HOPF25

Hopf-Galois Structures and Skew Braces

Nigel Byott

University of Exeter

Brussels, 22 April 2025

§1. Hopf-Galois Structures

Chase & Sweedler (1969) generalised Galois theory using Hopf algebras, in part to study inseparable field extensions.

Greither & Pareigis (1987) showed that this is interesting even in the case of finite separable field extensions.

§1. Hopf-Galois Structures

Chase & Sweedler (1969) generalised Galois theory using Hopf algebras, in part to study inseparable field extensions.

Greither & Pareigis (1987) showed that this is interesting even in the case of finite separable field extensions.

Definition: Let L/K be a finite separable field extension (not necessarily normal). Let H be a finite dimensional cocommutative K-Hopf algebra. Then L/K is an H-**Galois extension** if L is an H-module algebra via $\alpha : H \to \mathrm{End}_K(L)$, and the linear map $\mathrm{id}_L \otimes \alpha : L \otimes H \to \mathrm{End}_K(L)$ is bijective.

§1. Hopf-Galois Structures

Chase & Sweedler (1969) generalised Galois theory using Hopf algebras, in part to study inseparable field extensions.

Greither & Pareigis (1987) showed that this is interesting even in the case of finite separable field extensions.

Definition: Let L/K be a finite separable field extension (not necessarily normal). Let H be a finite dimensional cocommutative K-Hopf algebra. Then L/K is an H-**Galois extension** if L is an H-module algebra via $\alpha : H \to \mathrm{End}_K(L)$, and the linear map $\mathrm{id}_L \otimes \alpha : L \otimes H \to \mathrm{End}_K(L)$ is bijective.

Motivating Example (classical Galois Theory): If L/K is normal and $G = \mathrm{Gal}(L/K)$ then L/K is an H-Galois extension for the group algebra $H = K[G]$.

Given finite separable L/K, we would like to find all Hopf-Galois structures on L/K, i.e. pairs (H, α) (up to isomorphism) making L/K into an H-Galois algebra.

Let E be the Galois closure of L/K, let $G = \mathrm{Gal}(E/K)$, $G' = \mathrm{Gal}(E/L)$, and let X be the left coset space $X = G/G'$.

Theorem (Greither & Pareigis) The Hopf-Galois structures on L/K are given by subgroups $N \subseteq \mathrm{Perm}(X)$ which are regular (i.e. simply transitive) and normalised by the left translations $\{T_g : g \in G\}$ where $T_g(hG') = ghG'$. The Hopf algebra H corresponding to N is $E[N]^G$.

The **type** of a Hopf-Galois structure is the isomorphism type of N.

Let E be the Galois closure of L/K, let $G = \mathrm{Gal}(E/K)$, $G' = \mathrm{Gal}(E/L)$, and let X be the left coset space $X = G/G'$.

Theorem (Greither & Pareigis) The Hopf-Galois structures on L/K are given by subgroups $N \subseteq \mathrm{Perm}(X)$ which are regular (i.e. simply transitive) and normalised by the left translations $\{T_g : g \in G\}$ where $T_g(hG') = ghG'$. The Hopf algebra H corresponding to N is $E[N]^G$.

The **type** of a Hopf-Galois structure is the isomorphism type of N.

We will mainly consider the case where L/K is normal, i.e. L/K is a Galois extension (in the classical sense).

Then $G' = 1$, $X = G$, so N is a regular subgroup of $\mathrm{Perm}(G)$.

Some Sample Results (L/K normal)

1. (Kohl, 1998): If $G = C_{p^n}$ for an odd prime p, then there are p^{n-1} Hopf-Galois structures, all of cyclic type. [For $p = 2$, dihedral and quaternion types also occur.]

Some Sample Results (L/K normal)

1. (Kohl, 1998): If $G = C_{p^n}$ for an odd prime p, then there are p^{n-1} Hopf-Galois structures, all of cyclic type. [For $p = 2$, dihedral and quaternion types also occur.]
2. (Childs, 2005): If $G \cong (C_p)^m$ with $p > m \geq 3$, there are at least $p^{m(m-1)-1}(p-1)$ Hopf-Galois structures of type $(C_p)^m$ and also some nonabelian ones.

Some Sample Results (L/K normal)

1. (Kohl, 1998): If $G = C_{p^n}$ for an odd prime p, then there are p^{n-1} Hopf-Galois structures, all of cyclic type. [For $p = 2$, dihedral and quaternion types also occur.]
2. (Childs, 2005): If $G \cong (C_p)^m$ with $p > m \geq 3$, there are at least $p^{m(m-1)-1}(p-1)$ Hopf-Galois structures of type $(C_p)^m$ and also some nonabelian ones.
3. (B, 2004) If G is nonabelian simple, there are just two Hopf-Galois structures, both of type G.

Some Sample Results (L/K normal)

1. (Kohl, 1998): If $G = C_{p^n}$ for an odd prime p, then there are p^{n-1} Hopf-Galois structures, all of cyclic type. [For $p = 2$, dihedral and quaternion types also occur.]
2. (Childs, 2005): If $G \cong (C_p)^m$ with $p > m \geq 3$, there are at least $p^{m(m-1)-1}(p-1)$ Hopf-Galois structures of type $(C_p)^m$ and also some nonabelian ones.
3. (B, 2004) If G is nonabelian simple, there are just two Hopf-Galois structures, both of type G.

Some Sample Results (L/K normal)

1. (Kohl, 1998): If $G = C_{p^n}$ for an odd prime p, then there are p^{n-1} Hopf-Galois structures, all of cyclic type. [For $p = 2$, dihedral and quaternion types also occur.]
2. (Childs, 2005): If $G \cong (C_p)^m$ with $p > m \geq 3$, there are at least $p^{m(m-1)-1}(p-1)$ Hopf-Galois structures of type $(C_p)^m$ and also some nonabelian ones.
3. (B, 2004) If G is nonabelian simple, there are just two Hopf-Galois structures, both of type G.

An alternative formulation of Greither-Pareigis:

Given a regular subgroup $N \subseteq \mathrm{Perm}(X)$, there is a bijection

$$N \to X = G/G', \qquad \eta \mapsto \eta \cdot (e_G G').$$

We can "transport structure" between N and X so that G acts on N (with G' as the stabiliser of the identity). For an abstract group $\mathcal{N}$, embeddings $\mathcal{N} \to \mathrm{Perm}(X)$ with regular image correspond bijectively to embeddings $G \to \mathrm{Perm}(\mathcal{N})$ with transitive image, where the stabiliser of $e_{\mathcal{N}}$ is G'.

The image of a regular embedding $\mathcal{N} \to \mathrm{Perm}(X)$ is normalised by $\{T_g\}$ if and only if the image of the corresponding embedding $G \to \mathrm{Perm}(\mathcal{N})$ lies in

$$\mathcal{N} \rtimes \mathrm{Aut}(\mathcal{N}) =: \mathrm{Hol}(\mathcal{N}),$$

the **holomorph** of $\mathcal{N}$. Here $\mathcal{N}$ is identified with $\{T_\eta : \eta \in N\}$).

The image of a regular embedding $\mathcal{N} \to \mathrm{Perm}(X)$ is normalised by $\{T_g\}$ if and only if the image of the corresponding embedding $G \to \mathrm{Perm}(\mathcal{N})$ lies in

$$\mathcal{N} \rtimes \mathrm{Aut}(\mathcal{N}) =: \mathrm{Hol}(\mathcal{N}),$$

the **holomorph** of $\mathcal{N}$. Here $\mathcal{N}$ is identified with $\{T_\eta : \eta \in N\}$).

So Hopf-Galois structures of type $\mathcal{N}$ on L/K correspond to transitive subgroups $\mathcal{G}$ of $\mathrm{Hol}(\mathcal{N})$ isomorphic to $G = \mathrm{Gal}(E/K)$. This correspondence is not bijective, because different regular *embeddings* give the same regular *subgroup* if they differ by an automorphism of their domain.

The image of a regular embedding $\mathcal{N} \to \mathrm{Perm}(X)$ is normalised by $\{T_g\}$ if and only if the image of the corresponding embedding $G \to \mathrm{Perm}(\mathcal{N})$ lies in

$$\mathcal{N} \rtimes \mathrm{Aut}(\mathcal{N}) =: \mathrm{Hol}(\mathcal{N}),$$

the **holomorph** of $\mathcal{N}$. Here $\mathcal{N}$ is identified with $\{T_\eta : \eta \in N\}$).

So Hopf-Galois structures of type $\mathcal{N}$ on L/K correspond to transitive subgroups $\mathcal{G}$ of $\mathrm{Hol}(\mathcal{N})$ isomorphic to $G = \mathrm{Gal}(E/K)$. This correspondence is not bijective, because different regular *embeddings* give the same regular *subgroup* if they differ by an automorphism of their domain.

For L/K normal with Galois group G, the number of Hopf-Galois structures of type $\mathcal{N}$ on L/K is:

$$\frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(\mathcal{N})|} \times [\text{number of regular subgroups} \cong G \text{ in } \mathrm{Hol}(\mathcal{N})].$$

§2. Skew braces

To study combinatorial aspects of the Yang-Baxter Equation (YBE)

$$R_{12}R_{23}R_{12} = R_{23}R_{12}R_{23} : V \otimes V \otimes V \to V \otimes V \otimes V,$$

where $R : V \otimes V \to V \otimes V$ is a linear map, Drinfel'd (1992) suggested looking for functions $r : X \times X \to X \times X$, where X is a non-empty set, and

$$r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23} : X \times X \times X \to X \times X \times X.$$

Skew braces were introduced by Guarnieri & Vendramin (2017) to study such **set-theoretic solutions** of the YBE.

§2. Skew braces

To study combinatorial aspects of the Yang-Baxter Equation (YBE)

$$R_{12}R_{23}R_{12} = R_{23}R_{12}R_{23} : V \otimes V \otimes V \to V \otimes V \otimes V,$$

where $R : V \otimes V \to V \otimes V$ is a linear map, Drinfel'd (1992) suggested looking for functions $r : X \times X \to X \times X$, where X is a non-empty set, and

$$r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23} : X \times X \times X \to X \times X \times X.$$

Skew braces were introduced by Guarnieri & Vendramin (2017) to study such **set-theoretic solutions** of the YBE.

A **skew brace** $(B, +, \circ)$ is a set B with two operations $+$, $\circ$ making B into a group (not necessarily abelian), and satisfying

$$a \circ (b + c) = a \circ b - a + a \circ c \text{ for all } a, b, c \in B.$$

For $a \in A$, define

$$\lambda_a : B \to B, \qquad \lambda_a(b) = -a + a \circ b.$$

Then $\lambda_a \in \mathrm{Aut}(B, +)$ and $a \mapsto \lambda_a$ is a homomorphism $(B, \circ) \to \mathrm{Aut}(B, +)$, and

$$r : B \to B, \qquad r(a, b) = (\lambda_a(b), \lambda_a(b)^{-1} \circ a \circ b)$$

is a set-theoretic solution of the YBE. Moreover, it is non-degenerate, i.e., writing $r(a, b) = (\sigma_a(b), \tau_b(a))$, the functions σ_a and τ_b are permutations of B.

For $a \in A$, define

$$\lambda_a : B \to B, \qquad \lambda_a(b) = -a + a \circ b.$$

Then $\lambda_a \in \mathrm{Aut}(B, +)$ and $a \mapsto \lambda_a$ is a homomorphism $(B, \circ) \to \mathrm{Aut}(B, +)$, and

$$r : B \to B, \qquad r(a, b) = (\lambda_a(b), \lambda_a(b)^{-1} \circ a \circ b)$$

is a set-theoretic solution of the YBE. Moreover, it is non-degenerate, i.e., writing $r(a, b) = (\sigma_a(b), \tau_b(a))$, the functions σ_a and τ_b are permutations of B.

To any non-degenerate set-theoretic solution r of the YBE, one can associate a skew brace in a canonical way.

For $a \in A$, define

$$\lambda_a : B \to B, \qquad \lambda_a(b) = -a + a \circ b.$$

Then $\lambda_a \in \mathrm{Aut}(B, +)$ and $a \mapsto \lambda_a$ is a homomorphism $(B, \circ) \to \mathrm{Aut}(B, +)$, and

$$r : B \to B, \qquad r(a, b) = (\lambda_a(b), \lambda_a(b)^{-1} \circ a \circ b)$$

is a set-theoretic solution of the YBE. Moreover, it is non-degenerate, i.e., writing $r(a, b) = (\sigma_a(b), \tau_b(a))$, the functions σ_a and τ_b are permutations of B.

To any non-degenerate set-theoretic solution r of the YBE, one can associate a skew brace in a canonical way.

Skew braces generalise the previous notation of braces (Rump, 2007), where $+$ is required to be commutative. Braces correspond to involutive set-theoretic solutions r, i.e. $r^2 = \mathrm{id}_{X \times X}$.

§3. The connection between HGS & skew braces

For a skew brace B,

$$\{(b, \lambda_b) : b \in B\}$$

is a subgroup of $(B, +) \rtimes \mathrm{Aut}(B, +) =: \mathrm{Hol}(B, +)$, where the group operation is

$$(a, \lambda_a)(b, \lambda_b) = (a + \lambda_a(b), \lambda_a \lambda_b) = (a\lambda_b, \lambda_{a \circ b}).$$

This subgroup is regular as group of permutations on B.

§3. The connection between HGS & skew braces

For a skew brace B,

$$\{(b, \lambda_b) : b \in B\}$$

is a subgroup of $(B, +) \rtimes \mathrm{Aut}(B, +) =: \mathrm{Hol}(B, +)$, where the group operation is

$$(a, \lambda_a)(b, \lambda_b) = (a + \lambda_a(b), \lambda_a \lambda_b) = (a\lambda_b, \lambda_{a \circ b}).$$

This subgroup is regular as group of permutations on B.

So we have a regular subgroup of $\mathrm{Hol}(B, +)$ isomorphic to $(B, \circ)$. This gives a Hopf-Galois structure of type $(B, +)$ on any Galois extensions of fields with Galois group isomorphic to $(B, \circ)$.

Conversely, given a Hopf-Galois structure of type N on a Galois extension L/K with Galois group G, there is an embedding of G as a regular subgroup of $\mathrm{Hol}(N)$, via which we can define a group operation $\circ$ on N so that $(N, \circ) \cong G$ and $(N, +, \circ)$ is a skew brace.

Conversely, given a Hopf-Galois structure of type N on a Galois extension L/K with Galois group G, there is an embedding of G as a regular subgroup of $\mathrm{Hol}(N)$, via which we can define a group operation $\circ$ on N so that $(N, \circ) \cong G$ and $(N, +, \circ)$ is a skew brace.

This correspondence between skew braces and Hopf-Galois structures is not bijective. On the skew brace side, two regular subgroups of $\mathrm{Hol}(B, +)$ give isomorphic skew braces if they are conjugate under $\mathrm{Aut}(B, +)$. On the Hopf-Galois side, we need to allow for the correction factor $|\mathrm{Aut}(G)|/|\mathrm{Aut}(N)|$.

§4. Some consequences and open questions

1. Enumerative results can be obtained in parallel for Hopf-Galois structures and skew braces: e.g.
   (i) For L/K Galois with group G with $|G|$ squarefree, and given N with $|N| = |G|$, number of Hopf-Galois on L/K of type N, and number of skew braces $(B, +, \circ)$ with $(B, +) \cong N$ and $(B, \circ) \cong G$ have both been determined (Alabdali & Byott, 2020, 2021).
   (ii) Let $n = 2^m s$ with $m \geq 5$ and s odd and let G be a generalised quaternion or dihedral Galois group of order n.
   On a Galois extension with group G, there are $2^{m-2} \cdot 9s$ Hopf-Galois structures *of abelian type* (either $C_{2^m s}$ or $C_{2s} \times C_{2^{m-1]}}$)). There are 7 *braces* $(B, +\circ)$ (up to isomorphism) with $(B, \circ) \cong G$. (Byott & Ferri, 2024).
2. Simple skew braces $(B, +, \circ)$ with both $(B, +)$ and $(B, \circ)$ nonabelian and soluble. The first infinite family of such skew braces was constructed via regular subgroups of holomorphms. (B, to appear).

3. For a finite *brace*, i.e. $(B, +)$ abelian, it is known that $(B, \circ)$ is soluble. For a finite skew brace with $(B, +)$ soluble, must $(B, \circ)$ also be soluble? This is an open problem, but in a minimal counterexample, any non-abelian composition factor of $(B, \circ)$ must be $\mathrm{GL}_3(2)$, the non-abelian simple group of order 168. (B, 2024).

References

- [A.Alabdali, N.P.Byott 2020] Hopf-Galois structures of squarefree degree. J. Algebra **559** 58–86.
- [A.Alabdali, N.P.Byott 2021] Skew braces of squarefree order. J. Algebra Appl. **20**, paper no. 2150128.
- [N.P.Byott 2004] Hopf-Galois structures on field extensions with simple Galois groups, Bull. London Math. Soc **36**, 23–29.
- [N.P.Byott, to appear] On a family of simple skew braces. *arXiv:2405.16154*
- [N.P.Byott, 2024] On insoluble transitive subgroups in the holomorph of a finite soluble group. J. Algebra **638** 1–31.
- N.P.Byott & F.Ferri, 2025] On the number of dihedral and quaternions braces and Hopf-Galois structures. J. Algebra **665** 72–102.
- [S.U.Chase M.E.Sweedler, 1969] Hopf Algebras and Galois Theory, LNM 97.

- [L.N.Childs 2005] Elementary abelian Hopf Galois structures and polynomial formal groups. J. ALgebra **283**, 292–316.
- [V.G.Drindel'd 1992] On some unsolved problems in quantum group theory, in LNM 1510.
- [C.Greither, B.Paregis 1987] Hopf Galois Theory for separable extensions, J. Algebra **106**, 239–258.
- [L.Guarnieri, L. Vendramin 2017] Skew braces and the Yang-Baxter equation. Math. Comp. **86** 2519–2534.
- [T.Kohl 1998] Classification of the Hopf Galois structures on prime power radical extensions. J. Algebra **207** 525-546.
- [Rump, 2007] Braces, radical rings and the quantum Yang-Baxter equation. J. Algebra **307** 153–170.