# Some new examples of Hopf–Galois structures in which the Hopf–Galois correspondence is surjective

Lorenzo Stefanello

Joint work with Senne Trappeniers

Hopf algebras and Galois module theory, 31 May 2022

# Outline

- Preliminaries in Hopf–Galois theory
- The known connection between HG and SB
- A new connection between HG and SB
- New examples of surjective correspondences

# Preliminaries in Hopf–Galois theory

# Hopf–Galois structures

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

A *Hopf–Galois structure* on $L/K$ consists of a $K$-Hopf algebra $H$ together with an action $*$ of $H$ on $L$ such that

- $L$ is an $H$-module algebra;
- the following $K$-linear map is bijective:

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

### Example

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

Recall that a subgroup $N$ of $\mathrm{Perm}(G)$ is *regular* if $|N| = |G|$ and $N$ acts transitively on $G$.

Example

- $N = \lambda(G)$, where $\lambda(g)[h] = gh$;
- $N = \rho(G)$, where $\rho(g)[h] = hg^{-1}$.

# Describing Hopf–Galois structures $(L/K, G)$

**Theorem ([Greither and Pareigis, 1987])**

*Hopf–Galois structures on $L/K$ correspond bijectively to regular subgroups of* $\mathrm{Perm}(G)$ *normalised by* $\lambda(G)$.

Explicitly, $N \leftrightarrow L[N]^G$, where $G$ acts on $L$ via Galois action and on $N$ via conjugation by $\lambda(G)$. Moreover, $L[N]^G$ acts on $L$ as follows:

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

## Example

- $N = \rho(G)$ yields the classical structure.
- $N = \lambda(G)$ yields the *canonical nonclassical structure*.

The *type* of the structure is the isomorphism class of $N$.

Let $H = L[N]^G$ give a Hopf–Galois structure on $L/K$. For all $K$-sub Hopf algebras $H'$ of $H$, we can consider an intermediate field

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

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

- For $N = \rho(G)$, we find the classical Galois correspondence, which is surjective.
- For $N = \lambda(G)$, exactly the normal intermediate fields are in the image of the correspondence [Greither and Pareigis, 1987].

### Problem

*Study when the Hopf–Galois correspondence is surjective.*

## Rewrite the correspondence $(L/K,\ G,\ H = L[N]^G)$

**Theorem ([Crespo et al., 2016])**

*$K$-sub Hopf algebras of $L[N]^G$ correspond bijectively to subgroups of $N$ normalised by $\lambda(G)$.*

Explicitly, $N' \leftrightarrow L[N']^G$.

This provides a correspondence between subgroups of $N$ normalised by $\lambda(G)$ and subgroups of $G$ [Koch et al., 2019], which is "mysterious" but can be shown "quantitatively" to be surjective in some examples.

# The known connection between HG and SB

# Skew braces

### Definition ([Guarnieri and Vendramin, 2017])

A *skew brace* $(A, +, \star)$ consists of two groups $(A, +)$ and $(A, \star)$ related by the following property: for all $a, b, c \in A$,

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

Each skew brace is associated with a *gamma function*

$$\gamma \colon (A, \star) \to \mathrm{Aut}(A, +), \quad a \mapsto (b \mapsto -a + (a \star b)).$$

# Examples

## Example

- $(A, +, +)$ is the *trivial skew brace*.
- $(A, +^{\mathrm{op}}, +)$ is the *almost trivial skew brace*.

More in general, if $(A, +, \star)$ is a skew brace, then $(A, +^{\mathrm{op}}, \star)$ is a skew brace [Koch and Truman, 2020], called the *opposite skew brace*.

## Definition ([Childs, 2019])

A *bi-skew brace* is a skew brace $(A, +, \star)$ such that also $(A, \star, +)$ is a skew brace.

# Substructures

## Definition

Let $(A, +, \star)$ be a skew brace.

- A *left ideal* $A'$ is a subgroup of $A$ with respect to both operations such that for all $a \in A$ and $a' \in A'$,

$$^{\gamma(a)}(a') = -a + (a \star a') \in A'.$$

- An *ideal* is a left ideal with $(A', +)$ normal in $(A, +)$ and $(A', \star)$ normal in $(A, \star)$.

# The known connection

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

- Let $H = L[N]^G$ give a Hopf–Galois structure on $L/K$. Then $N$ is a regular subgroup of $\mathrm{Perm}(G)$ normalised by $\lambda(G)$. Transport the structure of $N$ to $G$ to find $(G, \circ)$.

  Then $(G, \circ, \cdot)$ is a skew brace.
- Let $(A, +, \star)$ be a skew brace with $(A, \star) \cong (G, \cdot)$. Use this isomorphism to obtain a skew brace $(G, \circ, \cdot)$. Take $N = \lambda_\circ(G)$.

  Then $L[N]^G$ gives a Hopf–Galois structure on $L/K$.

# Examples



## Example

- The classical structure given by $N = \rho(G)$ yields the almost trivial skew brace $(G, \cdot^{\mathrm{op}}, \cdot)$.
- The canonical nonclassical structure given by $N = \lambda(G)$ yields the trivial skew brace $(G, \cdot, \cdot)$.

Let $H = L[N]^G$ give a Hopf–Galois structure on $L/K$, and let $(G, \circ, \cdot)$ be the corresponding skew brace.

### Theorem ([Childs, 2018])

*Subgroups of $N$ normalised by $\lambda(G)$ correspond bijectively to subgroups of $(G, \circ)$ which are $\cdot$-stable.*

Here a subgroup $G'$ of $(G, \circ)$ is $\cdot$-*stable* if for all $g \in G$ and $g' \in G'$,

$$g \cdot (g' \circ g^{-1}) \in G'.$$

### Example

Suppose that $(G, \cdot)$ is cyclic of order $p^n$, where $p$ is an odd prime. Then $N$ is cyclic [Kohl, 1998] and the Hopf–Galois correspondence is surjective [Childs, 2017].

### Problem ([Childs, 2021])

*Study the ratio*

$$GC(L/K, H) = \frac{|\{\textit{fields in the image of the HG correspondence}\}|}{|\{\textit{intermediate fields}\}|}$$
$$= \frac{|\{\cdot\textit{-stable subgroups of } (G, \circ)\}|}{|\{\textit{subgroups of } (G, \cdot)\}|}.$$

### Proposition ([Koch and Truman, 2020])

*$\cdot$-stable ideals of $(G, \circ, \cdot)$ coincide with left ideals of $(G, \circ^{\mathrm{op}}, \cdot)$.*

# A new connection between HG and SB

# The idea

1. Use the opposite skew brace.
2. Make the connection a bijection.
3. Forget about the regular subgroup.

# The new connection

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

## Theorem

*The following data are equivalent:*

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

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

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

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

### Example

- The classical structure is associated with the trivial skew brace.
- The canonical nonclassical structure is associated with the almost trivial skew brace.

The *type* of the structure is the isomorphism class of $(G, \circ)$.

Consider the Hopf–Galois structure associated with a skew brace $(G, \circ, \cdot)$.

## Proposition

*Left ideals of $(G, \circ, \cdot)$ correspond bijectively to $K$-sub Hopf algebras of $L[G, \circ]^{(G,\cdot)}$.*

Explicitly, $(G', \circ, \cdot) \leftrightarrow L[G', \circ]^{(G,\cdot)}$.

## Fact

*Let $(G', \circ, \cdot)$ be a left ideal of $(G, \circ, \cdot)$, and consider $H' = L[G', \circ]^{(G,\cdot)}$. Then*

$$L^{G'} = L^{H'}.$$

Let $(G', \circ, \cdot)$ be an ideal of $(G, \circ, \cdot)$, and take $F = L^{G'}$. We find a short exact sequence of $K$-Hopf algebras

$$K \to L[G', \circ]^{(G,\cdot)} \to L[G, \circ]^{(G,\cdot)} \to L[G/G', \circ]^{(G,\cdot)} \to K.$$

- $L/F$ is Galois with Galois group $(G', \cdot)$, the skew brace $(G', \circ, \cdot)$ gives a Hopf–Galois structure on $L/F$, and

$$L[G', \circ]^{(G',\cdot)} = F \otimes_K L[G', \circ]^{(G,\cdot)}.$$

- $F/K$ is Galois with Galois group $(G/G', \cdot)$, $(G/G', \circ, \cdot)$ gives a Hopf–Galois structure on $F/K$, and

$$L[G/G', \circ]^{(G/G',\cdot)} = L[G/G', \circ]^{(G,\cdot)}.$$

# What more?

We can translate in setting of Hopf–Galois theory

- strong left ideals;
- direct product of skew braces;
- semidirect product of skew braces;
- short exact sequence of skew braces;
- right nilpotency of skew braces.

# New examples of surjective correspondences

# Rewriting the correspondence (for the last time!)

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

## Corollary

*Consider the Hopf–Galois structure associated with a skew brace $(G, \circ, \cdot)$.*

- *The Hopf–Galois correspondence is surjective if and only if every subgroup of $(G, \cdot)$ is a left ideal of $(G, \circ, \cdot)$.*
- *An intermediate field $K \leq L^{G'} \leq L$, for $G'$ subgroup of $(G, \cdot)$, is in the image of the Hopf–Galois correspondence if and only if $G'$ is a left ideal of $(G, \circ, \cdot)$.*

Finally,

$$GC(L/K, L[G, \circ]^{(G,\cdot)}) = \frac{|\{\text{left ideals of } (G, \circ, \cdot)\}|}{|\{\text{subgroups of } (G, \cdot)\}|}.$$

# Bi-skew braces

Let $L/K$ be a finite Galois extension with Galois group $(G, \cdot)$, and consider a Hopf–Galois structure such that the corresponding skew brace $(G, \circ, \cdot)$ is a bi-skew brace with gamma function $\gamma$.

## Fact

*For all $g \in G$, $\gamma(g) \in \mathrm{Aut}(G, \cdot)$.*

## Proposition

*All the intermediate fields $F = L^{G'}$ with $G'$ characteristic in $(G, \cdot)$ are in the image of the Hopf–Galois correspondence.*

## Corollary

*Suppose that $(G, \cdot)$ is cyclic. Then the Hopf–Galois correspondence is surjective.*

## Example

Suppose that $(G, \cdot)$ is cyclic of order 8. By [Rump, 2007] and easy considerations, there exists a bi-skew brace $(G, \circ, \cdot)$ with $(G, \circ) \cong Q_8$. In particular, the Hopf–Galois correspondence in the associated Hopf–Galois structure is surjective.

Suppose that $\gamma \colon G \to \mathrm{Inn}(G, \cdot)$ is surjective.

### Proposition

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

Write $\iota(g)$ for the conjugation by $g$.

### Example

- The gamma function of $(G, \cdot^{\mathrm{op}}, \cdot)$ is $\gamma(g) = \iota(g)$.
- Suppose that $(G, \cdot)$ has nilpotency class two, and take

  $$g \circ h = g \cdot h \cdot [g, h].$$

  By [Caranti and LS, 2022], $(G, \circ, \cdot)$ is a bi-skew brace with gamma function $\gamma(g) = \iota(g^{-1})$.

# Power automorphisms



Recall that $\psi \in \mathrm{Aut}(G, \cdot)$ is a *power automorphism* if $\psi(G') \leq G'$ for all subgroups $G'$ of $(G, \cdot)$.

## Proposition

*The Hopf–Galois correspondence is surjective if and only if for all $g \in G$, $\gamma(g) \in \mathrm{Aut}(G, \cdot)$ is a power automorphism.*

Recall that the *norm* $N(G)$ of $(G, \cdot)$ is the intersection of the normalisers of the subgroups of $(G, \cdot)$.

## Fact

*$\iota(g)$ is a power automorphism if and only if $g \in N(G)$.*

# An explicit construction

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

Theorem ([Schenkman, 1960])

*$N(G)$ is contained in the second center $Z_2(G)$ of $(G, \cdot)$.*

In particular, we can apply [LS and Trappeniers, 2022] to deduce that each different homomorphism $\psi\colon (G, \cdot) \to N(G)/Z(G)$ yields a different operation

$$g \circ_\psi h = g \cdot \psi(g) \cdot h \cdot \psi(g)^{-1}$$

such that $(G, \circ_\psi, \cdot)$ is a bi-skew brace, and for the associated Hopf–Galois structure the Hopf–Galois correspondence is surjective.

# Examples with the norm

Let $L/K$ be a Galois extension with Galois group $(G, \cdot) = Q_8$. Here $N(G) = G$, and the 16 different homomorphisms

$$G \to G/Z(G) \cong C_2 \times C_2$$

yield 16 different Hopf–Galois structures on $L/K$ for which the Hopf–Galois correspondence is surjective.

# Bi-skew braces

Let $(G, \circ, \cdot)$ be a finite bi-skew brace, let $L/K$ be a Galois extension with Galois group $(G, \cdot)$, and let $M/F$ be a Galois extension with Galois group $(G, \circ)$.

## Fact

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

Thus, the Hopf algebras $L[G, \circ]^{(G,\cdot)}$ and $M[G, \cdot]^{(G,\circ)}$ have the "same" lattice of sub Hopf algebras, and the same number of intermediate fields is in the image of the two Hopf–Galois structures.

Finally,

$$\frac{GC(L/K, L[G, \circ]^{(G,\cdot)})}{GC(M/F, M[G, \cdot]^{(G,\circ)})} = \frac{|\{\text{subgroups of } (G, \circ)\}|}{|\{\text{subgroups of } (G, \cdot)\}|}.$$

# Bibliography I


Caranti, A. and LS (2022).
Brace blocks from bilinear maps and liftings of endomorphisms.
*arXiv:2110.11028*.

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

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

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

# Bibliography II


Childs, L. N. (2021).
On the Galois correspondence for Hopf Galois structures arising from finite radical algebras and Zappa-Szép products.
*Publ. Mat.*, 65(1):141–163.

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 III


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.

Kohl, T. (1998).
Classification of the Hopf Galois structures on prime power radical extensions.
*J. Algebra*, 207(2):525–546.

LS and Trappeniers, S. (2022).
On bi-skew braces and brace blocks.
*arXiv:2205.15073*.

# Bibliography IV


Rump, W. (2007).
Classification of cyclic braces.
*J. Pure Appl. Algebra*, 209(3):671–685.

Schenkman, E. (1960).
On the norm of a group.
*Illinois J. Math.*, 4:150–152.