Hopf-Galois Structures and Skew Braces

Kayvan Nejabati Zenouz

University of Edinburgh

Noncommutative and non-associative structures, braces and applications workshop

Malta

March 14, 2018

Acknowledgements

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

Overview

The aim of the talk is to give an overview of

Hopf-Galois structures and their connection to skew braces

Automorphism groups of skew braces and examples

Hopf-Galois structures and skew braces of order p^3

Skew braces of semi-direct product type

Hopf-Galois Structures

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

Definition

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*.

The group algebra $K[G]$ endows L/K with the classical Hopf-Galois structure.

Hopf-Galois Structures: Motivations

Normal Basis Theorem

L is a free $K[G]$-module of rank one.

- Assume L/K is an extension of global or local fields (e.g., extensions of $\mathbb{Q}$ or $\mathbb{Q}_p$).
- Denote by $\mathcal{O}_L$ and $\mathcal{O}_K$ the rings of integers of L and K, respectively.
- Then $\mathcal{O}_L$ is also a module over $\mathcal{O}_K[G]$.
- Can $\mathcal{O}_L$ be free over $\mathcal{O}_K[G]$?

  ... No in general.

Hopf-Galois Structures: Applications

- Suppose H endows L/K with a Hopf-Galois structure.
- Define the associated order of $\mathcal{O}_L$ in H by

$$\mathfrak{A}_H = \{\alpha \in H \mid \alpha(\mathcal{O}_L) \subseteq \mathcal{O}_L\}.$$

- Can $\mathcal{O}_L$ be free over $\mathfrak{A}_H$?

  ... Sometimes, and depends on H.

Need a classification of Hopf-Galois structures.

Hopf-Galois structures are also related to the set-theoretic solutions of the QYBE via skew braces.

Hopf-Galois Structures:
A Theorem of Greither and Pareigis

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.

Hopf-Galois Structures: Some Results

- Byott (1996) showed if $|G| = n$, then L/K admits a unique Hopf-Galois structure if and only if $\gcd(n, \phi(n)) = 1$.
- Kohl (1998) classified Hopf-Galois structures for $G = C_{p^n}$ for a prime $p > 2$: there are p^{n-1}, all are of cyclic type. Byott (2007) studies $G = C_{2^n}$ case.
- Byott (1996, 2004) studied the problem for $|G| = p^2, pq$, also when G is a nonabelian simple group.
- Carnahan and Childs (1999, 2005) studied Hopf-Galois structures for $G = C_p^n$ and $G = S_n$.
- Alabadi and Byott (2017) studied the problem for $|G|$ is squarefree.
- NZ (2017) Hopf-Galois structures for $|G| = p^3$.

Skew Braces I

Definition

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, and the two operations are related by the *skew brace property*:

$$a \odot (b \oplus c) = (a \odot b) \ominus a \oplus (a \odot c) \text{ for every } a, b, c \in B, \qquad (1)$$

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

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

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 $(B, \oplus, \odot)$.

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 the left translations.
- N is a regular subgroup, 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

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

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

Skew Braces and Hopf-Galois Structures Correspondence

$$\left\{\begin{array}{c}\text{isomorphism classes}\\ \text{of } G\text{-skew braces,}\\ \text{i.e., with } (B,\odot)\cong G\end{array}\right\} \leftrightsquigarrow \left\{\begin{array}{c}\text{classes of Hopf-Galois structures}\\ \text{on } L/K \text{ under } L[N_1]^G \sim L[N_2]^G\\ \text{if } N_2=\alpha N_1\alpha^{-1} \text{ for some}\\ \alpha\in\mathrm{Aut}(G)\end{array}\right\}$$

Skew Braces II

Problem

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

Solution: 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, we have

$$\begin{tikzcd} (B, \odot_1) \arrow[r, hook, "m_1"] \arrow[d, "f", "\wr"'] & \mathrm{Hol}\,(B, \oplus) \arrow[d, "C_f", "\wr"'] \\ (B, \odot_2) \arrow[r, hook, "m_2"] & \mathrm{Hol}\,(B, \oplus) \end{tikzcd}$$

C_f is conjugation by f.

Skew Braces and Regular Subgroups of Holomorph Correspondence

Bachiller, Byott, Vendramin:

$$\left\{\begin{array}{c}\text{isomorphism classes}\\ \text{of skew braces of}\\ \text{type } N\text{, i.e., with}\\ (B,\oplus)\cong N\end{array}\right\} \leftrightsquigarrow \left\{\begin{array}{c}\text{classes of regular subgroup of}\\ \mathrm{Hol}(N) \text{ under } H_1\sim H_2 \text{ if}\\ H_2=\alpha H_1\alpha^{-1} \text{ for some}\\ \alpha\in\mathrm{Aut}(N)\end{array}\right\}$$

Upshot: Automorphism Groups of Skew Braces

In particular, if $f : (B, \oplus, \odot) \longrightarrow (B, \oplus, \odot)$ is an automorphism, then we have

$$\begin{tikzcd}
(B, \odot) \arrow[r, hook, "m"] \arrow[d, "f", "\wr"'] & \mathrm{Hol}\,(B, \oplus) \arrow[d, "C_f", "\wr"'] \\
(B, \odot) \arrow[r, hook, "m"] & \mathrm{Hol}\,(B, \oplus)\,;
\end{tikzcd}$$

using this observation we find

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

Skew Braces of C_{p^n} type

Example

Let $p > 2$, $n > 1$, and $C_{p^n} = \left\langle \sigma \mid \sigma^{p^n} = 1 \right\rangle$. Then

$$\mathrm{Hol}\left(C_{p^n}\right) = \langle \sigma \rangle \rtimes \langle \beta, \gamma \rangle$$

with $\beta\left(\sigma\right) = \sigma^{p+1}$. Then the *trivial* (skew) brace is $\langle \sigma \rangle$, and the *nontrivial* (skew) braces are given by

$$\left\langle \sigma \beta^{p^m} \right\rangle \cong C_{p^n} \text{ for } m = 0, ..., n-2.$$

We also have

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

Classifying Skew Braces and Hopf-Galois Structures

Skew braces

To find the non-isomorphic G-skew braces of type N for a fixed N, classify elements of the set

$$\mathcal{S}(G,N) = \{H \subseteq \mathrm{Hol}\,(N) \mid H \text{ is regular}, \ H \cong G\},$$

and extract a maximal subset whose elements are not conjugate by any element of $\mathrm{Aut}\,(N)$.

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

$$e(G,N) = \sum_{B_G^N} \frac{|\mathrm{Aut}\,(G)|}{|\mathrm{Aut}_{\mathcal{B}r}\,(B_G^N)|}. \tag{2}$$

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	$2p+1$	-
$C_p^2 \rtimes C_p$	-	-	$2p+1$	$2p^2-p-3$	-
$C_{p^2} \rtimes C_p$	-	$4p+1$	-	-	$4p^2-3p-1$

Remark

Note

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

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	-	-	$(p^4+p^3-1)p^2$	$(p^3-1)(p^2+p-1)p^2$	-
$C_p^2 \rtimes C_p$	-	-	$(p^2+p-1)p^2$	$(2p^3-3p^2+1)p^2$	-
$C_{p^2} \rtimes C_p$	-	$(2p-1)p^2$	-	-	$(2p-1)(p-1)p^2$

Remark

Note $p^2 \mid e(G, N)$ and

$$e(G,N) = \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|} e(N,G).$$

Skew Braces of Semi-direct Product Type

Question

How general is the pattern?

Partial Explanation

- Let P and Q be groups. Suppose $\alpha, \beta : Q \longrightarrow \mathrm{Aut}(P)$ are group homomorphisms such that $\mathrm{Im}\,\beta$ is an abelian group and $[\mathrm{Im}\,\alpha, \mathrm{Im}\,\beta] = 1$.
- We can form an $(P \rtimes_\alpha Q)$-skew brace of type $P \rtimes_\beta Q$.
- We also find an $(P \rtimes_\beta Q^{\mathrm{op}})$-skew brace of type $P \rtimes_\alpha Q$.

What is the relationship between $\widetilde{e}(G, N)$ and $\widetilde{e}(N, G)$ for N which is a general extensions of two groups?

Thank you for your attention!