

Minimal Hopf–Galois structures on Galois extensions

Cindy (Sin Yi) Tsang
Ochanomizu University

[arXiv:2602.09320](https://arxiv.org/abs/2602.09320)

This work is supported by JSPS KAKENHI 24K16891.

Hopf Algebras and Galois Module Theory
Agnes Scott College & Online

2026/5/25 ~ 2026/5/29

Hopf–Galois correspondence

- Let L/K be any finite extension.

Theorem (Chase–Sweedler 1969)

For any Hopf–Galois structure H on L/K , we have an **injective** correspondence

$$\begin{aligned}\Phi_H : \{K\text{-Hopf subalgebras of } H\} &\longrightarrow \{\text{intermediate fields of } L/K\} \\ J &\longmapsto L^J\end{aligned}$$

induced by the fixed field operator

$$L^J = \{x \in L \mid j \cdot x = \epsilon(j)x \text{ for all } j \in J\},$$

where $\epsilon : H \longrightarrow K$ denotes the counit. For example, we have

$$K \longmapsto L^K = L,$$

$$H \longmapsto L^H = K.$$

We shall refer to the above map Φ_H as the **Hopf–Galois correspondence** for H .

- In this talk, we will consider the case when L/K is a **Galois** extension.

- Let L/K be any finite Galois extension with Galois group G .
- The **classical structure** on L/K is the K -Hopf algebra

$$(L[G_1])^G = \underbrace{\left\{ \sum_{\sigma \in G} \ell_{\sigma} \sigma \in L[G_1] \mid \forall \tau \in G : \sum_{\sigma \in G} \tau(\ell_{\sigma}) \sigma = \sum_{\sigma \in G} \ell_{\sigma} \sigma \right\}}_{G \text{ acts on } L \text{ as the Galois group and on } G_1 = G \text{ trivially}} = K[G]$$

whose action on $x \in L$ is given by

$$\left(\sum_{\sigma \in G} \ell_{\sigma} \sigma \right) \cdot x = \sum_{\sigma \in G} \ell_{\sigma} \sigma(x).$$

- In this case, the Hopf–Galois correspondence

$$\begin{aligned} \Phi_1 : \{K\text{-Hopf subalgebras of } (L[G_1])^G\} &\longrightarrow \{\text{intermediate fields of } L/K\} \\ J &\longmapsto L^J \end{aligned}$$

is **bijjective** because it reduces to the classical Galois correspondence.

Canonical non-classical structure on a Galois extension

- Let L/K be any finite **Galois** extension with Galois group G .
- The **canonical non-classical structure** on L/K is the K -Hopf algebra

$$(L[G_2])^G = \underbrace{\left\{ \sum_{\sigma \in G} \ell_\sigma \sigma \in L[G_2] \mid \forall \tau \in G : \sum_{\sigma \in G} \tau(\ell_\sigma) \tau \sigma \tau^{-1} = \sum_{\sigma \in G} \ell_\sigma \sigma \right\}}_{G \text{ acts on } L \text{ as the Galois group and on } G_2 = G \text{ via conjugation}}$$

whose action on $x \in L$ is given by

$$\left(\sum_{\sigma \in G} \ell_\sigma \sigma \right) \cdot x = \sum_{\sigma \in G} \ell_\sigma \sigma^{-1}(x).$$

- In this case, the image of the Hopf–Galois correspondence

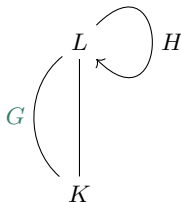
$$\begin{aligned} \Phi_2 : \{K\text{-Hopf subalgebras of } (L[G_2])^G\} &\longrightarrow \{\text{intermediate fields of } L/K\} \\ J &\longmapsto L^J \end{aligned}$$

consists exactly of the fixed fields L^I of the **normal subgroups** I of G .

- Remark.** $(L[G_1])^G \simeq (L[G_2])^G$ if and only if G is abelian.

Bijection of the Hopf–Galois correspondence

- **Question.** When is the Hopf–Galois correspondence bijective?



- **Question.** Fix the Galois group. When is the Hopf–Galois correspondence **always bijective** regardless of the Hopf–Galois structure?

Theorem (Stefanello–Trappeniers 2023)

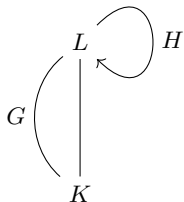
Fix a finite group G that is going to be the Galois group. The following are equivalent:

- 1 For any Galois G -extension L/K , the Hopf–Galois correspondence is bijective for any Hopf–Galois structure on L/K .
- 2 G is cyclic and $q \nmid p - 1$ for all prime divisors p, q of $|G|$.

(L. Stefanello, *Classifying Galois extensions with Childs's property*, *Hopf Algebras and Galois Module Theory*, 2024)

Fixing the type of the Hopf–Galois structure

- **Question.** When is the Hopf–Galois correspondence bijective?



$\exists N$ s.t. $L \otimes_K H \simeq L[N]$

The **type** of H is defined to be N .

This group N has the same order as G .

- **Question.** Fix the **type** of the Hopf–Galois structure. When is the Hopf–Galois correspondence **always bijective** regardless of the Galois group?

Theorem (Stefanello–T. 2025)

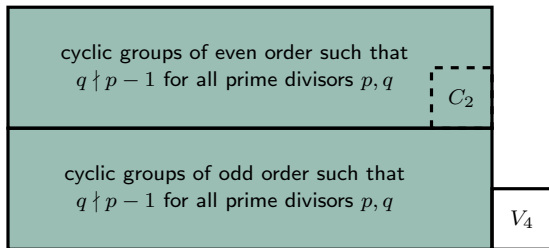
Fix a finite group N that is going to be the **type**. The following are equivalent:

- 1 For any Hopf–Galois structure H of type N on any Galois extension, the Hopf–Galois correspondence for H is bijective.
- 2 N is C_2 , V_4 , or cyclic of odd order and $q \nmid p - 1$ for all prime divisors p, q of $|N|$.

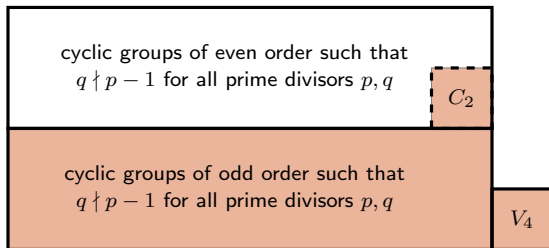
(C. Tsang, *Classification of the types for which every Hopf–Galois correspondence is bijective*, [Hopf Algebras and Galois Module Theory](#), 2025)

Comparison of the two results

The finite groups G such that for any Galois G -extension L/K , the Hopf–Galois correspondence is bijective for any Hopf–Galois structure on L/K .



The finite groups N such that for any Hopf–Galois structure H of type N on any Galois extension L/K , the Hopf–Galois correspondence for H is bijective.



Non-bijectionality of the Hopf–Galois correspondence

Minimal Hopf–Galois structure

- Let L/K be any finite extension.

Theorem (Chase–Sweedler 1969)

For any Hopf–Galois structure H on L/K , we have an **injective** correspondence

$$\begin{aligned}\Phi_H : \{K\text{-Hopf subalgebras of } H\} &\longrightarrow \{\text{intermediate fields of } L/K\} \\ J &\longmapsto L^J\end{aligned}$$

induced by the fixed field operator. For example, we have

$$K \longmapsto L^K = L, \quad H \longmapsto L^H = K.$$

We shall refer to the above map Φ_H as the **Hopf–Galois correspondence** for H .

Definition (Ezome–Greither 2021)

A Hopf–Galois structure H on L/K is **minimal** if $\dim_K(H) \neq 1$, and

- L and K are the only elements of $\text{Im}(\Phi_H)$, or equivalently
the map Φ_H is as far from being bijective as possible

- K and H are the only K -Hopf subalgebras of H .

- **Question.** Can one classify the minimal Hopf–Galois structures?

Theorem (T. arXiv:2602.09320)

Let H be a Hopf–Galois structure on some finite Galois extension L/K .

If H is **minimal**, then the type N of H is **characteristically simple**. Moreover:

- ① **Abelian case** $N \simeq \mathbb{F}_p^n$ with p a prime:

- ① $n = 1$ H is the **classical structure** and is obviously **minimal**

- ② $n \geq 2$ H is never **minimal**

- ② **Non-abelian case** $N \simeq T^n$ with T non-abelian simple:

- ① $n = 1$ H is **minimal** $\iff H$ is the **canonical non-classical structure**

- ② $n \geq 2$ If H is **minimal**, then some fairly restrictive conditions hold ...

Maybe H is never minimal when $n \geq 2$ in the non-abelian case also?



A skew brace-theoretic approach to the main result

Definition

A **skew brace** is a set $A = (A, +, \circ)$ equipped with two group operations such that

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

holds for all $a, b, c \in A$. Here $+$ need not be commutative. For each $a \in A$, the map

$$\lambda_a : (A, +) \longrightarrow (A, +); \quad \lambda_a(b) = -a + a \circ b$$

is clearly an automorphism, and the map

$$\lambda : (A, \circ) \longrightarrow \text{Aut}(A, +); \quad a \mapsto \lambda_a$$

is easily shown to be a group homomorphism.

A subset I of A is a **left ideal** if I is a subgroup of $(A, +)$ and $\lambda_a(I) \subseteq I$ for all $a \in A$.

- **Remark 1.** The **characteristic subgroups** of $(A, +)$ are all left ideals of A .
- **Remark 2.** The left ideals of A are automatically subgroups of (A, \circ) .
 - ① Closed under **multiplication** because $a \circ b = a + \lambda_a(b)$.
 - ② Closed under **inverses** because $0 = \bar{a} \circ a = \bar{a} + \lambda_{\bar{a}}(a)$ implies $\bar{a} = -\lambda_{\bar{a}}(a)$.

- Let L/K be any finite **Galois** extension with Galois group $G = (G, \circ)$.

Theorem (Stefanello–Trappeniers 2023)

There is an explicit one-to-one correspondence between the following:

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

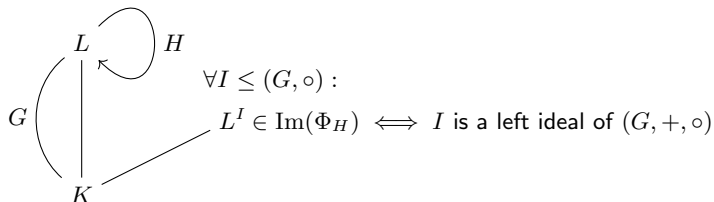
Under this correspondence, the type of H is given by $(G, +)$. Moreover:

$$\forall I \leq (G, \circ) : L^I \in \text{Im}(\Phi_H) \iff I \text{ is a left ideal of } (G, +, \circ).$$

- Trivial skew brace** (G, \circ, \circ) is a skew brace.
 - corresponds to the classical structure
 - left ideals are the **subgroups** of (G, \circ) because $\lambda_a(b) = b$
- Almost trivial skew brace** $(G, \circ^{\text{op}}, \circ)$ is a skew brace, where $a \circ^{\text{op}} b = b \circ a$.
 - corresponds to the canonical non-classical structure
 - left ideals are the **normal subgroups** of (G, \circ) because $\lambda_a(b) = a \circ b \circ \bar{a}$

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

$$\Phi_H : \{K\text{-Hopf subalgebras of } H\} \longrightarrow \{\text{intermediate fields of } L/K\}$$



Recall that H is said to be **minimal** if $\dim_K(H) \neq 1$, and

$$L = L^{\{0\}}, \quad K = L^G$$

are the only intermediate fields that lie in $\text{Im}(\Phi_H)$.

Definition (T. arXiv:2602.09320)

A skew brace $A = (A, +, \circ)$ is **left-simple** if $A \neq \{0\}$, and $\{0\}, A$ are the only left ideals.

- Therefore, minimal Hopf–Galois structures correspond to left-simple skew braces.

Main result (in the language of skew braces)

Theorem (T. arXiv:2602.09320)

Let $A = (A, +, \circ)$ be a finite skew brace.

Let H be a Hopf-Galois structure on some finite Galois extension L/K .

If A is **left-simple**, then $(A, +)$ is **characteristically simple**. Moreover:

If H is **minimal**, then the type \mathcal{N} of H is **characteristically simple**. Moreover:

① **Abelian case** $(A, +) \simeq \mathbb{F}_p^n$ with p a prime:

① $n = 1$ A is a **trivial skew brace** and is obviously **left-simple**

H is the **classical structure** and is obviously **minimal**

② $n \geq 2$ A is never **left-simple**

H is never **minimal**

② **Non-abelian case** $(A, +) \simeq T^n$ with T non-abelian simple:

① $n = 1$ A is **left-simple** \iff A is an **almost trivial skew brace**

H is **minimal** \iff H is the **canonical non-classical structure**

② $n \geq 2$ If A is **left-simple**, then some fairly restrictive conditions hold ...

If H is **minimal**, then some fairly restrictive conditions hold ...

Outline of the proof

Theorem (T. arXiv:2602.09320): Abelian case

Let $A = (A, +, \circ)$ be a finite skew brace and $(A, +) \simeq \mathbb{F}_p^n$ with p a prime.

- ① $n = 1$ A is a **trivial skew brace** and is obviously **left-simple**
- ② $n \geq 2$ A is never **left-simple**

- **Proof.** We can view the group homomorphism

$$\lambda : (A, \circ) \longrightarrow \text{Aut}(A, +) \simeq \text{GL}_n(\mathbb{F}_p); \quad a \mapsto \lambda_a \quad (\lambda_a(b) = -a + a \circ b)$$

as a representation of the p -group (A, \circ) over the finite field \mathbb{F}_p of characteristic p .

- The **left-simplicity** of A is then equivalent to the **irreducibility** of λ .
- As is well-known in Modular Representation Theory:
 - ① By the class equation, the action of (A, \circ) on \mathbb{F}_p^n has a fixed point $\vec{v} \neq \vec{0}$.
 - ② The subspace U generated by \vec{v} is a non-zero λ -invariant subspace.

This implies that λ is **irreducible if and only if** $n = 1$.

- For $n = 1$, clearly λ is trivial, which means that A is a trivial skew brace. \square

Theorem (T. arXiv:2602.09320): Non-abelian case

Let $A = (A, +, \circ)$ be a finite skew brace and $(A, +) \simeq T^n$ with T non-abelian simple.

- ① $n = 1$ A is **left-simple** \iff A is an **almost trivial skew brace**
- ② $n \geq 2$ If A is **left-simple**, then some fairly restrictive conditions hold ...

- **Idea of the proof.** The key is the fact that the homomorphisms

$$\lambda : (A, \circ) \longrightarrow \text{Aut}(A, +); \quad a \mapsto \lambda_a \quad (\lambda_a(b) = -a + a \circ b)$$

$$\rho : (A, \circ) \longrightarrow \text{Aut}(A, +); \quad a \mapsto \rho_a \quad (\rho_a(b) = a \circ b - a)$$

give rise to a subgroup

$$\text{Inn}(A, +) \subseteq \text{Im}(\lambda)\text{Inn}(A, +) = \text{Im}(\lambda)\text{Im}(\rho) = \text{Im}(\rho)\text{Inn}(A, +) \subseteq \text{Aut}(A, +).$$

Moreover, they give rise to two left ideals

$$\ker(\rho) \quad \text{and} \quad \text{conj}^{-1}(\text{Im}(\lambda))$$

of A , where $\text{conj} : (A, +) \longrightarrow \text{Aut}(A, +)$ is the natural homomorphism.

- We may **assume that A is not almost trivial**, for otherwise it is obvious that A is left-simple when $n = 1$, and A is not left-simple when $n \geq 2$.

- Suppose that A is **left-simple** and we want to obtain a contradiction.
- One can show that $\ker(\rho), \text{conj}^{-1}(\text{Im}(\lambda)) \neq A$, and so $\underbrace{\ker(\rho), \text{conj}^{-1}(\text{Im}(\lambda))}_{(*)} = 0$.

- $n = 1$ We have an almost simple group

$$\text{Inn}(T) \subseteq \text{Im}(\lambda)\text{Inn}(T) = \text{Im}(\lambda)\text{Im}(\rho) = \text{Im}(\rho)\text{Inn}(T) \subseteq \text{Aut}(T)$$

with socle T . It follows from $(*)$ that

- 1 $\text{Im}(\lambda) \cap \text{Inn}(T) = 1$;
- 2 $\text{Im}(\lambda)$ embeds into $\text{Out}(T)$ and so is **solvable** by Schreier's Conjecture;
- 3 $\text{Im}(\rho)$ is isomorphic to (A, \circ) and so has order $|T|$.

Moreover, by the trifactorization above, we have:

- 4 $\text{Im}(\rho)/\text{Im}(\rho) \cap \text{Inn}(T) \simeq \text{Im}(\lambda)$.
- Factorizations of almost simple groups with a **solvable factor** have been somewhat classified by Li and Xia (2022).
 - We ruled out every single possibility by considering the orders of the two factors.

- $n \geq 2$ Since $\ker(\rho) = 0$, we have an embedding

$$\rho : (A, \circ) \hookrightarrow \text{Aut}(A, +) \simeq \text{Aut}(T)^n \rtimes S_n$$

and one can show that the projection of $\text{Im}(\rho)$ onto S_n is a **transitive** subgroup.

- This implies that n has to divide $|A| = |T|^n$, so **the prime factors of n are among those of $|T|$** . In fact, one can show that

$$\exists R \leq T^n \text{ s.t. } n \mid [T^n : R] \text{ and } [T^n : R] \mid |\text{Out}(T)|^n \cdot n!.$$

This seems to be quite restrictive, but not enough to obtain a contradiction.

- There is no classification of the factorizations of the groups

$$\text{Inn}(T^n) \subseteq \text{Im}(\lambda)\text{Inn}(T^n) = \text{Im}(\lambda)\text{Im}(\rho) = \text{Im}(\rho)\text{Inn}(T^n) \subseteq \text{Aut}(T^n)$$

when $n \geq 2$, but we have some fairly restrictive conditions on the factors.

Can one somehow get a contradiction?



- 1 S. U. Chase and M. E. Sweedler, *Hopf Algebras and Galois Theory*, Lecture Notes in Mathematics, Vol. 97. Springer-Verlag, Berlin-New York, 1969.
- 2 L. Stefanello and S. Trappeniers, *On the connection between Hopf–Galois structures and skew braces*, Bull. Lond. Math. Soc. 55 (2023), no. 4, 1726–1748.
- 3 L. Stefanello and C. Tsang, *Classification of the types ... every Hopf–Galois correspondence is bijective*, J. Algebra 664 (2025), part A, 514–526.
- 4 T. Ezome and C. Greither, *Minimal Hopf–Galois structures on separable field extensions*, Note Mat. 41 (2021), no. 1, 55–67.
- 5 N. P. Byott, *Hopf–Galois structures on field extensions with simple Galois groups*, Bull. London Math. Soc. 36 (2004), no. 1, 23–29.
- 6 C. H. Li and B. Xia, *Factorizations of almost simple groups ... and Cayley graphs of solvable groups*, Mem. Amer. Math. Soc. 279 (2022), no. 1375.

ご清聴
ありがとうございました



The illustrations are credited to [this website](#).