Bi-skew braces in Hopf–Galois theory

Lorenzo Stefanello

Joint work with Senne Trappeniers

Hopf algebras and Galois module theory, 29 May 2023

Outline

- Introduction: Hopf–Galois structures and skew braces.
- Bi-skew braces in Hopf–Galois theory.

Introduction: Hopf–Galois structures and skew braces

Hopf–Galois structures

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 together with an action $\star$ of H on L such that

- L is an H-module algebra;
- the K-linear map

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

  is bijective.

Example

The *classical* structure consists of $H = K[G]$ with the usual Galois action.

The Hopf–Galois correspondence

Consider a Hopf–Galois structure $(H, \star)$ on L/K. For all K-Hopf subalgebras H' of H, we can consider an intermediate field

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

where ε denotes the counit of H.

We obtain in this way the *Hopf–Galois correspondence* (HGC), which is injective but not necessarily surjective.

In the classical case, we recover the usual bijective Galois correspondence.

Problem

- *When is the HGC surjective?*
- *Study the ratio $GC(L/K, H)$ of the number of fields in the image of the HGC to the number of intermediate fields.*

Skew braces

Definition ([Guarnieri and Vendramin, 2017])

A *skew brace* $(G, \cdot, \circ)$ consists of two groups $(G, \cdot)$ and $(G, \circ)$ related by the following property: for all $\sigma, \tau, \kappa \in G$,

$$\sigma \circ (\tau \cdot \kappa) = (\sigma \circ \tau) \cdot \sigma^{-1} \cdot (\sigma \circ \kappa).$$

(Given $\sigma \in G$, we write σ^{-1} for the inverse in $(G, \cdot)$ and $\overline{\sigma}$ for the inverse in $(G, \circ)$.)

Each skew brace is associated with a *gamma function*

$$\gamma\colon (G, \circ) \to \mathrm{Aut}(G, \cdot), \quad \sigma \mapsto (\tau \mapsto \sigma^{-1} \cdot (\sigma \circ \tau)).$$

First definitions

Let $(G, \cdot, \circ)$ be a skew brace.

Definition

A subgroup G' of $(G, \cdot)$ (or equivalently $(G, \circ)$) is a *left ideal* if G' is invariant under the action of $(G, \circ)$ via γ.

It is also necessarily a subgroup of $(G, \circ)$ (or $(G, \cdot)$).

Definition ([Childs, 2019])

We say that $(G, \cdot, \circ)$ is a *bi-skew brace* if also $(G, \circ, \cdot)$ is a skew brace.

Examples

Example

Let $(G, \circ)$ be a group. Then $(G, \circ, \circ)$ is the *trivial skew brace*.

Example $(*)$

Let $(G, \circ)$ be a cyclic group of order $2n$, where $n \geq 3$ is odd, written as $G = \{\sigma^i \tau^j \mid i = 0, \dots, n-1 \text{ and } j = 0, 1\}$. Define

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

Then $(G, \cdot, \circ)$ is a bi-skew brace, with $(G, \cdot)$ dihedral of order $2n$.

Some history on the connection

A (nonbijective) connection between skew braces and Hopf–Galois structures was presented in the appendix of Byott and Vendramin in [Smoktunowicz and Vendramin, 2018], building on the following works:

- [Greither and Pareigis, 1987];
- [Childs, 1989, Byott, 1996];
- [Bachiller, 2016]

A new (bijective) version of the connection was obtained in [LS and Trappeniers, 2023b], building on some observations of [Koch and Truman, 2020].

A new version of the connection

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

Theorem ([LS and Trappeniers, 2023b])

The following data are equivalent:

- *a Hopf–Galois structure on L/K;*
- *an operation $\cdot$ such that $(G, \cdot, \circ)$ is a skew brace.*

Explicitly, $(G, \cdot, \circ) \leftrightarrow L[G, \cdot]^{(G,\circ)}$, where $(G, \circ)$ acts on L via Galois action and on $(G, \cdot)$ via the gamma function γ of $(G, \cdot, \circ)$.

Moreover, $L[G, \cdot]^{(G,\circ)}$ 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 classical structure is associated with the trivial skew brace.

An explicit example

Let $n \geq 3$ be odd, and let L/K be a Galois extension with cyclic Galois group $(G, \circ) = \{\sigma^i \tau^j \mid i = 0, \dots, n-1 \text{ and } j = 0, 1\}$ of order $2n$. Consider $(G, \cdot, \circ)$ as in Example $(*)$. Then

$$\gamma(\sigma\tau) \colon G \to G, \quad g \to \overline{g}.$$

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

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

that is, $\sigma\tau(\ell_g) = \ell_{\overline{g}}$ for all $g \in G$. Moreover, H acts on L via

$$h \star x = \sum_{g \in G} \ell_g g(x).$$

Skew braces and the Hopf–Galois correspondence

Let L/K be a finite Galois extension with Galois group $(G, \circ)$. Consider the Hopf–Galois structure associated with a skew brace $(G, \cdot, \circ)$. Here $H = L[G, \cdot]^{(G,\circ)}$.

Proposition ([LS and Trappeniers, 2023b])

- *Left ideals of $(G, \cdot, \circ)$ correspond bijectively to K-Hopf subalgebras of H. Explicitly, $G' \leftrightarrow L[G', \cdot]^{(G,\circ)}$.*
- *Let G' be a left ideal of $(G, \cdot, \circ)$, and take $H' = L[G', \cdot]^{(G,\circ)}$. Then $L^{G'} = L^{H'}$.*

Corollary

An intermediate field $L^{G'}$ is in the image of the HGC if and only if G' is a left ideal of $(G, \cdot, \circ)$. Moreover,

$$GC(L/K, H) = \frac{|\{\textit{left ideals of } (G, \cdot, \circ)\}|}{|\{\textit{subgroups of } (G, \circ)\}|}.$$

Bi-skew braces in Hopf–Galois theory

Construction of Hopf–Galois structures

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

Fact

To obtain Hopf–Galois structures on L/K, we need to construct skew braces of the form $(G, \cdot, \circ)$. However...

- Constructing operations $\cdot$ such that $(G, \cdot, \circ)$ is a skew brace: "difficult" task.
- Constructing operations $\cdot$ such that $(G, \circ, \cdot)$ is a skew brace: "easier" task.

Idea: Construct skew braces $(G, \circ, \cdot)$ that happen to be bi-skew braces $\rightsquigarrow$ obtain Hopf–Galois structures on L/K given by $(G, \cdot, \circ)$.

Some known constructions: abelian maps

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

- If $\psi\colon (G, \circ) \to (G, \circ)$ is a homomorphism with abelian image, then $(G, \circ, \cdot)$ is a bi-skew brace [Koch, 2021], where

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

- Same conclusion if $\psi\colon G \to G$ is a set-theoretic map such that the composition

$$(G, \circ) \xrightarrow{\psi} G \to G/Z(G, \circ)$$

  is a homomorphism with abelian image;
  see [Caranti and LS, 2022, LS and Trappeniers, 2023a].

  For example, we obtain in this way 16 Hopf–Galois structures when $(G, \circ)$ is the quaternion group.

The associated skew brace is a bi-skew brace

Proposition ([Caranti, 2020])

Let $(G, \cdot, \circ)$ be a skew brace. The following are equivalent:

- $(G, \cdot, \circ)$ *is a bi-skew brace.*
- $\gamma(g) \in \mathrm{Aut}(G, \circ)$ *for all* $g \in G$.

Let L/K be a finite Galois extension with Galois group $(G, \circ)$, and consider a Hopf–Galois structure associated with a bi-skew brace.

In this case, we get a nice control on the HGC, as we need to study the subgroups of $(G, \circ)$ with respect to some of its automorphisms.

Fact

The HGC is surjective if and only if the gamma function takes values in the power automorphisms of $(G, \circ)$.

Hopf–Galois structures with surjective HGC

- The classical structure; here the skew brace is $(G, \circ, \circ)$, and $\gamma(g) = \mathrm{id}$.
- The Hopf–Galois structure associated with the skew brace of Example $(*)$; here if g is a generator of $(G, \circ)$, then $\gamma(g)$ is inversion in $(G, \circ)$.
- The 16 Hopf–Galois structures obtained via "abelian maps" for extensions with quaternion Galois group; here as $\gamma(g)$ is an inner automorphism, hence a power automorphism, of $(G, \circ)$.

Cyclic groups

Let L/K be a finite Galois extension with Galois group $(G, \circ)$. Consider a Hopf–Galois structure $(H, \star)$ on L/K associated with a bi-skew brace $(G, \cdot, \circ)$.

Corollary

Let $L' = L^{G'}$ be an intermediate field of L/K. If G' is characteristic in $(G, \circ)$, then L' is in the image of the HGC.

Example

If $(G, \circ)$ is cyclic, then the HGC for $(H, \star)$ is surjective.

Theorem ([LS and Trappeniers, 2023b])

The following are equivalent:

- *For all Hopf–Galois structures on L/K associated with bi-skew braces, the HGC is surjective.*
- *$(G, \circ)$ is cyclic.*

Childs's condition

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

Proposition ([Childs, 2017])

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

Theorem ([LS and Trappeniers, 2023b])

The following are equivalent:

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

Two different Hopf–Galois structures

Let $(G, \cdot, \circ)$ be a finite bi-skew brace, and take

- L_1/K_1 Galois extension with Galois group $(G, \circ)$, so that $(G, \cdot, \circ)$ yields a Hopf–Galois structure $(H_1, \star_1)$;
- L_2/K_2 Galois extension with Galois group $(G, \cdot)$, so that $(G, \circ, \cdot)$ yields a Hopf–Galois structure $(H_2, \star_2)$.

Fact

Left ideals of $(G, \cdot, \circ)$ *and* $(G, \circ, \cdot)$ *coincide.*

They are nicely related!

Theorem ([LS and Trappeniers, 2023b])

- *The lattices of K_1-Hopf subalgebras of H_1 and of K_2-Hopf algebras of H_2 are isomorphic.*
- *There is the same number of intermediate fields in the images of the HGC for the Hopf–Galois structures $(H_1, \star_1)$ on L_1/K_1 and $(H_2, \star_2)$ on L_2/K_2.*
- *The following equality holds:*

$$\frac{GC(L_1/K_1, H_1)}{GC(L_2/K_2, H_2)} = \frac{|\{\text{subgroups of } (G, \cdot)\}|}{|\{\text{subgroups of } (G, \circ)\}|}.$$

Soluble Galois extensions

Let L/K be a finite Galois extension with soluble Galois group. Consider a Hopf–Galois structure $(H, \star)$ on L/K associated with a bi-skew brace.

Theorem

There exists a tower of intermediate fields

$$K = K_1 \leq K_2 \leq \cdots \leq K_{n-1} \leq K_n = L$$

such that, for all i,

- *K_i is normal in L, and K_i/K_{i-1} is abelian.*
- *K_i is in the image of the HGC (say $K_i = L^{H_i}$).*
- *H_i is normal in H, and H_{i-1}/H_i is an abelian Hopf algebra.*
- *The Hopf–Galois structure on K_i/K_{i-1} yielded by $(H, \star)$ is the classical one.*

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.

Caranti, A. (2020).
Bi-skew braces and regular subgroups of the holomorph.
J. Algebra, 562:647–665.

Caranti, A. and LS (2022).
Brace blocks from bilinear maps and liftings of endomorphisms.
J. Algebra, 610:831–851.

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.

Childs, L. N. (2019).
Bi-skew braces and Hopf Galois structures.
New York J. Math., 25:574–588.

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

Bibliography

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

Koch, A. (2021).
Abelian maps, bi-skew braces, and opposite pairs of Hopf-Galois structures.
Proc. Amer. Math. Soc. Ser. B, 8:189–203.

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

LS and Trappeniers, S. (2023a).
On bi-skew braces and brace blocks.
J. Pure Appl. Algebra, 227(5):Paper No. 107295.

Bibliography

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

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.