Research Statement

Kayvan Nejabati Zenouz

Contents

1 Summary

My research is focused on exploring connections between certain areas of **number theory** and **mathematical physics** via **algebra**. In particular, I am interested in **Hopf-Galois structures**, which arise in certain number theory problems, and **skew braces**, which provide set-theoretic solutions of the **quantum Yang-Baxter equation** in mathematical physics. One of the main achievements of my research is providing a **classification** for the Hopf-Galois structures and skew braces of order p^3 for a prime number p.

In recent years the study of skew braces have found a particular importance as they rapidly find connections to other areas: they give rise to solutions of the quantum Yang-Baxter equation, parametrise Hopf-Galois structures on Galois extensions of fields, generalise radical rings, also have connections to the representation theory of lie algebras as well as quantum computing. To this end, my main research objective is to gain a deeper understanding on the structure of skew braces and further investigate their connection to the other areas. The results of my investigations will contribute significantly to the relevant literatures in group theory, mathematical physics, and algebraic number theory.

2 Background

2.1 Number Theory

Galois theory is the study of symmetries between roots of a polynomial equation and provides a connection between group theory and field theory. *Hopf-Galois structures* then arise naturally when studying the rings of integers of extensions of number fields as modules. For a field extension L/K a **Hopf-Galois structure** is a Hopf algebra which acts on L satisfying a technical property. For example, if L/K is Galois with group G, then the group algebra $K[G]$, with its natural action on L, endows L/K with a Hopf-Galois structure.

The concept of a Hopf-Galois extension was initially introduced by S. Chase and M. Sweedler [CS69] in 1969 with the aim of providing Galois theory for inseparable extensions of fields. Later, Hopf-Galois theory for separable extensions of fields was studied by C. Greither and B. Pareigis. They showed how to recast the problem of classifying all Hopf-Galois structures on Galois extensions of fields to a problem in group theory. More precisely, they proved that for L/K a finite Galois extension of fields with Galois group G, every Hopf-Galois structure on L/K is of the form $L[N]^G$, for a certain subgroup $N \subset \mathrm{Perm}(G)$. The isomorphism class of N as above is known as the **type** of the Hopf-Galois structure. Their work provided a viable method for classifying Hopf-Galois structures.

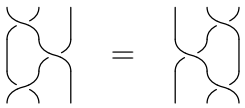
An application of Hopf-Galois structures in Galois module theory is the following. Given an extension of number fields L/K, understanding the structure of the ring of integers $\mathcal{O}_L$ of L is a subject of great interest in Galois module theory. Now for any Hopf algebra H, which endows L/K with a Hopf-Galois structure, one can define the associated order of $\mathcal{O}_L$ in H by

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

and study the behaviour of $\mathcal{O}_L$ as an $\mathfrak{A}_H$-module. It turns out that the structure of $\mathcal{O}_L$ as an $\mathfrak{A}_H$-module is highly dependent on the choice of the Hopf-Galois structure on L/K and this leads to a natural need for the classification of these objects.

2.2 Mathematical Physics

The *Yang-Baxter equation* is one of the basic equations in mathematical physics and statistical mechanics. This equation can be represented by a simple picture



and lies in the foundation of quantum group theory. More precisely, for a vector space V, an element $R \in \mathrm{GL}(V \otimes V)$ is a solution of the **Yang-Baxter equation**, or is called an R-matrix, if

$$(R \otimes \mathrm{id}_V)(\mathrm{id}_V \otimes R)(R \otimes \mathrm{id}_V) = (\mathrm{id}_V \otimes R)(R \otimes \mathrm{id}_V)(\mathrm{id}_V \otimes R)$$

holds in $\mathrm{Aut}(V \otimes V \otimes V)$. This equation was first introduced by Yang and Baxter in statistical mechanics and mathematical physics, it has since found connection to many other areas such as **integrable systems**, **knot theory**, **ring theory**, and **number theory**.

Finding R-matrices can be difficult, so in 1990 V. Drinfeld formulated a number of problems in quantum group theory, one of which was studying the set-theoretic solutions of the Yang-Baxter equation. He suggested studying pairs (X, r) where X is a nonempty set and $r : X \times X \longrightarrow X \times X$ a bijection such that

$$(r \times \mathrm{id})\,(\mathrm{id} \times r)\,(r \otimes \mathrm{id}) = (\mathrm{id} \times r)\,(r \times \mathrm{id})\,(\mathrm{id} \times r)$$

holds; in such case (X, r) is called a **set-theoretic solution** of the Yang-Baxter equation. These solution naturally produce R-matrices for vector spaces generated by X. Later, W. Rump [Rum07a] introduced braces, as a generalisation of radical rings, in order to study *non-degenerate involutive* set-theoretic solutions and found a correspondence between these solutions and braces. Recently, skew braces were introduced by L. Guarnieri and L. Vendramin [GV17] in order to study the non-degenerate (not necessarily involutive) set-theoretic solutions.

A (left) **skew brace** $(B, \oplus, \odot)$ is a set B with two operations $\oplus$, $\odot$ such that $(B, \oplus)$ and $(B, \odot)$ are groups, and the two operations are related by

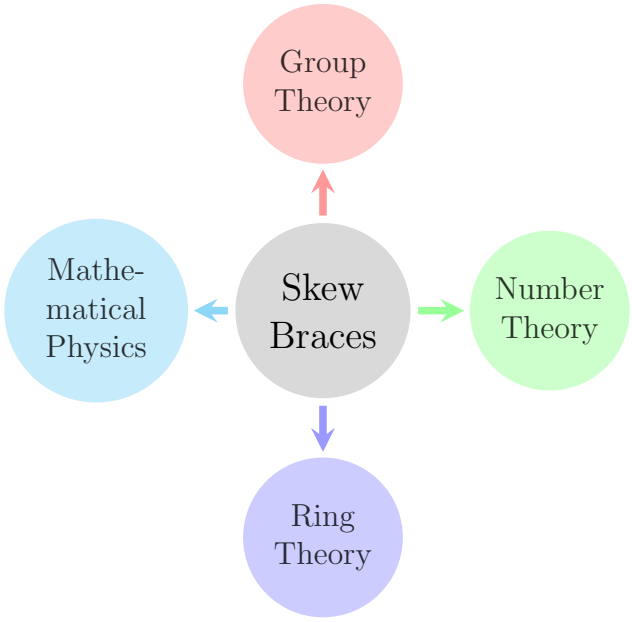
$$a \odot (b \oplus c) = (a \odot b) \ominus a \oplus (a \odot c) \text{ for every } a, b, c \in B.$$

An skew brace $(B, \oplus, \odot)$ is called a brace when $(B, \oplus)$ is an abelian group. The isomorphism class of the group $(B, \oplus)$ is known as the **type** of the skew brace $(B, \oplus, \odot)$.

It turns out that for a skew brace $(B, \oplus, \odot)$ the map

$$\begin{aligned} r_B : B \times B &\longrightarrow B \times B \\ (a, b) &\longmapsto \big(\ominus a \oplus (a \odot b), (\ominus a \oplus (a \odot b))^{-1} \odot a \odot b\big) \end{aligned}$$

gives a non-degenerate set-theoretic solution of the Yang-Baxter equation. Skew braces have since found connections to many other areas such as ring theory and number theory as well as mathematical physics. For example, some connections of skew braces to ring theory and Hopf-Galois theory was studied by N. Byott, A. Smoktunowicz, and L. Vendramin [SV18]. Understanding the structure of skew braces and their connection and applications to other areas, as well as obtaining a good classification of skew braces of a given order, are among the main topics of study in this area.



2.3 Connection Between Hopf-Galois Structures and Skew Braces

An interesting discovery, noticed first by D. Bachiller, linked Hopf-Galois theory to skew braces. In particular, it can be shown that for a Galois extension of fields L/K with Galois group G there exists a bijective correspondence

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

and so **skew braces parametrise Hopf-Galois structures**. This creates a new bridge between number theory and mathematical physics. The above connection is what makes the research in these topics exhilarating since by studying skew braces one can expect at the same time as finding information relating to the non-degenerate set-theoretic solutions of the Yang-Baxter equation to find information relating to Hopf-Galois theory and vice versa. In particular, as this discovery is relatively new there are numerous open problems and the translation of results and tools from one area to another has not yet been fully established.

3 Main Contributions

The classification of Hopf-Galois structures and skew braces remain among important topics of study, for example see [Byo96, Byo04, Byo07, Koh98, CC99, AB18, TS18] for results in Hopf-Galois theory and [Rum07b, Bac15, CCS18, Die18] for skew braces. To this end, among the main achievements of my research is **the classification of Hopf-Galois structures on field extensions of degree p^3 and skew braces of size p^3 for a prime number p** in [NZ18, NZ19, PhD Thesis and an extracted article accepted for publication in the Journal of Algebra]. These results thus enable us to obtain a classification for the set-theoretic solutions

of the Yang-Baxter equation (X, r) with the cardinality of X equal to p^3. In particular, I can also determine the automorphism groups, structure groups, socles, and annihilators of the skew braces we classify. A summary of my findings is provided below (cf. [NZ18, Section 4.6] and [NZ19]), where p is assumed to be greater than 3 for simplicity.

Theorem 3.1. *Let L/K be a Galois extension of fields of degree p^3 for a prime $p > 3$ with Galois group G. Then the number of Hopf-Galois structures on L/K of type N, $e(G, N)$, is given by the table*

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

Table 1: Number of Hopf-Galois structures of order p^3 for $p > 3$

where rows correspond to G and columns to N.

Theorem 3.2. *Let G be a group of order p^3 for a prime $p > 3$. Then the number of G-skew braces of type N, $\widetilde{e}(G, N)$, is given by the table*

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

Table 2: Number of skew braces of order p^3 for $p > 3$

where rows correspond to G and columns to N.

Remark 3.3. In Table 3.1 we have $p^2 \mid e(G, N)$ and

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

In Table 3.2 we have

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

4 Research Projects

There are a vast number of open problems in my area, for example see [Ven18] for some of these relating to skew braces. However, my main projects focus on there avenues in which I am expanding my results, a brief summary of these is listed below.

1. Skew braces in group theory: The generalisations of patterns observed in our results have become one of the main subjects of our further research. In particular, I would like to know under what conditions on G and N we must have

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

Answering this question is very important as it provides a simplification for the classification of skew braces and Hopf-Galois structures. There are two ways in which I am currently attacking this problem. I have already established that the relationship above holds for cases when N has a special semi-direct product form, in this way our next step is to study skew braces whose type is an extension of two groups and prove under what conditions we have $\widetilde{e}\,(G,N) = \widetilde{e}\,(N,G)$. My second gaol is to study skew braces (and Hopf-Galois structures) whose type is a group of the form

$$\left(C_{p^e} \times C_{p^f}\right) \rtimes C_{p^g},$$

for positive integers e, f, g, for some prime p to find an explicit classification for these objects through generalising our methods. Currently, I am composing a paper studying skew braces of type $C_{p^e} \rtimes C_p$, which uses a direct generalisation of methods in our PhD thesis, but studying groups of the form $\left(C_{p^e} \times C_{p^f}\right) \rtimes C_{p^g}$ is a significantly more complex proposal and will lead to significant discoveries in the theory of finite p-groups, p-skew braces, and properties of p-extensions of global fields.

2. Skew braces in Galois module theory: Since skew braces parametrise Hopf-Galois structures, my second project is concerned with the study of invariants of families of Hopf-Galois structures which correspond to a skew brace. In particular, I use my classification of Hopf-Galois structures to study integral Hopf-Galois structures for p^3-extensions of p-adic fields. Similar work to this was done, for example, by N. Byott [Byo02] for p^2-extensions of p-adic fields. N. Byott by using a classification of Hopf-Galois structures studies a totally ramified normal extension of p-adic fields L/K of degree p^2 to understand the behaviour of the valuation ring $\mathcal{O}_L$ in various Hopf-Galois structures on L/K. Using my results, Byott's results can now be further extended to the case of normal extension of p-adic fields of degree p^3. Through this project I aim to deepen my understanding of the connections between skew braces and Hopf-Galois theory.

3. Skew braces in ring theory: Skew braces generalise radical rings: if $(B, \oplus, \odot)$ is a two-sided brace, i.e., $(B, \oplus)$ is abelian and

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

then $(B, \oplus, \otimes)$ where

$$a \otimes b = \ominus a \oplus (a \odot b) \ominus b$$

is a radical ring, so one can use ring theoretic tools to study $(B, \oplus, \otimes)$. Now when $(B, \oplus, \odot)$ is any general skew brace, one can still define the operation

$$a \otimes b = \ominus a \oplus (a \odot b) \ominus b,$$

but now $(B, \oplus, \otimes)$ is far from being a ring in general, although it should still be possible to use some ring (near-ring) theoretic methods to study this object. This line of research

was initially looked into by by A. Konovalov, A. Smoktunowicz, L. Vendramin in [KSL18] to study the ideals of skew braces, but the full structure and properties of $(B, \oplus, \otimes)$ remain unknown. In this project I investigate the structure of $(B, \oplus, \otimes)$ and determine what ring theoretic tools are available when studying this object.

5 Delivery Plan and Expected Output

I expect the first two items in my research projects to take around a 1 year for completion, with a minimum output of two papers, which would be aimed for publications in either Journal of Algebra, Journal of Combinatorial Algebra, or the Journal of Algebra and its Application. The third item in my research projects is expected to take at least 6 months to around a year to complete, and I plan to receive a further publication from this item.

References

[AB18] Ali A. Alabdali and Nigel P. Byott. Counting Hopf-Galois structures on cyclic field extensions of squarefree degree. *J. Algebra*, 493:1–19, 2018.

[Bac15] David Bachiller. Classification of braces of order p^3. *J. Pure Appl. Algebra*, 219(8):3568–3603, 2015.

[Byo96] N. P. Byott. Uniqueness of Hopf-Galois structure for separable field extensions. *Comm. Algebra*, 24(10):3217–3228, 1996.

[Byo02] Nigel P. Byott. Integral Hopf-Galois structures on degree p^2 extensions of p-adic fields. *J. Algebra*, 248(1):334–365, 2002.

[Byo04] Nigel P. Byott. Hopf-Galois structures on Galois field extensions of degree pq. *J. Pure Appl. Algebra*, 188(1-3):45–57, 2004.

[Byo07] Nigel P. Byott. Hopf-Galois structures on almost cyclic field extensions of 2-power degree. *J. Algebra*, 318(1):351–371, 2007.

[CC99] Scott Carnahan and Lindsay Childs. Counting Hopf-Galois structures on non-abelian Galois field extensions. *J. Algebra*, 218(1):81–92, 1999.

[CCS18] Francesco Catino, Ilaria Colazzo, and Paola Stefanelli. Skew left braces with non-trivial annihilator. *Journal of Algebra and Its Applications*, 2018.

[CS69] Stephen U. Chase and Moss E. Sweedler. *Hopf algebras and Galois theory*. Lecture Notes in Mathematics, Vol. 97. Springer-Verlag, Berlin-New York, 1969.

[Die18] Carsten Dietzel. Braces of order p^2q. *Preprint on ArXiv.org*, Feb 2018. https://arxiv.org/abs/1801.06911.

[GV17] L. Guarnieri and L. Vendramin. Skew braces and the Yang-Baxter equation. *Math. Comp.*, 86(307):2519–2534, 2017.

[Koh98] Timothy Kohl. Classification of the Hopf-Galois structures on prime power radical extensions. *J. Algebra*, 207(2):525–546, 1998.

[KSL18] A. Konovalov, A. Smoktunowicz, and Vendramin L. On skew braces and their ideals. *Preprint on ArXiv.org*, Apr 2018. https://arxiv.org/abs/1804.04106.

[NZ18] Kayvan Nejabati Zenouz. *On Hopf-Galois Structures and Skew Braces of Order p^3*. The University of Exeter, PhD Thesis, Supervised by Prof N. Byott, Funded by EPSRC DTG, January 2018. https://ore.exeter.ac.uk/repository/handle/10871/32248.

[NZ19] Kayvan Nejabati Zenouz. Skew Braces and Hopf-Galois Structures of Heisenberg Type. *J. Algebra*, Jan 2019. https://doi.org/10.1016/j.jalgebra.2019.01.012.

[Rum07a] Wolfgang Rump. Braces, radical rings, and the quantum Yang-Baxter equation. *J. Algebra*, 307(1):153–170, 2007.

[Rum07b] Wolfgang Rump. Classification of cyclic braces. *J. Pure Appl. Algebra*, 209(3):671–685, 2007.

[SV18] Agata Smoktunowicz and Leandro Vendramin. On skew braces (with an appendix by N. Byott and L. Vendramin). *J. Comb. Algebra*, 2(1):47–86, 2018.

[TS18] Crespo Teresa and Marta Salguero. Hopf galois structures on separable field extensions of odd prime power degree. *Preprint on ArXiv.org*, Jul 2018. https://arxiv.org/abs/1807.11409.

[Ven18] Leandro Vendramin. Problems on skew left braces. *Preprint on ArXiv.org*, Sep 2018. https://arxiv.org/abs/1807.06411.