Classification of the types for which every Hopf–Galois correspondence is bijective

Cindy (Sin Yi) Tsang

Ochanomizu University

Joint work with Lorenzo Stefanello

J. Algebra 664 (2025), part A, 514–526

This work is supported by JSPS KAKENHI 24K16891.

Hopf Algebras and Galois Module Theory

Online

2025/6/4 $\sim$ 2025/6/5

Many thanks to Griff for organizing this conference every year!

Our project actually started last year at this conference from Lorenzo's talk.

Background

Theorem (Chase-Sweedler 1969)

Let L/K be any finite extension.

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

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

$$H' \longmapsto L^{H'}$$

induced by the fixed field operator

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

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.
- **Notation.** For any group G, we shall write $\mathrm{Sym}(G)$ for its symmetric group, and

$$\begin{cases} \lambda : G \longrightarrow \mathrm{Sym}(G); & \lambda(\sigma) = (x \mapsto \sigma x) \\ \rho : G \longrightarrow \mathrm{Sym}(G); & \rho(\sigma) = (x \mapsto x\sigma^{-1}) \end{cases}$$

for its left and right regular representations, respectively.

Theorem (Greither-Pareigis 1987)

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

There is a one-to-one correspondence between

$$\left\{ \begin{array}{c} \text{regular subgroups of } \mathrm{Sym}(G) \\ \text{that are normalized by } \lambda(G) \end{array} \right\} \longrightarrow \{\text{Hopf–Galois structures on } L/K\}$$

$$N \longmapsto H_N$$

that is explicitly defined by

$$H_N = (L[N])^G = \left\{ \sum_{\eta \in N} \ell_\eta \eta \in L[N] \;\middle|\; \sigma(\ell_\eta) = \ell_{\lambda(\sigma)\eta\lambda(\sigma)^{-1}} \text{ for all } \sigma \in G \right\}.$$

Note: G acts on N via conjugation by $\lambda(G)$. The action of H_N on L is given by

$$\left(\sum_{\eta \in N} \ell_\eta \eta \right) \cdot x = \sum_{\eta \in N} \ell_\eta \eta^{-1}(1_G)(x) \text{ for all } x \in L.$$

The type of H_N is defined to be the isomorphism class of the regular subgroup N.

The classical and canonical non-classical structures

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

$$\left\{\begin{array}{c}\text{regular subgroups of } \mathrm{Sym}(G) \\ \text{that are normalized by } \lambda(G)\end{array}\right\} \leftrightsquigarrow \{\text{Hopf–Galois structures on } L/K\}$$

- Obviously, the images of the left and right regular representations

$$\begin{cases} \lambda : G \longrightarrow \mathrm{Sym}(G); & \lambda(\sigma) = (x \mapsto \sigma x) \\ \rho : G \longrightarrow \mathrm{Sym}(G); & \rho(\sigma) = (x \mapsto x\sigma^{-1}) \end{cases}$$

of G are regular subgroups of $\mathrm{Sym}(G)$ that are normalized by $\lambda(G)$.

Definition

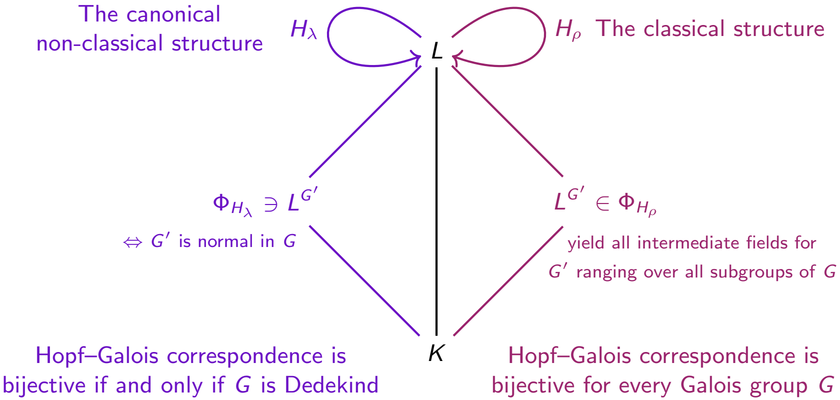
The classical structure on L/K is the Hopf–Galois structure $H_\rho := H_{\rho(G)}$.

The canonical non-classical structure on L/K is the Hopf–Galois structure $H_\lambda := H_{\lambda(G)}$.

- **Remark 1.** In the case that G is abelian, of course $\rho(G) = \lambda(G)$, so the classical and canonical non-classical structures coincide.

- **Remark 2.** The classical structure can be identified with the group ring $K[G]$, and the Hopf–Galois correspondence for H_ρ is the usual Galois correspondence.

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



Theorem (Dedekind) The original slides contained a mistake here. I am very grateful to Andrea Caranti for pointing it out.

A finite non-abelian group G is Dedekind if and only if $G \simeq Q_8 \times T \times O$, where Q_8 is the quaternion group, T is an elementary 2-group, and O is an abelian group of odd order.

Bijectivity of the Hopf–Galois correspondence

Problem I: Fix the Galois group G

- It is natural to ask whether the Hopf–Galois correspondence, which is only injective in general, is actually bijective for a given Hopf–Galois structure.
- In Lorenzo's talk

  Classifying Galois extensions with Childs's property

  last year at this conference, he fixed the Galois group G and posed the following:

Problem I

Classify 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.

- **Note.** By the canonical non-classical structure, clearly G must be Dedekind.

Theorem I (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. The group G is cyclic and $q \nmid p - 1$ for all prime divisors p, q of $|G|$.

Problem II: Fix the type N of the Hopf–Galois structure

- After Lorenzo's talk, I asked him:

  What if one fixes the type of the Hopf–Galois structure instead?

  In other words, is it possible to solve the following:

Problem II

Classify 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 is bijective for H.

- **Note.** By the canonical non-classical structure, clearly N must be Dedekind.

Theorem II (Stefanello & T. 2025)

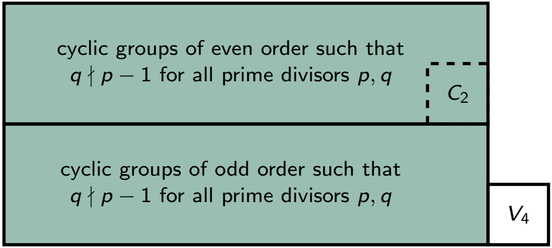
Fix a finite group N that is going to be the type. The following are equivalent:

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

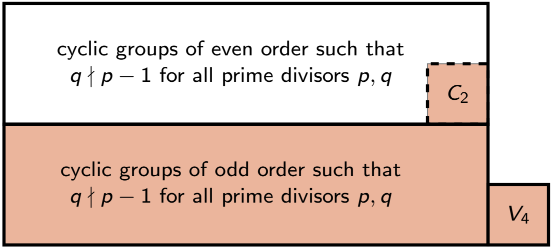
- The conditions on N are similar to but not quite the same as those of G.

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



The key technique used in the proof

Hopf–Galois structures and skew braces

- Both of the theorems make use of the connection between Hopf–Galois structures and skew braces in the proof.

Definition

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

1. $(A, +)$ is a group. (the additive group)
2. $(A, \circ)$ is a group. (the circle/adjoint/multiplicative group)
3. The brace relation $a \circ (b + c) = (a \circ b) - a + (a \circ c)$ holds for all $a, b, c \in A$.

- Given any group $(A, \circ)$, there are two obvious ways to define the $+$ operation such that $(A, +, \circ)$ is a skew brace.
  1. The same operation: $a + b = a \circ b$ for all $a, b \in A$.
  2. The opposite operation: $a + b = a \circ^{\mathrm{op}} b = b \circ a$ for all $a, b \in A$.

Definition

A skew brace of the form $(A, \circ, \circ)$ is said to be trivial.

A skew brace of the form $(A, \circ^{\mathrm{op}}, \circ)$ is said to be almost trivial.

Hopf–Galois structures and skew braces

For any finite groups G and N of the same order:

Hopf–Galois structures of type N on a G-Galois extension

Greither-Pareigis 1987

one-to-one

regular subgroups of $\mathrm{Sym}(G)$ that are isomorphic to N and normalized by $\lambda(G)$

Galois group $\leftrightsquigarrow$ circle group

type $\leftrightsquigarrow$ additive group

Byott 1996

the operations $\circ$ on $N = (N, +)$ for which $(N, +, \circ)$ is a skew brace and $(N, \circ) \simeq G$

one-to-one

Guarnieri-Vendramin 2017

regular subgroups of $N \rtimes \mathrm{Aut}(N)$ that are isomorphic to G

- The connection between Hopf–Galois structures and skew braces was known.
- It was slightly modified and improved by Stefanello & Trappeniers.

Theorem (Stefanello-Trappeniers 2023)

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

There is a one-to-one correspondence between

$$\left\{ \begin{array}{c} \text{operations } + \text{ on } G \text{ such that} \\ (G, +, \circ) \text{ is a skew brace} \end{array} \right\} \longrightarrow \{\text{Hopf–Galois structures on } L/K\}$$

$$+ \longmapsto H_+$$

that is explicitly defined by

$$H_+ = (L[(G,+)])^{(G,\circ)} = \left\{ \sum_{\tau \in G} \ell_\tau \tau \in L[(G,+)] \;\middle|\; \sigma(\ell_\tau) = \ell_{\gamma_\sigma(\tau)} \text{ for all } \sigma, \tau \in G \right\}.$$

Note: $(G, \circ)$ acts on $(G, +)$ via the gamma map γ of $(G, +, \circ)$. The action of H_+ on L is given by

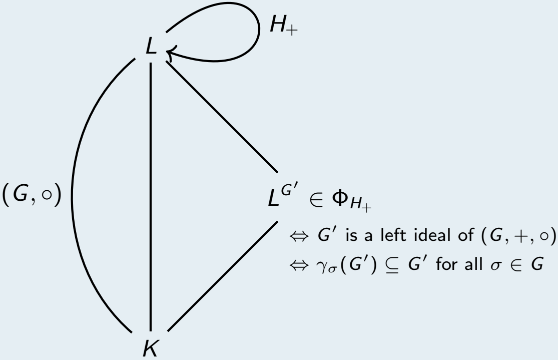
$$\left(\sum_{\tau \in G} \ell_\tau \tau \right) \cdot x = \sum_{\tau \in G} \ell_\tau \tau(x) \text{ for all } x \in L.$$

In this case the type of H_+ is the isomorphism class of the corresponding group $(G, +)$.

Theorem (Stefanello & Trappeniers 2023)

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

Let $+$ be an operation on G such that $(G, +, \circ)$ is a skew brace and let H_+ denote the corresponding Hopf–Galois structure on L/K. Then:

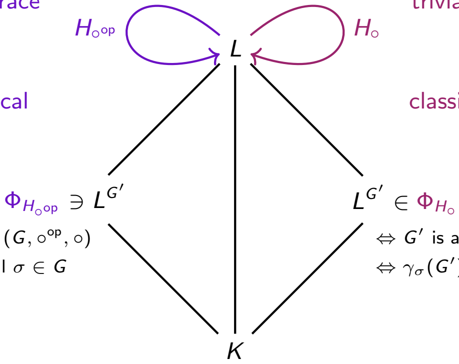


Thus, the Hopf–Galois correspondence for H_+ is bijective if and only if every subgroup G' of $(G, \circ)$ is a left ideal of $(G, +, \circ)$.

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

almost trivial skew brace
$(G, \circ^{\mathrm{op}}, \circ)$
$\updownarrow$
canonical non-classical structure

trivial skew brace
$(G, \circ, \circ)$
$\updownarrow$
classical structure



$\Leftrightarrow$ G' is a left ideal of $(G, \circ^{\mathrm{op}}, \circ)$
$\Leftrightarrow$ $\gamma_\sigma(G') \subseteq G'$ for all $\sigma \in G$

$\Leftrightarrow$ G' is a left ideal of $(G, \circ, \circ)$
$\Leftrightarrow$ $\gamma_\sigma(G') \subseteq G'$ for all $\sigma \in G$

- For the trivial skew brace, we have $\gamma_\sigma(\tau) = \sigma^{-1} \circ (\sigma \circ \tau) = \tau$.
  $\therefore L^{G'} \in \Phi_{H_\circ}$ for all subgroups G' of G. $\Phi_{H_\circ}$ is always bijective.
- For the almost trivial skew brace, we have $\gamma_\sigma(\tau) = \sigma^{-1} \circ^{\mathrm{op}} (\sigma \circ \tau) = \sigma \circ \tau \circ \sigma^{-1}$.
  $\therefore L^{G'} \in \Phi_{H_{\circ^{\mathrm{op}}}}$ if and only if G' is normal in G. $\Phi_{H_{\circ^{\mathrm{op}}}}$ is bijective $\Leftrightarrow$ G is Dedekind.

Skew-brace-theoretic versions of the proposed problems

Problem I

Classify 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.

Problem I: skew-brace-theoretic version

Classify the finite groups $G = (G, \circ)$ such that for any group operation $+$ on G making $(G, +, \circ)$ into a skew brace, every subgroup of $(G, \circ)$ is a left ideal of $(G, +, \circ)$.

- Theorem I (Stefanello & Trappeniers 2023) was proven using this reduction.

Problem II

Classify 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 is bijective for H.

Problem II: skew-brace-theoretic version

Classify the finite groups $N = (N, +)$ such that for any group operation $\circ$ on N making $(N, +, \circ)$ into a skew brace, every subgroup of $(N, \circ)$ is a left ideal of $(N, +, \circ)$.

- Theorem II (Stefanello & T. 2025) was proved using the reduction.

Outline of the proof of Theorem II

A reduction lemma

Theorem II (Stefanello & T. 2025)

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

- (i) For any Hopf–Galois structure H of type N on any Galois extension, the Hopf–Galois correspondence for H is bijective.
- (ii) The group N is either isomorphic to C_2 or V_4, or is cyclic of odd order and $q \nmid p-1$ for all prime divisors p, q of $|N|$.

Theorem II: skew-brace-theoretic version (Stefanello & T. 2025)

Fix a finite group $N = (N, +)$ that is going to be the type. The following are equivalent:

- (i) For any operation $\circ$ on N making $(N, +, \circ)$ into a skew brace, every subgroup of $(N, \circ)$ is a left ideal of $(N, +, \circ)$.
- (ii) The group N is either isomorphic to C_2 or V_4, or is cyclic of odd order and $q \nmid p-1$ for all prime divisors p, q of $|N|$.

Lemma

If M does not satisfy (i), then $M \times M'$ does not satisfy (i) for all groups M'.

The implication (i) $\Rightarrow$ (ii)

Theorem II: skew-brace-theoretic version (Stefanello & T. 2025)

Fix a finite group $N = (N, +)$ that is going to be the type. The following are equivalent:

1. For any operation $\circ$ on N making $(N, +, \circ)$ into a skew brace, every subgroup of $(N, \circ)$ is a left ideal of $(N, +, \circ)$.
2. The group N is either isomorphic to C_2 or V_4, or is cyclic of odd order and $q \nmid p - 1$ for all prime divisors p, q of $|N|$.

- Recall that either N is abelian or N is a direct product of Q_8 with an abelian group.
- One can show that the following groups do not satisfy (i).
  - a. Q_8 $\rightsquigarrow$ abelian
  - b. $C_2 \times C_2 \times C_2$ $\rightsquigarrow$ C_2 or V_4 or not elementary 2-abelian
  - c. C_{2n} for any $n \geq 2$ $\rightsquigarrow$ C_2 or V_4 or odd order
  - d. $C_{p^n} \times C_{p^m}$ for any odd primes p and m, n $\rightsquigarrow$ C_2 or V_4 or cyclic of odd order
  - e. $C_{p^n} \times C_{q^m}$ for any primes p, q with $q \mid p - 1$ and m, n
- It follows that N must satisfy (ii).

The implication ⓘⓘ $\Rightarrow$ ⓘ

Theorem II: skew-brace-theoretic version (Stefanello & T. 2025)

Fix a finite group $N = (N, +)$ that is going to be the type. The following are equivalent:

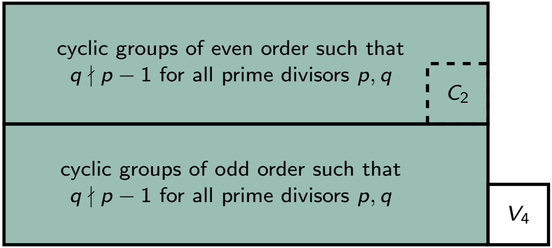
1. For any operation $\circ$ on N making $(N, +, \circ)$ into a skew brace, every subgroup of $(N, \circ)$ is a left ideal of $(N, +, \circ)$.
2. The group N is either isomorphic to C_2 or V_4, or is cyclic of odd order and $q \nmid p - 1$ for all prime divisors p, q of $|N|$.

- The case $N \simeq C_2$ is obvious.
- The case $N \simeq V_4$ can also be dealt with very easily.
- The case $N \simeq C_n$ with $q \nmid p - 1$ for all prime divisors p, q of n:
  - a. $(N, \circ)$ is a C-group, i.e. the Sylow subgroups are all cyclic. (Rump 2019)
  - b. $(N, \circ) \simeq C_d \rtimes C_e$ for some $\gcd(d, e) = 1$ (Murty & Murty 1984)
  - c. $(N, \circ) \simeq C_n \simeq (N, +)$ (the hypothesis on the prime divisors of n)
- It then follows that N must satisfy ⓘ. See Remark 2.9 of the paper for the details.

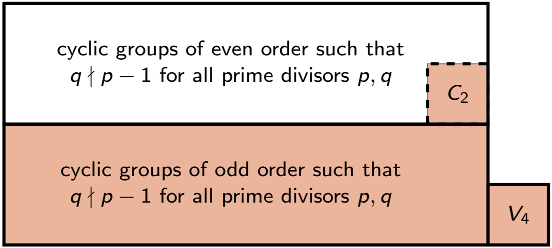
The difference in the Klein four-group

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



The two non-trivial skew braces of order four

- First non-trivial skew brace: $(A,+) \simeq V_4$ and $(A,\circ) \simeq C_4$

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +, \circ): \quad \vec{x} \circ \vec{y} = \left[\begin{smallmatrix} x_1+y_1+x_2y_2 \\ x_2+y_2 \end{smallmatrix}\right], \ \ \gamma_{\vec{x}}(\vec{y}) = \left[\begin{smallmatrix} 1 & x_2 \\ 0 & 1 \end{smallmatrix}\right] \vec{y}$$

There is only one non-trivial proper subgroup of $(A,\circ)$:

$$\{\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]\}$$

This is a left ideal of $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +, \circ)$.

- Second non-trivial skew brace: $(A,+) \simeq C_4$ and $(A,\circ) \simeq V_4$

$$(\mathbb{Z}/4\mathbb{Z}, +, \circ): \quad x \circ y = x + y + 2xy, \ \ \gamma_x(y) = (1+2x)y$$

There are three non-trivial proper subgroups of $(A,\circ)$:

$$\{0,1\}, \quad \{0,2\}, \quad \{0,3\}$$

Only $\{0,2\}$ is a left ideal of $(\mathbb{Z}/4\mathbb{Z}, +, \circ)$.

$\boxed{\text{Thus, we have to exclude } V_4 \text{ when we are fixing the Galois group.}}$

References in order of appearance

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. C. Greither and B. Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra 106 (1987), no. 1, 239–258.
3. 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.
4. N. P. Byott, *Galois structure for separable field extension*, Comm. Algebra 24 (1996), no. 10, 3217–3228. Corrigendum, *ibid.* no. 11, 3705.
5. L. Guarnieri and L. Vendramin, *Skew braces and the Yang–Baxter equation*, Math. Comp. 86 (2017), no. 307, 2519–2534.
6. W. Rump, *Classification of cyclic braces, II*, Trans. Amer. Math. Soc. 372 (2019), no. 1, 305–328.
7. M. R. Murty and V. K. Murty, *On groups of squarefree order*, Math. Ann. 267 (1984), no. 3, 299–309.


Thank you!!
Thank you
ありがとう
ありがとう!!
Thank you
ありがとう!
ペコリ
Thank you
ありがとう
Thank you