Journal of Algebra 524 (2019) 187–225

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

# Skew braces and Hopf–Galois structures of Heisenberg type

Kayvan Nejabati Zenouz

*School of Engineering, Computing and Mathematics, Oxford Brookes University, Oxford, OX33 1HX, United Kingdom of Great Britain and Northern Ireland*

A R T I C L E I N F O

*Article history:*
Received 17 May 2018
Available online 28 January 2019
Communicated by Nicolás Andruskiewitsch

*Keywords:*
Skew braces
Hopf–Galois structures
Heisenberg group
Field extensions
The Yang–Baxter equation

A B S T R A C T

We classify all skew braces of Heisenberg type for a prime number $p > 3$. Furthermore, we determine the automorphism group of each one of these skew braces (as well as their socle and annihilator). Hence, by utilising a link between skew braces and Hopf–Galois theory, we can determine all Hopf–Galois structures of Heisenberg type on Galois field extensions of fields of degree $p^3$.



**Contents**



*E-mail address:* knejabati-zenouz@brookes.ac.uk.

https://doi.org/10.1016/j.jalgebra.2019.01.012
0021-8693/

## 1. Introduction

Braces were introduced by W. Rump [1], as a generalisation of radical rings, in order to study the non-degenerate involutive set-theoretic solutions of the quantum Yang–Baxter equation. He also obtained a correspondence between these solutions and braces. Later, through the efforts of D. Bachiller, F. Cedó, E. Jespers, and J. Okniński [2,3] the classification of involutive set-theoretic solutions of the quantum Yang–Baxter equation was reduced to that of braces, and they provided many new classes of such solutions. Recently, skew braces were introduced by L. Guarnieri and L. Vendramin [4] in order to study the non-degenerate (not necessarily involutive) set-theoretic solutions.

On the other hand, S. Chase and M. Sweedler [5] introduced the concept of Hopf–Galois extensions in order to generalise the classical Galois theory. Later, Hopf–Galois theory for separable extensions of fields was studied by C. Greither and B. Pareigis [6]. They showed how to recast the problem of classifying all Hopf–Galois structures on a finite separable extension of fields as a problem in group theory. Many advances relating to the classification of Hopf–Galois structures were made by N. Byott [7–9], S. Carnahan, L. Childs [10], and T. Kohl [11]. Recent work by A. Alabadi and N. Byott [12] studied the cyclic extensions of fields of squarefree degree, also T. Crespo and M. Salguero obtained results on the properties of Hopf–Galois structures on a separable field extension of degree $p^n$ [13].

A fruitful discovery, which was initially noticed by D. Bachiller [14], revealed a connection between Hopf–Galois theory and skew braces, which linked the classification of Hopf–Galois structures to that of skew braces; thus making skew braces objects of interest in number theory as well as group theory, ring theory, and mathematical physics. The connection of skew braces to ring theory and Hopf–Galois structures was further studied by N. Byott, A. Smoktunowicz, and L. Vendramin [15]. L. Childs [16] investigated certain correspondence between Hopf–Galois structures and skew braces.

Despite many efforts both the classification of skew braces and Hopf–Galois structures remain widely open. For example, in [17] cyclic braces were classified, and in [18] braces of order $p^3$ were classified. Recently, in [19] a method for describing skew braces with non-trivial annihilator was given, and braces of order $p^2q$ have been studied in [20]. The classification and understanding the structure of skew braces has become more important as they find connections to other areas, for example to concepts in ring theory, see [21,22], and quantum information [23], as well as number theory. Recently, a list of open problems on skew braces has been posed by L. Vendramin [24], a few of which were looked at by T. Nasybullov [25].

To this end, in the author's PhD thesis [26], an explicit and complete classification of skew braces and Hopf–Galois structures of order $p^3$ for a prime number $p$ was provided.

In particular, the work includes an independent proof of the results by D. Bachiller [18] on braces of order $p^3$. In this paper, as our main results, we provide a classification for skew braces and Hopf–Galois structures of Heisenberg type for a prime $p$, which we have chosen to be greater than 3 for simplicity. However, our methods can be adapted for $p = 2, 3$ as well ($p = 2, 3$ has been treated in the author's PhD thesis). We classify these skew braces and Hopf–Galois structures using methods of N. Byott [8] and by conducting a deep study into the holomorph of the Heisenberg group.

Furthermore, we determine the automorphism group of each skew brace that we classify, and as a result we are able to determine all the Hopf–Galois structures of Heisenberg type on a Galois field extensions of degree $p^3$. In our subsequent two papers we aim to provide our findings relating to the classification of skew braces and Hopf–Galois structures of Extraspecial type (of the type $C_{p^2} \rtimes C_p$) in one paper, and skew braces and Hopf–Galois structures of type $C_p^3$ in the second paper. These results are currently available in the author's PhD thesis [26] Sections 4.2, 4.3, and 4.5.

We shall begin by providing relevant background information and stating a summary of our main results in the next subsection. The subsequent sections are devoted to the calculations relating to proofs. In particular, Lemmas 4.2, 4.4, and 4.6 are devoted to the classification of skew braces. In Subsection 4.1 there is a list of all skew braces classified in this paper. The automorphism groups of these skew braces and the number of corresponding Hopf–Galois structures are determined in Lemmas 4.3, 4.5, and 4.6. For readers interested to have the list of regular subgroups of the holomorphs of groups of order $p^3$, we refer them to the author's PhD thesis [26]. Finally, we determine the *socle* and *annihilator* of these skew braces. We show that there are non-trivial skew braces of Heisenberg type with trivial socle and annihilator, so these cannot be described by methods of [19].

### 1.1. Background

A *skew (left) brace* [cf. 15] 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 (they need not be abelian), and the two operations are related by the *skew brace property*:

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

where $\ominus a$ is the inverse of $a$ with respect to the operation $\oplus$. The group $(B, \oplus)$ is known as the *additive group* of the skew brace $(B, \oplus, \odot)$ and $(B, \odot)$ as the *multiplicative group*. A morphism, or a map, between two skew braces

$$\varphi : (B_1, \oplus_1, \odot_1) \longrightarrow (B_2, \oplus_2, \odot_2)$$

is a map of sets $\varphi : B_1 \longrightarrow B_2$ such that the maps

$$\varphi : (B_1, \oplus_1) \longrightarrow (B_2, \oplus_2) \text{ and } \varphi : (B_1, \odot_1) \longrightarrow (B_2, \odot_2)$$

are group homomorphisms; the map $\varphi$ is an isomorphism if it is a bijection.

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** $N$; we refer to the *isomorphism type* of $(B, \odot)$ as the **structure** of the skew brace $(B, \oplus, \odot)$. If $\oplus$ is abelian, nonabelian respectively, we call $(B, \oplus, \odot)$ a skew brace of abelian, nonabelian type respectively. We note that a skew brace of abelian type coincides with the one that was initially defined by W. Rump called a brace (aka a classical brace). Skew braces provide non-degenerate (not necessarily involutive) set-theoretic solutions of the quantum Yang–Baxter equation. The paper of A. Smoktunowicz, and L. Vendramin (also N. Byott) [15] provides an excellent introduction to skew braces and their connection to noncommutative algebra, mathematical physics, and other areas.

We recall some definitions and facts relating to Hopf–Galois structures and their connection to skew braces. For $L/K$ a finite Galois extension of fields with Galois group $G$, a *Hopf–Galois structure* on $L/K$ consists of a finite dimensional cocommutative $K$-*Hopf algebra* $H$, with an action on $L$, which makes $L$ into an $H$-*Galois extension*, i.e., $H$ acts on $L$ in such way that the $K$-module homomorphism

$$j : L \otimes_K H \longrightarrow \mathrm{End}_K(L) \text{ given by } j(x \otimes y)(z) = xy(z) \text{ for } x, z \in L, y \in H$$

is an isomorphism. For example, the group algebra $K[G]$ endows $L/K$ with the *classical* Hopf–Galois structure. However, in general there can be more than one Hopf–Galois structure on $L/K$. Hopf–Galois structures have many applications in Galois module theory, for example, when studying the freeness of rings of integers of extensions of global or local fields as modules (e.g., see [27]). Through the work of C. Greither and B. Pareigis [6] the classification of Hopf–Galois structures was reduced to a group theoretic problem via the following theorem.

**Theorem 1.1** *(C. Greither and B. Pareigis). Hopf–Galois structures on $L/K$ correspond bijectively to regular subgroups $N \subseteq \mathrm{Perm}(G)$ which are normalised by the image of $G$, as left translations, inside* $\mathrm{Perm}(G)$.

In particular, every $K$-Hopf algebra $H$ which endows $L/K$ with a Hopf–Galois structure is of the form $L[N]^G$ for some $N \subseteq \mathrm{Perm}(G)$ a regular subgroup normalised by the image of $G$, as left translations, inside $\mathrm{Perm}(G)$. Here $G$ acts on the group algebra $L[N]$ through its action on $L$ as field automorphism and on $N$ by conjugation inside $\mathrm{Perm}(G)$. Subsequently, the *isomorphism type* of $N$ became known as the **type** of the Hopf–Galois structure, and we shall refer to the cardinality of $N$, which is the same as the degree of the extension $L/K$, as the **order** of the Hopf–Galois structure.

The connection between Hopf–Galois structures and braces was initially noticed by D. Bachiller [14], later this connection was made more explicit by N. Byott and L. Vendramin in [15]. For example, one can prove (see Section 2) that given a $G$-skew brace $(B, \oplus, \odot)$, the map

$$d : (B, \oplus) \longmapsto \mathrm{Perm}\,(B, \odot)$$
$$a \longmapsto (d_a : b \longmapsto a \oplus b) \ \text{ for all } a, b \in B$$

is a regular embedding, i.e., $d$ is an injective map whose image $\mathrm{Im}\,d$ is a regular subgroup. In particular, $\mathrm{Im}\,d$ is normalised by the image of $(B, \odot)$ in $\mathrm{Perm}\,(B, \odot)$. This together with Theorem 1.1 enables us to obtain a Hopf–Galois structure on $L/K$. Conversely, one always obtains a skew brace from a Hopf–Galois structure. However, there are more Hopf–Galois structures than skew braces, in particular skew braces parametrise Hopf–Galois structures.

Finally, we remark that since working with $\mathrm{Perm}(G)$ can often be difficult, as it becomes rapidly large as size of $G$ increases, in order to overcome this, N. Byott [7] proves the following statement – here L. Childs reformulation [cf. 28, p. 57, (7.3) Theorem (Byott)] is given.

**Theorem 1.2** *(N. Byott). Let $N$ be a group. Then there is a bijection between the sets*

$$\mathcal{N} \stackrel{\mathrm{def}}{=} \{\alpha : N \hookrightarrow \mathrm{Perm}(G) \mid \alpha(N) \text{ is regular on } G\} \ \ \textit{and}$$
$$\mathcal{G} \stackrel{\mathrm{def}}{=} \{\beta : G \hookrightarrow \mathrm{Perm}(N) \mid \beta(G) \text{ is regular on } N\}\,.$$

*Under this bijection, if $\alpha, \alpha' \in \mathcal{N}$ correspond to $\beta, \beta' \in \mathcal{G}$, then $\alpha(N) = \alpha'(N)$ if and only if $\beta(G)$ and $\beta'(G)$ are conjugate by an element of* $\mathrm{Aut}(N)$. *Furthermore, $\alpha(N)$ is normalised by the left translation if and only if $\beta(G)$ is contained in* $\mathrm{Hol}(N)$.

Using Theorem 1.2, N. Byott shows that if $e'(G, N)$ is the number of regular subgroups of $\mathrm{Hol}(N)$ isomorphic to $G$, then the number of Hopf–Galois structures on $L/K$ of type $N$ is given by

$$e(G, N) = \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|} e'(G, N). \tag{1}$$

In the author's thesis [26] we used formula (1) to find the number of Hopf–Galois structures, but in the current paper we parametrise Hopf–Galois structures along skew braces and count them using the orbit stabiliser theorem. We obtain the same results, but in the process we additionally find the automorphism groups of our skew braces too.

### 1.2. Summary of the main results

We give a summary of our main results in this subsection. First, for the rest of this paper we shall assume $p > 3$ is a prime number. We shall denote by $C_{p^r}$ the cyclic group of order $p^r$ for any natural number $r$. Unless otherwise stated we shall always assume $G$ and $N$ are finite groups.

Recall there are two nonabelian groups of order $p^3$: the exponent $p$ nonabelian group of order $p^3$, or otherwise known as the Heisenberg group,

$$M_1 \stackrel{\text{def}}{=} \langle \rho, \sigma, \tau \mid \rho^p = \sigma^p = \tau^p = 1,\ \sigma\rho = \rho\sigma,\ \tau\rho = \rho\tau,\ \tau\sigma = \rho\sigma\tau \rangle \cong C_p^2 \rtimes C_p,$$

and the exponent $p^2$ nonabelian group of order $p^3$, or otherwise known as the Extraspecial group of order $p^3$,

$$M_2 \stackrel{\text{def}}{=} \left\langle \sigma, \tau \mid \sigma^{p^2} = \tau^p = 1,\ \tau\sigma = \sigma^{p+1}\tau \right\rangle \cong C_{p^2} \rtimes C_p.$$

In this paper we are concerned with $M_1$. We fix as our type the group $M_1$ and find all skew braces and Hopf–Galois structures of type $M_1$. The main results of this paper can be summarised as follows.

**Theorem 1.3.** *The skew braces of $M_1$ type are precisely*

$$2p^2 - p + 3$$

*$M_1$-braces and*

$$2p + 1$$

*$C_p^3$-braces.*

**Proof.** Follows from adding the numbers found in Lemmas 4.2, 4.4, 4.6 of Section 4, see Proposition 4.1. □

**Theorem 1.4.** *Let $L/K$ be an $M_1$ extension of fields. Then there are*

$$(2p^3 - 3p + 1)p^2$$

*Hopf–Galois structures of $M_1$ type. Let $L/K$ be a $C_p^3$ extension of fields. Then there are*

$$(p^3 - 1)(p^2 + p - 1)p^2$$

*Hopf–Galois structures of $M_1$ type.*

**Proof.** Follows from adding the numbers found in Lemmas 4.3, 4.5, 4.6 of Section 4 see Proposition 4.1. □

## 2. Preliminaries

In this section we provide the necessary preliminaries and describe our strategy for classifying skew braces and Hopf–Galois structures.

### 2.1. Skew braces and Hopf–Galois structures

The following proposition provides an explicit connection between Hopf–Galois structures and skew braces (where ideas of the proof are similar to [15, Proposition A.3]).

**Proposition 2.1** *(Skew braces and Hopf–Galois structures correspondence). There exists a bijective correspondence between isomorphism classes of $G$-skew braces and classes of Hopf–Galois structures on an extension $L/K$ with Galois group $G$, where we identify two Hopf algebras $L[N_1]^G$ and $L[N_2]^G$ giving Hopf–Galois structures (as in Theorem 1.1) on $L/K$ if $N_2 = \alpha N_1 \alpha^{-1}$ for some $\alpha \in \mathrm{Aut}(G)$.*

**Proof.** Let $(B, \oplus, \odot)$ be a $G$-skew brace i.e., $(B, \odot) \cong G$, we can assume $(B, \odot) = G$. Then the map

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

is a regular embedding. Now, for any $a \in (B, \oplus)$ and $b, c \in (B, \odot)$, using the skew brace property, we have

$$b \odot \left(d_a \left(b^{-1} \odot c\right)\right) = b \odot \left(a \oplus \left(b^{-1} \odot c\right)\right) = ((b \odot a) \ominus b) \oplus c = d_{(b \odot a) \ominus b}(c),$$

where $b^{-1}$ is the inverse of $b$ with respect to $\odot$. This shows that the image of $(B, \oplus)$ is normalised by the image of $(B, \odot)$ inside $\mathrm{Perm}\,(B, \odot)$ as left translations. We also find an action of $(B, \odot)$ on $(B, \oplus)$ by $b \cdot a = (b \odot a) \ominus b$ for $b \in (B, \odot)$ and $a \in (B, \oplus)$. Now for

$$\alpha : (B, \oplus_1, \odot) \longrightarrow (B, \oplus_2, \odot)$$

an isomorphism of skew braces, we have a commutative diagram

$$\begin{array}{ccc} (B, \oplus_1) & \overset{d_1}{\hookrightarrow} & \mathrm{Perm}\,(B, \odot) \\ \wr \downarrow \alpha & & \wr \downarrow C_\alpha \\ (B, \oplus_2) & \overset{d_2}{\hookrightarrow} & \mathrm{Perm}\,(B, \odot), \end{array}$$

where $C_\alpha$ is conjugation by $\alpha \in \mathrm{Aut}\,(B, \odot)$ inside $\mathrm{Perm}\,(B, \odot)$. Furthermore, if we fix a Galois extension of fields $L/K$ with Galois group $(B, \odot)$, then $L[(B, \oplus)]^{(B, \odot)}$ endows $L/K$ with a Hopf–Galois structure corresponding to the skew brace $(B, \oplus, \odot)$ and when two skew braces with the same multiplication group are isomorphic then the corresponding Hopf–Galois structures can be identified.

Conversely, suppose we have a Hopf–Galois structure on $L/K$ which can always be given by $L[N]^G$ for some regular subgroup $N \subseteq \mathrm{Perm}(G)$ which is normalised by the image of $G$ as left translations inside $\mathrm{Perm}(G)$. The fact that $N$ is a regular subgroup implies that the map

$$\begin{aligned} \epsilon : \mathrm{Perm}(G) &\longrightarrow G \\ \eta &\longmapsto \eta \cdot 1_G, \end{aligned}$$

induces a bijection $\phi = \epsilon|_N : N \longrightarrow G$, $\epsilon$ restricted to $N$, as subgroups of $\mathrm{Perm}(G)$. Now we can define a skew brace $B$ by setting $(B, \odot) \stackrel{\text{def}}{=} G$, considered as a subgroup of $\mathrm{Perm}(G)$ via the left translations, and defining

$$g_1 \oplus g_2 \stackrel{\text{def}}{=} \phi\left(\phi^{-1}(g_1)\phi^{-1}(g_2)\right) \text{ for } g_1, g_2 \in G.$$

The fact that $N \subseteq \mathrm{Perm}(G)$ is normalised by $G$ implies that for all $g \in G$ and $n \in N$ we have $gn = f_{g,n}g$ for some $f_{g,n} \in N$. Therefore, for $g_1 = \phi(n_1), g_2 = \phi(n_2), g_3 = \phi(n_3) \in G$, we aim to show

$$g_1 \odot (g_2 \oplus g_3) = (g_1 \odot g_2) \ominus g_1 \oplus (g_1 \odot g_3).$$

Note by definition we have

$$g_1 \odot (g_2 \oplus g_3) = \phi(n_1) \odot (\phi(n_2) \oplus \phi(n_3)) = \phi(n_1)\phi(n_2 n_3).$$

Now consider the element $\phi(n_1)n_2n_3 \in \mathrm{Perm}(G)$. Using the relation $gn = f_{g,n}g$ we have

$$\phi(n_1)n_2n_3 = f_{\phi(n_1),n_2n_3}\phi(n_1)$$

for some $f_{\phi(n_1),n_2n_3} \in N$. Now applying $\epsilon$ to both side we get the relation

$$\phi(n_1)\phi(n_2n_3) = f_{\phi(n_1),n_2n_3}(\phi(n_1))$$

in $G$. Note, in general for elements $\eta$ and $\rho$ of $\mathrm{Perm}(G)$ we have

$$\epsilon(\eta\rho) = (\eta\rho) \cdot 1_G = \eta(\rho \cdot 1_G) = \eta(\epsilon(\rho)),$$

so $f_{\phi(n_1),n_2n_3}(\phi(n_1)) = \phi\left(f_{\phi(n_1),n_2n_3}n_1\right)$ in $G$. Note also that $f_{g,n}$ is a homomorphism on $n$:

$$f_{g,n_1n_2}g = gn_1n_2 = f_{g,n_1}gn_2 = f_{g,n_1}f_{g,n_2}g$$

Therefore, we find

$$\begin{aligned} g_1 \odot (g_2 \oplus g_3) &= \phi\left(f_{\phi(n_1),n_2 n_3} n_1\right) = \phi\left(f_{\phi(n_1),n_2} f_{\phi(n_1),n_3} n_1\right) \\ &= \phi\left(\phi^{-1}\phi\left(f_{\phi(n_1),n_2} n_1\right) n_1^{-1} \phi^{-1}\phi\left(f_{\phi(n_1),n_3} n_1\right)\right) \\ &= \phi\left(\phi^{-1}\left(\phi(n_1)\phi(n_2)\right) n_1^{-1} \phi^{-1}\left(\phi(n_1)\phi(n_3)\right)\right) \\ &= \phi\left(\phi^{-1}\left(g_1 g_2\right)\left(\phi^{-1}(g_1)\right)^{-1} \phi^{-1}\left(g_1 g_3\right)\right) \\ &= (g_1 \odot g_2) \ominus g_1 \oplus (g_1 \odot g_3), \end{aligned}$$

thus we have a skew brace $(B, \oplus, \odot)$ which is a $G$-skew brace of type $N$. In particular, if $N_1 \subseteq \mathrm{Perm}(G)$ is a regular subgroup whose image is normalised by $G$ and $\alpha \in \mathrm{Aut}(G)$, then $N_2 \overset{\mathrm{def}}{=} \alpha N_1 \alpha^{-1}$ is a regular subgroup whose image is normalised by $G$, and the two skew braces corresponding to $N_1$ and $N_2$ are isomorphic by $\alpha$. □

**Remark 2.2.** Note in fact Proposition 2.1 above is implied by Theorem 1.2 and [15, Proposition A.3]. We shall state [15, Proposition A.3] later (see Proposition 2.5). However, we decided to include the calculations for a direct proof of Proposition 2.1 for completeness, which leads to an explicit relationship between the Hopf–Galois structures and skew braces. The question relating to the explicit relationship between the Hopf–Galois structures and skew braces was first asked from the author by Prof Agata Smoktunowicz. The answer can be reached by unravelling Theorem 1.2 and [15, Proposition A.3] which is what has been done in Proposition 2.1.

The above proposition also helps us to understand the automorphism groups of skew braces.

**Corollary 2.3** *(Automorphism groups of skew braces). Let $(B, \oplus, \odot)$ be a skew brace. Then there exists a natural identification*

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

**Proof.** Note that if $(B, \oplus, \odot)$ is a skew brace and

$$\alpha : (B, \oplus, \odot) \longrightarrow (B, \oplus, \odot)$$

an automorphism, we obtain a commutative diagram

$$\begin{array}{ccc} (B, \oplus) & \overset{d}{\hookrightarrow} & \mathrm{Perm}\,(B, \odot) \\ \wr\downarrow \alpha & & \wr\downarrow C_\alpha \\ (B, \oplus) & \overset{d}{\hookrightarrow} & \mathrm{Perm}\,(B, \odot)\,, \end{array}$$

implying that $\alpha\,(\operatorname{Im} d)\,\alpha^{-1} \subseteq \operatorname{Im} d$. On the other hand, if $\alpha\,(\operatorname{Im} d)\,\alpha^{-1} \subseteq \operatorname{Im} d$ for some $\alpha \in \operatorname{Aut}(B, \odot)$, then $\alpha$ gives rise to an automorphism of $(B, \oplus, \odot)$. From this observation one can see that

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

Next corollary shows how to obtain the number of Hopf–Galois structures using skew braces. Let $e(G, N)$ be the number of Hopf–Galois structures of type $N$ on the field extension $L/K$ whose Galois group is $G$. Denote by $G_N$ the isomorphism class of a $G$-skew brace of type $N$. For later use we also set $\widetilde{e}(G, N)$ to be the number of isomorphism classes of $G$-skew braces of type $N$.

**Corollary 2.4** *(Number of Hopf–Galois structures parametrised by skew braces). We have*

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

**Proof.** Fix $G$ and let

$$\mathcal{S}(G, N) = \{M \subseteq \operatorname{Perm}(G) \mid M \cong N \text{ and } M \text{ is regular normalised by } G\}.$$

Firstly, note that $\operatorname{Aut}(G)$ acts on $\mathcal{S}(G, N)$, induced by conjugation in $\operatorname{Perm}(G)$, and a set of orbit representatives, say $\{N_1, ..., N_s\}$, give a list of non-isomorphic skew braces according to Proposition 2.1. Secondly, by Theorem 1.1 we find $e(G, N) = |\mathcal{S}(G, N)|$, and so we have

$$e(G, N) = \sum_{i=1}^{s} |\operatorname{Orb}(N_i)| = \sum_{i=1}^{s} \frac{|\operatorname{Aut}(G)|}{|\operatorname{Stab}(N_i)|} = \sum_{G_N} \frac{|\operatorname{Aut}(G)|}{|\operatorname{Aut}_{\mathcal{B}r}(G_N)|}. \quad \square$$

Therefore, to find skew braces and Hopf–Galois structures of order $n$, it suffices to find the regular subgroups $N \subseteq \operatorname{Perm}(G)$ for every group $G$ of size $n$. However, in many cases $\operatorname{Perm}(G)$ can be too large to handle. Fortunately, by somehow reversing the role of $G$ and $N$, instead of studying the regular subgroups of $\operatorname{Perm}(G)$, one can study regular subgroups of a smaller group, the *holomorph* of $N$:

$$\operatorname{Hol}(N) \overset{\text{def}}{=} N \rtimes \operatorname{Aut}(N) = \{\eta\alpha \mid \eta \in N,\ \alpha \in \operatorname{Aut}(N)\},$$

also we can organise these objects in an easily manageable manner as we shall explain shortly. These ideas in Hopf–Galois theory were initially developed by N. Byott [7,8].

Let us start with skew braces. Suppose $(B, \oplus, \odot)$ is a skew brace. Then the group $(B, \odot)$ acts on $(B, \oplus)$ by $(a, b) \longmapsto a \odot b$, and we obtain a map

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

which is a regular embedding. To see this one needs to check that the map

$$\begin{aligned} \lambda_a : (B, \oplus) &\longrightarrow (B, \oplus) \\ b &\longmapsto \ominus a \oplus (a \odot b) \end{aligned}$$

is an automorphism, and that the map

$$\begin{aligned} \lambda : (B, \odot) &\longmapsto \operatorname{Aut}(B, \oplus) \\ a &\longmapsto \lambda_a \end{aligned}$$

is a group homomorphism. Then one has $m_a = a\lambda_a \in \operatorname{Hol}(B, \oplus)$ for all $a \in B$. Additionally, for $\alpha : (B, \oplus, \odot_1) \longrightarrow (B, \oplus, \odot_2)$ an isomorphism of skew braces, we have

$$\begin{array}{ccc} (B, \odot_1) & \xhookrightarrow{m_1} & \operatorname{Hol}(B, \oplus) \\ \wr \downarrow \alpha & & \wr \downarrow C_\alpha \\ (B, \odot_2) & \xhookrightarrow{m_2} & \operatorname{Hol}(B, \oplus), \end{array}$$

where $C_\alpha$ is conjugation by $\alpha \in \operatorname{Aut}(B, \oplus)$ considered naturally as an element of $\operatorname{Hol}(B, \oplus)$. This with similar procedure as used to prove Proposition 2.1 gives the following proposition of [15].

**Proposition 2.5.** *There exists a bijective correspondence between isomorphism classes of skew braces of type $N$ and classes of regular subgroups of* $\operatorname{Hol}(N)$ *under conjugation by elements of* $\operatorname{Aut}(N)$.

**Proof.** [15, Proposition A.3]. □

In particular, we find another way of computing the automorphism groups of skew braces:

$$\operatorname{Aut}_{\mathcal{B}r}(B, \oplus, \odot) \cong \left\{ \alpha \in \operatorname{Aut}(B, \oplus) \mid \alpha (\operatorname{Im} m) \alpha^{-1} \subseteq \operatorname{Im} m \right\}. \tag{3}$$

Therefore, in this way to find the set of non-isomorphic $G$-skew braces of type $N$, it suffices to find the set containing regular subgroups of $\operatorname{Hol}(N)$ which are isomorphic to $G$, and then extract a maximal subset whose elements are not conjugate by any element of $\operatorname{Aut}(N)$. In particular, [cf. 8] one can organise these regular subgroups, and hence the corresponding skew braces and Hopf–Galois structures, according to the size of their image under the natural projection

$$\begin{aligned} \Theta : \operatorname{Hol}(N) &\longrightarrow \operatorname{Aut}(N) \\ \eta\alpha &\longmapsto \alpha. \end{aligned} \tag{4}$$

In other words, if $\widetilde{\mathcal{S}}(G,N,r)$ is the set of regular subgroups of $\mathrm{Hol}(N)$ isomorphic to $G$ whose image under the natural projection $\Theta$ has size $r$, then the set of regular subgroups of $\mathrm{Hol}(N)$ isomorphic to $G$ is a finite disjoint union

$$\widetilde{\mathcal{S}}(G,N) = \coprod_r \widetilde{\mathcal{S}}(G,N,r).$$

Furthermore, $\mathrm{Aut}(N)$ acts on each $\widetilde{\mathcal{S}}(G,N,r)$ via conjugation inside $\mathrm{Hol}(N)$, and a set of orbit representatives provides a set of isomorphism classes of $G$-skew brace of type $N$, whose size upon embedding in $\mathrm{Hol}(N)$ and projecting to $\mathrm{Aut}(N)$ is $r$, which we shall denote by $G_N(r)$. In order to find the number of Hopf–Galois structures of type $N$ it suffices to find the automorphism group of each $G$-skew braces of type $N$ using (3) and use the formula given in (2). We shall set $e'(G,N,r) = |\widetilde{\mathcal{S}}(G,N,r)|$ and denote by $\widetilde{e}(G,N,r)$ the number of isomorphism classes of skew braces $G_N(r)$.

### *2.2. Regular subgroups of holomorphs*

In this subsection we outline our strategy for finding regular subgroups contained in $\mathrm{Hol}(N)$. Let us denote by

$$\Theta : \mathrm{Hol}(N) \longrightarrow \mathrm{Aut}(N),$$

the natural projection with kernel $N$. Then the first step is to organise the regular subgroups of $\mathrm{Hol}(N)$ according to the size of their image under the map $\Theta$.

Now suppose we want to parametrise subgroups $H \subseteq \mathrm{Hol}(N)$ with $|\Theta(H)| = m$, where $m$ divides $|N|$. In order to do this, we first take a subgroup of order $m$ of $\mathrm{Aut}(N)$, which may be generated by some elements $\alpha_1, ..., \alpha_s \in \mathrm{Aut}(N)$, say

$$H_2 \stackrel{\text{def}}{=} \langle \alpha_1, ..., \alpha_s \rangle \subseteq \mathrm{Aut}(N).$$

Next, we take a subgroup of order $\frac{|N|}{m}$ of $N$, which may be generated by $\eta_1, ..., \eta_r \in N$, say

$$H_1 \stackrel{\text{def}}{=} \langle \eta_1, ..., \eta_r \rangle \subseteq N.$$

We also take 'general elements' $v_1, ..., v_s \in N$, and we consider a subgroup of $\mathrm{Hol}(N)$ of the form

$$H = \langle \eta_1, ..., \eta_r, v_1\alpha_1, ..., v_s\alpha_s \rangle .$$

Now we need to classify the constraints on $v_1, ..., v_s$ such that $H$ is regular, i.e., $H$ has the same size as $N$ and acts freely on $N$. It is easy to see that there are many restrictions on $v_1, ..., v_s$ and in many cases no choice of $v_1, ..., v_s$ will result in a regular subgroup.

Notice that $|H| \geq |N|$ since we have the following commutative diagram

$$\begin{array}{ccccc} H_1 & \hookrightarrow & H & \overset{\Theta}{\twoheadrightarrow} & H_2 \\ \downarrow & & \downarrow & & \downarrow \\ N & \hookrightarrow & \mathrm{Hol}(N) & \overset{\Theta}{\twoheadrightarrow} & \mathrm{Aut}(N), \end{array}$$

where the hook arrows are natural inclusion, and the second row is exact, but the first row is not necessarily exact. One of our goals is to select $v_1, ..., v_s$ such that the first row is exact, which would imply that $|H| = |N|$. In particular, we need $H \cap N = H_1$. That is for example, if there is a relation say $\alpha^{a_1} = 1$ in $H_2$, then we need to ensure that $(v_1 a_1)^{a_1} = v_1 v_1^{\alpha_1} \cdots v_1^{\alpha_1^{a_1-1}} \in H_1$. Furthermore, we need to ensure that $H$ acts freely on $N$, and so for example, if $v_i \in H_1$ for some $i$, then $H$ will not be acting freely.

More generally we require the following. For $H$ to have the same size as $N$, we require for every relation $R(\alpha_1, ..., \alpha_s) = 1$ on $H_2$ to have

$$R\left(u_1\left(v_1\alpha_1\right)w_1, ..., u_s\left(v_s\alpha_s\right)w_s\right) \in H_1,$$

for every $u_1, w_1, ..., u_s, w_s \in H_1$. For $H$ to act freely on $N$, it is necessary that for every word $W(\alpha_1, ..., \alpha_s) \neq 1$ on $H_2$ we require

$$W(u_1\left(v_1\alpha_1\right)w_1, ..., u_s(v_s\alpha_s)w_s)\, W\left(\alpha_1, ..., \alpha_s\right)^{-1} \notin H_1,$$

for every $u_1, w_1, ..., u_s, w_s \in H_1$; so in fact we must have

$$\langle \eta_1, ..., \eta_r, v_1, ..., v_s \rangle = N.$$

However, in general there may be other conditions on $v_i$ that need to be taken into account – for example, some elements of $H$ need to satisfy relations between generators of a group of order $|N|$. Therefore, as already mentioned, it can happen that desirable $v_i$ cannot be found. To find all regular subgroups we repeat this process for every $m$, every subgroup of order $m$ of $\mathrm{Aut}(N)$, and every subgroup of order $\frac{|N|}{m}$ of $N$.

Finally, in order to find non-isomorphic skew braces, we need to check which of these regular subgroups are conjugate to one another by elements of $\mathrm{Aut}(N)$. Note, if $H$ and $\widetilde{H}$ are regular subgroups of $\mathrm{Hol}(N)$ with $|\Theta(H)| = |\Theta(\widetilde{H})| = m$, then $H$ and $\widetilde{H}$ are conjugate by an element of $\beta \in \mathrm{Aut}(N)$ if

$$\beta(H_1) \subseteq \widetilde{H}_1 \text{ and } \beta H_2 \beta^{-1} \subseteq \widetilde{H}_2,$$

i.e., when $H = \langle \eta_1, ..., \eta_r, v_1\alpha_1, ..., v_s\alpha_s \rangle$, we need

$$\left\langle \eta_1^{\beta}, ..., \eta_r^{\beta}, v_1^{\beta}\beta\alpha_1\beta^{-1}, ..., v_s^{\beta}\beta\alpha_s\beta^{-1} \right\rangle \subseteq \widetilde{H}.$$

Our starting point is studying the Heisenberg group of order $p^3$ and its automorphism group.

## 3. The Heisenberg group $M_1$

For $p > 2$ the exponent $p$ nonabelian group of order $p^3$, or otherwise known as the Heisenberg group, which we denote by $M_1$, has a presentation

$$M_1 \stackrel{\text{def}}{=} \langle \rho, \sigma, \tau \mid \rho^p = \sigma^p = \tau^p = 1,\ \sigma\rho = \rho\sigma,\ \tau\rho = \rho\tau,\ \tau\sigma = \rho\sigma\tau \rangle \cong C_p^2 \rtimes C_p.$$

Note, the above relations imply that for positive integers $a_1, a_2, a_3, a_4$, we have

$$\sigma^{a_1}\tau^{a_2}\sigma^{a_3}\tau^{a_4} = \rho^{a_2 a_3}\sigma^{a_1+a_3}\tau^{a_2+a_4}$$

from which we also obtain the relation

$$(\sigma^{a_1}\tau^{a_2})^n = \rho^{\frac{1}{2}a_1 a_2 n(n-1)}\sigma^{na_1}\tau^{na_2}. \tag{5}$$

We note that the group $M_1$ contains $p^3 - 1$ elements of order $p$, thus $p^2 + p + 1$ subgroups of order $p$, which are of the form

$$\langle \rho \rangle, \langle \rho^a \sigma \rangle, \langle \rho^b \sigma^c \tau \rangle \text{ for } a, b, c = 0, ..., p-1.$$

Also $M_1$ contains $p + 1$ subgroups of order $p^2$, which are all isomorphic to $C_p^2$, of the form

$$\langle \rho, \tau \rangle, \langle \rho, \sigma\tau^d \rangle \text{ for } d = 0, ..., p-1.$$

The next proposition determines the automorphism group of $M_1$. For the analogous result over $\mathbb{Z}$ see [29].

**Proposition 3.1.** *We have* $|\mathrm{Aut}(M_1)| = (p^2 - 1)(p - 1)p^3$ *and*

$$\mathrm{Aut}(M_1) \cong C_p^2 \rtimes \mathrm{GL}_2(\mathbb{F}_p),$$

*where* $C_p^2$ *in the semi-direct product above is generated by the automorphisms* $\beta, \gamma \in \mathrm{Aut}(M_1)$ *defined by*

$$\sigma^\beta = \sigma,\ \tau^\beta = \rho\tau \text{ and}$$
$$\sigma^\gamma = \rho\sigma,\ \tau^\gamma = \tau.$$

*The (left) action of* $\mathrm{GL}_2(\mathbb{F}_p)$ *on* $C_p^2 = \langle \beta, \gamma \rangle$*, in the semi-direct product, is given by*

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \beta = \beta^{a_1}\gamma^{-a_3} \text{ and } \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \gamma = \beta^{-a_2}\gamma^{a_4},$$

*where* $\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$.

**Proof.** Let $\alpha \in \mathrm{Aut}(M_1)$. Then we have

$$\sigma^\alpha = \rho^{b_1}\sigma^{a_1}\tau^{a_3}$$
$$\tau^\alpha = \rho^{b_2}\sigma^{a_2}\tau^{a_4}$$

for some $a_1, a_2, a_3, a_4, b_1, b_2 \in \mathbb{Z}/p\mathbb{Z}$. Note, $\rho^\alpha$ is determined by this:

$$\rho^\alpha = \tau^\alpha\sigma^\alpha\left(\sigma^\alpha\tau^\alpha\right)^{-1} = \rho^{a_1a_4-a_2a_3},$$

so $\alpha$ is bijective if and only if $a_1a_4 - a_2a_3 \not\equiv 0 \bmod p$. We shall write

$$\begin{bmatrix} a_1a_4 - a_2a_3 & b_1 & b_2 \\ 0 & a_1 & a_2 \\ 0 & a_3 & a_4 \end{bmatrix} \text{ or } \begin{bmatrix} \det(A) & b_1 \quad b_2 \\ 0 & A \end{bmatrix}$$

to represent $\alpha$. This is only a representation, and not a matrix, so composition of automorphisms does not in general correspond to matrix multiplication. In fact composition of automorphisms yields the following.

$$\begin{aligned} &\begin{bmatrix} \det(A) & b_1 \quad b_2 \\ 0 & A \end{bmatrix} \circ \begin{bmatrix} \det(A') & b_1' \quad b_2' \\ 0 & A' \end{bmatrix} \\ &= \left[\begin{pmatrix} \det(A) & b_1 \quad b_2 \\ 0 & A \end{pmatrix}\begin{pmatrix} \det(A') & b_1' \quad b_2' \\ 0 & A' \end{pmatrix} + \begin{pmatrix} 0 & C_1 \quad C_2 \\ 0 & 0 \end{pmatrix}\right] \end{aligned}$$

for

$$C_1 = \frac{1}{2}a_1a_3a_1'(a_1'-1) + \frac{1}{2}a_2a_4a_3'(a_3'-1) + a_3a_1'a_2a_3'$$
$$C_2 = \frac{1}{2}a_1a_3a_2'(a_2'-1) + \frac{1}{2}a_2a_4a_4'(a_4'-1) + a_3a_2'a_2a_4'.$$

The group $M_1$ has centre $Z = \langle \rho \rangle$ of order $p$ and

$$M_1/Z = \langle \overline{\sigma}, \overline{\tau} \rangle \cong C_p^2,$$

where $\overline{\sigma}, \overline{\tau} \in M_1/Z$ are the images of $\sigma, \tau \in M_1$. Thus we obtain a natural homomorphism

$$\Psi : \mathrm{Aut}(M_1) \longrightarrow \mathrm{Aut}(M_1/Z) \cong \mathrm{GL}_2(\mathbb{F}_p).$$

Since $M_1/Z \cong C_p^2$ is abelian, we see that the set of inner automorphisms of $M_1$ is contained in the kernel of $\Psi$ i.e., $\mathrm{Inn}(M_1) \subseteq \mathrm{Ker}\,\Psi$. Note $\mathrm{Inn}(M_1) \cong M_1/Z$. Now if $\alpha \in \mathrm{Ker}\,\Psi$, then we must have $\tau^\alpha\tau^{-1} \in Z$ and $\sigma^\alpha\sigma^{-1} \in Z$ i.e.,

$$\sigma^\alpha = \rho^{r_1}\sigma$$
$$\tau^\alpha = \rho^{r_2}\tau$$

for some integers $r_1, r_2 = 0, ..., p-1$, which implies that $\rho^\alpha = \rho$. There can be at most $p^2$ choices for such $\alpha$, which implies that $\mathrm{Inn}(M_1) = \mathrm{Ker}\,\Psi$. We further find $\mathrm{Ker}\,\Psi = \langle\beta, \gamma\rangle$ where

$$\beta \overset{\text{def}}{=} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \ \gamma \overset{\text{def}}{=} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

To show that the map $\Psi$ is surjective, for any element

$$A \overset{\text{def}}{=} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$$

define a map

$$\alpha_A : M_1 \longrightarrow M_1 \text{ given by } \alpha_A \overset{\text{def}}{=} \begin{bmatrix} ad-bc & \frac{ac}{2} & \frac{bd}{2} \\ 0 & a & b \\ 0 & c & d \end{bmatrix}.$$

It is easy to check that $A \longmapsto \alpha_A$ is a group homomorphism. Therefore, we find a split exact sequence

$$1 \longrightarrow C_p^2 \longrightarrow \mathrm{Aut}(M_1) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p) \longrightarrow 1.$$

One can check that the left action of $\mathrm{GL}_2(\mathbb{F}_p)$ on $C_p^2$ is given by

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \beta = \beta^{a_1}\gamma^{-a_3} \text{ and } \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \gamma = \beta^{-a_2}\gamma^{a_4}.$$

Note the above corresponds to

$$\alpha_A\beta = \beta^{a_1}\gamma^{-a_3}\alpha_A \text{ and } \alpha_A\gamma = \beta^{-a_2}\gamma^{a_4}\alpha_A. \quad \square$$

## 4. Skew braces of $M_1$ type

In this section we classify the skew braces and Hopf–Galois structures of $M_1$ type. The main result of this section is the following (which is a proof of Theorems 1.3 and 1.4). Recall, $\widetilde{e}(G, N)$ is the number of $G$-skew braces of type $N$ and $e(G, N)$ is the number of Hopf–Galois structures on a Galois extension with Galois group $G$ of type $N$.

**Proposition 4.1.** *We have*

$$\widetilde{e}(M_1, M_1) = 2p^2 - p + 3,$$
$$\widetilde{e}(C_p^3, M_1) = 2p + 1,$$

*and* $\widetilde{e}(G, M_1) = 0$ *for* $G \ncong M_1$ *or* $C_p^3$.

*Furthermore, we have*

$$e(M_1, M_1) = (2p^3 - 3p + 1)p^2,$$
$$e(C_p^3, M_1) = (p^3 - 1)(p^2 + p - 1)p^2,$$

*and* $e(G, M_1) = 0$ *for* $G \ncong M_1$ *or* $C_p^3$.

**Proof.** This follows from the calculation in the rest of this section, particularly the first part follows by adding the relevant numbers from Lemmas 4.2, 4.4, and 4.6

$$\widetilde{e}(M_1, M_1) = 1 + 2(p-1) + (2p-3)p + 4 = 2p^2 - p + 3,$$
$$\widetilde{e}(C_p^3, M_1) = 2 + 2p - 1 = 2p + 1,$$

and the second part follows by adding relevant numbers from Lemmas 4.3, 4.5, and 4.6

$$\begin{aligned} e(M_1, M_1) &= 1 + (p^3 - p^2 - 1)(p+1) + (p^4 - p^3 - 2p^2 + 2p + 1)p + (p^2 - 1)p^3 \\ &= (2p^3 - 3p + 1)p^2, \\ e(C_p^3, M_1) &= (p^3 - 1)(p+1)p^2 + (p^3 - 1)(p^2 - 2)p^2 = (p^3 - 1)(p^2 + p - 1)p^2. \quad \square \end{aligned}$$

We note that at the end of Lemmas 4.2, 4.4, and 4.6 there are lists of non-isomorphic skew braces together with a description of their automorphism groups.

Before we begin to prove Lemmas 4.2, 4.3, 4.4, 4.5, and 4.6, we need to set up some notations. Let us denote by

$$\alpha_1 \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \ \alpha_2 \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \ \alpha_3 \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Note in Proposition 3.1, we had $\alpha_1 = \gamma$ and $\alpha_3 = \beta$. Furthermore, we showed that $\mathrm{Aut}(M_1)$ can be written as

$$\mathrm{Aut}(M_1) \cong C_p^2 \rtimes \mathrm{GL}_2(\mathbb{F}_p),$$

where the factor $C_p^2$ is generated by automorphisms $\alpha_1, \alpha_3 \in \mathrm{Aut}(M_1)$. The (left) action of $\mathrm{GL}_2(\mathbb{F}_p)$ on $C_p^2$ is given by

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \alpha_1 = \alpha_1^{a_4}\alpha_3^{-a_2}, \ \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \alpha_3 = \alpha_1^{-a_3}\alpha_3^{a_1}. \tag{6}$$

Therefore, the holomorph of $M_1$ can be identified with

$$\mathrm{Hol}(M_1) \cong M_1 \rtimes (C_p^2 \rtimes \mathrm{GL}_2(\mathbb{F}_p)).$$

Now the image in $\mathrm{GL}_2(\mathbb{F}_p)$ of a subgroup $G \subseteq \mathrm{Hol}(M_1)$ of order $p^3$ under the composition of projections

$$\Theta : \mathrm{Hol}(M_1) \longrightarrow \mathrm{Aut}(M_1) \text{ and } \Psi : \mathrm{Aut}(M_1) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

must lie in one of the $p+1$ Sylow $p$-subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, which are conjugate to the subgroup generated by $\beta_1 \stackrel{\text{def}}{=} \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$; thus we have

$$\Theta(G) \subseteq \mathrm{A}_\beta(M_1) \stackrel{\text{def}}{=} C_p^2 \rtimes \left\langle \beta\beta_1\beta^{-1} \right\rangle \cong M_1 \text{ for some } \beta \in \mathrm{GL}_2(\mathbb{F}_p),$$

and so any subgroup of $\mathrm{Hol}(M_1)$ of order $p^3$ lies in a subgroup of the form

$$M_1 \rtimes \mathrm{A}_\beta(M_1) \text{ for some } \beta \in \mathrm{GL}_2(\mathbb{F}_p).$$

Note, the elements $\alpha_1, \alpha_2, \alpha_3 \in \mathrm{Aut}(M_1)$ have order $p$, and they satisfy

$$\alpha_2\alpha_1 = \alpha_1\alpha_2, \ \alpha_3\alpha_1 = \alpha_1\alpha_3, \ \alpha_3\alpha_2 = \alpha_1\alpha_2\alpha_3. \tag{7}$$

Thus, we have that $\langle \alpha_1, \alpha_2, \alpha_3 \rangle \cong M_1$ is one of the $p+1$ Sylow $p$-subgroups of $\mathrm{Aut}(M_1)$, which is the one we can, and shall, without loss of generality, work with. First, note that for $|\Theta(G)| = 1$, we have

$$\begin{aligned} e(M_1, M_1, 1) &= \widetilde{e}(M_1, M_1, 1) = 1 \text{ and} \\ e(G, M_1, 1) &= \widetilde{e}(G, M_1, 1) = 0 \text{ if } G \neq M_1. \end{aligned}$$

We shall deal with the cases $|\Theta(G)| = p, p^2, p^3$ in the following lemmas.

It will be useful for our calculations to derive the explicit formula for $(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r$ for natural numbers $r, a_i$ for $i = 1, 2, 3$ and an element $v = \rho^{v_1}\sigma^{v_2}\tau^{v_3} \in M_1$. For this we first note that we have

$$\begin{aligned} \alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3} \cdot v &= \begin{bmatrix} 1 & a_1 & a_3 \\ 0 & 1 & 0 \\ 0 & a_2 & 1 \end{bmatrix} \cdot v \\ &= \rho^{a_1 v_2 + \frac{1}{2} a_2 v_2 (v_2 - 1) + a_3 v_3} v \tau^{a_2 v_2}. \end{aligned} \tag{8}$$

Now by using (7) and (8) we find

$$\begin{aligned}\left(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)^r &= \left(\prod_{j=0}^{r-1}\rho^{k_j}v\tau^{a_2v_2j}\right)\left(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)^r \\ &= \rho^{l_1}v^r\tau^{l_2a_2v_2}\left(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)^r, \end{aligned} \tag{9}$$

(note order of the product matters and is in increasing $j$) with

$$k_j \overset{\text{def}}{=} \left(a_1v_2j + \frac{1}{2}a_2a_3v_2j\,(j-1) + \frac{1}{2}a_2v_2\,(v_2-1)\,j + a_3v_3j\right),$$

for $j = 0, ..., r-1$,

$$\begin{aligned} l_1 = l_1(r) &\overset{\text{def}}{=} \sum_{j=1}^{r-1}k_j + \frac{a_2v_2^2}{2}\sum_{j=1}^{r-2}j\,(j+1)\,, \text{ and} \\ l_2 = l_2(r) &\overset{\text{def}}{=} \sum_{j=1}^{r-1}j. \end{aligned}$$

The second summation in $l_1$ arises by moving the $\tau^{a_2v_2j}$ terms to gather them in one place using the relation $\tau\sigma = \rho\sigma\tau$. Note, here $l_1$ and $l_2$ are divisible by $r$ for $r > 3$ a prime number, so we find

$$\left(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)^p = 1 \tag{10}$$

for every $v \in M_1$ since $p > 3$. Note further that in (9), when $a_2 = 0$, we have

$$\left(v\alpha_1^{a_1}\alpha_3^{a_3}\right)^r \in v^r\alpha_1^{ra_1}\alpha_3^{ra_3}\,\langle\rho\rangle\,, \tag{11}$$

where $\langle\rho\rangle$ is a normal subgroup of $\mathrm{Hol}(M_1)$ since it is a characteristic subgroup of $M_1$.

It will further be useful, when finding the non-isomorphic skew braces, to derive the explicit formula for a term of the form $\alpha\left(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)\alpha^{-1}$ for an automorphism $\alpha \in \mathrm{Aut}(M_1)$. Now if

$$\begin{gathered}\alpha = \gamma\beta \in \mathrm{Aut}(M_1) \cong C_p^2 \rtimes \mathrm{GL}_2(\mathbb{F}_p) \text{ where} \\ \gamma \overset{\text{def}}{=} \alpha_1^{r_1}\alpha_3^{r_3} \in C_p^2,\ \beta \overset{\text{def}}{=} \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p),\end{gathered}$$

then, using (6), we have

$$\begin{aligned}&\alpha\left(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)\alpha^{-1} \\ &\quad= (\alpha\cdot v)\,\alpha_1^{r_1}\alpha_3^{r_3}\alpha_1^{(a_1-a_2a_3)b_4-a_3b_3}\alpha_3^{-(a_1-a_2a_3)b_2+a_3b_1}\beta\alpha_2^{a_2}\beta^{-1}\alpha_1^{-r_1}\alpha_3^{-r_3},\end{aligned}$$

where using the section of the exact sequence in Proposition 3.1, we have

$$\beta \cdot v = \rho^{\det(\beta)v_1+\frac{1}{2}(b_1b_3v_2+b_2b_4v_3)} \left(\sigma^{b_1}\tau^{b_3}\right)^{v_2} \left(\sigma^{b_2}\tau^{b_4}\right)^{v_3},$$

which gives

$$\alpha\cdot v = \rho^{\widetilde{v}_1}\sigma^{b_1v_2+b_2v_3}\tau^{b_3v_2+b_4v_3}, \text{ where} \tag{12}$$
$$\widetilde{v}_1 \overset{\text{def}}{=} \det(\beta)v_1 + \frac{1}{2}\left(b_3b_1v_2^2 + b_4b_2v_3^2\right) + b_2b_3v_2v_3 + r_1\left(b_1v_2+b_2v_3\right) + r_3\left(b_3v_2+b_4v_3\right)$$

The above implies that, when $a_2 = 0$, we have

$$\alpha\left(v\alpha_1^{a_1}\alpha_3^{a_3}\right)\alpha^{-1} = (\alpha\cdot v)\,\alpha_1^{a_1b_4-a_3b_3}\alpha_3^{a_3b_1-a_1b_2}, \tag{13}$$

with $\alpha\cdot v$ as given in (12), and when $a_2 \neq 0$, we can set $b_2 = 0$, since we want to remain within $\langle\alpha_1,\alpha_2,\alpha_3\rangle$, and in this case since we have

$$\beta\alpha_2^{a_2}\beta^{-1} = \alpha_1^{\frac{1}{2}a_2b_4\left(b_1^{-1}-1\right)}\alpha_2^{a_2b_1^{-1}b_4},$$

so (when $b_2 = 0$) we get

$$\alpha\left(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)\alpha^{-1} = (\alpha\cdot v)\,\alpha_1^{a_1b_4-a_3b_3+r_3a_2b_1^{-1}b_4+\frac{1}{2}a_2b_4\left(b_1^{-1}-1\right)}\alpha_2^{a_2b_1^{-1}b_4}\alpha_3^{a_3b_1}, \tag{14}$$

where $\alpha\cdot v$ can be calculated using (12). Now we can start our main calculations.

**Lemma 4.2.** *For $|\Theta(G)| = p$ there are exactly $2(p-1)$ $M_1$-skew braces of $M_1$ type and two $C_p^3$-skew braces of $M_1$ type.*

**Proof.** If $G \subseteq \mathrm{Hol}(M_1)$ with $|\Theta(G)| = p$ is a regular subgroup, then we can assume, without loss of generality, that $\Theta(G) \subseteq \langle\alpha_1,\alpha_2,\alpha_3\rangle$ is a subgroup of order $p$. We also have that $G\cap M_1$ is a subgroup of order $p^2$. Therefore, $\Theta(G)$ is one of

$$\langle\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\rangle \text{ for } a_1,a_2,a_3 = 0,...,p-1 \text{ with } (a_1,a_2,a_3) \neq (0,0,0),$$

(each occurring $p-1$ times) and $G\cap M_1$ is one of

$$\langle\rho,\tau\rangle, \langle\rho,\sigma\tau^d\rangle \text{ for } d = 0,...,p-1.$$

Suppose we consider subgroups of the form

$$G = \langle\rho,\sigma\tau^d,h\rangle \text{ where } h \overset{\text{def}}{=} \tau\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}.$$

Note, using (8), we must have

$$h\left(\sigma\tau^d\right)h^{-1} = \tau\left(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\cdot\left(\sigma\tau^d\right)\right)\tau^{-1} = \rho^{a_3d+a_1+1}\sigma\tau^{a_2+d} \in \langle\rho,\sigma\tau^d\rangle,$$

and since for a natural number $r$ we have

$$\left(\sigma\tau^{d}\right)^{r}=\rho^{\frac{1}{2}dr(r-1)}\sigma^{r}\tau^{rd},$$

the pairing is possible only when $a_2=0$. Therefore, we consider subgroups of the form

$$G=\left\langle\rho,\sigma\tau^{d},h\right\rangle \text{ where } h\stackrel{\text{def}}{=}\tau\alpha_1^{a_1}\alpha_3^{a_3}.$$

But now since the automorphism of $M_1$ corresponding to $\left(\begin{smallmatrix} d & -1\\ 1-d & 1\end{smallmatrix}\right)\in \mathrm{GL}_2(\mathbb{F}_p)$ maps the subgroup $\left\langle\rho,\sigma\tau^{d}\right\rangle$ to $\langle\rho,\tau\rangle$, we can assume every one of these skew braces is isomorphic to one containing the subgroup $\langle\rho,\tau\rangle$.

Hence, up to conjugation, we must have

$$G=\langle\rho,\tau,g\rangle \text{ where } g\stackrel{\text{def}}{=}\sigma\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}.$$

Note, using (8), we have

$$\begin{aligned} g\tau g^{-1}&=\sigma\left(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\cdot\tau\right)\sigma^{-1}=\rho^{(a_3-1)}\tau\in\langle\rho,\tau\rangle \text{ and}\\ g\rho g^{-1}&=\sigma\left(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\cdot\rho\right)\sigma^{-1}=\rho\in\langle\rho,\tau\rangle, \end{aligned}$$

so the pairing is possible. Further, it follows from (10) that $g^p=1$. Now, for $r\neq 0$, using (8), we have

$$g\tau^{r}=\left(\sigma\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)\tau^{r}=\rho^{ra_3}\sigma\tau^{r}\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}=\rho^{r(a_3-1)}\tau^{r}g, \tag{15}$$

so $G$ is abelian if and only if $a_3=1$. Furthermore, all these subgroups are regular since they have order $p^3$ and $\langle\rho,\tau\rangle\cup\{\sigma\}\subseteq \mathrm{Orb}(1)$, i.e., since $|\mathrm{Orb}(1)|>p^2$, their action on $M_1$ is transitive.

Therefore, for $a_3=1$ we find regular subgroups isomorphic to $C_p^3$ of the form

$$\begin{aligned} &\left\langle\rho,\tau,\sigma\alpha_1^{a}\alpha_3\right\rangle,\left\langle\rho,\tau,\sigma\alpha_1^{a}\alpha_2^{b}\alpha_3\right\rangle\cong C_p^3\\ &\text{for } a=0,\dots,p-1,\ b=1,\dots,p-1, \end{aligned} \tag{16}$$

and for $a_3\neq 1$, setting $r=(1-a_3)^{-1}$ in (15), we find regular subgroups isomorphic to $M_1$ of the form

$$\begin{aligned} &\left\langle\rho,\tau,\sigma\alpha_1^{b}\right\rangle,\left\langle\rho,\tau,\sigma\alpha_1^{a}\alpha_2^{b}\right\rangle,\left\langle\rho,\tau,\sigma\alpha_1^{a}\alpha_3^{c}\right\rangle,\left\langle\rho,\tau,\sigma\alpha_1^{a}\alpha_2^{b}\alpha_3^{c}\right\rangle\cong M_1\\ &\text{for } a=0,\dots,p-1,\ b,c=1,\dots,p-1 \text{ with } c\neq 1. \end{aligned} \tag{17}$$

To find the non-isomorphic skew braces corresponding to the above regular subgroups, we let

$$\alpha=\gamma\beta\in\mathrm{Aut}(M_1)\cong C_p^2\rtimes\mathrm{GL}_2(\mathbb{F}_p) \text{ where}$$

$$\gamma \stackrel{\text{def}}{=} \alpha_1^{r_1}\alpha_3^{r_3} \in C_p^2,\ \beta \stackrel{\text{def}}{=} \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p),$$

and we work with automorphisms which fix the subgroup $\langle \rho, \tau\rangle$, i.e., when $b_2 = 0$. In such case, using (14), we have

$$\alpha\left(\sigma\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)\alpha^{-1} = (\alpha\cdot\sigma)\,\alpha_1^{a_1b_4-a_3b_3+r_3a_2b_1^{-1}b_4+\frac{1}{2}a_2b_4\left(b_1^{-1}-1\right)}\alpha_2^{a_2b_1^{-1}b_4}\alpha_3^{a_3b_1},$$

where using (12)

$$\alpha\cdot\sigma = \rho^{\frac{1}{2}b_1b_3-r_1b_1+r_3b_3}\sigma^{b_1}\tau^{b_3}.$$

Now since

$$\alpha\left(\sigma\alpha_1^{a}\alpha_3^{c}\right)\alpha^{-1} = (\alpha\cdot\sigma)\,\alpha_1^{ab_4-cb_3}\alpha_3^{cb_1} \in \sigma^{b_1}\alpha_1^{ab_4-cb_3}\alpha_3^{cb_1}\left\langle\rho,\tau\right\rangle,$$

we have

$$\alpha\left(\sigma\alpha_1^{a}\alpha_3^{c}\right)^{b_1^{-1}}\alpha^{-1} \in \sigma\alpha_1^{ab_1^{-1}b_4-cb_1^{-1}b_3}\alpha_3^{c}\left\langle\rho,\tau\right\rangle.$$

Thus if we conjugate the subgroup $\langle\rho,\tau,\sigma\alpha_3^c\rangle$ with the automorphism corresponding to $\left(\begin{smallmatrix} 1 & 0 \\ -ac^{-1} & 1\end{smallmatrix}\right)$ we get $\langle\rho,\tau,\sigma\alpha_1^a\alpha_3^c\rangle$, and now the subgroups $\langle\rho,\tau,\sigma\alpha_3^c\rangle$ for different values of $c$ cannot be conjugate to each other.

Next, working similar to above, we have

$$\alpha\left(\sigma\alpha_1^{a}\alpha_2^{b}\alpha_3^{c}\right)^{b_1^{-1}}\alpha^{-1} \in \sigma\alpha_1^{ab_1^{-1}b_4-cb_1^{-1}b_3+r_3bb_1^{-2}b_4+\frac{1}{2}bb_1^{-1}b_4\left(b_1^{-1}-1\right)(c+1)}\alpha_2^{bb_1^{-2}b_4}\alpha_3^{c}\left\langle\rho,\tau\right\rangle.$$

Thus, if we conjugate the subgroup $\langle\rho,\tau,\sigma\alpha_2\alpha_3^c\rangle$ with the automorphism corresponding to $\left(\begin{smallmatrix} 1 & 0 \\ -ac^{-1} & b\end{smallmatrix}\right)$, we get $\left\langle\rho,\tau,\sigma\alpha_1^a\alpha_2^b\alpha_3^c\right\rangle$, and now again the subgroups $\langle\rho,\tau,\sigma\alpha_2\alpha_3^c\rangle$ for different values of $c$ cannot be conjugate. Finally, we note that

$$\alpha\left(\sigma\alpha_1^{a}\alpha_2^{b}\right)^{b_1^{-1}}\alpha^{-1} \in \sigma\alpha_1^{ab_1^{-1}b_4+r_3bb_1^{-2}b_4+\frac{1}{2}bb_1^{-1}b_4\left(b_1^{-1}-1\right)}\alpha_2^{bb_1^{-2}b_4}\left\langle\rho,\tau\right\rangle,$$

so

$$\alpha\left(\sigma\alpha_1^{a}\right)^{b_1^{-1}}\alpha^{-1} \in \sigma\alpha_1^{ab_1^{-1}b_4}\left\langle\rho,\tau\right\rangle,$$

which implies that conjugating the subgroup $\langle\rho,\tau,\sigma\alpha_1\rangle$ with the automorphism corresponding to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & b\end{smallmatrix}\right)$, we get $\left\langle\rho,\tau,\sigma\alpha_1^b\right\rangle$, and conjugating the subgroup $\langle\rho,\tau,\sigma\alpha_2\rangle$ with the automorphism corresponding to $\alpha_3^{ab^{-1}}\left(\begin{smallmatrix} 1 & 0 \\ 0 & b\end{smallmatrix}\right)$, we get $\left\langle\rho,\tau,\sigma\alpha_1^a\alpha_2^b\right\rangle$.

Therefore, we have non-isomorphic skew braces

$$\begin{aligned} &\langle \rho, \tau, \sigma\alpha_3 \rangle, \langle \rho, \tau, \sigma\alpha_2\alpha_3 \rangle \cong C_p^3; \\ &\langle \rho, \tau, \sigma\alpha_1 \rangle, \langle \rho, \tau, \sigma\alpha_2 \rangle, \langle \rho, \tau, \sigma\alpha_3^c \rangle, \langle \rho, \tau, \sigma\alpha_2\alpha_3^c \rangle \cong M_1 \text{ for } c = 2, ..., p-1, \end{aligned} \tag{18}$$

and counting them we find that there are $2(p-1)$ $M_1$-skew braces of $M_1$ type and two $C_p^3$-skew braces of $M_1$ type. □

**Lemma 4.3.** *There are*

$$(p^3 - p^2 - 1)(p + 1)$$

*Hopf–Galois structures of $M_1$ type on Galois extensions of fields with Galois group $G \cong M_1$ and $|\Theta(G)| = p$, and exactly*

$$(p^3 - 1)(p + 1)p^2$$

*Hopf–Galois structures of $M_1$ type on Galois extensions of fields with Galois group $G \cong C_p^3$ and $|\Theta(G)| = p$.*

**Proof.** To find the number of Hopf–Galois structures corresponding to the skew braces in (18) of Lemma 4.2,

$$\begin{aligned} &\langle \rho, \tau, \sigma\alpha_3 \rangle, \langle \rho, \tau, \sigma\alpha_2\alpha_3 \rangle \cong C_p^3; \\ &\langle \rho, \tau, \sigma\alpha_1 \rangle, \langle \rho, \tau, \sigma\alpha_2 \rangle, \langle \rho, \tau, \sigma\alpha_3^c \rangle, \langle \rho, \tau, \sigma\alpha_2\alpha_3^c \rangle \cong M_1 \text{ for } c = 2, ..., p-1, \end{aligned}$$

we need to find the automorphism groups of these skew braces.

We let

$$\alpha = \gamma\beta \in \mathrm{Aut}(M_1) \text{ where } \gamma \overset{\text{def}}{=} \alpha_1^{r_1}\alpha_3^{r_3},\ \beta \overset{\text{def}}{=} \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix},$$

and since we need $\alpha(\langle \rho, \tau \rangle) = \langle \rho, \tau \rangle$, we must set $b_2 = 0$. Now, if $\alpha \in \mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \tau, \sigma\alpha_3^c \rangle)$, since we have

$$\alpha\left(\sigma\alpha_3^c\right)^{b_1^{-1}} \alpha^{-1} \in \sigma\alpha_1^{-cb_1^{-1}b_3}\alpha_3^c \langle \rho, \tau \rangle,$$

we must have $b_3 = 0$, thus we find

$$\mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \tau, \sigma\alpha_3^c \rangle) = \left\{ \alpha \in \mathrm{Aut}(M_1) \mid \alpha = \alpha_1^{r_1}\alpha_3^{r_3}\left(\begin{smallmatrix} b_1 & 0 \\ 0 & b_4 \end{smallmatrix}\right) \right\}.$$

If $\alpha \in \mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \tau, \sigma\alpha_2\alpha_3^c \rangle)$, since we have

$$\alpha\left(\sigma\alpha_2\alpha_3^c\right)^{b_1^{-1}}\alpha^{-1}\in\sigma\alpha_1^{-cb_1^{-1}b_3+r_3b_1^{-2}b_4+\frac{1}{2}b_1^{-1}b_4\left(b_1^{-1}-1\right)(c+1)}\alpha_2^{b_1^{-2}b_4}\alpha_3^c\left\langle\rho,\tau\right\rangle,$$

we must have $b_4=b_1^2$ and

$$\begin{aligned}&-cb_1^{-1}b_3+r_3b_1^{-2}b_4+\frac{1}{2}b_1^{-1}b_4\left(b_1^{-1}-1\right)(c+1)\\&=-cb_1^{-1}b_3+r_3+\frac{1}{2}b_1\left(b_1^{-1}-1\right)(c+1)=0,\end{aligned}$$

so we find

$$\mathrm{Aut}_{\mathcal{B}r}(\langle\rho,\tau,\sigma\alpha_2\alpha_3^c\rangle)=\left\{\alpha\in\mathrm{Aut}(M_1)\mid\alpha=\alpha_1^{r_1}\alpha_3^{cb_1^{-1}b_3+\frac{1}{2}(b_1-1)(c+1)}\left(\begin{smallmatrix}b_1&0\\b_3&b_1^2\end{smallmatrix}\right)\right\}.$$

If $\alpha\in\mathrm{Aut}_{\mathcal{B}r}(\langle\rho,\tau,\sigma\alpha_1\rangle)$, since we have

$$\alpha\left(\sigma\alpha_1\right)^{b_1^{-1}}\alpha^{-1}\in\sigma\alpha_1^{b_1^{-1}b_4}\left\langle\rho,\tau\right\rangle,$$

we must have $b_1=b_4$, and we find

$$\mathrm{Aut}_{\mathcal{B}r}(\langle\rho,\tau,\sigma\alpha_1\rangle)=\left\{\alpha\in\mathrm{Aut}(M_1)\mid\alpha=\alpha_1^{r_1}\alpha_3^{r_3}\left(\begin{smallmatrix}b_1&0\\b_3&b_1\end{smallmatrix}\right)\right\}.$$

Finally, if $\alpha\in\mathrm{Aut}_{\mathcal{B}r}(\langle\rho,\tau,\sigma\alpha_2\rangle)$, since we have

$$\alpha\left(\sigma\alpha_2\right)^{b_1^{-1}}\alpha^{-1}\in\sigma\alpha_1^{r_3b_1^{-2}b_4+\frac{1}{2}b_1^{-1}b_4\left(b_1^{-1}-1\right)}\alpha_2^{b_1^{-2}b_4}\left\langle\rho,\tau\right\rangle,$$

we must have $b_4=b_1^2$ and $r_3=\frac{1}{2}(b_1-1)$, we find

$$\mathrm{Aut}_{\mathcal{B}r}(\langle\rho,\tau,\sigma\alpha_2\rangle)=\left\{\alpha\in\mathrm{Aut}(M_1)\mid\alpha=\alpha_1^{r_1}\alpha_3^{\frac{1}{2}(b_1-1)}\left(\begin{smallmatrix}b_1&0\\b_3&b_1^2\end{smallmatrix}\right)\right\}.$$

Therefore, we have

$$\begin{aligned}&e(M_1,M_1,p)=\sum_{(M_1)_{M_1}(p)}\frac{|\mathrm{Aut}(M_1)|}{|\mathrm{Aut}_{\mathcal{B}r}((M_1)_{M_1})|}=\\&\frac{|\mathrm{Aut}(M_1)|}{|\mathrm{Aut}_{\mathcal{B}r}(\langle\rho,\tau,\sigma\alpha_1\rangle)|}+\frac{|\mathrm{Aut}(M_1)|}{|\mathrm{Aut}_{\mathcal{B}r}(\langle\rho,\tau,\sigma\alpha_2\rangle)|}+\sum_{c=2}^{p-1}\frac{|\mathrm{Aut}(M_1)|}{|\mathrm{Aut}_{\mathcal{B}r}(\langle\rho,\tau,\sigma\alpha_3^c\rangle)|}\\&+\frac{|\mathrm{Aut}(M_1)|}{|\mathrm{Aut}_{\mathcal{B}r}(\langle\rho,\tau,\sigma\alpha_2\alpha_3^c\rangle)|}\\&=(p^2-1)(p-1)p^3\left(\frac{1}{(p-1)p^3}+\frac{1}{(p-1)p^2}+\sum_{c=2}^{p-1}\frac{1}{(p-1)^2p^2}+\frac{1}{(p-1)p^2}\right)\\&=(p^3-p^2-1)(p+1),\end{aligned}$$

and similarly

$$e(C_p^3, M_1, p) = \sum_{(C_p^3)_{M_1}(p)} \frac{\left|\mathrm{Aut}(C_p^3)\right|}{\left|\mathrm{Aut}_{\mathcal{B}r}((C_p^3)_{M_1})\right|} =$$

$$\frac{\left|\mathrm{Aut}(C_p^3)\right|}{\left|\mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \tau, \sigma\alpha_3\rangle)\right|} + \frac{\left|\mathrm{Aut}(C_p^3)\right|}{\left|\mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \tau, \sigma\alpha_2\alpha_3\rangle)\right|}$$

$$= (p^3-1)(p^3-p)(p^3-p^2)\left(\frac{1}{(p-1)^2p^2} + \frac{1}{(p-1)p^2}\right) = (p^3-1)(p+1)p^2. \quad \square$$

**Lemma 4.4.** *For $|\Theta(G)| = p^2$ there are exactly $(2p-3)p$ $M_1$-skew braces of $M_1$ type and $2p-1$ $C_p^3$-skew braces of $M_1$ type.*

**Proof.** If $G \subseteq \mathrm{Hol}(M_1)$ with $|\Theta(G)| = p^2$ is a regular subgroup, then we can assume, without loss of generality, that we have $\Theta(G) \subseteq \langle \alpha_1, \alpha_2, \alpha_3\rangle$ a subgroup of order $p^2$. We also have $G \cap M_1$ a subgroup of order $p$. Therefore, $\Theta(G)$ is one of

$$\langle \alpha_1, \alpha_3\rangle, \langle \alpha_1, \alpha_2\alpha_3^a\rangle \text{ for } a = 0, ..., p-1,$$

and $G \cap M_1$ is of the form

$$\left\langle \rho^b\sigma^c\tau^d \right\rangle \text{ for } b, c, d = 0, ..., p-1 \text{ with } (b, c, d) \neq (0, 0, 0),$$

each occurring $p-1$ times. We shall consider all subgroups of order $p$ in $M_1$ and always of pairing them with a subgroup of order $p^2$ of $\langle \alpha_1, \alpha_2, \alpha_3\rangle$.

Let us consider a subgroup of the form

$$G = \langle u, v\alpha_1, w\alpha_2^{a_2}\alpha_3^{a_3}\rangle \text{ for } (a_2, a_3) \neq (0, 0),\ u, v, w \neq 1.$$

Suppose $u = \rho^{u_1}\sigma^{u_2}\tau^{u_3}$, $v = \rho^{v_1}\sigma^{v_2}\tau^{v_3}$, and $w = \rho^{w_1}\sigma^{w_2}\tau^{w_3}$. Then, we need the following.

$$(v\alpha_1)\, u\, (v\alpha_1)^{-1} = v\,(\alpha_1 \cdot u)\, v^{-1}u^{-1} = \rho^{u_2+u_2v_3-u_3v_2} \in \langle u\rangle, \tag{19}$$

$$(w\alpha_2^{a_2}\alpha_3^{a_3})\, u\, (w\alpha_2^{a_2}\alpha_3^{a_3})^{-1} = w\,(\alpha_2^{a_2}\alpha_3^{a_3}\cdot u)\, w^{-1}u^{-1} =$$

$$\rho^{\frac{1}{2}a_2u_2(u_2-1)+a_3u_3+u_2w_3-u_3w_2-a_2u_2w_2-a_2u_2^2}\tau^{a_2u_2} \in \langle u\rangle, \tag{20}$$

$$(v\alpha_1)\,(w\alpha_2^{a_2}\alpha_3^{a_3})\,((w\alpha_2^{a_2}\alpha_3^{a_3})\,(v\alpha_1))^{-1} =$$

$$(\rho^{w_2}vw\alpha_1\alpha_2^{a_2}\alpha_3^{a_3})\left(\rho^{\frac{1}{2}a_2v_2(v_2-1)+a_3v_1-a_2v_2^2+v_2w_1-v_1w_2}\tau^{a_2v_2}vw\alpha_1\alpha_2^{a_2}\alpha_3^{a_3}\right)^{-1}$$

$$= \rho^{w_2-\frac{1}{2}a_2v_2(v_2-1)-a_3v_1+a_2v_2^2-v_2w_1+v_1w_2}\tau^{-a_2v_2} \in \langle u\rangle. \tag{21}$$

First assume $u_3 = 1$. Then, multiplying $v\alpha_1$ and $w\alpha_2^{a_2}\alpha_3^{a_3}$ by suitable powers of $u$ if necessary, we can further assume $v_3 = w_3 = 0$. Now (19) implies that $u_2 = v_2$ and (20) implies that we need

$$\rho^{\frac{1}{2}a_2u_2(u_2-1)+a_3-w_2-a_2u_2w_2-a_2u_2^2}\tau^{a_2u_2} \in \langle \rho^{u_1}\sigma^{u_2}\tau \rangle ,$$

so $u_2 = v_2 = 0$ and $a_3 = w_2$. In such case (21) implies that we need

$$\rho^{w_2} \in \langle \rho^{u_1}\sigma^{u_2}\tau \rangle ,$$

so $w_2 = 0$, which implies that $G$ cannot be regular. Thus, we cannot have any pairing with subgroups of the form $\langle \rho^b\sigma^c\tau \rangle$. Similarly, if $u_2 = 1$, then we can assume $v_2 = w_2 = 0$. Now (19) gives $v_3 = -1$, also (20) gives $a_2 = 0$, and (21) gives $a_3 = 0$ which is not possible. Thus, the only possibility for $u$ is $u = \rho$ and then (21) implies that we also need $a_2v_2 = 0$.

Therefore, we may only consider subgroups of the form

$$G = \langle \rho, v\alpha_1, w\alpha_2^{a_2}\alpha_3^{a_3} \rangle \text{ with } a_2v_2 = v_1 = w_1 = 0.$$

There are two main cases to consider.

**Case I:** Let us consider

$$G = \langle \rho, u\alpha_1, v\alpha_3 \rangle .$$

Then $(u\alpha_1)\,\rho = \rho\,(u\alpha_1)$ and $(v\alpha_3)\,\rho = \rho\,(v\alpha_3)$, also we have

$$\begin{aligned} (u\alpha_1)\,(v\alpha_3) &= \rho^{v_2}uv\alpha_1\alpha_3 \text{ and} \\ (v\alpha_3)\,(u\alpha_1) &= \rho^{u_3}vu\alpha_1\alpha_3 = \rho^{u_3+u_2v_3-u_3v_2}uv\alpha_1\alpha_3, \end{aligned} \tag{22}$$

so $G$ has order $p^3$ and is abelian if and only if $v_2 \equiv u_3 + u_2v_3 - u_3v_2 \bmod p$; furthermore, for $G$ to be regular we need $u_2v_3 - u_3v_2 \not\equiv 0 \bmod p$.

Therefore, for $u_2v_3 - u_3v_2 \not\equiv 0 \bmod p$ we have regular subgroups isomorphic to $C_p^3$ of the form

$$\begin{aligned} &\langle \rho, u\alpha_1, v\alpha_3 \rangle \cong C_p^3 \\ &\text{for } A = \begin{pmatrix} u_2 & v_2 \\ u_3 & v_3 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \text{ with } v_2 = u_3 + \det(A). \end{aligned} \tag{23}$$

For $v_2 - u_3 - u_2v_3 + u_3v_2 \not\equiv 0 \bmod p$, we find regular subgroups isomorphic to $M_1$ of the form

$$\begin{aligned} &\langle \rho, u\alpha_1, v\alpha_3 \rangle \cong M_1 \\ &\text{for } A = \begin{pmatrix} u_2 & v_2 \\ u_3 & v_3 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \text{ with } v_2 - u_3 - \det(A) \not\equiv 0 \bmod p. \end{aligned} \tag{24}$$

To find the non-isomorphic skew braces corresponding to the above regular subgroups, we let $\beta_0 \overset{\text{def}}{=} \left(\begin{smallmatrix} u_2 & v_2 \\ u_3 & v_3 \end{smallmatrix}\right)$ and note that considering (12) and (14), it suffices to work with an automorphism corresponding to $\beta \overset{\text{def}}{=} \left(\begin{smallmatrix} b_1 & b_2 \\ b_3 & b_4 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_p)$ with $b \overset{\text{def}}{=} \det(\beta)^{-1}$, and we find

$$\beta\,(u\alpha_1)^{b_1 b}\,(v\alpha_3)^{b_2 b}\,\beta^{-1} = \rho^{\kappa_1}\left(b\beta\beta_0\beta^T\right)\cdot\sigma\alpha_1,$$
$$\beta\,(u\alpha_1)^{b_3 b}\,(v\alpha_3)^{b_4 b}\,\beta^{-1} = \rho^{\kappa_2}\left(b\beta\beta_0\beta^T\right)\cdot\tau\alpha_3$$

for some $\kappa_1, \kappa_2$, where superscript $T$ denotes the transpose of a matrix.

Now if $u_2 \neq 0$, then

$$u_2^{-1}\begin{pmatrix} 1 & 0 \\ -u_3 & u_2 \end{pmatrix}\begin{pmatrix} u_2 & v_2 \\ u_3 & v_3 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -u_3 & u_2 \end{pmatrix}^T = \begin{pmatrix} 1 & v_2 - u_3 \\ 0 & \det(\beta_0) \end{pmatrix};$$

if $v_3 \neq 0$, then

$$v_3^{-1}\begin{pmatrix} 0 & 1 \\ -v_3 & v_2 \end{pmatrix}\begin{pmatrix} u_2 & v_2 \\ u_3 & v_3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -v_3 & v_2 \end{pmatrix}^T = \begin{pmatrix} 1 & v_2 - u_3 \\ 0 & \det(\beta_0) \end{pmatrix};$$

if $u_2 = v_3 = 0$ and $u_3 \neq -v_2$, then

$$(u_3 + v_2)^{-1}\begin{pmatrix} 1 & 1 \\ -u_3 & v_2 \end{pmatrix}\begin{pmatrix} 0 & v_2 \\ u_3 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -u_3 & v_2 \end{pmatrix}^T = \begin{pmatrix} 1 & v_2 - u_3 \\ 0 & \det(\beta_0) \end{pmatrix},$$

and finally if $u_2 = v_3 = 0$ and $u_3 = -v_2$, then

$$bI\beta_0 I^T = \beta_0.$$

Thus every one of our regular subgroups above is conjugate to one of the form

$$\left\langle \rho, \sigma\alpha_1, \sigma^{t_2}\tau^{t_3}\alpha_3 \right\rangle, \left\langle \rho, \tau^{-t_4}\alpha_1, \sigma^{t_4}\alpha_3 \right\rangle \text{ for some } t_2, t_3, t_4,$$

and these for different values of $t_2, t_3$, and $t_4$ are not conjugate to each other.

Therefore, we find non-isomorphic skew braces

$$\begin{aligned} &\left\langle \rho, \sigma\alpha_1, \sigma^{u_2}\tau^{u_2}\alpha_3 \right\rangle, \left\langle \rho, \tau^{-2}\alpha_1, \sigma^2\alpha_3 \right\rangle \cong C_p^3, \\ &\left\langle \rho, \sigma\alpha_1, \sigma^{u_3}\tau^{u_4}\alpha_3 \right\rangle, \left\langle \rho, \tau^{-u_5}\alpha_1, \sigma^{u_5}\alpha_3 \right\rangle \cong M_1 \\ &\text{for } u_4 = 0, ..., p-1,\ u_2, u_3, u_5 = 1, ..., p-1 \text{ with } u_5 \neq 2,\ u_3 - u_4 \not\equiv 0 \bmod p. \end{aligned} \tag{25}$$

**Case II:** Next, we consider subgroups of the form

$$G = \langle \rho, x\alpha_1, y\alpha_2\alpha_3^a \rangle \text{ with } x_2 = 0.$$

Note, we have

$$\begin{aligned}(x\alpha_1)\left(y\alpha_2\alpha_3^a\right) &= \rho^{y_2}xy\alpha_1\alpha_2\alpha_3^a \text{ and}\\ \left(y\alpha_2\alpha_3^a\right)(x\alpha_1) &= \rho^{ax_3-x_3y_2}xy\alpha_1\alpha_2\alpha_3^a,\end{aligned} \tag{26}$$

so $G$ is abelian if and only if $y_2 \equiv ax_3 - x_3y_2 \bmod p$; furthermore, we need $x_3, y_2 \neq 0$ for $G$ to be regular.

Therefore, for $y_2 \equiv ax_3 - x_3y_2 \bmod p$ we find regular subgroups isomorphic to $C_p^3$ of the form

$$\left\langle \rho, \tau^{x_3}\alpha_1, \sigma^{y_2}\tau^{y_3}\alpha_2\alpha_3^{(1+x_3)y_2x_3^{-1}} \right\rangle \cong C_p^3 \tag{27}$$
$$\text{for } y_3 = 0, ..., p-1,\ y_2, x_3 = 1, ..., p-1,$$

and for $ax_3 \not\equiv y_2 + x_3y_2 \bmod p$, we find regular subgroups isomorphic to $M_1$ of the form

$$\langle \rho, \tau^{x_3}\alpha_1, y\alpha_2\alpha_3^a \rangle \cong M_1 \tag{28}$$
$$\text{for } a, y_3 = 0, ..., p-1,\ x_3, y_2 = 1, ..., p-1 \text{ with } ax_3 - y_2 - x_3y_2 \not\equiv 0 \bmod p.$$

Note, in the abelian case we have $y_2 \equiv ax_3 - x_3y_2 \bmod p$, and since $x_3 \neq 0$, we can rearrange to get $a = (1 + x_3)y_2x_3^{-1}$.

To find the non-isomorphic skew braces corresponding to the above regular subgroups, it suffices to work with automorphisms corresponding to elements of the form $\beta \overset{\text{def}}{=} \left(\begin{smallmatrix} b_1 & 0 \\ b_3 & b_4 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_p)$. Then, using (12) and (14), we have

$$\begin{aligned}
&\left(\alpha_3^{r_3}\beta\right)\left(\tau^{x_3}\alpha_1\right)^{b_4^{-1}}\left(\alpha_3^{r_3}\beta\right)^{-1} = \rho^{\kappa_1}\tau^{x_3}\alpha_1 \text{ and}\\
&\left(\alpha_3^{r_3}\beta\right)\left(\tau^{x_3}\alpha_1\right)^{ab_1b_3b_4^{-2}-r_3b_4^{-1}-\frac{1}{2}b_4^{-1}(1-b_1)-\frac{1}{2}ab_1b_4^{-1}\left(b_1b_4^{-1}-1\right)}\left(y\alpha_2\alpha_3^a\right)^{b_1b_4^{-1}}\left(\alpha_3^{r_3}\beta\right)^{-1}\\
&= \rho^{\kappa_2}\sigma^{y_2b_1^2b_4^{-1}}\tau^{\left(ab_1b_3b_4^{-2}-r_3b_4^{-1}-\frac{1}{2}b_4^{-1}(1-b_1)-\frac{1}{2}ab_1b_4^{-1}\left(b_1b_4^{-1}-1\right)\right)x_3+b_1y_3+\frac{1}{2}b_1\left(b_1b_4^{-1}-1\right)y_2}\alpha_2\alpha_3^{ab_1^2b_4^{-1}},
\end{aligned}$$

for some $\kappa_1, \kappa_2$, and $r_3$. Now conjugating the subgroup $\langle \rho, \tau^{x_3}\alpha_1, y\alpha_2\alpha_3^a \rangle$ with the automorphism corresponding to $\alpha_3^{\frac{1}{2}(y_2^{-1}-1)-y_2x_3^{-1}}\left(\begin{smallmatrix} y_2^{-1} & 0 \\ 0 & y_2^{-1} \end{smallmatrix}\right)$ we get $\left\langle \rho, \tau^{x_3}\alpha_1, \sigma\alpha_2\alpha_3^{ay_2^{-1}} \right\rangle$, and these subgroups for different values of $a$ and $x_3$ and $y_2$ are not conjugate to each other.

Therefore, we find non-isomorphic skew braces

$$\left\langle \rho, \tau^{\tilde{x}_3}\alpha_1, \sigma\alpha_2\alpha_3^{(1+\tilde{x}_3)\tilde{x}_3^{-1}} \right\rangle \cong C_p^3,\ \langle \rho, \tau^{x_3}\alpha_1, \sigma\alpha_2\alpha_3^a \rangle \cong M_1 \tag{29}$$
$$\text{for } a = 0, ..., p-1,\ \tilde{x}_3, x_3 = 1, ..., p-1 \text{ with } a - (1+x_3)x_3^{-1} \not\equiv 0 \bmod p.$$

Thus, the corresponding non-isomorphic skew braces, combining (25) and (29), are

$$\langle \rho, \sigma\alpha_1, \sigma^{u_3}\tau^{u_4}\alpha_3 \rangle, \langle \rho, \tau^{-u_5}\alpha_1, \sigma^{u_5}\alpha_3 \rangle, \langle \rho, \tau^{x_3}\alpha_1, \sigma\alpha_2\alpha_3^a \rangle \cong M_1,$$

$$\langle\rho,\sigma\alpha_1,\sigma^{u_2}\tau^{u_2}\alpha_3\rangle,\langle\rho,\tau^{-2}\alpha_1,\sigma^2\alpha_3\rangle,\left\langle\rho,\tau^{\tilde{x}_3}\alpha_1,\sigma\alpha_2\alpha_3^{(1+\tilde{x}_3)\tilde{x}_3^{-1}}\right\rangle\cong C_p^3 \text{ for}$$
$$a,u_3=0,...,p-1,\ u_2,u_4,u_5,\tilde{x}_3,x_3,=1,...,p-1$$
$$\text{with } u_5\neq 2,\ u_3-u_4\not\equiv 0 \bmod p,\ ax_3-(1+x_3)\not\equiv 0 \bmod p.$$

Therefore, there are

$$(p-1)p-(p-1)+(p-2)+(p-1)p-(p-1)=(2p-3)p$$

$M_1$-skew braces of $M_1$ type and

$$(p-1)+1+(p-1)=2p-1$$

$C_p^3$-skew braces of $M_1$ type. □

**Lemma 4.5.** *There are*

$$(p^4-p^3-2p^2+2p+1)p$$

*Hopf–Galois structures of $M_1$ type on Galois extensions of fields with Galois group $G\cong M_1$ and $|\Theta(G)|=p^2$, and exactly*

$$(p^3-1)(p^2-2)p^2$$

*Hopf–Galois structures of $M_1$ type on Galois extensions of fields with Galois group $G\cong C_p^3$ and $|\Theta(G)|=p^2$.*

**Proof.** To find the number of Hopf–Galois structures corresponding to the skew braces of Lemma 4.4, we need to find the automorphism groups of the skew braces

$$\langle\rho,\sigma\alpha_1,\sigma^{u_3}\tau^{u_4}\alpha_3\rangle,\langle\rho,\tau^{-u_5}\alpha_1,\sigma^{u_5}\alpha_3\rangle,\langle\rho,\tau^{x_3}\alpha_1,\sigma\alpha_2\alpha_3^{a}\rangle\cong M_1,$$
$$\langle\rho,\sigma\alpha_1,\sigma^{u_2}\tau^{u_2}\alpha_3\rangle,\langle\rho,\tau^{-2}\alpha_1,\sigma^2\alpha_3\rangle,\left\langle\rho,\tau^{\tilde{x}_3}\alpha_1,\sigma\alpha_2\alpha_3^{(1+\tilde{x}_3)\tilde{x}_3^{-1}}\right\rangle\cong C_p^3 \text{ for}$$
$$a,u_3=0,...,p-1,\ u_2,u_4,u_5,x_3,\tilde{x}_3=1,...,p-1$$
$$\text{with } u_5\neq 2,\ u_3-u_4\not\equiv 0 \bmod p,\ ax_3-(1+x_3)\not\equiv 0 \bmod p.$$

We let

$$\alpha=\gamma\beta\in\mathrm{Aut}(M_1)\text{ where }\gamma\stackrel{\text{def}}{=}\alpha_1^{r_1}\alpha_3^{r_3},\ \beta\stackrel{\text{def}}{=}\begin{pmatrix}b_1 & b_2\\ b_3 & b_4\end{pmatrix},$$

and set $b\stackrel{\text{def}}{=}\det(\beta)^{-1}$.

**For skew braces of Case I of Lemma 4.4**: If $\alpha\in\mathrm{Aut}_{\mathcal{B}r}(\langle\rho,\sigma\alpha_1,\sigma^{u_2}\tau^{u_3}\alpha_3\rangle)$, since we have

$$\alpha\left(\sigma\alpha_1\right)^{b_1 b}\left(\sigma^{u_2}\tau^{u_3}\alpha_3\right)^{b_2 b}\alpha^{-1} = \rho^{\kappa_1}\left(b\beta\left(\begin{smallmatrix} 1 & u_2 \\ 0 & u_2 \end{smallmatrix}\right)\beta^T\right)\cdot\sigma\alpha_1,$$
$$\alpha\left(\sigma\alpha_1\right)^{b_3 b}\left(\sigma^{u_2}\tau^{u_3}\alpha_3\right)^{b_4 b}\alpha^{-1} = \rho^{\kappa_2}\left(b\beta\left(\begin{smallmatrix} 1 & u_2 \\ 0 & u_2 \end{smallmatrix}\right)\beta^T\right)\cdot\tau\alpha_3,$$

we must have

$$b\beta\begin{pmatrix} 1 & u_2 \\ 0 & u_3 \end{pmatrix}\beta^T = b\begin{pmatrix} b_1^2 + b_2(b_1u_2 + b_2u_3) & b_1(b_3 + b_4u_2) + b_2b_4u_3 \\ b_1b_3 + b_2(b_3u_2 + b_4u_3) & b_3^2 + b_4(b_3u_2 + b_4u_3) \end{pmatrix} = \begin{pmatrix} 1 & u_2 \\ 0 & u_3 \end{pmatrix}.$$

Thus we need

$$\begin{aligned} b_1^2 + b_2(b_1u_2 + b_2u_3) &= b_1b_4 - b_2b_3 \\ b_1b_3 + b_2(b_3u_2 + b_4u_3) &= 0 \\ b_3^2 + b_4(b_3u_2 + b_4u_3) &= (b_1b_4 - b_2b_3)u_3. \end{aligned}$$

The second and third equations give

$$\begin{aligned} b_1b_3b_4 + b_2b_4(b_3u_2 + b_4u_3) &= 0 \\ b_2b_3^2 + b_2b_4(b_3u_2 + b_4u_3) &= b_2(b_1b_4 - b_2b_3)u_3, \end{aligned}$$

so we must have

$$-b_1b_3b_4 + b_2b_3^2 = b_2(b_1b_4 - b_2b_3)u_3,$$

which implies that we must set $b_3 = -b_2u_3$ and $b_4 = b_1 + b_2u_2$ which satisfies all three equations. Thus we must have

$$\mathrm{Aut}_{\mathcal{B}r}(\langle\rho, \sigma\alpha_1, \sigma^{u_2}\tau^{u_3}\alpha_3\rangle) = \left\{\alpha \in \mathrm{Aut}(M_1) \mid \alpha = \alpha_1^{r_1}\alpha_3^{r_3}\left(\begin{smallmatrix} b_1 & b_2 \\ -b_2u_3 & b_1+b_2u_2 \end{smallmatrix}\right)\right\},$$

where we need $b_1^2 + b_1b_2u_2 + b_2^2u_3 \neq 0$, i.e.,

$$\left(b_1u_2 + 2b_2u_3\right)^2 \neq b_1^2\left(u_2^2 - 4u_3\right).$$

We now need to consider three cases for $u_2^2 - 4u_3 = 0$ and when $u_2^2 - 4u_3$ is a square modulo $p$ or not. We find

$$\begin{aligned} \left|\mathrm{Aut}_{\mathcal{B}r}\left(\left\langle\rho, \sigma\alpha_1, \sigma^{u_2}\tau^{u_2^2/4}\alpha_3\right\rangle\right)\right| &= (p-1)p^3 \text{ for } u_2 \neq 0, \\ \left|\mathrm{Aut}_{\mathcal{B}r}\left(\langle\rho, \sigma\alpha_1, \sigma^{u_2}\tau^{u_3}\alpha_3\rangle\right)\right| &= (p-1)^2p^2 \text{ if } u_3 \neq 0 \text{ and } u_2^2 - 4u_3 \neq 0 \text{ is a square}, \\ \left|\mathrm{Aut}_{\mathcal{B}r}\left(\langle\rho, \sigma\alpha_1, \sigma^{u_2}\tau^{u_3}\alpha_3\rangle\right)\right| &= (p^2-1)p^2 \text{ if } u_3 \neq 0 \text{ and } u_2^2 - 4u_3 \neq 0 \text{ is not a square}. \end{aligned}$$

We also have

$$\mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \tau^{-v_2}\alpha_1, \sigma^{v_2}\alpha_3\rangle) = \left\{\alpha \in \mathrm{Aut}(M_1) \mid \alpha = \alpha_1^{r_1}\alpha_3^{r_3}\left(\begin{smallmatrix} b_1 & b_2 \\ b_3 & b_4 \end{smallmatrix}\right)\right\}.$$

**For skew braces of Case II of Lemma 4.4**: If $\alpha \in \mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \tau^{x_3}\alpha_1, \sigma\alpha_2\alpha_3^a\rangle)$, we need to set $b_2 = 0$, now since we have

$$\alpha\left(\tau^{x_3}\alpha_1\right)^{b_4^{-1}}\alpha^{-1} = \rho^{\kappa_1}\tau^{x_3}\alpha_1 \text{ and}$$
$$\alpha\left(\tau^{x_3}\alpha_1\right)^{ab_1b_3b_4^{-2}-r_3b_4^{-1}-\frac{1}{2}b_4^{-1}(1-b_1)-\frac{1}{2}ab_1b_4^{-1}\left(b_1b_4^{-1}-1\right)}\left(y\alpha_2\alpha_3^a\right)^{b_1b_4^{-1}}\alpha^{-1}$$
$$= \rho^{\kappa_2}\sigma^{b_1^2b_4^{-1}}\tau^{\left(ab_1b_3b_4^{-2}-r_3b_4^{-1}-\frac{1}{2}b_4^{-1}(1-b_1)-\frac{1}{2}ab_1b_4^{-1}\left(b_1b_4^{-1}-1\right)\right)x_3+\frac{1}{2}b_1\left(b_1b_4^{-1}-1\right)}\alpha_2\alpha_3^{ab_1^2b_4^{-1}},$$

we must have $b_4 = b_1^2$ and

$$r_3 = ab_1^{-1}b_3 + \frac{1}{2}(b_1-1)(1+a) + \frac{1}{2}b_1^2x_3^{-1}(b_1+1);$$

thus we must have

$$\mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \tau^{x_3}\alpha_1, \sigma\alpha_2\alpha_3^a\rangle) = \left\{\alpha \in \mathrm{Aut}(M_1) \mid \alpha = \alpha_1^{r_1}\alpha_3^{ab_1^{-1}b_3+\frac{1}{2}(b_1-1)(1+a)+\frac{1}{2}b_1^2x_3^{-1}(b_1+1)}\left(\begin{smallmatrix} b_1 & 0 \\ b_3 & b_1^2 \end{smallmatrix}\right)\right\}.$$

Therefore, we have

$$e(M_1, M_1, p^2) = \sum_{(M_1)_{M_1}(p^2)} \frac{|\mathrm{Aut}(M_1)|}{|\mathrm{Aut}_{\mathcal{B}r}((M_1)_{M_1})|} =$$
$$\sum_{u_2\neq 0,4} \frac{|\mathrm{Aut}(M_1)|}{\left|\mathrm{Aut}_{\mathcal{B}r}(\left\langle \rho, \sigma\alpha_1, \sigma^{u_2}\tau^{\frac{u_2^2}{4}}\alpha_3\right\rangle)\right|} + \sum_{\substack{u_2-u_3,u_3,u_2^2-4u_3\neq 0\\ u_2^2-4u_3 \text{ is a square}}} \frac{|\mathrm{Aut}(M_1)|}{|\mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \sigma\alpha_1, \sigma^{u_2}\tau^{u_3}\alpha_3\rangle)|} +$$
$$\sum_{\substack{u_2-u_3,u_3,u_2^2-4u_3\neq 0\\ u_2^2-4u_3 \text{ is not a square}}} \frac{|\mathrm{Aut}(M_1)|}{|\mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \sigma\alpha_1, \sigma^{u_2}\tau^{u_2}\alpha_3\rangle)|} + \sum_{v_2\neq 0,2} \frac{|\mathrm{Aut}(M_1)|}{|\mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \tau^{-v_2}\alpha_1, \sigma^{v_2}\alpha_3\rangle)|} +$$
$$\sum_{\substack{x_3\neq 0,\ a\\ (1+x_3)x_3^{-1}\neq a}} \frac{|\mathrm{Aut}(M_1)|}{|\mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \tau^{x_3}\alpha_1, \sigma\alpha_2\alpha_3^a\rangle)|}$$
$$= (p^2-1)(p^2-p)p^2\times$$
$$\left(\frac{p-2}{(p-1)p^3} + \frac{\frac{p-1}{2} + \left(\frac{p-1}{2}-1\right)(p-2)}{(p-1)^2p^2} + \frac{\frac{p-1}{2} + \left(\frac{p-1}{2}\right)(p-2)}{(p^2-1)p^2} + \frac{p-2}{(p^2-1)(p^2-p)p^2}\right.$$
$$\left. + \frac{(p-1)^2}{(p-1)p^2}\right)$$
$$= (p^4 - p^3 - 2p^2 + 2p + 1)p,$$

and similarly

$$e(C_p^3, M_1, p^2) = \sum_{(C_p^3)_{M_1}(p^2)} \frac{\left|\mathrm{Aut}(C_p^3)\right|}{\left|\mathrm{Aut}_{\mathcal{B}r}((C_p^3)_{M_1})\right|} =$$

$$\frac{\left|\mathrm{Aut}(C_p^3)\right|}{\left|\mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \sigma\alpha_1, \sigma^4\tau^4\alpha_3\rangle)\right|} + \sum_{\substack{u_2^2-4u_2\neq 0 \\ \text{is a square}}} \frac{\left|\mathrm{Aut}(C_p^3)\right|}{\left|\mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \sigma\alpha_1, \sigma^{u_2}\tau^{u_2}\alpha_3\rangle)\right|} +$$

$$\sum_{\substack{u_2^2-4u_2\neq 0 \\ \text{is not a square}}} \frac{\left|\mathrm{Aut}(C_p^3)\right|}{\left|\mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \sigma\alpha_1, \sigma^{u_2}\tau^{u_2}\alpha_3\rangle)\right|} + \frac{\left|\mathrm{Aut}(C_p^3)\right|}{\left|\mathrm{Aut}_{\mathcal{B}r}(\langle \rho, \tau^{-2}\alpha_1, \sigma^2\alpha_3\rangle\right|} +$$

$$\sum_{x_3\neq 0} \frac{\left|\mathrm{Aut}(C_p^3)\right|}{\left|\mathrm{Aut}_{\mathcal{B}r}(\left\langle \rho, \tau^{x_3}\alpha_1, \sigma\alpha_2\alpha_3^{(1+x_3)x_3^{-1}}\right\rangle)\right|}$$

$$= (p^3-1)(p^3-p)(p^3-p^2)\times$$

$$\left(\frac{1}{(p-1)p^3} + \frac{\frac{p-1}{2}-1}{(p-1)^2p^2} + \frac{\frac{p-1}{2}}{(p^2-1)p^2} + \frac{1}{(p^2-1)(p^2-p)p^2} + \frac{p-1}{(p-1)p^2}\right)$$

$$= (p^3-1)(p^2-2)p^2. \quad \square$$

**Lemma 4.6.** *For $|\Theta(G)| = p^3$ there are exactly four $M_1$-skew braces of $M_1$ type and no other. Furthermore, there are only*

$$(p^2-1)p^3$$

*Hopf–Galois structures of $M_1$ type on Galois extensions of fields with Galois group $G \cong M_1$ and $|\Theta(G)| = p^3$.*

**Proof.** If $G \subseteq \mathrm{Hol}(M_1)$ with $|\Theta(G)| = p^3$, then we can assume, without loss of generality, that $\Theta(G) = \langle \alpha_1, \alpha_2, \alpha_3\rangle$, and so

$$G = \langle u\alpha_1, v\alpha_2, w\alpha_3\rangle$$

where $u = \rho^{u_1}\sigma^{u_2}\tau^{u_3}$, $v = \rho^{v_1}\sigma^{v_2}\tau^{v_3}$, $w = \rho^{w_1}\sigma^{w_2}\tau^{w_3}$, and $G$ is isomorphic to $\Theta(G) \cong M_1$. Now

$$(u\alpha_1)(v\alpha_2) = \rho^{v_2}uv\alpha_1\alpha_2 \text{ and}$$
$$(v\alpha_2)(u\alpha_1) = \rho^{\frac{1}{2}u_2(u_2-1)+v_3u_2-u_3v_2-u_2^2-u_2v_2}\tau^{u_2}uv\alpha_1\alpha_2,$$

so we need $u_2 = 0$ and $v_2 \equiv -u_3v_2 \bmod p$. We have

$$(u\alpha_1)(w\alpha_3) = \rho^{w_2} uw\alpha_1\alpha_3 \text{ and}$$
$$(w\alpha_3)(u\alpha_1) = \rho^{u_3+w_3u_2-u_3w_2} uw\alpha_1\alpha_3,$$

so, since $u_2 = 0$, we need $w_2 \equiv u_3 - u_3w_2 \bmod p$. Finally, we have

$$\begin{aligned}(u\alpha_1)(v\alpha_2)(w\alpha_3) &= (\rho^{v_2} uv\alpha_1\alpha_2)(w\alpha_3)\\ &= \rho^{u_1-v_2(w_2-1)-\frac{1}{2}w_2(w_2-1)}\tau^{u_3+w_2} vw\alpha_1\alpha_2\alpha_3 \text{ and}\\ (w\alpha_3)(v\alpha_2) &= \rho^{v_3+w_3v_2-v_3w_2} vw\alpha_3\alpha_2,\end{aligned}$$

so we need $u_3 + w_2 \equiv 0 \bmod p$ and

$$u_1 - v_2(w_2 - 1) - \frac{1}{2}w_2(w_2 - 1) \equiv v_3 + w_3v_2 - v_3w_2 \bmod p.$$

Combining the above information, for $G$ to be a group of order $p^3$, we need, modulo $p$,

$$\begin{aligned}&u_2 = 0,\ v_2 = -u_3v_2,\ w_2 = u_3 - u_3w_2,\ u_3 = -w_2,\\ &u_1 - v_2(w_2 - 1) - \frac{1}{2}w_2(w_2 - 1) = v_3 + w_3v_2 - v_3w_2.\end{aligned} \tag{30}$$

Now the equations $w_2 = u_3 - u_3w_2$ and $u_3 = -w_2$ imply that

$$u_3 = -w_2 = 0, -2.$$

Given this, the equation $v_2 = -u_3v_2$ implies that $v_2 = 0$. Now the final equation in (30) reduces to

$$u_1 - \frac{1}{2}w_2(w_2 - 1) = v_3 - v_3w_2.$$

Thus, we can consider two cases for $w_2 = 0$ and $w_2 = 2$. If $w_2 = 0$, then $u, v$ and $w$ are of the form

$$u = \rho^{u_1},\ v = \rho^{v_1}\tau^{u_1},\ w = \rho^{w_1}\tau^{w_3},$$

and in this case $G$ cannot be regular. Therefore, we must set $w_2 = 2$, hence $u, v$, and $w$ are of the form

$$u = \rho^{u_1}\tau^{-2},\ v = \rho^{v_1}\tau^{1-u_1},\ w = \rho^{w_1}\sigma^2\tau^{w_3}.$$

Now for $G$ to be regular we need

$$(u\alpha_1)^{\frac{1}{2}(1-u_1)}(w\alpha_3) = \rho^{v_1+\frac{1}{2}u_1(1-u_1)}\alpha_1^{\frac{1}{2}(1-u_1)}\alpha_3 \notin \mathrm{Aut}(M_1),$$

so we need $v_1 + \frac{1}{2}u_1(1-u_1) \not\equiv 0 \bmod p$. Therefore, $G$ is conjugate to

$$\left\langle \rho^{u_1}\tau^{-2}\alpha_1, \rho^{v_1}\tau^{1-u_1}\alpha_2, \rho^{w_1}\sigma^2\tau^{w_3}\alpha_3 \right\rangle \cong M_1$$
$$\text{for } u_1, v_1, w_1, w_3 = 0, ..., p-1 \text{ with } v_1 + \frac{1}{2}u_1(1-u_1) \not\equiv 0 \bmod p,$$

and there are (taking into account the $p+1$ conjugates)

$$(p+1)(p-1)p^3$$

of these.

To find the non-isomorphic skew braces corresponding to the above regular subgroups, it suffices to conjugate by automorphisms of the form $\alpha \overset{\text{def}}{=} \beta\gamma \in \operatorname{Aut}(M_1)$, where $\beta \overset{\text{def}}{=} \left(\begin{smallmatrix} b_1 & 0 \\ b_3 & b_4 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_p)$ and $\gamma \overset{\text{def}}{=} \alpha_1^{r_1}\alpha_3^{r_3} \in C_p^2$. Now using (12) and (14) we have

$$\begin{aligned}
\alpha\left(u\alpha_1\right)^{b_4^{-1}}\alpha^{-1} &= \left(\alpha\cdot u^{b_4^{-1}}\right)\alpha_1,\\
\alpha\left(v\alpha_2\right)^{b_1b_4^{-1}}\alpha^{-1} &= \left(\alpha\cdot v^{b_1b_4^{-1}}\right)\alpha_1^{r_3+\frac{1}{2}(1-b_1)}\alpha_2,\\
\alpha\left(w\alpha_3\right)^{b_1^{-1}}\alpha^{-1} &= \left(\alpha\cdot\left(\rho^{\frac{1}{2}w_3b_1^{-1}\left(b_1^{-1}-1\right)}w^{b_1^{-1}}\right)\right)\alpha_1^{-b_1^{-1}b_3}\alpha_3,
\end{aligned}$$

so we have

$$\begin{aligned}
&\alpha\left(u\alpha_1\right)^{b_4^{-1}}\alpha^{-1} = \left(\alpha\cdot u^{b_4^{-1}}\right)\alpha_1,\\
&\alpha\left(u\alpha_1\right)^{-r_3b_4^{-1}-\frac{1}{2}b_4^{-1}(1-b_1)}\left(v\alpha_2\right)^{b_1b_4^{-1}}\alpha^{-1} = \left(\alpha\cdot\left(u^{-r_3b_4^{-1}-\frac{1}{2}b_4^{-1}(1-b_1)}v^{b_1b_4^{-1}}\right)\right)\alpha_2,\\
&\alpha\left(u\alpha_1\right)^{b_1^{-1}b_3b_4^{-1}}\left(w\alpha_3\right)^{b_1^{-1}}\alpha^{-1} = \left(\left(\alpha\cdot u^{b_1^{-1}b_3b_4^{-1}}\right)\alpha\alpha_1^{b_1^{-1}b_3b_4^{-1}}\cdot\left(\rho^{\frac{1}{2}w_3b_1^{-1}\left(b_1^{-1}-1\right)}w^{b_1^{-1}}\right)\right)\alpha_3.
\end{aligned}$$

Note that we have

$$\alpha = \begin{bmatrix} b_1b_4 & \frac{1}{2}b_1b_3+r_1b_1+r_3b_3 & r_3b_4 \\ 0 & b_1 & 0 \\ 0 & b_3 & b_4 \end{bmatrix}.$$

We let $b_5 \overset{\text{def}}{=} \frac{1}{2}b_1b_3 + r_1b_1 + r_3b_3$. Now

$$\begin{aligned}
&\alpha\cdot u^{b_4^{-1}} = \rho^{u_1b_1-2r_3}\tau^{-2},\\
&\alpha\cdot\left(u^{-r_3b_4^{-1}-\frac{1}{2}b_4^{-1}(1-b_1)}v^{b_1b_4^{-1}}\right) = \rho^{r_3(2r_3+1)+v_1b_1^2+\frac{1}{2}u_1b_1(b_1-1)-2r_3u_1b_1}\tau^{1+2r_3-u_1b_1},\\
&\left(\alpha\cdot u^{b_1^{-1}b_3b_4^{-1}}\right)\left(\alpha\alpha_1^{b_1^{-1}b_3b_4^{-1}}\cdot\left(\rho^{\frac{1}{2}w_3b_1^{-1}\left(b_1^{-1}-1\right)}w^{b_1^{-1}}\right)\right) = \rho^{b_3u_1-2r_3b_1^{-1}b_3}\tau^{-2b_1^{-1}b_3}\\
&\rho^{\frac{3}{2}w_3b_4\left(b_1^{-1}-1\right)+b_4w_1+2b_1^{-1}b_3+2b_1^{-1}b_5+b_3(2b_1^{-1}-1)}\sigma^2\tau^{2b_1^{-1}b_3+w_3b_1^{-1}b_4}
\end{aligned}$$

$$= \rho^{2r_1+\frac{3}{2}w_3b_4\left(b_1^{-1}-1\right)+b_4w_1+u_1b_3}\sigma^2\tau^{w_3b_1^{-1}b_4}.$$

We let

$$r_1 = -\frac{3}{4}w_3b_4\left(b_1^{-1}-1\right) - \frac{1}{2}b_4w_1 - \frac{1}{2}u_1b_3,$$
$$r_3 = \frac{1}{2}u_1b_1,$$

which gives us

$$\alpha \cdot u^{b_4^{-1}} = \tau^{-2},$$
$$\alpha\cdot\left(u^{-r_3b_4^{-1}-\frac{1}{2}b_4^{-1}(1-b_1)}v^{b_1b_4^{-1}}\right) = \rho^{(v_1+\frac{1}{2}u_1(1-u_1))b_1^2}\tau,$$
$$\left(\alpha\cdot u^{b_1^{-1}b_3b_4^{-1}}\right)\left(\alpha\alpha_1^{b_1^{-1}b_3b_4^{-1}}\cdot\left(\rho^{\frac{1}{2}w_3b_1^{-1}\left(b_1^{-1}-1\right)}w^{b_1^{-1}}\right)\right) = \sigma^2\tau^{w_3b_1^{-1}b_4}.$$

Next, for a fixed $\delta \in \mathbb{F}_p^{\times}$ which is not a square, we can write

$$\left(v_1 + \frac{1}{2}u_1\left(1-u_1\right)\right) = s_1^2 s$$

where $s_1 \in \mathbb{F}_p^{\times}$ and $s = 1, \delta$. Letting $b_1 = \pm s_1^{-1}$ we get

$$\alpha \cdot u^{b_4^{-1}} = \tau^{-2},$$
$$\alpha\cdot\left(u^{-r_3b_4^{-1}-\frac{1}{2}b_4^{-1}(1-b_1)}v^{b_1b_4^{-1}}\right) = \rho^{s}\tau,$$
$$\left(\alpha\cdot u^{b_1^{-1}b_3b_4^{-1}}\right)\left(\alpha\alpha_1^{b_1^{-1}b_3b_4^{-1}}\cdot\left(\rho^{\frac{1}{2}w_3b_1^{-1}\left(b_1^{-1}-1\right)}w^{b_1^{-1}}\right)\right) = \sigma^2\tau^{\pm s_1w_3b_4}.$$

Therefore, every such regular subgroup is conjugate to

$$\left\langle \tau^{-2}\alpha_1, \rho^s\tau\alpha_2, \sigma^2\tau^{t_3}\alpha_3\right\rangle \cong M_1 \text{ for } t_3 = 0,1,\ s = 1,\delta, \tag{31}$$

and these subgroups are not further conjugate to each other, so they give us four non-isomorphic skew braces.

To find the number of corresponding Hopf–Galois structures we determine the automorphism groups of above skew braces. We let

$$\alpha = \gamma\beta \in \mathrm{Aut}(M_1) \text{ where } \gamma \stackrel{\text{def}}{=} \alpha_1^{r_1}\alpha_3^{r_3},\ \beta \stackrel{\text{def}}{=} \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$$

and set $b_2 = 0$. If $\alpha \in \mathrm{Aut}_{\mathcal{B}r}(\langle \tau^{-2}\alpha_1, \rho^s\tau\alpha_2, \sigma^2\tau^{t_3}\alpha_3\rangle)$, since by our notation above we have

$$\alpha \cdot u^{b_4^{-1}} = \rho^{-2r_3}\tau^{-2},$$

$$\alpha\cdot \left(u^{-r_3 b_4^{-1} - \frac{1}{2}b_4^{-1}(1-b_1)}v^{b_1 b_4^{-1}}\right) = \rho^{r_3(2r_3+1)+sb_1^2}\tau^{1+2r_3},$$

$$\left(\alpha \cdot u^{b_1^{-1}b_3b_4^{-1}}\right)\left(\alpha\alpha_1^{b_1^{-1}b_3b_4^{-1}}\cdot\left(\rho^{\frac{1}{2}t_3b_1^{-1}\left(b_1^{-1}-1\right)}w^{b_1^{-1}}\right)\right) = \rho^{2r_1+\frac{3}{2}t_3b_4\left(b_1^{-1}-1\right)}\sigma^2\tau^{t_3b_1^{-1}b_4},$$

we must have $r_3 = 0$, $b_1^2 = 1$, $r_1 = \frac{3}{4}t_3b_4\left(1-b_1^{-1}\right)$, further $b_1 = b_4$ if $t_3 = 1$. Therefore, we have

$$\mathrm{Aut}_{\mathcal{B}r}(\langle\tau^{-2}\alpha_1, \rho^s\tau\alpha_2, \sigma^2\alpha_3\rangle) = \left\{\alpha \in \mathrm{Aut}(M_1) \mid \alpha = \left(\begin{smallmatrix}\pm1 & 0\\ b_3 & b_4\end{smallmatrix}\right)\right\},$$

$$\mathrm{Aut}_{\mathcal{B}r}(\langle\tau^{-2}\alpha_1, \rho^s\tau\alpha_2, \tau\sigma^2\alpha_3\rangle) = \left\{\alpha \in \mathrm{Aut}(M_1) \mid \alpha = \alpha_1^{\frac{3}{4}(\pm1-1)}\left(\begin{smallmatrix}\pm1 & 0\\ b_3 & \pm1\end{smallmatrix}\right)\right\}.$$

Now again we find

$$e(M_1, M_1, p^3) = \sum_{(M_1)_{M_1}(p^3)} \frac{|\mathrm{Aut}(M_1)|}{|\mathrm{Aut}_{\mathcal{B}r}((M_1)_{M_1}(p^3)|} =$$

$$\frac{2\,|\mathrm{Aut}(M_1)|}{|\mathrm{Aut}_{\mathcal{B}r}(\langle\tau^{-2}\alpha_1, \rho\tau\alpha_2, \sigma^2\alpha_3\rangle)|} + \frac{2\,|\mathrm{Aut}(M_1)|}{|\mathrm{Aut}_{\mathcal{B}r}(\langle\tau^{-2}\alpha_1, \rho\tau\alpha_2, \tau\sigma^2\alpha_3\rangle)|}$$

$$= \frac{2(p^2-1)(p-1)p^3}{2(p-1)p} + \frac{2(p^2-1)(p-1)p^3}{2p} = (p^2-1)p^3. \quad \square$$

### 4.1. Socle and annihilator of skew braces of $M_1$ type

Finally, we note that from our classification of skew braces we are also able to determine their *socle* and *annihilator*. Let $B = (B, \oplus, \odot)$ be a skew brace. As before we let

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

and set

$$\Theta : \mathrm{Hol}\,(B, \oplus) \longrightarrow \mathrm{Aut}\,(B, \oplus)$$
$$\eta\alpha \longmapsto \alpha.$$

We shall denote by $\lambda = \Theta m$. Then $\mathrm{Ker}\,\lambda = \mathrm{Im}\,m \cap (B, \oplus)$ inside $\mathrm{Hol}\,(B, \oplus)$.

First we note that [cf. 15, p. 23] an *ideal* of a skew brace $B = (B, \oplus, \odot)$ is defined to be a subset $I \subseteq B$, such that $I$ is a normal subgroup with respect to both operations $\oplus$ and $\odot$, and $\lambda_a(I) \subseteq I$ for all $a \in B$. The *socle* of $B$ is defined to be

$$\mathrm{Soc}(B) \stackrel{\text{def}}{=} \{a \in B \mid a \oplus b = a \odot b,\ b \oplus (b \odot a) = (b \odot a) \oplus b \text{ for all } b \in B\},$$

which is an ideal of $B$, and one has $\mathrm{Soc}(B) = \mathrm{Ker}\,\lambda \cap \mathrm{Z}\,(B,\oplus)$. Finally, [cf. 19, Definition 7], the *annihilator* of $B$ is defined to be

$$\mathrm{Ann}(B) \stackrel{\mathrm{def}}{=} \mathrm{Soc}(B) \cap \mathrm{Z}\,(B,\odot) = \mathrm{Ker}\,\lambda \cap \mathrm{Z}\,(B,\oplus) \cap \mathrm{Z}\,(B,\odot)\,,$$

which is also an ideal of $B$.

Now we aim to explain what each of these terms, ideal, socle, and annihilator, correspond to if we are given a regular subgroup $H \subseteq \mathrm{Hol}\,(N)$ and we consider it as a skew brace. Recall first from Subsection 2.2, given a regular subgroup $H \subseteq \mathrm{Hol}\,(N)$, it can be represented as

$$H = \langle \eta_1, ..., \eta_r, v_1\alpha_1, ..., v_s\alpha_s \rangle\,,$$

for $H_1 \stackrel{\mathrm{def}}{=} \langle \eta_1, ..., \eta_r \rangle \subseteq N$ and $H_2 \stackrel{\mathrm{def}}{=} \langle \alpha_1, ..., \alpha_s \rangle \subseteq \mathrm{Aut}\,(N)$ and some $v_1, ..., v_s \in N$. Note also that we have a bijection

$$\begin{aligned} \psi : H &\longrightarrow N \\ g &\longmapsto g_1 \stackrel{\mathrm{def}}{=} g(1_N). \end{aligned}$$

To get a skew brace we can set $(H,\odot) = H$ and define $\oplus$ on $H$ by

$$g \oplus h = \psi^{-1}\,(g_1 h_1)\,,$$

which makes $(H,\oplus,\odot)$ into a skew brace with $(H,\oplus) \stackrel{\psi}{\cong} N$. Note the map $\psi$ now induces an isomorphism

$$\begin{aligned} \mathrm{Hol}\,(H,\oplus) &\longrightarrow \mathrm{Hol}\,(N) \\ g\beta &\longmapsto g_1\psi\beta\psi^{-1}, \end{aligned}$$

which maps $\mathrm{Ker}\,\lambda$ to $H_1$, and $\mathrm{Im}\,\lambda$ to $H_2$.

Now for a subset $I \subseteq H$ to be an ideal of $H$ considered as a skew brace, we need $I \subseteq (H,\odot)$ to be a normal subgroup, $\psi\,(I) \subseteq N$ to be a normal subgroup (so $I \subseteq \psi^{-1}\,(N) = (H,\oplus)$ is a normal subgroup) and $H_2\,(\psi\,(I)) \subseteq \psi\,(I)$. Furthermore, one has

$$\mathrm{Soc}(H) = \mathrm{Ker}\,\lambda \cap \mathrm{Z}\,(H,\oplus) = H_1 \cap \psi^{-1}\,(Z\,(N))\,,$$

and

$$\mathrm{Ann}(H) = H_1 \cap \psi^{-1}\,(Z\,(N)) \cap \mathrm{Z}\,(H)\,.$$

Recall the skew braces of $M_1$ type, apart from the trivial skew brace $\langle \rho, \sigma, \tau \rangle$, as found in Lemmas 4.2, 4.4, 4.6 are as follows.

- For $|\mathrm{Ker}\,\lambda| = p^2$ from Lemma 4.2, (18) we have non-isomorphic skew braces

$$\langle \rho, \tau, \sigma\alpha_3 \rangle, \langle \rho, \tau, \sigma\alpha_2\alpha_3 \rangle \cong C_p^3,\ \langle \rho, \tau, \sigma\alpha_1 \rangle, \langle \rho, \tau, \sigma\alpha_2 \rangle,$$
$$\langle \rho, \tau, \sigma\alpha_3^c \rangle, \langle \rho, \tau, \sigma\alpha_2\alpha_3^c \rangle \cong M_1 \text{ for } c = 2, ..., p-1,$$

so in all these cases we have

$$\mathrm{Soc}(H) = \mathrm{Ann}(H) = \langle \rho \rangle.$$

- For $|\mathrm{Ker}\,\lambda| = p$ from Lemma 4.4, (25) and (29), we have non-isomorphic skew braces

$$\langle \rho, \sigma\alpha_1, \sigma^{u_3}\tau^{u_4}\alpha_3 \rangle, \langle \rho, \tau^{-u_5}\alpha_1, \sigma^{u_5}\alpha_3 \rangle, \langle \rho, \tau^{x_3}\alpha_1, \sigma\alpha_2\alpha_3^a \rangle \cong M_1,$$
$$\langle \rho, \sigma\alpha_1, \sigma^{u_2}\tau^{u_2}\alpha_3 \rangle, \langle \rho, \tau^{-2}\alpha_1, \sigma^2\alpha_3 \rangle, \left\langle \rho, \tau^{\tilde{x}_3}\alpha_1, \sigma\alpha_2\alpha_3^{(1+\tilde{x}_3)\tilde{x}_3^{-1}} \right\rangle \cong C_p^3 \text{ for}$$
$$a, u_3 = 0, ..., p-1,\ u_2, u_4, u_5, x_3, \tilde{x}_3 = 1, ..., p-1$$
$$\text{with } u_5 \neq 2,\ u_3 - u_4 \not\equiv 0 \bmod p,\ ax_3 - (1 + x_3) \not\equiv 0 \bmod p,$$

so in all these cases we also have

$$\mathrm{Soc}(H) = \mathrm{Ann}(H) = \langle \rho \rangle.$$

- For $|\mathrm{Ker}\,\lambda| = 1$ from Lemma 4.6, (31) we have non-isomorphic skew braces

$$\langle \tau^{-2}\alpha_1, \rho^s\tau\alpha_2, \sigma^2\tau^{t_3}\alpha_3 \rangle \cong M_1 \text{ for } t_3 = 0, 1,\ s = 1, \delta,$$

so in all these cases have

$$\mathrm{Soc}(H) = \mathrm{Ann}(H) = 1.$$

## Acknowledgments

The author is ever indebted to Prof Nigel Byott and Prof Agata Smoktunowicz for their continued support and useful suggestions. The author is ever grateful for the referee's comments which lead to numerous improvements to the manuscript.

This research was partially supported by the ERC Advanced grant 320974. The author obtained part of the results in this paper while studying for a PhD degree at the University of Exeter funded by an EPSRC Doctoral Training Grant.

## References

[1] W. Rump, Braces, radical rings, and the quantum Yang–Baxter equation, J. Algebra 307 (1) (2007) 153–170, https://doi.org/10.1016/j.jalgebra.2006.03.040.

[2] F. Cedó, E. Jespers, J. Okniński, Braces and the Yang–Baxter equation, Comm. Math. Phys. 327 (1) (2014) 101–116, https://doi.org/10.1007/s00220-014-1935-y.

[3] D. Bachiller, F. Cedó, E. Jespers, Solutions of the Yang–Baxter equation associated with a left brace, J. Algebra 463 (2016) 80–102, https://doi.org/10.1016/j.jalgebra.2016.05.024.

[4] L. Guarnieri, L. Vendramin, Skew braces and the Yang–Baxter equation, Math. Comp. 86 (307) (2017) 2519–2534, https://doi.org/10.1090/mcom/3161.

[5] S.U. Chase, M.E. Sweedler, Hopf Algebras and Galois Theory, Lecture Notes in Mathematics, vol. 97, Springer-Verlag, Berlin–New York, 1969.

[6] C. Greither, B. Pareigis, Hopf–Galois theory for separable field extensions, J. Algebra 106 (1) (1987) 239–258, https://doi.org/10.1016/0021-8693(87)90029-9.

[7] N.P. Byott, Uniqueness of Hopf–Galois structure for separable field extensions, Comm. Algebra 24 (10) (1996) 3217–3228, https://doi.org/10.1080/00927879608825743.

[8] N.P. Byott, Hopf–Galois structures on Galois field extensions of degree $pq$, J. Pure Appl. Algebra 188 (1–3) (2004) 45–57, https://doi.org/10.1016/j.jpaa.2003.10.010.

[9] N.P. Byott, Hopf–Galois structures on almost cyclic field extensions of 2-power degree, J. Algebra 318 (1) (2007) 351–371, https://doi.org/10.1016/j.jalgebra.2007.04.010.

[10] S. Carnahan, L. Childs, Counting Hopf–Galois structures on non-abelian Galois field extensions, J. Algebra 218 (1) (1999) 81–92, https://doi.org/10.1006/jabr.1999.7861.

[11] T. Kohl, Classification of the Hopf–Galois structures on prime power radical extensions, J. Algebra 207 (2) (1998) 525–546, https://doi.org/10.1006/jabr.1998.7479.

[12] A.A. Alabdali, N.P. Byott, Counting Hopf–Galois structures on cyclic field extensions of squarefree degree, J. Algebra 493 (2018) 1–19, https://doi.org/10.1016/j.jalgebra.2017.09.009.

[13] T. Crespo, M. Salguero, Hopf Galois structures on separable field extensions of odd prime power degree, J. Algebra 519 (2019) 424–439, https://doi.org/10.1016/j.jalgebra.2018.11.004.

[14] D. Bachiller, Counterexample to a conjecture about braces, J. Algebra 453 (2016) 160–176, https://doi.org/10.1016/j.jalgebra.2016.01.011.

[15] A. Smoktunowicz, L. Vendramin, On skew braces (with an appendix by N. Byott and L. Vendramin), J. Algebraic Combin. 2 (1) (2018) 47–86, https://doi.org/10.4171/JCA/2-1-3.

[16] L.N. Childs, Skew braces and the Galois correspondence for Hopf Galois structures, J. Algebra 511 (2018) 270–291, https://doi.org/10.1016/j.jalgebra.2018.06.023.

[17] W. Rump, Classification of cyclic braces, J. Pure Appl. Algebra 209 (3) (2007) 671–685, https://doi.org/10.1016/j.jpaa.2006.07.001.

[18] D. Bachiller, Classification of braces of order $p^3$, J. Pure Appl. Algebra 219 (8) (2015) 3568–3603, https://doi.org/10.1016/j.jpaa.2014.12.013.

[19] F. Catino, I. Colazzo, P. Stefanelli, Skew left braces with non-trivial annihilator, J. Algebra Appl. 222 (2018) 1670–1691, https://doi.org/10.1142/S0219498819500336.

[20] C. Dietzel, Braces of order $p^2q$, preprint on arXiv.org, https://arxiv.org/abs/1801.06911.

[21] A. Konovalov, A. Smoktunowicz, L. Vendramin, On skew braces and their ideals, preprint on arXiv.org, https://arxiv.org/abs/1804.04106.

[22] F. Cedó, A. Smoktunowicz, L. Vendramin, Skew left braces of nilpotent type, preprint on arXiv.org, https://arxiv.org/abs/1806.01127.

[23] A. (Agata) Smoktunowicz, A. (Alicia) Smoktunowicz, Set-theoretic solutions of the Yang–Baxter equation and new classes of R-matrices, preprint on arXiv.org, https://arxiv.org/abs/1704.03558.

[24] L. Vendramin, Problems on skew left braces, preprint on arXiv.org, https://arxiv.org/abs/1807.06411.

[25] T. Nasybullov, Connections between properties of the additive and the multiplicative groups of a two-sided skew brace, preprint on arXiv.org, https://arxiv.org/abs/1809.09418.

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

[27] N.P. Byott, Integral Hopf–Galois structures on degree $p^2$ extensions of $p$-adic fields, J. Algebra 248 (1) (2002) 334–365, https://doi.org/10.1006/jabr.2001.9053.

[28] L.N. Childs, Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, Providence, RI, 2000.

[29] D.V. Osipov, Discrete Heisenberg group and its automorphism group, preprint on arXiv.org, https://arxiv.org/abs/1505.00348.