Skew braces and the Hopf–Galois correspondence

Lorenzo Stefanello

The Interplay Between Skew Braces and Hopf-Galois Theory,
18 April 2023

Hopf–Galois theory

Let L/K be a finite Galois extension with Galois group G.

Definition

A *Hopf–Galois structure* $(H, \star)$ on L/K consists of

- a K-Hopf algebra H;
- an action $\star$ of H on L such that
  1. L is an H-module algebra;
  2. the map

$$L \otimes_K H \to \mathrm{End}_K(L), \quad x \otimes h \mapsto (y \mapsto x(h \star y))$$

  is bijective.

The classical structure

Example

The *classical* structure on L/K consists of the group algebra

$$K[G] = \left\{ \sum_{\sigma \in G} k_\sigma \sigma \mid k_\sigma \in K \right\},$$

with its natural action on L:

$$\left(\sum_{\sigma \in G} k_\sigma \sigma \right) \star x = \sum_{\sigma \in G} k_\sigma \sigma(x).$$

Fact

There may be more Hopf–Galois structures on the same extension. Which is the correct one?

Some Galois theory

For all subgroups G' of G, define

$$L^{G'} = \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in G'\}.$$

- $L^{G'}$ is an intermediate field of L/K.
- $L/L^{G'}$ is Galois with Galois group G'.
- If G' is normal in G, then $L^{G'}/K$ is Galois with Galois group (isomorphic to) G/G'.
- The assignment $G' \mapsto L^{G'}$ gives an injective and inclusion-reversing correspondence from the subgroups of G to the intermediate fields of L/K.
- Every intermediate field arises in this way.

Galois theory and Hopf subalgebras

Fact

The subgroups of G correspond bijectively to the Hopf subalgebras of $K[G]$, via $G' \leftrightarrow K[G']$.

Moreover,

$$L^{G'} = \{x \in L \mid h \star x = \varepsilon(h)x \text{ for all } h \in K[G']\},$$

where ε denotes the counit of $K[G]$:

$$\varepsilon\colon K[G] \to K, \quad \sum_{\sigma \in G} k_\sigma \sigma \mapsto \sum_{\sigma \in G} k_\sigma.$$

The Hopf–Galois correspondence

Consider a Hopf–Galois structure $(H, \star)$ on L/K. For all Hopf subalgebras H' of H, define

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

- $L^{H'}$ is an intermediate field of L/K.
- $L^{H'} \otimes_K H'$ yields a Hopf–Galois structure on $L/L^{H'}$.
- If H' is normal in H, then H/H' yields a Hopf–Galois structure on $L^{H'}/K$.
- The assignment $H' \mapsto L^{H'}$ gives an injective and inclusion-reversing correspondence from the Hopf subalgebras of H to the intermediate fields of L/K.
- This *Hopf–Galois correspondence* is not necessarily surjective!

The main questions

Consider a Hopf–Galois structure $(H, \star)$ on L/K.

Questions

1. *Is the Hopf–Galois correspondence surjective? (If so, why? If not, how far is it?)*
2. *Given an intermediate field, is it in the image of the Hopf–Galois correspondence?*

Summarising, how well can we control the image of the Hopf–Galois correspondence?

Greither–Pareigis theory

Let L/K be a finite Galois extension with Galois group G. Denote by $\mathcal{L}(G)$ the subgroup of $\mathrm{Perm}(G)$ of left translations.

Theorem ([Greither and Pareigis, 1987])

There exists a bijection between

- *Hopf–Galois structures on L/K;*
- *regular subgroups N of $\mathrm{Perm}(G)$ normalised by $\mathcal{L}(G)$.*

Explicitly, $N \leftrightarrow L[N]^G$, where G acts on L via Galois action and on N via conjugation (after the identification $G \leftrightarrow \mathcal{L}(G)$).

Moreover, $L[N]^G$ acts on L as follows:

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

Examples

Example

- The subgroup $\mathcal{R}(G)$ of right translations yields the classical structure.
- The Hopf–Galois structure given by $\mathcal{L}(G)$ is called *canonical nonclassical*.

Let L/K be a finite Galois extension with Galois group G, and consider a Hopf–Galois structure $(H, \star)$ on L/K, with regular subgroup N.

The first main question via Greither–Pareigis

Question

Is the Hopf–Galois correspondence surjective?

Theorem ([Crespo et al., 2016])

The subgroups of N normalised by $\mathcal{L}(G)$ correspond bijectively to the Hopf subalgebras of $L[N]^G$, via $N' \leftrightarrow L[N']^G$.

Corollary

The Hopf–Galois correspondence surjective if and only if the numbers of the subgroups of G and the subgroups of N normalised by $\mathcal{L}(G)$ are the same.

The second main question via Greither–Pareigis

Question

Given an intermediate field, is it in the image of the Hopf–Galois correspondence?

Proposition ([Koch et al., 2019])

Let N' be a subgroup of N normalised by $\mathcal{L}(G)$, and take its corresponding intermediate field $L^{N'}$. Then

$$\mathrm{Gal}(L/L^{N'}) = \{\eta[1_G] \mid \eta \in N'\}.$$

Corollary

An intermediate field F is in the image of the Hopf–Galois correspondence if and only if there exists a subgroup N' of N normalised by $\mathcal{L}(G)$ such that

$$\mathrm{Gal}(L/F) = \{\eta[1_G] \mid \eta \in N'\}.$$

Examples

Example

- When we consider the classical structure, we recover the usual Galois correspondence, which is surjective.
- If $N = \mathcal{L}(G)$, then the image of the Hopf–Galois correspondence consists of the normal intermediate fields. In particular, if G is Hamiltonian, then the Hopf–Galois correspondence is surjective [Greither and Pareigis, 1987].
- Examples in degree 42 via Gap calculations [Koch et al., 2019].

Skew braces

Definition ([Guarnieri and Vendramin, 2017])

A skew brace is a triple $(B, +, \circ)$, where $(B, +), (B, \circ)$ are groups and

$$a \circ (b + c) = (a \circ b) - a + (a \circ c).$$

- Given $(B, +, \circ)$, $(B, \circ)$ acts on $(B, +)$ via λ:

$$\lambda \colon (B, \circ) \to \mathrm{Aut}(B, +), \quad a \mapsto \lambda_a \colon b \to -a + (a \circ b).$$

- The *left ideals* of $(B, +, \circ)$ are the subgroups of $(B, +)$ and $(B, \circ)$ which are invariant under λ_a for all $a \in B$.

First examples of skew braces

- For all groups $(B, \circ)$, $(B, \circ, \circ)$ is the trivial skew brace.
- For all groups $(B, \circ)$, $(B, \circ^{\mathrm{op}}, \circ)$ is the almost trivial skew brace.
- More in general, given a skew brace $(B, +, \circ)$, $(B, +^{\mathrm{op}}, \circ)$ is the *opposite* skew brace [Koch and Truman, 2020].

Notation

Given a group $(B, \circ)$, we denote by $\overline{b}$ the inverse of $b \in B$.

Some history

- In [Childs, 1989, Byott, 1996], translation of Greither–pareigis theory via holomorphs of groups.
- In [Bachiller, 2016], hinted a connection between Hopf–Galois structure and skew braces.
- In the appendix of Byott and Vendramin in [Smoktunowicz and Vendramin, 2018], the connection was made precise.

Fact

Consider a Hopf–Galois structure on L/K with regular subgroup N. Then we can attach to it a skew brace $(B, +, \circ)$ with $(B, +) \cong N$ and $(B, \circ) \cong G$.

Example

- The classical structure yields the almost trivial skew brace.
- The canonical nonclassical structure yields the trivial skew brace.

Old connection and Hopf subalgebras

Consider a Hopf–Galois structure $(H, \star)$ on L/K, yielding a skew brace $(B, +, \circ)$. In [Childs, 2018], Childs proposed a bijective correspondence between Hopf subalgebras of H and certain substructures of $(B, +, \circ)$.

Proposition ([Childs, 2017])

Suppose that G is cyclic of odd prime power order. Then the Hopf–Galois correspondence is surjective for all Hopf–Galois structures on L/K.

Lemma ([Koch and Truman, 2020])

Childs's substructures are the left ideals of the opposite skew brace.

The new connection

Let L/K be a finite Galois extension with Galois group $(G, \circ)$.

Theorem ([LS and Trappeniers, 2023])

There exists a bijection between:

- *Hopf–Galois structures on L/K;*
- *operations $+$ such that $(G, +, \circ)$ is a skew brace.*

Explicitly, $(G, +, \circ) \leftrightarrow L[G, +]^{(G,\circ)}$, where $(G, \circ)$ acts on L via Galois action and on $(G, +)$ via the λ map of $(G, +, \circ)$.

Moreover, $L[G, +]^{(G,\circ)}$ acts on L as follows:

$$\left(\sum_{\sigma \in G} a_\sigma \sigma\right) \star x = \sum_{\sigma \in G} a_\sigma \sigma(x).$$

Example

The trivial skew brace $(G, \circ, \circ)$ yields the classical structure.

Hopf subalgebras via skew braces

Let L/K be a finite Galois extension with Galois group $(G, \circ)$, and consider a Hopf–Galois structure $(H, \star)$ on L/K, with skew brace $(G, +, \circ)$ (hence $H = L[G, +]^{(G,\circ)}$).

Proposition

There exists a bijection between

- *Hopf subalgebras of H;*
- *left ideals of $(G, +, \circ)$.*

Explicitly, G' yields the Hopf subalgebra $L[G', +]^{(G,\circ)}$.

The Hopf–Galois correspondence via skew braces

Let G' be a left ideal of $(G, +, \circ)$. We can attach to G'

- an intermediate field $L^{L[G',+]^{(G,\circ)}}$, via Hopf–Galois theory.
- an intermediate field $L^{G'}$, via Galois theory.

Proposition ([LS and Trappeniers, 2023])

The equality $L^{L[G',+]^{(G,\circ)}} = L^{G'}$ *holds.*

The first main question via skew braces

Question

Is the Hopf–Galois correspondence surjective?

Corollary

The Hopf–Galois correspondence is surjective if and only if every subgroup of $(G, \circ)$ is a left ideal of $(G, +, \circ)$.

Moreover,

$$\frac{|\{\text{intermediate field in the image}\}|}{|\{\text{intermediate fields}\}|} = \frac{|\{\text{left ideals of } (G, +, \circ)\}|}{|\{\text{subgroups of } (G, \circ)\}|}.$$

The second main question via skew braces

Question

Given an intermediate field, is it in the image of the Hopf–Galois correspondence?

Corollary

An intermediate field F is in the image of the Hopf–Galois correspondence if and only if $\mathrm{Gal}(L/F)$ *is a left ideal of* $(G, +, \circ)$.

An example

Suppose that $(G, \circ) = \{\sigma^i\tau^j \mid i = 0, \dots, n,\ j = 0, 1\}$ is cyclic of order $2n$ with n odd, and consider the skew brace $(G, +, \circ)$ with

$$\sigma^i\tau^j + \sigma^a\tau^b = \sigma^{i+(-1)^j a}\tau^{j+b}.$$

To define the Hopf–Galois structure it is enough to compute $\lambda_{\sigma\tau}$:

$$\lambda_{\sigma\tau} \colon G \to G, \quad g \to \overline{g}.$$

Therefore $h = \sum_{g \in G} \ell_g g$ is in $L[G, +]^{(G,\circ)}$ if and only if

$$h = \sum_{g \in G} \sigma\tau(\ell_g)\overline{g},$$

that is, $\sigma\tau(\ell_g) = \ell_{\overline{g}}$.

Moreover, as every subgroup of $(G, \circ)$ is invariant under the action of $\lambda_{\sigma\tau}$, the Hopf–Galois correspondence is surjective.

A class of examples

Let L/K be a finite Galois extension with Galois group $(G, \circ)$, and denote by N its norm, that is, the intersection of the normalisers of all subgroups. Let $\psi\colon (G, \circ) \to N$ be a group homomorphism, and define

$$\sigma + \tau = \sigma \circ \psi(\sigma) \circ \tau \circ \overline{\psi(\sigma)}.$$

Proposition

$(G, +, \circ)$ is a skew brace, and every subgroup of $(G, \circ)$ is a left ideal of $(G, +, \circ)$.

Corollary

Suppose that $(G, \circ)$ is the quaternion group. Then there are exactly 16 (out of 24) Hopf–Galois structures on L/K for which the Hopf–Galois correspondence is surjective.

Childs's condition

Let L/K be a finite Galois extension with Galois group $(G, \circ)$.

Theorem ([LS and Trappeniers, 2023])

The following are equivalent:

- *For all Hopf–Galois structures on L/K, the Hopf–Galois correspondence is surjective.*
- $(G, \circ)$ *is cyclic, and for all primes p, q dividing the order of G, p does not divide $q - 1$.*

Example

Let $(G, \circ)$ cyclic of prime power order. Then for all Hopf–Galois structures on L/K, the Hopf–Galois correspondence is surjective.

Normal subgroups

Let L/K be a finite Galois extension with Galois group $(G, \circ)$, and consider a Hopf–Galois structure on L/K, given by a skew brace $(G, +, \circ)$ such that $\lambda_G = \mathrm{Inn}(G, \circ)$.

Proposition

The image of the Hopf–Galois correspondence consists precisely of the normal intermediate fields.

Example

- The canonical nonclassical structure, given by the skew brace $(G, \circ^{\mathrm{op}}, \circ)$, for which λ_g is conjugation by g in $(G, \circ)$.
- Suppose that $(G, \circ)$ has nilpotency class two, and define

$$g + h = g \circ h \circ [g, h]_\circ.$$

Then $(G, +, \circ)$ is a skew brace and λ_g is conjugation by $\overline{g}$ in $(G, \circ)$.

Bibliography

Bachiller, D. (2016).
Counterexample to a conjecture about braces.
J. Algebra, 453:160–176.

Byott, N. P. (1996).
Uniqueness of Hopf Galois structure for separable field extensions.
Comm. Algebra, 24(10):3217–3228.

Childs, L. N. (1989).
On the Hopf Galois theory for separable field extensions.
Comm. Algebra, 17(4):809–825.

Childs, L. N. (2017).
On the Galois correspondence for Hopf Galois structures.
New York J. Math., 23:1–10.

Bibliography

Childs, L. N. (2018).
Skew braces and the Galois correspondence for Hopf Galois structures.
J. Algebra, 511:270–291.

Crespo, T., Rio, A., and Vela, M. (2016).
On the Galois correspondence theorem in separable Hopf Galois theory.
Publ. Mat., 60(1):221–234.

Greither, C. and Pareigis, B. (1987).
Hopf Galois theory for separable field extensions.
J. Algebra, 106(1):239–258.

Guarnieri, L. and Vendramin, L. (2017).
Skew braces and the Yang–Baxter equation.
Math. Comp., 86(307):2519–2534.

Bibliography

Koch, A., Kohl, T., Truman, P. J., and Underwood, R. (2019).
Normality and short exact sequences of Hopf-Galois structures.
Comm. Algebra, 47(5):2086–2101.

Koch, A. and Truman, P. J. (2020).
Opposite skew left braces and applications.
J. Algebra, 546:218–235.

LS and Trappeniers, S. (2023).
On the connection between Hopf–Galois structures and skew braces.
Bulletin of the London Mathematical Society.

Bibliography

Smoktunowicz, A. and Vendramin, L. (2018).
On skew braces (with an appendix by N. Byott and L. Vendramin).
J. Comb. Algebra, 2(1):47–86.