Hopf-Galois Structures and Skew Braces of Order p^3

Kayvan Nejabati Zenouz

University of Exeter, UK

Viva

February 23, 2018

Overview

The aim of the talk is to give an overview on

- Motivations
- Achievements
- Contributions
- Scopes

for the project.

Motivations

- Galois module theory:

  Hopf-Galois Structures (HGS)

- Quantum group theory:

  The Yang-Baxter Equation (YBE)

Motivation I: Galois Module Theory

Suppose L/K is a finite Galois extension of local or global fields with Galois group $G = \mathrm{Gal}(L/K)$.

Normal Basis Theorem

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

Motivation I: Galois Module Theory

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 $\mathcal{O}_K[G]$?

Define the associated order of $\mathcal{O}_L$ in $K[G]$ by

$$\mathfrak{A}_{K[G]} = \{\alpha \in K[G] \mid \alpha(\mathcal{O}_L) \subseteq \mathcal{O}_L\}.$$

- Can $\mathcal{O}_L$ be free over $\mathfrak{A}_{K[G]}$?
- Can we replace $K[G]$ with other algebras?

Hopf-Galois structures on L/K

Motivation II: Quantum Group Theory

The YBE is studied in quantum group theory and has application in many areas of mathematical physics.

For a vector space V, the YBE is a matrix equation for elements of $\mathrm{GL}(V \otimes V)$.

In 1992 Drinfeld suggested studying the simplest class of solutions arising from the *set-theoretic* version of this equation.

Motivation II: Quantum Group Theory

Definition (Set-theoretic solution of the YBE)

Let X be a nonempty set. Then a bijective map

$$r : X \times X \longrightarrow X \times X$$

is a *set-theoretic solution* of the YBE if

$$r^{12} r^{23} r^{12} = r^{23} r^{12} r^{23} \tag{1}$$

holds in $\mathrm{Aut}(X \times X \times X)$, where $r^{12} = r \times \mathrm{id}_X$ and $r^{23} = \mathrm{id}_X \times r$.

- How can we find solutions with $|X| = n$?

Skew braces

Classification for

Hopf-Galois structures on Galois field extensions of degree p^3

Skew braces of order p^3

Hopf-Galois Structures: Preliminaries

For the rest of the talk we fix L/K to be a finite extension of fields with Galois group G.

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*.

Theorem (Greither-Pareigis 1987)

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* $\mathrm{Perm}(G)$.

The isomorphism type of a subgroup of $\mathrm{Perm}(G)$ which corresponds to a Hopf-Galois structure is called the **type** of the Hopf-Galois structure.

Hopf-Galois Structures: Byott's Translation

Problem

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

Instead of working with groups of permutations, work with *holomorphs*.

Theorem (Byott 1996)

Let G and N be finite groups. There exists a bijection between the sets

$$\mathcal{N} = \{\alpha : N \hookrightarrow \mathrm{Perm}(G) \mid \alpha(N) \text{ is regular } NBLT\}$$

$$\mathcal{G} = \{\beta : G \hookrightarrow \mathrm{Hol}(N) \mid \beta(G) \text{ is regular}\},$$

where $\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N)$.

Hopf-Galois Structures: Classification

Classify regular subgroups of holomorphs of groups of order p^3 for a prime number p.

That is, for each group N of order p^3, we determine explicitly the set

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

and range G over all groups of order p^3.

This enables classification of the Hopf-Galois structures

Skew Braces: Preliminaries

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*:

$$a \odot (b \oplus c) = (a \odot b) \ominus a \oplus (a \odot c) \text{ for every } a, b, c \in B, \qquad (2)$$

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. When the *additive group* $(B, \oplus)$ of our skew brace is abelian we call it a brace.

Skew Braces: Classification

Proposition (Vendramin and Byott 2017)

Let N be a finite group. There exists a bijective correspondence between isomorphism classes of skew braces with additive group isomorphic to N and classes of regular subgroups of $\mathrm{Hol}(N)$ *under conjugation by elements of* $\mathrm{Aut}(N)$.

To find the non-isomorphic G-skew braces of type N for a fixed N, use the classification

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

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

Contributions: Hopf Galois Theory

- 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 HGS for C_{p^n} extensions and a prime $p > 2$: there are p^{n-1}, all are of cyclic type. Byott (2007) studies 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 HGS for C_p^n and S_n extensions.
- Alabadi and Byott (2017) studied the problem for $|G|$ squarefree.
- NZ (2017) HGS for $|G| = p^3$.

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

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

Remark

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

$$e(G,N) = \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|} e(N,G). \tag{3}$$

Contributions: Skew Braces

- Rump (2007) studied cyclic braces.
- Bachiller (2015) classified braces of order p^3.
- Bachiller, Cedo, Jespers, Okninski (2017) studied matched products of braces.
- Guarnieri, Vendramin (2017) obtained computer assisted results on some skew braces.
- NZ (2017) skew braces of order p^3.

Contributions:
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

$$\widetilde{e}(G, N) = \widetilde{e}(N, G). \tag{4}$$

Scopes

Hopf-Galois Theory:

1. For L/K a Galois extension of local or global fields of degree p^3 one can study the structure of $\mathcal{O}_L$ as a module.
2. For L/K as above one can study the non-classical *Galois scaffolds* on L/K.
3. One would like to study families of HGS corresponding to a skew brace.

Skew Braces:

1. One can study automorphism groups of skew braces of order p^3.
2. Some methods can be used to study skew braces of type $\left(C_{p^e} \times C_{p^f}\right) \rtimes C_{p^g}$ for natural numbers e, f, g.
3. One would like to study skew braces whose type is an extension of two abelian groups. Does the pattern

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

still hold?

Thank you for your attention!