# Classifying Galois extensions with Childs's property

Lorenzo Stefanello

Joint work with Senne Trappeniers

Algebraic structures in the Yang-Baxter equation, 4 June 2024

# Hopf–Galois structures

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

## Definition

A *Hopf–Galois structure* $(H, \cdot)$ on $L/K$ consists of a $K$-Hopf algebra $H$ and an action $\cdot$ of $H$ on $L$ such that

- $L$ is a left $H$-module algebra;
- the linear map

$$L \otimes_K H \to \mathrm{End}_K(L), \quad \ell \otimes h \mapsto (x \mapsto \ell(h \cdot x))$$

  is bijective.

## Example

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

# The type

Given a Hopf–Galois structure $(H, \cdot)$ on $L/K$, there exists a finite group $N$ such that

$$L \otimes_K H \cong L[N]$$

as $L$-Hopf algebras.

## Definition

The *type* of the Hopf–Galois structure $(H, \cdot)$ is the isomorphism class of $N$.

# The Hopf–Galois correspondence

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

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

is called the *Hopf–Galois correspondence* (HGC). It is injective but not necessarily surjective.

### Example

For the classical structure, we recover the usual bijective Galois correspondence.

### Example (Greither–Pareigis, 1987)

The image of the Hopf–Galois correspondence for the *canonical nonclassical structure* consists of the normal intermediate fields.

# Childs's property

### Example

Suppose that $G$ is cyclic of odd prime power order. Then every Hopf–Galois structure on $L/K$ has

- cyclic type [Kohl, 1998];
- a bijective HGC [Childs, 2017].

### Definition

We say that $L/K$ satisfies *Childs's property* if every Hopf–Galois structure on $L/K$ has a bijective Hopf–Galois correspondence.

### Problem

*Classify Galois extension with Childs's property.*

# 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 $a, b, c \in A$,

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

If $(A, +, \circ)$ is a skew brace, then there is a group homomorphism

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

## 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 $\lambda_A$.

# A connection between HGS and skew braces

- Hinted by Bachiller (2016).
- Made precise by Byott and Vendramin (2018).
- Alternative formulation in [LS–Trappeniers, 2023], employing opposite skew braces [Koch–Truman, 2020].

# A connection between HGS and skew braces

**Theorem**

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

*There exists a "connection" between*

- *the Hopf–Galois structures $(H, \cdot)$ on $L/K$ of type $N$;*
- *the skew braces $(A, +, \circ)$ with $(A, +) \cong N$ and $(A, \circ) \cong G$.*

*Under this connection, the Hopf subalgebras of $H$ correspond bijectively to the left ideals of $(A, +, \circ)$.*

# The HGC via skew braces

**Theorem (LS–Trappeniers, 2023)**

*Suppose that $(A, +, \circ) \leftrightarrow (H, \cdot)$. The HGC is bijective if and only if every subgroup of $(A, \circ)$ is a left ideal of $(A, +, \circ)$.*

**Corollary**

*Let $(H, \cdot)$ be a Hopf–Galois structure on $L/K$ of type $N$. If the number of characteristic subgroups of $N$ equals the number of subgroups of $G$, then the HGC is bijective.*

# The even prime

### Proposition (LS–Trappeniers, 2023)

*Suppose that $G$ is cyclic of order $2^m$, with $m \geq 1$. Then $L/K$ satisfies Childs's property.*

### Proof.

The cases $m = 1, 2$ can be done “by hand” via skew braces.

Suppose that $m \geq 3$. Consider a Hopf–Galois structure on $L/K$ of type $N$. By [Byott, 2007], $N$ may be cyclic, dihedral, or generalised quaternion.

- If $N$ is cyclic, dihedral, or generalised quaternion with $m \neq 3$, then the number of characteristic subgroups of $N$ equals the number of subgroups of $G$, so the HGC is bijective.
- In the case $N \cong Q_8$, use quotients of skew braces to reduce to the case $m = 2$ and then “lift back” information.

## Some direct products

### Proposition (LS–Trappeniers, 2023)

*Suppose that $G$ is cyclic and for all prime divisors $p$ and $q$ of its order, $p \nmid q - 1$. Then $L/K$ satisfies Childs's property.*

### Proof.

If $n = |G|$ is even, then $|G| = 2^m$ for some $m$, so we are done.

Let $n$ be odd, and take a Hopf–Galois structure on $L/K$ of type $N$.

- By [Tsang, 2022], $N \cong C_a \rtimes C_b$, with $n = ab$ and $(a, b) = 1$.
- By the assumption on $n$, this has to be a direct product.
- In particular, $N$ is cyclic, and we conclude as before.

# The final statement

### Theorem (LS–Trappeniers, 2023)

*Let $L/K$ be a finite Galois extension with Galois group $G$. The following are equivalent:*

- *$L/K$ satisfies Childs's property.*
- *$G$ is cyclic, and for all primes $p, q$ dividing the order of $G$, $p$ does not divide $q - 1$.*

### Proof (idea):

- One direction has been discussed.
- For the other: assume that $G$ has not the desired form, and find a skew brace $(A, +, \circ)$ with $(A, \circ) \cong G$ for which not all subgroups of $(A, \circ)$ are left ideals.

# Why the condition on the primes

Suppose that $G$ is cyclic of order $p^m q^n$, where $p, q$ distinct prime numbers such that $p \mid q-1$. Take the Sylow $P, Q$ of $G$.

- There exists a skew brace $(A, +, \circ)$ with $(A, +) = Q \rtimes P$ (nontrivial) and $(A, \circ) = Q \times P \cong G$; by the general theory, also $(A, +_{\mathrm{op}}, \circ)$ is a skew brace.
- A left ideal of $(A, +, \circ)$ is also a left ideal of $(A, +_{\mathrm{op}}, \circ)$ if and only if it is normal in $(A, +)$.
- If $L/K$ satisfies Childs's property, then $P$ is a left ideal of both $(A, +, \circ)$ and $(A, +_{\mathrm{op}}, \circ)$, and therefore is normal in $Q \rtimes P$; contradiction.

# The final statement

**Theorem (LS–Trappeniers, 2023)**

*Let $L/K$ be a finite Galois extension with Galois group $G$. The following are equivalent:*

- *$L/K$ satisfies Childs's property.*
- *$G$ is cyclic, and for all primes $p, q$ dividing the order of $G$, $p$ does not divide $q - 1$.*