This research was partially supported by the ERC Advanced grant 320974.

Hopf-Galois Structures and Skew Braces

Kayvan Nejabati Zenouz

University of Edinburgh

The aim of this poster is to give a short introduction to

① Hopf-Galois Structures ② Skew Braces and ③, ④ their Relationship

⑤ Skew Braces and ⑦ Hopf-Galois Structures Classification

⑥ Automorphism Groups of Skew Braces and Examples

⑧ Skew Braces of Semi-direct Product Type

For simplicity we assume L/K is a Galois extension of fields with Galois group G.

① Hopf-Galois structures

A *Hopf-Galois structure* on L/K consists of a finite dimensional cocommutative K-*Hopf algebra* H together with an action on L which makes L into an H-*Galois extension*.

Hopf-Galois Structures: Example, History, and Applications

- The group algebra $K[G]$ endows L/K with the classical Hopf-Galois structure. In general there may be more than one Hopf-Galois structure on L/K.
- Hopf-Galois theory for inseparable extensions of fields was introduced by Chase & Sweedler in 1969 in order to generalised the classical Galois theory.
- Hopf-Galois extensions have applications in Galois module theory.
- They can be studied in algebro geometric settings: affine group scheme torsors over $\mathrm{Spec}(K)$.
- Finally, they are connected to skew braces, and hence to the set-theoretic solutions of the quantum Yang-Baxter equation.

Question

How to find all Hopf-Galois structures on L/K?

Theorem (Greither and Pareigis)

Hopf-Galois structures on L/K correspond bijectively to regular subgroups of $\mathrm{Perm}(G)$ *which are normalised by the image of G, as left translations, inside* $\mathrm{Perm}(G)$.

Every K-Hopf algebra which endows L/K with a Hopf-Galois structure is of the form $L[N]^G$ for some regular subgroup $N \subseteq \mathrm{Perm}(G)$ normalised by the left translations.

Notation: The *isomorphism type* of N is known as the **type** of the Hopf-Galois structure.

② Skew Braces

a (left) *skew brace* is a triple $(B, \oplus, \odot)$ which consists of a set B together with two operations $\oplus$ and $\odot$ such that $(B, \oplus)$ and $(B, \odot)$ are groups (neither necessarily abelian), and the two operations are related by the *skew brace property*:

$$a \odot (b \oplus c) = (a \odot b) \ominus a \oplus (a \odot c) \quad \text{for every } a, b, c \in B,$$

where $\ominus a$ is the inverse of a with respect to the operation $\oplus$.

Braces were introduced by Rump in 2007. Many properties of braces were investigated by Bachiller, Cedó, Jespers, Okniński et al.

Skew braces, as a generalisation of braces, and their connections to other areas, were studied by Byott, Guarnieri, Smoktunowicz, and Vendramin.

Notation: We call a G-skew brace of **type** N a skew brace $(B, \oplus, \odot)$ such that $(B, \oplus) \cong N$ and $(B, \odot) \cong G$.

Skew Braces of Order p^3 for $p > 3$

The number of G-skew braces of type N, $\widetilde{e}(G, N)$, is given by

$\widetilde{e}(G,N)$	C_{p^3}	$C_{p^2} \times C_p$	C_p^3	$C_p^2 \rtimes C_p$	$C_{p^2} \rtimes C_p$
C_{p^3}	3	-	-	-	-
$C_{p^2} \times C_p$	-	9	-	-	$4p+1$
C_p^3	-	-	5	$2p+1$	-
$C_p^2 \rtimes C_p$	-	-	$2p+1$	$2p^2-p-3$	-
$C_{p^2} \rtimes C_p$	-	$4p+1$	-	-	$4p^2-3p-1$

Note $\widetilde{e}(G, N) = \widetilde{e}(N, G)$.

③ From Hopf-Galois Structures to Skew Braces

- Suppose H endows L/K with a Hopf-Galois structure.
- Then $H = L[N]^G$ for some $N \subseteq \mathrm{Perm}(G)$ which is a regular subgroup normalised by the left translations.
- The subgroup N is a regular implies that we have a bijection

$$\begin{aligned} \phi : N &\longrightarrow G \\ n &\longmapsto n \cdot 1_G. \end{aligned}$$

- Set $(B, \oplus) = N$ and define a new group operation by

$$n_1 \odot n_2 = \phi^{-1}(\phi(n_1)\phi(n_2)) \quad \text{for } n_1, n_2 \in N.$$

- The subgroup N is normalised by the left translations implies that $(B, \oplus, \odot)$ is a G-skew brace of type N corresponding to H.

④ From Skew Braces to Hopf-Galois Structures

- Suppose $(B, \oplus, \odot)$ is a G-skew brace of type N.
- The map

$$\begin{aligned} d : (B, \oplus) &\longrightarrow \mathrm{Perm}(B, \odot) \\ a &\longmapsto (d_a : b \longmapsto a \oplus b) \end{aligned}$$

is a regular embedding.

- The skew brace property implies that for all $a, b, c \in B$

$$b \odot \left(d_a\left(b^{-1} \odot c\right)\right) = d_{(b \odot a) \ominus b}(c) \quad \text{i.e., } \; b d_a b^{-1} = d_{(b \odot a) \ominus b}.$$

- Thus $L[(B, \oplus)]^{(B, \odot)}$ endows L/K with a Hopf-Galois structure corresponding to the skew brace $(B, \oplus, \odot)$.

Problem

The group $\mathrm{Perm}(G)$ can be large.

⑤ Classifying Skew Braces: working with holomorphs

For a skew brace $(B, \oplus, \odot)$ the map

$$\begin{aligned} m : (B, \odot) &\longrightarrow \mathrm{Hol}(B, \oplus) \\ a &\longmapsto (m_a : b \longmapsto a \odot b) \end{aligned}$$

is a regular embedding, where $\mathrm{Hol}(B, \oplus) = (B, \oplus) \rtimes \mathrm{Aut}(B, \oplus)$. For $f : (B, \oplus, \odot_1) \longrightarrow (B, \oplus, \odot_2)$ an isomorphism of skew braces, we have

$$\begin{array}{ccc} (B, \odot_1) & \xrightarrow{m_1} & \mathrm{Hol}(B, \oplus) \\ \wr \downarrow f & & \wr \downarrow C_f \\ (B, \odot_2) & \xrightarrow{m_2} & \mathrm{Hol}(B, \oplus) \end{array} \qquad C_f \text{ is conjugation by } f.$$

Classifying Skew Braces

To find the non-isomorphic G-skew braces of type N for a fixed N, classify elements of the set $\{H \subseteq \mathrm{Hol}(N) \mid H \text{ is regular}, \; H \cong G\}$, and extract a maximal subset whose elements are not conjugate by any element of $\mathrm{Aut}(N)$.

⑥ Upshot: Automorphism Groups of Skew Braces

We find $\mathrm{Aut}_{\mathcal{B}r}(B, \oplus, \odot) \cong \left\{\alpha \in \mathrm{Aut}(B, \oplus) \mid \alpha(\mathrm{Im}\, m)\alpha^{-1} \subseteq \mathrm{Im}\, m\right\}$.

Example (Skew Braces of $C_{p^n} = \langle \sigma \mid \sigma^{p^n} = 1 \rangle$ type for $p > 2$ and $n > 1$)

$\mathrm{Hol}(C_{p^n}) = \langle \sigma \rangle \rtimes \langle \beta, \gamma \rangle$ with $\beta(\sigma) = \sigma^{p+1}$. Then the *trivial* skew brace is $\langle \sigma \rangle$, and the *nontrivial* skew braces are given by

$$\left\langle \sigma \beta^{p^m} \right\rangle \cong C_{p^n} \text{ with } \mathrm{Aut}_{\mathcal{B}r}\left(\left\langle \sigma \beta^{p^m} \right\rangle\right) = \left\langle \beta^{p^{n-m-1}} \right\rangle \text{ for } m = 0, \ldots, n-2.$$

⑦ Finding Hopf-Galois Structures

Denote by B_G^N the isomorphism class of a G-skew brace of type N given by $(B, \oplus, \odot)$. Then the number of Hopf-Galois structures on L/K of type N is given by

$$\sum_{B_G^N} \frac{|\mathrm{Aut}(G)|}{\left|\mathrm{Aut}_{\mathcal{B}r}\left(B_G^N\right)\right|}.$$

Hopf-Galois Structures of Order p^3 for $p > 3$

The number of Hopf-Galois structures on L/K of type N, $e(G, N)$, is given by

$e(G,N)$	C_{p^3}	$C_{p^2} \times C_p$	C_p^3	$C_p^2 \rtimes C_p$	$C_{p^2} \rtimes C_p$
C_{p^3}	p^2	-	-	-	-
$C_{p^2} \times C_p$	-	$(2p-1)p^2$	-	-	$(2p-1)(p-1)p^2$
C_p^3	-	-	$(p^4+p^3-1)p^2$	$(p^3-1)(p^2+p-1)p^2$	-
$C_p^2 \rtimes C_p$	-	-	$(p^2+p-1)p^2$	$(2p^3-3p^2+1)p^2$	-
$C_{p^2} \rtimes C_p$	-	$(2p-1)p^2$	-	-	$(2p-1)(p-1)p^2$

Note $p^2 \mid e(G, N)$ and $e(G, N) = \dfrac{\mathrm{Aut}(G)}{\mathrm{Aut}(N)} e(N, G)$.

⑧ Skew Braces of Semi-direct Product Type

How general is this pattern?

Let P and Q be groups, $\alpha, \beta : Q \longrightarrow \mathrm{Aut}(P)$ group homomorphisms such that $\mathrm{Im}\,\beta$ is an abelian group, and $[\mathrm{Im}\,\alpha, \mathrm{Im}\,\beta] = 1$. We can simultaneously form a $(P \rtimes_\alpha Q)$-skew brace of type $P \rtimes_\beta Q$ and a $(P \rtimes_\beta Q^{\mathrm{op}})$-skew brace of type $P \rtimes_\alpha Q$.
Is this true for more general extensions of groups?