On some semidirect products of skew braces arising in Hopf-Galois theory

Paul Truman

Keele University, UK

Hopf algebras and Galois module theory

UConn (Online), June 2025

Overview

- The Hopf-Galois correspondence and extension problem
- The connection with skew braces and their substructures
- A family of semidirect products of skew braces
- Classifying skew braces in this family
- Consequences for Hopf-Galois theory

The Hopf-Galois correspondence

- Let L/K be a finite H-Hopf-Galois extension of fields.
- Given a Hopf subalgebra H' of H let

$$L' = L^{H'} = \{x \in L \mid h(x) = \varepsilon(h)x \text{ for all } h \in H'\}.$$

- Say that L' is *realized* by H.
- L/L' is $(L' \otimes H')$-Galois.
- If H' is a *normal* Hopf subalgebra of H then L'/K is $\overline{H}$-Galois, where $\overline{H} = H//H'$, and there is a short exact sequence of K-Hopf algebras

$$K \to H' \to H \to \overline{H} \to K.$$

$$\begin{tikzcd}
L \arrow[d, dash, "L' \otimes H'"] \arrow[dd, dash, bend right=40, "H"'] \\
L' \arrow[d, dash, "\overline{H}"] \\
K
\end{tikzcd}$$

The Hopf-Galois extension problem

Now suppose we are given

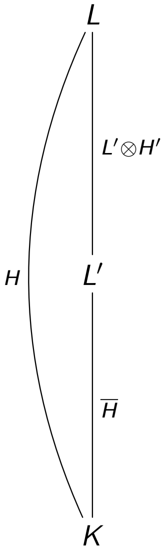
- a finite extension of fields L/K and an intermediate field L',
- K-Hopf algebras H' and $\overline{H}$ such that L/L' is $L' \otimes H'$-Galois and L'/K is $\overline{H}$-Galois.

Problem

Construct K-Hopf algebras H that fit into a short exact sequence

$$K \to H' \to H \to \overline{H} \to K$$

and such that L/K is H-Galois in a way compatible with the given structures on L/L' and L'/K.



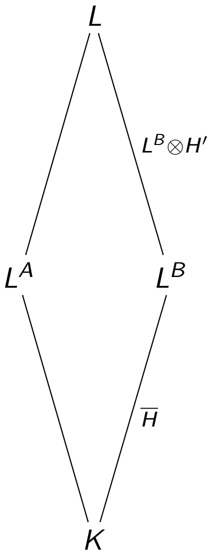
Induced Hopf-Galois structures

- Suppose that L/K is Galois with $\mathrm{Gal}(L/K) = G$, and write $L' = L^B$.

Theorem (Crespo, Rio, Vela, 2016)

Suppose that B has a normal complement A in G. Then we can solve the Hopf-Galois extension problem on the tower L/L^B and L^B/K.

- A Hopf-Galois structure constructed in this way satisfies $H \cong H' \otimes_K \overline{H}$.
- It also realizes both L^B and L^A via normal Hopf subalgebras.
- Note that L^B/K need not be Galois.



The connection with skew braces

- Now write $\mathrm{Gal}(L/K) = (G, \circ)$.
- Given a further binary operation $\cdot$ on G, the triple $(G, \cdot, \circ)$ is *skew brace* iff $(G, \cdot)$ is a group and for each $x \in G$ the function

$$\gamma_x(y) = x^{-1} \cdot (x \circ y)$$

  is an automorphism of $(G, \cdot)$.
- In this case the function $\gamma : (G, \circ) \to \mathrm{Aut}(G, \cdot)$ is a homomorphism, called the γ-*function* of the skew brace.

Theorem (Stefanello & Trapenniers, 2023)

- *There is a bijection between binary operations $\cdot$ on G such that $(G, \cdot, \circ)$ is a skew brace and Hopf-Galois structures on L/K.*
- *We have $(G, \cdot, \circ) \leftrightsquigarrow L[G, \cdot]^{(G,\circ)}$, where $(G, \circ)$ acts on L as the Galois group and on $(G, \cdot)$ via γ.*

Hopf subalgebras and ideals

- Recall: $\mathrm{Gal}(L/K) = (G, \circ)$ and $(G, \cdot, \circ) \leftrightsquigarrow H = L[G, \cdot]^{(G,\circ)}$.
- The Hopf subalgebras of H are $H_A = L[A, \cdot]^{(G,\circ)}$ with $(A, \cdot, \circ)$ a subskew brace of $(G, \cdot, \circ)$ that is stable under $\gamma(G)$; a *left ideal*.
- H_A is a normal Hopf subalgebra if and only if $(A, \cdot) \trianglelefteq (G, \cdot)$.
- $L^{H_A} = L^{(A,\circ)}$ is a normal extension of K if and only if $(A, \circ) \trianglelefteq (G, \circ)$.
- Hence normal Hopf subalgebras whose fixed fields are normal over K correspond with *ideals* $(A, \cdot, \circ)$ of $(G, \cdot, \circ)$.

Punchline

The Hopf-Galois extension problem on a tower of Galois extensions $L/L^{(A,\circ)}$ and $L^{(A,\circ)}/K$ is equivalent to the skew brace extension problem

$$\{e\} \to (A, \cdot, \circ) \to (G, \cdot, \circ) \to (G/A, \cdot, \circ) \to \{e\}.$$

Semidirect products

- Recall: The Hopf-Galois extension problem on tower of Galois extensions $L/L^{(A,\circ)}$ and $L^{(A,\circ)}/K$ is equivalent to

$$\{e\} \to (A, \cdot, \circ) \to (G, \cdot, \circ) \to (G/A, \cdot, \circ) \to \{e\}.$$

- A natural class to study are the *split extensions* (semidirect products).

Definition (Facchini and Pompili, 2024)

A skew brace $G = (G, \cdot, \circ)$ is said to be the *internal semidirect product* of an ideal A and a subskew brace B if

- $A \cap B = \{e\}$;
- $A \cdot B = A \circ B = G$.

- There is a corresponding notion of the *external semidirect product*, but these are complicated to construct.

Simplifying the external construction

Simplification

We shall classify skew braces that are the internal semidirect product of an ideal A and a left ideal B.

Example

Suppose $(G, \circ) = (A, \circ) \rtimes (B, \circ)$, and consider $(G, \circ, \circ)$.

We have $\gamma_x(y) = y$ for all $x, y \in G$, so A is an ideal of G, B is a left ideal of G, and G is the semidirect product of these.

Example

Suppose $(G, \circ) = (A, \circ) \rtimes (B, \circ)$, and consider $(G, \circ^{op}, \circ)$.

We have $\gamma_x(y) = x \circ y \circ \overline{x}$ for all $x, y \in G$. Hence A is an ideal of G, and B is subskew brace, but not a left ideal.

Here G is the semidirect product of an ideal and a subskew brace.

Notation for external semidirect products

Definition

Given skew braces $A = (A, \cdot, \circ)$ and $B = (B, \cdot, \circ)$ and group homomorphisms

$$\varphi : (B, \circ) \to \mathrm{Aut}(A, \circ)$$
$$\theta : (B, \cdot) \to \mathrm{Aut}(A, \cdot),$$

let $A \rtimes_\theta^\varphi B$ denote the Cartesian product $A \times B$, together with the operations

$$(a, b) \circ (a', b') = (a \circ \varphi_b(a'), b \circ b')$$
$$(a, b) \cdot (a', b') = (a \cdot \theta_b(a'), b \cdot b').$$

- Note that $A \rtimes_\theta^\varphi B$ is not a skew brace in general.

From internal to external

Proposition

If $A \rtimes_\theta^\varphi B$ is a skew brace then it is the internal semidirect product of the ideal $A \times \{e\}$ and the left ideal $\{e\} \times B$.

Proposition

Suppose that $G = (G, \cdot, \circ)$ is a skew brace which is the internal semidirect product of an ideal A and a left ideal B. Define

$$\varphi : (B, \circ) \to \mathrm{Aut}(A, \circ) \text{ by } \varphi_b(a) = b \circ a \circ \overline{b}$$

and

$$\theta : (B, \cdot) \to \mathrm{Aut}(A, \cdot) \text{ by } \theta_b(a) = b \cdot a \cdot b^{-1}.$$

Then $A \rtimes_\theta^\varphi B$ is a skew brace and $G \cong A \rtimes_\theta^\varphi B$.

Classifying external semidirect products in our family

- Recall: $\varphi : (B, \circ) \to \mathrm{Aut}(A, \circ)$ and $\theta : (B, \cdot) \to \mathrm{Aut}(A, \cdot)$ are group homomorphisms.

Theorem

$A \rtimes_{\theta}^{\varphi} B$ is a skew brace if and only if

- $\varphi_b \in \mathrm{Aut}(A, \cdot)$ *for each* $b \in B$;
- $\gamma_a \theta_b = \theta_b \gamma_a$ *for all* $a \in A$ *and* $b \in B$;
- $\varphi_b \theta_{b'} = \theta_{b\gamma_b(b')b^{-1}} \varphi_b$ *for all* $b, b' \in B$.

- We shall usually think of A, B and φ as being given, and seek *admissible* θ for this data.

Some examples

Recall: $\varphi : (B, \circ) \to \mathrm{Aut}(A, \circ)$ and $\theta : (B, \cdot) \to \mathrm{Aut}(A, \cdot)$.

Seek

- $\varphi_b \in \mathrm{Aut}(A, \cdot)$ for each $b \in B$;
- $\gamma_a \theta_b = \theta_b \gamma_a$ for all $a \in A$ and $b \in B$;
- $\varphi_b \theta_{b'} = \theta_{b\gamma_b(b')b^{-1}} \varphi_b$ for all $b, b' \in B$.

Example

Let $(A, \cdot, \circ)$ and $(B, \cdot, \circ)$ be skew braces.

Choose $\theta_b = \mathrm{id}$ for all $b \in B$.

Then θ is admissible if and only if $\varphi_b \in \mathrm{Aut}(A, \cdot)$ for all $b \in B$.

Some examples

Recall: $\varphi : (B, \circ) \to \mathrm{Aut}(A, \circ)$ and $\theta : (B, \cdot) \to \mathrm{Aut}(A, \cdot)$.

Seek

- $\varphi_b \in \mathrm{Aut}(A, \cdot)$ for each $b \in B$;
- $\gamma_a \theta_b = \theta_b \gamma_a$ for all $a \in A$ and $b \in B$;
- $\varphi_b \theta_{b'} = \theta_{b\gamma_b(b')b^{-1}} \varphi_b$ for all $b, b' \in B$.

Example

Let $(A, \circ, \circ)$ and $(B, \circ, \circ)$ be trivial skew braces.

Fix $i \in \mathbb{N}$ and choose $\theta_b = \varphi_{b^i}$ for all $b \in B$.

Then θ is admissible.

If $i = 1$ then $A \rtimes_{\theta}^{\varphi} B$ is the trivial skew brace on $(A, \circ) \rtimes (B, \circ)$.

Some examples

Recall: $\varphi : (B, \circ) \to \mathrm{Aut}(A, \circ)$ and $\theta : (B, \cdot) \to \mathrm{Aut}(A, \cdot)$. Seek

- $\varphi_b \in \mathrm{Aut}(A, \cdot)$ for each $b \in B$;
- $\gamma_a \theta_b = \theta_b \gamma_a$ for all $a \in A$ and $b \in B$;
- $\varphi_b \theta_{b'} = \theta_{b\gamma_b(b')b^{-1}} \varphi_b$ for all $b, b' \in B$.

Example

Let $(A, \circ, \circ)$ be trivial and cyclic and let $(B, \circ, \circ)$ be trivial and abelian. Then all $\theta : (B, \circ) \to \mathrm{Aut}(A, \circ)$ are admissible.

Some examples

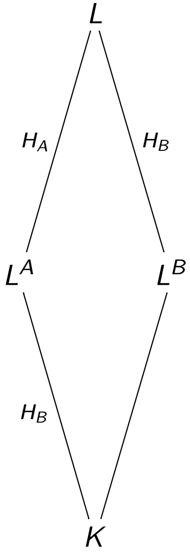
Recall: If $(A, \circ, \circ)$ is trivial and cyclic, $(B, \circ, \circ)$ is trivial and abelian, and $\varphi : (B, \circ) \to \mathrm{Aut}(A, \circ)$ is any homomorphism, then all $\theta : (B, \circ) \to \mathrm{Aut}(A, \circ)$ are admissible.

Example

Let p, q be primes with $p \equiv 1 \pmod{q}$.
Let $(A, \circ, \circ)$ have order p and $(B, \circ, \circ)$ have order q, and fix $\varphi : (B, \circ) \to \mathrm{Aut}(A, \circ)$.
There are q homomorphisms $\theta : (B, \circ) \to \mathrm{Aut}(A, \circ)$, and they are all admissible.

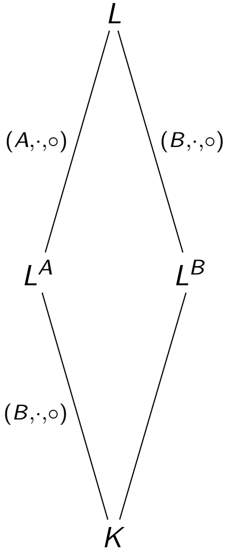
Back to the Hopf-Galois picture

- Let L/K be a Galois extension with $\mathrm{Gal}(L/K) = (G, \circ) \cong (A, \circ) \rtimes (B, \circ)$.
- Suppose that $G = A \rtimes_{\theta}^{\varphi} B$.
- Then $H = L[G, \cdot]^{(G,\circ)}$ has a normal Hopf subalgebra $H_A = L[A, \cdot]^{(G,\circ)}$ and a Hopf subalgebra $H_B = L[B, \cdot]^{(G,\circ)}$.
- Hence H solves the Hopf-Galois extension problem on $L/L^{(A,\circ)}$ and $L^{(A,\circ)}/K$, and in addition realizes $L^{(B,\circ)}$.
- In fact, we have classified all Hopf-Galois structures with these properties.



Induced Hopf-Galois structures again

- Suppose that $(G, \circ) \cong (A, \circ) \rtimes (B, \circ)$.
- Suppose we are given HGS on $L/L^{(B,\circ)}$ and $L^{(B,\circ)}/K$.
- The former corresponds to a skew brace $(B, \cdot, \circ)$.
- The latter can be translated to a HGS on the Galois extension $L/L^{(A,\circ)}$.
- This corresponds to a skew brace $(A, \cdot, \circ)$.
- We find that $\varphi_b \in \mathrm{Aut}(A, \cdot)$ for each $b \in B$.
- Hence we can construct the skew brace $A \rtimes^{\varphi}_{\mathrm{id}} B$.
- The corresponding HGS on L/K is the one induced from those on $L/L^{(B,\circ)}$ and $L^{(B,\circ)}/K$.



The structure of H

- Recall $(G, \cdot, \circ) \leftrightsquigarrow L[G, \cdot]^{(G,\circ)}$.
- If $(G, \cdot)$ is the semidirect product of $(A, \cdot)$ and $(B, \cdot)$ then we have

$$L[G, \cdot] \cong L[A, \cdot] \#_L L[B, \cdot].$$

Proposition

If $(G, \cdot, \circ)$ is the semidirect product of an ideal A and a left ideal B then

$$L[G, \cdot]^{(G,\circ)} \cong L[A, \cdot]^{(G,\circ)} \#_K L[B, \cdot]^{(G,\circ)}.$$

- In the case of induced Hopf-Galois structures B is also an ideal, and we have $L[G, \cdot]^{(G,\circ)} \cong L[A, \cdot]^{(G,\circ)} \otimes_K L[B, \cdot]^{(G,\circ)}$.
- If L/K is an extension of local or global fields this description can be used to address questions of integral module structure.

Questions

Question

Four of the five groups of order p^3 (with p an odd prime) are semidirect products. Which of the skew braces of order p^3 arise via our construction?

Question

A group of order p^2q (with p, q distinct primes) is necessarily a semidirect product. Which of the skew braces of order p^2q arise via our construction?

Question

A group of squarefree order is necessarily a semidirect product. Which of the skew braces of squarefree order arise via our construction?

Question

Can we generalize our construction to allow cocycles with respect to $\circ$ or $\cdot$?

Thank you for your attention.