab) \cdot x \\
&= a \cdot (b \cdot x) \text{ (L is an H-module)} \\
&= a \cdot (\varphi(b) \cdot x) \text{ (definition of φ)} \\
&= \varphi(b) \cdot (a \cdot x) \text{ (actions of H, H' on L commute)} \\
&= \varphi(b) \cdot (\varphi(a) \cdot x) \text{ (definition of φ)} \\
&= (\varphi(b)\varphi(a)) \cdot x) \text{ (L is an H'-module).}
\end{aligned}$$

Isomorphism problems for H, H' in general

Proof continued.

We have seen that for $a, b \in H$ we have

$$\varphi(ab) \cdot x = (\varphi(b)\varphi(a)) \cdot x.$$

Since x is a free generator of L as an H'-module, this implies that

$$\varphi(ab) = \varphi(b)\varphi(a).$$

Therefore φ is an anti-isomorphism of K-algebras.

Composing with the antipode of H gives an isomorphism of K-algebras. □

Isomorphism problems for H, H' in general

Conjecture

If H is non-commutative then $H \not\cong H'$ as K-Hopf algebras.

Example

- We have seen that $K[G] \not\cong L[\lambda(G)]^G$ for G nonabelian.
- If $G \cong Q_8$ then L/K admits 6 structures of dihedral type.

  The conjecture holds for these.
- Suppose that $|G| = pq$ with p, q primes and $p \equiv 1 \pmod{q}$.
  - If G is cyclic then there are $2(q-1)$ structures of nonabelian type.
  - If G is nonabelian then there are $2p(q-2)$ structures of nonabelian type.

  The conjecture holds for all of these.
- If $|G| = p^3$ then ...?

Opposite Braces

Recall that L/K is a Galois extension of fields with Galois group G.
If $H = L[N]^G$ gives a Hopf-Galois structure on L/K then H yields a (skew left) brace $\mathfrak{B} = (B, \cdot, \circ)$ with $(B, \cdot) \cong N$ and $(B, \circ) \cong G$.

Lemma

The brace corresponding to the Hopf-Galois structure given by H' is $\mathfrak{B}' = (B, \cdot', \circ)$, where

$$x \cdot' y = y \cdot x \text{ for all } x, y \in B.$$

In general: given a brace $\mathfrak{B}$, call the brace $\mathfrak{B}'$ the *Opposite Brace* to $\mathfrak{B}$.
Note that if $(B, \cdot)$ is abelian then $\mathfrak{B} \cong \mathfrak{B}'$ as braces.

Some wishful thinking...

Distinct Hopf-Galois structures can yield isomorphic braces.

Question

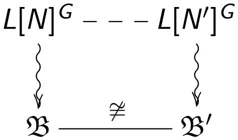
If two Hopf-Galois structures involve isomorphic Hopf algebras, do they yield isomorphic braces?

We have seen that $\mathfrak{B} \cong \mathfrak{B}'$ as braces if $(B, \cdot)$ is abelian.

Question

Do we have $\mathfrak{B} \cong \mathfrak{B}'$ only if $(B, \cdot)$ is abelian?

If the answer to both of these questions is "yes" then we can prove the conjecture:



Unfortunately . . .

. . . the answer to both of the questions on the previous slide is "no":

- Hopf-Galois structures involving isomorphic Hopf algebras need not yield isomorphic braces.
- It is possible for $\mathfrak{B} \cong \mathfrak{B}'$ to hold with $(B, \cdot)$ nonabelian.

The silver lining: since the answer to *both* questions is "no", the original conjecture is still open!

And we have lots of new questions to think about:

- Are there any conditions under which Hopf algebra isomorphism implies brace isomorphism, or vice-versa?
- Can we characterize braces that are isomorphic to their opposites?
- . . . ?

Thank you for your attention.