Describing Hopf–Galois structures via skew braces

Lorenzo Stefanello

Joint work with Senne Trappeniers

Groups & Algebras in Bicocca for Young algebraists,
20 June 2024

The classical structure

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

The group algebra

$$K[G] = \left\{ \sum_{\sigma \in G} k_\sigma \sigma \mid k_\sigma \in K \right\}$$

acts naturally on L:

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

Fact

The group algebra $K[G]$ is a K-Hopf algebra.

Hopf–Galois structures

Definition

A *Hopf–Galois structure* $(H, \cdot)$ on L/K consists of

- a K-Hopf algebra H;
- an action $\cdot$ of H on L that "mimics" the action of $K[G]$ on L.

Example

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

Motivation

More Hopf–Galois structures on the same extension
$\rightsquigarrow$ *setting for problems in Galois module theory.*

Known descriptions

Problem

Find an effective description of Hopf–Galois structures.

- Group theoretic description by Greither–Pareigis (1987).
- Connection with skew braces by Byott–Vendramin (2018).

Both give few results in the study of the Hopf–Galois correspondence.

The Hopf–Galois correspondence

Consider a Hopf–Galois structure $(H, \cdot)$ on L/K. The map

$$\{\text{Hopf subalgebras of } H\} \to \{\text{intermediate fields of } L/K\}$$
$$J \mapsto L^J \text{ (fixed field)}$$

is called the *Hopf–Galois correspondence* (HGC).

It is injective but not necessarily surjective.

Question

When (and why) is the HGC bijective?

Bijective Hopf–Galois correspondence

- When we consider the classical structure, we recover the usual Galois correspondence.
- If G is Hamiltonian, then there exists a Hopf–Galois structure on L/K for which the HGC is bijective (Greither–Pareigis, 1987).
- If G is cyclic of odd prime power order, then the HGC is bijective for all Hopf–Galois structures (Childs, 2017).

Skew braces

Definition (Guarnieri–Vendramin, 2017)

A *skew brace* is a triple $(A, +, \circ)$, where $(A, +)$ and $(A, \circ)$ are groups such that for all $a, b, c \in A$,

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

$(A, +)$ is the *additive* group, and $(A, \circ)$ is the *multiplicative* group.

Skew braces are related (among the others) with

- radical rings;
- set-theoretic solutions of the Yang–Baxter equation;
- regular subgroups of holomorphs of groups;
- Hopf–Galois structures.

Examples

Example

If $(A, \circ)$ is a group, then $(A, \circ, \circ)$ is a (*trivial*) skew brace.

Example

Take $A = \{\sigma^i \mid i = 0, \dots, n-1\}$, with $n \geq 4$ even, and consider the operations

$$\sigma^i + \sigma^j = \sigma^{i+(-1)^i j},$$
$$\sigma^i \circ \sigma^j = \sigma^{i+j}.$$

Then $(A, +, \circ)$ is a skew brace, with $(A, +)$ dihedral and $(A, \circ)$ cyclic of order n.

Gamma function and left ideals

If $(A, +, \circ)$ is a skew brace, then the map

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

is a group homomorphism.

Definition

A *left ideal* of a skew brace $(A, +, \circ)$ is a subgroup of $(A, +)$ and $(A, \circ)$ (one is enough) that is invariant under the action of $\gamma(A)$.

A new version of the connection

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

Theorem (LS–Trappeniers, 2023)

There exists a bijection between

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

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

Moreover, $L[G_+]^{G_\circ}$ acts on L as follows:

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

Example

The classical structure is associated with the trivial skew brace.

The Hopf–Galois correspondence via skew braces

Consider $(G, +, \circ) \leftrightarrow L[G_+]^{G_\circ}$.

Theorem (LS–Trappeniers, 2023)

There exists a bijective correspondence between

- *the left ideals* I *of* $(G, +, \circ)$*;*
- *the Hopf subalgebras* J *of* $L[G_+]^{G_\circ}$*.*

Specifically, $I \leftrightarrow J = L[I_+]^{G_\circ}$*, and*

$$\text{(Galois theory)} \quad L^I = L^J \quad \text{(Hopf–Galois theory)}.$$

Corollary (LS–Trappeniers, 2023)

The HGC is bijective if and only if every subgroup of $(G, \circ)$ *is a left ideal of* $(G, +, \circ)$*.*

An example

Suppose that $(G, \circ) = \{\sigma^i \mid i = 0, \dots, n-1\}$ is cyclic of even order $n \geq 4$, and consider the skew brace $(G, +, \circ)$ with

$$\sigma^i + \sigma^j = \sigma^{i+(-1)^i j}.$$

To obtain the Hopf–Galois structure it is enough to apply $\gamma(\sigma)$:

$$\gamma(\sigma)\colon \sigma^i \mapsto -\sigma + (\sigma \circ \sigma^i) = \sigma + \sigma^{1+i} = \sigma^{1-(1+i)} = \sigma^{-i}.$$

Therefore

$$H = L[G_+]^{G_\circ} = \left\{ \sum_{i=0}^{n-1} \ell_i \sigma^i \in L[G_+] \mid \sigma(\ell_i) = \ell_{-i} \text{ for all } i \right\}.$$

Moreover, the HGC is bijective, as every subgroup of $(G, \circ)$ is invariant under the action of $\gamma(\sigma)$ (via inversion).