University of Exeter
Department of Mathematics

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

Kayvan Nejabati Zenouz

January 2018

Supervised by Prof Nigel Byott

Submitted by Kayvan Nejabati Zenouz to the University of Exeter as a thesis for the degree of Doctor of Philosophy in Mathematics on 22nd January, 2018

I certify that all material in this thesis which is not my own work has been identified and that no material has previously been submitted and approved for the award of a degree by this or any other University.

Signature: .....

Abstract

The concept of Hopf-Galois extensions was introduced by S. Chase and M. Sweedler in 1969 and provides a generalisation of classical Galois theory. Later, Hopf-Galois theory for separable extensions of fields was studied by C. Greither and B. Pareigis. They showed how to recast the problem of classifying all Hopf-Galois structures on a finite separable extension of fields as a problem in group theory. Many major advances relating to the classification of Hopf-Galois structures were made by N. Byott, S. Carnahan, L. Childs, and T. Kohl.

On the other hand, and seemingly unrelated to Hopf-Galois theory, in 1992 V. Drinfeld formulated a number of problems in quantum group theory. In particular, he suggested considering set-theoretic solutions of the Yang-Baxter equation. Later, W. Rump introduced braces as a tool to study non-degenerate involutive set-theoretic solutions, and through the efforts of D. Bachiller, F. Cedó, E. Jespers, and J. Okniński the classification of these solutions was reduced to that of braces. Recently, skew braces were introduced by L. Guarnieri and L. Vendramin in order to study the non-degenerate (not necessarily involutive) set-theoretic solutions. Additionally, a fruitful discovery, initially noticed by D. Bachiller, revealed a connection between Hopf-Galois theory and skew braces, which linked the classification of Hopf-Galois structures to that of skew braces.

Currently, the classification of Hopf-Galois structures and skew braces of a given order remains among important topics of research. In this thesis, as our main results, we determine all Hopf-Galois structures on Galois extensions of fields of degree p^3, and at the same time we provide a complete classification of all skew braces of order p^3, for a prime number p. These findings hence offer applications to Galois module theory in number theory on the one hand, and to the study of the solutions of the quantum Yang-Baxter equation in mathematical physics on the other hand.

Contents

Part I

Introduction and Preliminaries

Chapter 1

Introduction

1.1 Overview

Hopf-Galois structures on a separable extension of fields is a subject of interest in the area of Galois module theory, with application in number theory, and have been under investigation since the later part of the 1980s. On the other hand, skew braces, used as a tool to study set-theoretic solutions of the Yang-Baxter equation, are an important topic of research in quantum group theory. The Yang-Baxter equation is one of the basic equations in theoretical physics, which lies in the foundation of the theory of quantum groups. The study of this equation has applications in other areas of mathematical and theoretical physics such as statistical mechanics, quantum field theory, differential equations, and knot theory. Recently, efforts of many researchers have established a link between Hopf-Galois theory and skew braces.

Many advances have been made towards the classification of Hopf-Galois structures and skew braces, however, the problem of classifying these objects remains widely open. To this end, in the main part of our work, we have endeavoured to provide the classification of Hopf-Galois structures on Galois field extensions of degree p^3 for a prime number p, and furthermore, by utilising the link between the two areas, to give a complete classification of all skew braces of order p^3.

The notion of Hopf-Galois extensions provides a generalisation of classical Galois theory. For L/K a finite Galois extension of fields with Galois group G, a *Hopf-Galois structure* on L/K is defined to be a K-Hopf algebra H, with an action on L, making L into a 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 are studied within a branch

of algebraic number theory, called Galois module theory, which is concerned with the properties of rings of integers of Galois extensions of number fields as modules over the integral group ring of the Galois group. Classification of Hopf-Galois structures on Galois field extensions enables Galois module theoretic study of Galois extensions of fields; for example, the study of non-classical *Galois scaffolds*.

The concept of Hopf-Galois extensions for arbitrary field extensions is due to Chase and Sweedler [CS69]. Later, Hopf-Galois theory for separable extensions of fields was studied by Greither and Pareigis [GP87]. They showed how to recast the problem of classifying all Hopf-Galois structures on L/K as a problem in group theory. Consequently, they proved that every K-Hopf algebra H which endows L/K with a Hopf-Galois structure is of the form $L[N]^G$ for some $N \subseteq \mathrm{Perm}(G)$ which is a regular subgroup normalised by the image of G, as left translations, inside $\mathrm{Perm}(G)$, the permutation group of 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 class of N became known as the type of the Hopf-Galois structure. There has since been many comprehensive studies of Hopf-Galois structures; we have gathered some of the relevant existing literature.

Byott [Byo96] showed that if L/K is a finite Galois extension of fields of degree n, then L/K admits a unique Hopf-Galois structure if and only if n is a *Burnside number* – i.e., $\gcd(n, \phi(n)) = 1$, where ϕ is the Euler's totient function. On the other hand, Kohl [Koh98] studied Hopf-Galois structures on Galois field extensions with cyclic Galois group of order p^n, for an odd prime p; in such case there are precisely p^{n-1} Hopf-Galois structures of cyclic type. Later, Byott's work [Byo07] also solved the problem for $p = 2$.

In addition, results obtained by Byott [Byo96, Byo04b] classify the Hopf-Galois structures on Galois field extensions of degree p^2 and pq for two primes p and q as follows. Let L/K be a Galois extension with Galois group G. If G is cyclic of order p^2, then L/K has exactly p distinct Hopf-Galois structures of cyclic type for odd p; for $p = 2$ there is one cyclic type and one elementary abelian type. If G is elementary abelian of order p^2, then L/K has exactly p^2 distinct Hopf-Galois structures all of which are of elementary abelian type when p is odd; for $p = 2$ there is one of cyclic type and 3 of elementary abelian type. For groups of order pq the following holds. Suppose G has size pq for $p > q$ two primes. If $p \not\equiv 1 \bmod q$, then L/K has exactly one Hopf-Galois structure. If G is cyclic of order pq with $p \equiv 1 \bmod q$, then L/K admits exactly one Hopf-Galois structure of cyclic type and $2(q-1)$ Hopf-Galois structures of nonabelian type, and finally, if G is nonabelian of order pq with $p \equiv 1 \bmod q$, then L/K admits exactly $2 + 2p(q-2)$ Hopf-Galois structures of nonabelian type and p Hopf-Galois structures of cyclic type.

Carnahan and Childs [CC99] obtained results relating to Hopf-Galois structures on Galois field extensions whose Galois group is the symmetric group S_n with $n \geq 5$

or the holomorph of a cyclic group of order p^e. Byott [Byo04a] showed that if L/K is a finite Galois extension of fields whose Galois group is a nonabelian simple group, then L/K admits exactly two Hopf-Galois structures. Finally, recently, Alabadi and Byott [AB18] studied Hopf-Galois structures on Galois field extensions whose Galois group is cyclic of squarefree order.

In this document, we use some methods of Byott [Byo96, Byo04b] to study Hopf-Galois structures on Galois field extensions of degree p^3 for a prime number p. This is achieved by studying the automorphism groups of groups of order p^3, and then by classifying all regular subgroups of the holomorph of these groups. We divide our study into two cases according to $p > 3$ and $p = 2, 3$. We first solve our problem for $p > 3$, since everything works uniformly in this case. Later, we adapt our methods to study the problem for the case when $p = 2, 3$ separately. In passing we also reproduce some of the contents of [Byo96, Byo07] relating to Hopf-Galois structures on Galois field extensions of degree p^2 and of degree 8. Subsequently, we turn our attention to skew braces, and we relate our results on the classification of regular subgroups of the holomorph of groups of order p^3 to study skew braces of order p^3.

In 1992 Drinfeld [Dri92] formulated a number of problems in quantum group theory. In particular, he suggested considering set-theoretic solutions of the Yang-Baxter equation. Later, Rump [Rum07a] introduced braces as a tool to study non-degenerate involutive set-theoretic solutions, and through the works of Bachiller, Cedó, Jespers, and Okniński [CJO14, BCJ16] the classification of these solutions was reduced to that of braces. Skew braces, a later generalisation of braces were initially defined in Bachiller's PhD thesis, he also noticed a connection between braces and Hopf-Galois structures. However, a detailed account of study of skew braces appeared in a paper by Guarnieri and Vendramin in [GV17], and their connection to ring theory and Hopf-Galois structures was studied by Byott, Smoktunowicz, and Vendramin in [SV17]. Skew braces are related to non-degenerate (not necessarily involutive) set-theoretic solutions of the Yang-Baxter equation. A (left) *skew brace* is a triple $(B, \oplus, \odot)$ which consists of a set B together with two operations $\oplus$ and $\odot$ such that $(B, \oplus)$ and $(B, \odot)$ are groups (neither necessarily abelian), and the two operations are related by the *skew brace property*:

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

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

In this document 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; also if $\oplus$ is abelian, we may call $(B, \oplus, \odot)$ a skew brace of abelian type. Now a skew brace of abelian type is precisely the one that was initially defined by Rump, called a brace (aka a classical brace) – the name 'brace' is said to have been chosen to resemble an object which is more than a group but does not satisfy all properties of a ring. It can be shown that for every skew brace

$(B, \oplus, \odot)$, the group $(B, \odot)$ can be embedded as a regular subgroup of $\mathrm{Hol}(B, \oplus)$, and every regular subgroup of $\mathrm{Hol}(B, \oplus)$ gives rise to a skew brace; furthermore, isomorphic skew braces correspond to regular subgroups which are conjugate by an element of $\mathrm{Aut}(B, \oplus)$.

The classification of skew braces has become one of the important topics of research. To this end, there has been an extensive study of the structure of these objects – cyclic braces were studied by Rump [Rum07b], and braces of order p^3 were classified by Bachiller [Bac15]. In this document, as a consequence of our results, we first obtain the content of [Bac15] relating to the classification of braces of order p^3; we go further and produce the classification of skew braces of order p^3. We observe the patterns emerging from these results and give information relating to the automorphism groups of some of these skew braces.

Classification of Hopf-Galois structures and skew braces are both related to classifying regular subgroups inside the holomorph of groups, and although it is easy to write computer programs (say using Magma [BCP97]) to find regular subgroups in the holomorph of a finite group with a fixed relatively small size, it appears computationally rather difficult to do this for groups with a larger size. For example, through a communication we had with Vendramin, we learnt that his script for Magma software to find regular subgroups of the holomorph of the elementary abelian group C_p^3 never terminates even for a relatively small primes – see the end part of [GV17] or [SV17] for a more complete survey of results and open problems.

This document consists of two parts which are organised as follows. Part I contains introductory materials and preliminaries, and Part II contains the calculations in order to prove our results. Part I has three chapters: In Chapter 1, we give an overview of our investigations and a summary of our main results whose proofs are in Part II. In Chapter 2, we review some preliminaries relating to Hopf-Galois structures, skew braces, and their relationship to regular subgroups of the holomorph of groups, and in Chapter 3 we study automorphism groups of groups of order p^3.

Part II has two chapters: In Chapter 4, we fix a prime number $p > 3$ and explicitly classify all regular subgroups contained in the holomorphs of groups of order p^3. Subsequently, we use this to find Hopf-Galois structures and skew braces of order p^3. In each of the first five sections of Chapter 4, we start with some information on the holomorph and a summary of the main results of the section, as a proposition, which gives the number of Hopf-Galois structures and skew braces of certain type. Then we have two or three lemmas in which we classify the regular subgroups and prove the proposition. In some sections we also provide some information about the automorphism groups of some of the skew braces that we find. The final section of Chapter 4 summarises the results of this chapter; in this section there is a list of all skew braces of order p^3 for $p > 3$; there is also a small discussion on the patterns emerging from these results and a few research questions. In Chapter 5,

we repeat some of our procedures in Chapter 4 and investigate the cases $p = 2, 3$, here most of the procedures are the same as in the previous chapter, but there are some differences which we will point out to.

In Chapters 4 and 5 we relate our findings to the classification of braces of order p^3, up to isomorphism, constructively. For the abelian groups, i.e., first three sections of Chapter 4, our results match the classification obtained by Bachiller [Bac15]. Further, for the first three section of Chapter 5 our results match the classification of Bachiller [Bac15], but we appear to find two errors in [Bac15]). In the nonabelian setting our findings yield new results in the direction of classification of skew braces.

Acknowledgements

I am enormously indebted, and would like to extend my gratitude, to my PhD adviser Prof Nigel Byott for introducing me to these interesting topics and providing me with his technical expertise in the area, his advice in formatting this document, as well as his constant encouragement and support, which enabled me to undertake and accomplish this investigation. I would like to thank my PhD co-adviser Dr Henri Johnston for his advice, continually supporting my progress, sharing with me his useful experiences, and for teaching me writing techniques in mathematics. I further express my gratitude to Prof Trevor Bailey, Dr Robin Chapman, and Dr Chris Ferro for their advice and support. Finally, but not least, I would like to thank my wife Parisa, my mother Roya, and my family and friends who have bestowed upon me their endless love and encouragement in all stages of my development.

1.2 Summary of main results

In this section we provide a summary of our main results. Note, for a prime number $p > 2$, up to isomorphism, there are 5 different groups of order p^3. Three of these are abelian: the cyclic group, C_{p^3}, the exponent p^2 abelian group, $C_{p^2} \times C_p$, and the elementary abelian group, C_p^3. The remaining two are nonabelian: the exponent p nonabelian group, or otherwise known as the Heisenberg group of order p^3,

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

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

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

For $p = 2$ the abelian groups of order 8 are the same as for $p > 2$, but for nonabelian groups of order 8 we have the dihedral group

$$D_8 \stackrel{\text{def}}{=} \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1,\ \tau\sigma = \sigma^{-1}\tau \rangle$$

and the quaternion group

$$Q_8 \stackrel{\text{def}}{=} \langle \sigma, \tau \mid \sigma^4 = 1,\ \sigma^2 = \tau^2,\ \tau\sigma = \sigma^{-1}\tau \rangle .$$

For a Galois extension of fields L/K with Galois group G, we shall denote by $e(G, N)$ the number of Hopf-Galois structures on L/K of type N. For a group G we denote by $\widetilde{e}(G, N)$ the number of G-skew braces of type N up to isomorphism. Our main results are summarised below.

Theorem 1.2.1. *Let L/K be a Galois extension of fields of degree p^3 for a prime $p > 3$ with Galois group G. Then the number of Hopf-Galois structures on L/K of type N, $e(G, N)$, is given by the table*

$e(G,N)$	C_{p^3}	$C_{p^2} \times C_p$	C_p^3	M_1	M_2
C_{p^3}	p^2	-	-	-	-
$C_{p^2} \times C_p$	-	$(2p-1)p^2$	-	-	$(2p-1)(p-1)p^2$
C_p^3	-	-	$(p^4+p^3-1)p^2$	$(p^3-1)(p^2+p-1)p^2$	-
M_1	-	-	$(p^2+p-1)p^2$	$(2p^3-3p^2+1)p^2$	-
M_2	-	$(2p-1)p^2$	-	-	$(2p-1)(p-1)p^2$

Table 1.1: Number of Hopf-Galois structures of order p^3 for $p > 3$

where rows correspond to G and columns to N.

In the table in Theorem 1.2.1, the result in the first row also follows as a consequence of a more general work of Kohl [Koh98]. The other four rows are new results. The proofs of the columns one up to five are contained in Chapter 4, Sections 4.1 - 4.5, respectively. The results corresponding to the classification of skew braces of order p^3 for $p > 3$ are as follows.

Theorem 1.2.2. *Let G be a group of order p^3 for a prime $p > 3$. Then the number of G-skew braces of type N, $\widetilde{e}(G, N)$, is given by the table*

$\widetilde{e}(G,N)$	C_{p^3}	$C_{p^2} \times C_p$	C_p^3	M_1	M_2
C_{p^3}	3	-	-	-	-
$C_{p^2} \times C_p$	-	9	-	-	$4p+1$
C_p^3	-	-	5	$2p+1$	-
M_1	-	-	$2p+1$	$2p^2-p-3$	-
M_2	-	$4p+1$	-	-	$4p^2-3p-1$

Table 1.2: Number of skew braces of order p^3 for $p > 3$

where rows correspond to G and columns to N.

In the table in Theorem 1.2.2, the result of the first column also follows as a more general work by Rump [Rum07b], the second and third columns also follow from a work by Bachiller, namely [Bac15, Theorem 3.2], we reprove these results using different methods. The final two columns are new results in the classification of skew braces of nonabelian type. The proofs of the results in columns one up to five and the construction of the skew braces are contained in Chapter 4, Sections 4.1 - 4.5, respectively. For $p = 2, 3$ we have the following theorems, whose proofs are contained in Chapter 5, Sections 5.2 - 5.8, respectively.

Theorem 1.2.3. *Let L/K be a Galois extension of fields of degree 27 with Galois group G. Then the number of Hopf-Galois structures on L/K of type N, $e(G, N)$, is given by the table*

$e(G,N)$	C_{27}	$C_9 \times C_3$	C_3^3	M_1	M_2
C_{27}	9	-	-	-	-
$C_9 \times C_3$	-	39	6	12	78
C_3^3	-	624	339	1300	1248
M_1	-	48	51	317	96
M_2	-	39	6	12	78

Table 1.3: Number of Hopf-Galois structures of order 27

where rows correspond to G and columns to N.

The results corresponding to the classification of skew braces of order 27 are as follows.

Theorem 1.2.4. *Let G be a group of order 27. Then the number of G-skew braces of type N, $\widetilde{e}(G, N)$, is given by the table*

$\widetilde{e}(G,N)$	C_{27}	$C_9 \times C_3$	C_3^3	M_1	M_2
C_{27}	3	-	-	-	-
$C_9 \times C_3$	-	8	1	2	11
C_3^3	-	1	4	5	2
M_1	-	2	5	14	4
M_2	-	11	2	4	22

Table 1.4: Number of skew braces of order 27

where rows correspond to G and columns to N.

In the table in Theorem 1.2.4, the first three columns also follow from the work by Bachiller [Bac15, Theorem 3.2]. We notice two errors in [Bac15, Theorem 3.2, 2]: first one is in [Bac15, Theorem 3.2, 2, Socle of order p^2] where for $p = 3$ the final brace should be, using his notation, $M(p)$ brace (or M_1 brace) rather than $M_3(p)$ brace (or M_2 brace), and second one is in [Bac15, Theorem 3.2, 2, Socle of order p^3] the brace should be, again using his notation, $\mathbb{Z}/(p) \times \mathbb{Z}/(p^2)$ rather than $M_3(p)$. The final two columns are new results in the classification of skew braces.

Theorem 1.2.5. *Let L/K be a Galois extension of fields of degree 8 with Galois group G. Then the number of Hopf-Galois structures on L/K of type N, $e(G,N)$, is given by the table*

$e(G,N)$	C_8	$C_4 \times C_2$	C_2^3	D_8	Q_8
C_8	2	-	-	2	2
$C_4 \times C_2$	4	10	4	6	2
C_2^3	-	42	8	42	14
D_8	2	14	6	6	2
Q_8	6	6	2	6	2

Table 1.5: Number of Hopf-Galois structures of order 8

where rows correspond to G and columns to N.

In the table in Theorem 1.2.5, the first row also follows from a work by Byott, namely [Byo07, Theorem 5.1]. The other four rows are new. The results corresponding to the classification of skew braces of order 8 are as follows.

Theorem 1.2.6. *Let G be a group of order 8. Then the number of G-skew braces of type N, $\widetilde{e}(G,N)$, is given by the table*

$\widetilde{e}(G,N)$	C_8	$C_4 \times C_2$	C_2^3	D_8	Q_8
C_8	2	-	-	2	2
$C_4 \times C_2$	1	6	3	3	1
C_2^3	-	2	2	1	1
D_8	1	5	2	4	2
Q_8	1	1	1	2	2

Table 1.6: Number of skew braces of order 8

where rows correspond to G and columns to N.

Vendramin communicated to us that he is also able to obtained the results for $p = 2, 3$ by his Magma script, but here we give a explicit description of the above objects.

We have also produced a few tables summarising the number Hopf-Galois structures and braces of degree p^2.

$p > 2$

$e(G,N)$	C_{p^2}	C_p^2
C_{p^2}	p	-
C_p^2	-	p^2

$p = 2$

$e(G,N)$	C_4	C_2^2
C_4	1	1
C_2^2	1	3

Table 1.7: Number of Hopf-Galois structures of order p^2

$p > 2$

$\widetilde{e}(G,N)$	C_{p^2}	C_p^2
C_{p^2}	2	-
C_p^2	-	2

$p = 2$

$\widetilde{e}(G,N)$	C_4	C_2^2
C_4	1	1
C_2^2	1	1

Table 1.8: Number of braces of order p^2

where rows correspond to G and columns correspond to N of the $e(G,N)$, respectively $\widetilde{e}(G,N)$.

Chapter 2

Preliminaries I: Hopf-Galois structures and skew braces

The aim of this chapter is to provide relevant background information on Hopf-Galois structures and skew braces, together with an overview of the general approach we have taken in order to carry out our investigations. Now since both Hopf-Galois structures and skew braces are related to regular subgroups of the holomorphs of groups, we first review some information on the holomorph of a group, regular subgroups, and a procedure for finding regular subgroups contained in the holomorph, in Section 2.1. Then in Section 2.2, we provide background information about Hopf-Galois structure, and in Section 2.3, we give some information about skew braces. Finally, in Section 2.4, we discuss the interaction and explicit connection between the number of Hopf-Galois structures and skew braces.

2.1 Holomorph of a group and regular subgroups

For a finite group N, we denote by $\mathrm{Aut}(N)$ the set of all automorphisms of the group N, which is a group under composition of maps. For an automorphism $\alpha \in \mathrm{Aut}(N)$ and an element $\sigma \in N$, we denote by $\sigma^\alpha \stackrel{\text{def}}{=} \alpha(\sigma)$ the image of σ under α. In this notation we have

$$(\sigma^\alpha)^\beta = \beta(\sigma^\alpha) = \beta(\alpha(\sigma)) = \beta\alpha(\sigma) = \sigma^{\beta\alpha} \text{ for all } \alpha, \beta \in \mathrm{Aut}(N) \text{ and } \sigma \in N.$$

We define the *holomorph* of N as

$$\mathrm{Hol}(N) \stackrel{\text{def}}{=} N \rtimes \mathrm{Aut}(N) = \{[\eta, \alpha] \mid \eta \in N,\ \alpha \in \mathrm{Aut}(N)\},$$

where multiplication is given by

$$[\eta_1, \alpha_1][\eta_2, \alpha_2] \stackrel{\text{def}}{=} [\eta_1 \eta_2^{\alpha_1}, \alpha_1\alpha_2] \text{ for } [\eta_1, \alpha_1], [\eta_2, \alpha_2] \in \mathrm{Hol}(N).$$

The action of $\mathrm{Hol}(N)$ on N is given by sending $[\eta, \alpha] \in \mathrm{Hol}(N)$ and $\sigma \in N$ to

$$[\eta, \alpha] \cdot \sigma \stackrel{\text{def}}{=} \eta\sigma^{\alpha} \in N.$$

In some cases we may simplify our notations and write $\eta\alpha$ to denote the element $[\eta, \alpha] \in \mathrm{Hol}(N)$ and identify N with its image inside $\mathrm{Hol}(N)$, i.e., write η for the element $[\eta, \mathrm{id}] \in \mathrm{Hol}(N)$, which helps us avoid too many brackets and commas. In the alternative notation for $\eta\alpha \in \mathrm{Hol}(N)$ and $\sigma \in N$, we shall write

$$(\eta\alpha)\sigma \stackrel{\text{def}}{=} [\eta\sigma^{\alpha}, \alpha] \in \mathrm{Hol}(N) \text{ and } (\eta\alpha) \cdot \sigma \stackrel{\text{def}}{=} \eta\sigma^{\alpha} \in N.$$

This simplified notation is also the one adopted in [Chi00] and [Byo04b].

We remark that according to [Chi00, p. 56, (7.1) Definition] one can alternatively define the holomorph of a group N as the normaliser of the image of N, as left translations, inside the permutation group $\mathrm{Perm}(N)$ of N. Finally, we recall that a subgroup $H \subseteq \mathrm{Perm}(N)$ is called *regular* if the map

$$H \times N \longrightarrow N \times N \text{ given by } (f, \sigma) \longmapsto (f(\sigma), \sigma)$$

is a bijection – see [Chi00, p. 48, (6.2) Definition] for equivalent definitions.

2.1.1 Regular subgroups contained in the holomorph

Here for a finite group N, we outline our strategy for finding regular subgroup contained in $\mathrm{Hol}(N)$. Let us denote by Θ the natural projection

$$\Theta : \mathrm{Hol}(N) \longrightarrow \mathrm{Aut}(N) \text{ given by } \eta\alpha \longmapsto \alpha.$$

Then one may organise the regular subgroups of $\mathrm{Hol}(N)$ according to the size of their image under the map Θ.

In finding the regular subgroups $H \subseteq \mathrm{Hol}(N)$ with $|\Theta(H)| = m$, where m divides $|N|$, we work as follows. We take a subgroup of order m of $\mathrm{Aut}(N)$, which may be generated by $\alpha_1, ..., \alpha_s \in \mathrm{Aut}(N)$, say

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

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 take general elements $v_1, ..., v_s \in N$. Then 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 search for $v_1, ..., v_s$ such that H is regular, i.e., H has the same size as N and acts freely on N.

For H to have the same size as N, it is necessary that v_i, for each $i = 1, ..., s$, satisfy

$$(v_i\alpha_i)\eta_j(v_i\alpha_i)^{-1} = \left(v_i\eta_j^{\alpha_i}\alpha_i\right)\left(\left(v_i^{-1}\right)^{\alpha_i^{-1}}\alpha_i^{-1}\right) = v_i\eta_j^{\alpha_i}v_i^{-1} \in H_1 \text{ for all } i, j,$$

or equivalently to satisfy

$$\left((v_i\alpha_i)\eta_j\right)\left(\eta_j v_i\alpha_i\right)^{-1} = \left(v_i\eta_j^{\alpha_i}\alpha_i\right)\left(\left(v_i^{-1}\right)^{\alpha_i^{-1}}\alpha_i^{-1}\right)\eta_j^{-1} = v_i\eta_j^{\alpha_i}v_i^{-1}\eta_j^{-1} \in H_1 \text{ for all } i, j,$$

which also implies that H_1 is a normal subgroup of H. More generally, 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

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

for every $u_1, w_1, ..., u_s, w_s \in H_1$.

Furthermore, for H to act freely on N, it is necessary that $v_i \notin H_1$ for all i. More generally, for every word $W(\alpha_1, ..., \alpha_s) \neq 1$ on H_2 we require

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

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, 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, we remark 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

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

2.2 Hopf-Galois structures

In this section we review some background information relating to Hopf-Galois structures and discuss their relationship to regular subgroups. Our main references are the articles by Byott [Byo96, Byo04b, Byo07] and the book by Childs [Chi00]. In this section we fix R to be a commutative ring with a unit. Then an R-algebra A is defined to be a ring with a unit together with a ring homomorphism $\iota : R \longrightarrow A$ such that the image of R is contained in the centre of A. Our starting point is the notions of R-coalgebra and R-bialgebra.

Definition 2.2.1 (R-coalgebra)**.** An *R-coalgebra* is an R-module H with multiplication map $\mu : R \otimes_R H \longrightarrow H$ and R-module homomorphisms

$$\begin{aligned} \Delta &: H \longrightarrow H \otimes_R H \text{ (comultiplication)} \\ \varepsilon &: H \longrightarrow R \text{ (counit)}, \end{aligned}$$

where $H \otimes_R H$ has component-wise multiplication, such that

i) the map Δ is *coassociative*, i.e., $(\Delta \otimes 1)\Delta = (1 \otimes \Delta)\Delta$ and

ii) the *counitary property* holds, i.e.,

$$\mu(1 \otimes \varepsilon)\Delta(h) = h \text{ and } \mu(\varepsilon \otimes 1)\Delta(h) = h \text{ for all } h \in H.$$

Definition 2.2.2 (R-bialgebra)**.** An *R-bialgebra* is an R-algebra which is also an R-coalgebra, i.e., an *R-bialgebra* is an R-algebra H with multiplication map $\mu : H \otimes_R H \longrightarrow H$ and unit map $\iota : R \longrightarrow H$, together with R-module homomorphisms $\Delta : H \longrightarrow H \otimes_R H$, comultiplication map, and $\varepsilon : H \longrightarrow R$, counit map, which are R-algebra homomorphisms such that the map Δ is coassociative and the counitary property holds.

Let H be an R-bialgebra and define $\tau : H \otimes_R H \longrightarrow H \otimes_R H$ to be the *switch map*, $\tau(h_1 \otimes h_2) = h_2 \otimes h_1$. Then an R-Hopf algebra is defined as follows.

Definition 2.2.3 (R-Hopf algebra)**.** An R-bialgebra H is an *R-Hopf algebra* if there is an R-module homomorphism

$$\lambda : H \longrightarrow H \text{ (antipode)}$$

which is both an R-algebra and an R-coalgebra antihomomorphism, i.e.,

$$\begin{aligned} &\lambda(hh') = \lambda(h')\lambda(h) \text{ and} \\ &\Delta\lambda(h) = (\lambda \otimes \lambda)\tau\Delta(h) \text{ for all } h \in H, \end{aligned}$$

and satisfies the *antipode property*: $\mu(1 \otimes \lambda)\Delta = \iota\varepsilon$ and $\mu(\lambda \otimes 1)\Delta = \iota\varepsilon$.

An R-Hopf algebra H is called *cocommutative* if $\tau\Delta = \Delta$ and *commutative* if H is commutative as an algebra, i.e., $\mu\tau = \mu$. The R-Hopf algebra H is called *abelian* if it is both cocommutative and commutative.

Example 2.2.4 (Group algebras). The classical example of an R-Hopf algebra is $R[G]$, the group ring of a finite group G. In this case since Δ, ε, and λ are required to be R-linear homomorphisms, they are uniquely determined by their values on elements of G and given by

$$\begin{aligned}\Delta(\sigma) &= \sigma \otimes \sigma,\\ \varepsilon(\sigma) &= 1, \text{ and}\\ \lambda(\sigma) &= \sigma^{-1} \text{ for } \sigma \in G.\end{aligned}$$

Here the R-Hopf algebra $R[G]$ is cocommutative.

Now let H be an R-Hopf algebra which is a finitely generated and projective R-module. Such an algebra is called a *finite* R-algebra. Further, let S be an R-algebra which is an H-module. Then S is called an *H-module algebra* if

$$h(st) = \sum_{(h)} h_{(1)}(s)h_{(2)}(t) \text{ and } h(1) = \varepsilon(h)1 \text{ for all } h \in H \ s,t \in S.$$

Now we can define the notion of an H-Galois extension.

Definition 2.2.5 (H-Galois extension)**.** Let us suppose in addition to above that H is also cocommutative. Then a finite commutative R-algebra S is an *H-Galois extension* over R if S is a left H-module algebra and the R-module homomorphism

$$j : S \otimes_R H \longrightarrow \mathrm{End}_R(S) \text{ given by } j(s \otimes h)(t) = sh(t) \text{ for } s,t \in S, \ h \in H$$

is an isomorphism.

Having briefly reviewed relevant definitions, we next provide some information on *Greither-Pareigis* theory, which is concerned with the classification of Hopf-Galois structures. Let L/K be a finite separable extension of fields.

Definition 2.2.6 (Hopf-Galois structure on L/K)**.** A *Hopf-Galois structure* on L/K is a K-Hopf algebra H, with an action on L, so that L is an H-module algebra, and such that the action makes L into a H-Galois extension.

Now let E be the normal closure of L/K and $G \stackrel{\text{def}}{=} \mathrm{Gal}(E/K)$. Denote by $G' \stackrel{\text{def}}{=} \mathrm{Gal}(E/L)$ and set $X \stackrel{\text{def}}{=} G/G'$. Note that since E is the normal closure of L/K, the left translation action of G on X is faithful, i.e., the homomorphism $\lambda : G \longrightarrow \mathrm{Perm}(X)$ induced by this action is injective – here $\mathrm{Perm}(X)$ is the group of all permutations of the set X. Now the following is [Chi00, p. 52, (6.8) Theorem] which is originally due to Greither and Pareigis [GP87].

Theorem 2.2.7 (Hopf-Galois structures and regular subgroups)**.** *There is a bijection between regular subgroups $N \subseteq \mathrm{Perm}(X)$ normalised by $\lambda(G)$ and Hopf-Galois structures on L/K.*

In the proof of the Theorem 2.2.7, it is shown that every Hopf-Galois structure on L/K corresponds to $L[N]^G$ for some regular $N \subseteq \mathrm{Perm}(X)$ which is normalised by $\lambda(G)$ – here the action of G on $L[N]$ is induced by the action of G on N by conjugation inside $\mathrm{Perm}(G)$ and on L by field automorphisms. This group N is known as the *type* of the Hopf-Galois structures, and we shall call the cardinality of N, which is the same as the degree of the extension L/K, as the *order* of the Hopf-Galois structure. According to [Chi00, p. 56], one difficulty with the Greither-Pareigis theory is that it requires the classification of regular subgroups contained in $\mathrm{Perm}(X)$ which are normalised by G, and the number of these subgroups rapidly increases as with the size of X. This is where the *Byott's translation* idea is introduced, which reverses the relationship between G and N and reduces this complexity to some extent. Hence Byott [Byo96] proves the following statement – here Childs reformulation [cf. Chi00, p. 57, (7.3) Theorem (Byott)] is given.

Theorem 2.2.8. *Let N be a group. Then there is a bijection between the sets*

$$\mathcal{N} \stackrel{\text{def}}{=} \{\alpha : N \hookrightarrow \mathrm{Perm}(X) \mid \alpha(N) \text{ is regular}\} \text{ and}$$

$$\mathcal{G} \stackrel{\text{def}}{=} \{\beta : G \hookrightarrow \mathrm{Perm}(N) \mid \beta(G') \text{ is the stabiliser of the identity of } N\}.$$

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 $\lambda(G)$ if and only if $\beta(G)$ is contained in* $\mathrm{Hol}(N)$*.*

In fact Byott [Byo96] finds that if one lets $a(N, G, G')$ to be the number of Hopf-Galois structures of type N on L/K and $b(N, G, G')$ to be the number subgroups G^* of $\mathrm{Hol}(N)$ such that there is an isomorphism $\theta : G \longrightarrow G^*$ with $\theta(G') = G^* \cap \mathrm{Aut}(N)$, then one has

$$a(N, G, G') = \frac{|\mathrm{Aut}(G, G')|}{|\mathrm{Aut}(N)|} b(N, G, G'),$$

where $\mathrm{Aut}(G, G')$ denotes the set of automorphisms of G which map G' to itself.

In the case when L/K is Galois, with Galois group G, following the notation of [Byo04b], we can use a refined version of the above formula, in order to count the Hopf-Galois structures, as follows. Recall, the map Θ

$$\Theta : \mathrm{Hol}(N) \longrightarrow \mathrm{Aut}(N) \text{ given by } \eta\alpha \longmapsto \alpha.$$

Let $e'(G, N, m)$ to be the number of regular subgroups of $\mathrm{Hol}(N)$ isomorphic to G

whose image under Θ has size m. Then we define $e(G, N, m)$ as

$$e(G, N, m) \stackrel{\text{def}}{=} \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|} e'(G, N, m). \tag{2.1}$$

Further we set $e(G, N)$ to be the number of Hopf-Galois structures of type N on the field extension L/K whose Galois group is G. Then we find

$$e(G, N) \stackrel{\text{def}}{=} \sum_m e(G, N, m),$$

where the sum is taken over all divisors of $|G|$.

2.3 Skew braces

In this section we review some information relating to skew braces, and we discuss their relationship to regular subgroups. We remark that our main reference for some of the materials here is the article by Smoktunowicz and Vendramin [GV17]. Braces were introduced by Rump [Rum07a] as part of his study of the non-degenerate involutive set-theoretic solutions of the Yang-Baxter equation. Rump showed that every involutive non-degenerate solution of the Yang-Baxter equation can be in a good way embedded in a brace, and that on the other hand every brace gives a solution of the quantum Yang-Baxter equation. Later, the classification of non-degenerate involutive set-theoretic solutions of the Yang-Baxter equation was reduced to the classification of braces by Bachiller, Cedó, Jespers, and Okniński in [CJO14, BCJ16]. Skew braces, which initially appeared in D. Bachiller PhD thesis, were recently studied extensively by Guarnieri, Smoktunowicz, and Vendramin (also Byott) [GV17, SV17]. Skew braces are concerned with non-degenerate (not necessarily involutive) set-theoretic solutions of the Yang-Baxter equation and have application in theoretical physics.

A *set-theoretic solution* of the Yang-Baxter equation is a pair (X, r), where X is a nonempty set and r is a bijective map

$$r : X \times X \longrightarrow X \times X \text{ with } (x, y) \longmapsto (\sigma_x(y), \tau_y(x))$$

such that $(r \times \mathrm{id})(\mathrm{id} \times r)(r \times \mathrm{id}) = (\mathrm{id} \times r)(r \times \mathrm{id})(\mathrm{id} \times r)$. The map r is called a *braiding map*. A solution (X, r) is called *non-degenerate* if the maps σ_x and τ_x are bijections for every $x \in X$. The solution (X, r) is called *involutive* if $r^2 = \mathrm{id}_{X \times X}$.

Definition 2.3.1 (Skew brace)**.** A (left) *skew brace* is a set B with two operations $\oplus$ and $\odot$ such that $(B, \oplus)$ and $(B, \odot)$ are groups (neither necessarily abelian), and the two operations are related by the *skew brace property*:

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

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

We shall denote a skew brace by $(B, \oplus, \odot)$ or sometimes simply by B. We refer to $(B, \oplus)$ as the *additive group* and $(B, \odot)$ as the *multiplicative* group of the skew brace B. Further, we call B a skew brace of *abelian type*, or simply a brace, if $(B, \oplus)$ is abelian. More generally, we shall call a skew brace $(B, \oplus, \odot)$ with $(B, \odot) \cong G$ and $(B, \oplus) \cong N$ a G-skew brace of type N (or simply a G-brace of type N). For any group $(B, \odot)$, a *brace type* on B is an operation $\oplus$ on B making $(B, \oplus, \odot)$ a skew brace; also for a group $(B, \oplus)$ a *brace structure* on B is an operation $\odot$ on B making $(B, \oplus, \odot)$ a skew brace.

Remark 2.3.2 (Simpler terminology). Note after calling a skew brace $(B, \oplus, \odot)$ such that $(B, \oplus) \cong N$ and $(B, \odot) \cong G$ a G-skew brace of type N, the word 'skew' becomes redundant; for example, as mentioned above, if $\oplus$ is abelian, we may call $(B, \oplus, \odot)$ a brace of abelian type. Now a brace of abelian type would be the one that was initially defined in [Rum07a] as a brace, and a brace of nonabelian type would be the generalisation in [GV17], so with this terminology one can simply refer to a skew brace as a 'certain brace' of 'certain type', and the type of the brace makes clear if this is a skew brace or a classical brace, suggesting that the word 'skew' can safely be dropped. However, to avoid any possible confusion, we have tried to use the skew brace terminology as already established in [GV17] throughout the document.

Note, 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. Therefore, one has

$$\begin{aligned} \mathrm{Hom}_{\mathcal{B}r}\left((B_1, \oplus_1, \odot_1), (B_2, \oplus_2, \odot_2)\right) &\hookrightarrow \mathrm{Hom}_{\mathcal{G}r}\left((B_1, \oplus_1), (B_2, \oplus_2)\right), \\ \mathrm{Hom}_{\mathcal{B}r}\left((B_1, \oplus_1, \odot_1), (B_2, \oplus_2, \odot_2)\right) &\hookrightarrow \mathrm{Hom}_{\mathcal{G}r}\left((B_1, \odot_1), (B_2, \odot_2)\right), \end{aligned}$$

where $\mathrm{Hom}_{\mathcal{B}r}(-,-)$ denote the set of skew brace homomorphisms between two skew braces and $\mathrm{Hom}_{\mathcal{G}r}(-,-)$ denotes the set of group homomorphisms between two groups. In other words, the two forgetful functors from the category of skew braces to the categories of groups, which forget the skew brace and remember the brace structure or the brace type, are faithful.

For a skew brace B, an element $a \in B$, and an integer n, we shall write

$$na \overset{\text{def}}{=} \underbrace{a \oplus \cdots \oplus a}_{\text{n-times}}, \quad a^n \overset{\text{def}}{=} \underbrace{a \odot a \cdots \odot a}_{\text{n-times}},$$

also we denote by 0 the identity for $(B, \oplus)$ and by 1 the identity for $(B, \odot)$. Finally, we write $\ominus a$ for the inverse of a with respect of $\oplus$ and a^{-1} for the inverse of a with respect of $\odot$. We investigate a few properties of skew braces, whose equivalent versions may also be found in [GV17, p. 4-5].

Lemma 2.3.3. *Suppose $(B, \oplus, \odot)$ is a skew brace, $a, b \in B$, and let n be an integer. Then the following holds.*

i) We have $0 = 1$.

ii) We have $a \odot (\ominus b) = a \ominus (a \odot b) \oplus a$.

iii) We have $a \odot (nb) = n(\ominus a \oplus (a \odot b))$.

Proof. i) By definition we have

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

thus for any $a \in B$ we have

$$a \odot 0 = a \odot (0 \oplus 0) = (a \odot 0) \ominus a \oplus (a \odot 0),$$

which implies that by applying $\ominus (a \odot 0)$ to both sides we get

$$0 = \ominus a \oplus (a \odot 0).$$

Now applying $a\oplus$ to both sides we get $a = a \odot 0$, and applying $a^{-1}\odot$, we get

$$a^{-1} \odot a = a^{-1} \odot a \odot 0,$$

so $1 = 0$.

ii) By i) for any $a, b \in B$ we have

$$a = a \odot 0 = a \odot (b \ominus b) = (a \odot b) \ominus a \oplus (a \odot (\ominus b))$$

applying $\ominus((a \odot b) \ominus a) = a \ominus (a \odot b)$ to both side we get

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

iii) For $a, b \in B$ and an integer n we have

$$a \odot (nb) = a \odot (\underbrace{a \oplus \cdots \oplus a}_{\text{n-times}}) = (a \odot ((n-1)b)) \ominus a \oplus (a \odot b),$$

so by induction $a \odot (nb) = n(\ominus a \oplus (a \odot b))$.

□

Lemma 2.3.4. *Suppose $(B, \oplus, \odot)$ is a skew brace, and for $a \in B$ define a map*

$$\lambda_a : B \longrightarrow B \text{ given by } \lambda_a(b) \stackrel{\text{def}}{=} \ominus a \oplus (a \odot b).$$

Then the followings hold.

i) We have $\lambda_a \in \mathrm{Aut}(B, \oplus)$ for all $a \in B$.

ii) The map $\lambda : (B, \odot) \longrightarrow \mathrm{Aut}(B, \oplus)$ given by $a \longmapsto \lambda_a$ is a group homomorphism.

iii) Let $m_a : B \longrightarrow B$ be given by $m_a(b) \stackrel{\text{def}}{=} a \odot b$. Then the map

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

is a well-defined injective homomorphism, and the image of m is a regular subgroup of $\mathrm{Hol}(B, \oplus)$.

Proof. i) Note by Lemma 2.3.3, *i*) we have $0 = 1$, so

$$\lambda_a(0) = \ominus a \oplus (a \odot 0) = 0,$$

also for $b, c \in B$ we have

$$\lambda_a(b \oplus c) = \ominus a \oplus (a \odot (b \oplus c)) = \ominus a \oplus ((a \odot b) \ominus a \oplus (a \odot c))$$

$$= \lambda_a(b) \oplus \lambda_a(c),$$

which show λ_a is an endomorphism. Now if $\ominus a \oplus (a \odot b) = 0$, then we have $a \odot b = a$ and so $b = 1 = 0$, which shows λ_a is injective. Further, for any given $y \in B$, let $b = a^{-1} \odot (a \oplus y)$. Then

$$\lambda_a(b) = \ominus a \oplus (a \odot a^{-1} \odot (a \oplus y)) = y$$

which shows that λ_a is surjective, and so λ_a is an automorphism.

ii) Let $a, b \in B$. Then by Lemma 2.3.3, *ii*) we have

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

thus for any $c \in B$ we find

$$\begin{aligned} \lambda_{a \odot b}(c) &= \ominus (a \odot b) \oplus ((a \odot b) \odot c) = (\ominus a \oplus (a \odot (\ominus b)) \ominus a) \oplus (a \odot (b \odot c)) \\ &= \ominus a \oplus (a \odot (\ominus b)) \ominus a \oplus (a \odot (b \odot c)) = \ominus a \oplus (a \odot (\ominus b \oplus (b \odot c))) \\ &= \lambda_a \lambda_b(c). \end{aligned}$$

iii) It follows by definition that

$$m_a(b) = a \oplus \lambda_a(b) \text{ for all } b \in B,$$

so $m_a = a\lambda_a$ is an element of the $\mathrm{Hol}(B, \oplus)$ since $\lambda_a \in \mathrm{Aut}(B, \oplus)$ by $i)$. Now consider the map

$$m : (B, \odot) \longrightarrow \mathrm{Hol}(B, \oplus) \text{ given by } a \longmapsto m_a.$$

For $a_1, a_2 \in B$ we have

$$m_{a_1} = a_1\lambda_{a_1} \text{ and } m_{a_2} = a_2\lambda_{a_2} \in \mathrm{Hol}(B, \oplus).$$

Now $m_{a_1 \odot a_2}(b) = a_1 \odot a_2 \odot b$ for all $b \in B$ and

$$m_{a_1} m_{a_2} = (a_1\lambda_{a_1})(a_2\lambda_{a_2})$$

$$= (a_1 \oplus a_2^{\lambda_{a_1}})\lambda_{a_1}\lambda_{a_2} = (a_1 \odot a_2)\lambda_{a_1 \odot a_2} = m_{a_1 \odot a_2} \text{ for all } a_1, a_2 \in B.$$

It is also clear that the map m is injective and its image is a regular subgroup. □

The following proposition shows how skew braces and regular subgroups are related which is also in [SV17, Proposition A.3].

Proposition 2.3.5. *There exists a bijective correspondence between isomorphism classes of skew braces with additive group isomorphic to* $(B, \oplus)$ *and classes of regular subgroups of* $\mathrm{Hol}(B, \oplus)$ *under conjugation by elements of* $\mathrm{Aut}(B, \oplus)$.

Proof. Lemma 2.3.4 shows that every skew brace $(B, \oplus, \odot)$ corresponds to a regular subgroup of $\mathrm{Hol}(B, \oplus)$ by the embedding map

$$m : (B, \odot) \longrightarrow \mathrm{Hol}(B, \oplus) \text{ given by } a \longmapsto m_a.$$

Now suppose

$$f : (B, \oplus, \odot_1) \longrightarrow (B, \oplus, \odot_2)$$

is an isomorphism of skew braces. Then we must have $f \in \mathrm{Aut}(B, \oplus)$. Let

$$C_f : \mathrm{Hol}(B, \oplus) \longrightarrow \mathrm{Hol}(B, \oplus) \text{ given by } C_f(\eta\alpha) = \eta^f f\alpha f^{-1},$$

which is an inner automorphism of $\mathrm{Hol}(B, \oplus)$ whose inverse is $C_{f^{-1}}$. Then the

following diagram is commutative

$$\begin{array}{ccc} (B,\odot_1) & \xhookrightarrow{m_1} & \mathrm{Hol}(B,\oplus) \\ \Big\downarrow{\scriptstyle f} & & \Big\downarrow{\scriptstyle C_f} \\ (B,\odot_2) & \xhookrightarrow{m_2} & \mathrm{Hol}(B,\oplus), \end{array}$$

which show that images of m_1 and m_2 are conjugate in $\mathrm{Hol}(B,\oplus)$.

Therefore, it remains to show that a regular subgroup of $\mathrm{Hol}(B,\oplus)$ corresponds to a skew brace. Let us fix a regular subgroup $G \subseteq \mathrm{Hol}(B,\oplus)$. Then G has an operation inherited from the group structure of $\mathrm{Hol}(B,\oplus)$, we take this to be the $\odot$ operation on G, if G is to be a skew brace. Since G is regular, the map

$$G \times (B,\oplus) \longrightarrow (B,\oplus) \times (B,\oplus) \text{ given by } (\eta\alpha, b) \longmapsto (\eta \oplus b^{\alpha}, b)$$

is a bijection, so for every $b \in B$ we can have a bijection

$$\varepsilon_b : G \longrightarrow (B,\oplus) \text{ given by } \eta\alpha \longmapsto \eta \oplus \alpha(b);$$

thus we can define a second operation on G by pulling back the operation of $(B,\oplus)$ on G, through $\varepsilon \stackrel{\text{def}}{=} \varepsilon_1$, so we let

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

Thus, if $g_1 = \eta_1\alpha_1$, $g_2 = \eta_2\alpha_2$, and $g_3 = \eta_3\alpha_3$, then

$$\begin{aligned} &g_1 \oplus g_2 = \varepsilon^{-1}(\eta_1 \oplus \eta_2) = (\eta_1 \oplus \eta_2)\beta_{12} \text{ for some } \beta_{12} \in \mathrm{Aut}(B,\oplus), \text{ whereas} \\ &g_1 \odot g_2 = (\eta_1 \oplus \eta_2^{\alpha_1})\alpha_1\alpha_2 \text{ and } g_1 \odot g_3 = (\eta_1 \oplus \eta_3^{\alpha_1})\alpha_1\alpha_3. \end{aligned}$$

Now since for some $\beta \in \mathrm{Aut}(B,\oplus)$

$$\varepsilon^{-1}(\eta_2 \oplus \eta_3) = (\eta_2 \oplus \eta_3)\beta \in G,$$

we have

$$\begin{aligned} &\eta_1\alpha_1 \odot ((\eta_2\alpha_2) \oplus (\eta_3\alpha_3)) = \eta_1\alpha_1 \odot (\varepsilon^{-1}(\eta_2 \oplus \eta_3)) = \eta_1\alpha_1 \odot ((\eta_2 \oplus \eta_3)\beta) \\ &= (\eta_1 \oplus (\eta_2 \oplus \eta_3)^{\alpha_1})\alpha_1\beta = \varepsilon^{-1}(\eta_1 \oplus (\eta_2 \oplus \eta_3)^{\alpha_1}) \text{ and} \\ &((\eta_1 \oplus \eta_2^{\alpha_1})\alpha_2) \ominus (\eta_1\alpha_1) \oplus ((\eta_1 \oplus \eta_3^{\alpha_1})\alpha_3) = \varepsilon^{-1}(\eta_1 \oplus (\eta_2 \oplus \eta_3)^{\alpha_1}), \end{aligned}$$

and so we see that $(G,\oplus,\odot)$ is a skew brace. Similarly, one checks that if G_1 and G_2 are regular subgroups which are conjugate by an element of $\varphi \in \mathrm{Aut}(B,\oplus)$, then the skew braces corresponding to G_1 and G_2 are isomorphic, which proves the proposition. □

Finally, the theorem below [cf. GV17, Theorem 3.1] shows the relationship between skew braces and the solutions to the Yang-Baxter equation.

Theorem 2.3.6. *Let $(B, \oplus, \odot)$ be a skew brace. Then the map*

$$r_B : B \times B \longrightarrow B \times B \text{ given by } (a,b) \longmapsto \left(\lambda_a(b), \lambda^{-1}_{\lambda_a(b)}\left(\ominus(a \odot b) \oplus a \oplus (a \odot b)\right)\right)$$

is a non-degenerate set-theoretic solution of the Yang-Baxter equation. Furthermore, r_B is involutive if and only if $(B, \oplus)$ is an abelian group.

2.3.1 Morphisms between skew braces

In this subsection we briefly study morphisms between skew braces and the automorphism group of skew braces. Recall, by Proposition 2.3.5, we can think of a skew brace of type N as a regular subgroup $G \subseteq \mathrm{Hol}(N)$ where the $\odot$-operation is inherited from $\mathrm{Hol}(N)$ and the $\oplus$-operation on G is given by

$$g_1 \oplus g_2 \stackrel{\text{def}}{=} \varepsilon^{-1}(\varepsilon(g_1)\varepsilon(g_2)) \text{ for all } g_1, g_2 \in G,$$

where $\varepsilon : G \longrightarrow N$ is the evaluation by 1 map (which is the restriction of the natural set-theoretic projection map from $\varepsilon : \mathrm{Hol}(N) \longrightarrow N$). Now for any subgroup $G \subseteq \mathrm{Hol}(N)$, and identifying $\mathrm{Aut}_{\mathcal{G}r}(N)$ as a subgroup of $\mathrm{Hol}(N)$, we define

$$\mathrm{Stab}(G) \stackrel{\text{def}}{=} \left\{\beta \in \mathrm{Aut}_{\mathcal{G}r}(N) \mid \beta G \beta^{-1} \subseteq G\right\}.$$

Note, $\mathrm{Stab}(G) \subseteq \mathrm{Aut}_{\mathcal{G}r}(N)$ and $\mathrm{Stab}(G) \hookrightarrow \mathrm{Aut}_{\mathcal{G}r}(G)$.

Now, we note that if $(B, \oplus, \odot)$ is a G-skew brace of type N, and

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

is an automorphism of skew braces, then we must have $f \in \mathrm{Aut}(B, \oplus)$ such that the diagram

$$\begin{array}{ccc} (B, \odot) & \stackrel{m}{\hookrightarrow} & \mathrm{Hol}(B, \oplus) \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle C_f} \\ (B, \odot) & \stackrel{m}{\hookrightarrow} & \mathrm{Hol}(B, \oplus). \end{array}$$

is commutative, where C_f is conjugating by f in $\mathrm{Hol}(B, \oplus)$ and $m_a(b) = a \odot b$ for $a, b \in B$ is the map defined in Lemma 2.3.4, *iii*). It can be seen that $\mathrm{Aut}_{\mathcal{B}r}(G) \cong \mathrm{Stab}(G)$. We shall discuss this in more detail.

Lemma 2.3.7. *Let N_1 and N_2 be groups. Let $G \subseteq \mathrm{Hol}(N_1)$ and $H \subseteq \mathrm{Hol}(N_2)$ be regular subgroups, and suppose that we are given a map $f \in \mathrm{Hom}_{\mathcal{G}r}(G, H)$. Then we have $f \in \mathrm{Hom}_{\mathcal{B}r}(G, H)$ if and only if $\varepsilon_2 f \varepsilon_1^{-1} \in \mathrm{Hom}_{\mathcal{G}r}(N_1, N_2)$, where $\varepsilon_1 : G \longrightarrow N_1$ and $\varepsilon_2 : H \longrightarrow N_2$ are evaluation on the identities of N_1 and N_2 maps, respectively.*

Proof. First suppose $f \in \mathrm{Hom}_{\mathcal{B}r}(G, H)$. Then we must have

$$f(g_1 \oplus g_2) = f(g_1) \oplus f(g_2) \text{ for all } g_1, g_2 \in G,$$

which means

$$f(\varepsilon_1^{-1}(\varepsilon_1(g_1)\varepsilon_1(g_2))) = \varepsilon_2^{-1}(\varepsilon_2(f(g_1))\varepsilon_2(f(g_2))) \text{ for all } g_1, g_2 \in G.$$

Now let $n_1 = \varepsilon_1(g_1)$ and $n_2 = \varepsilon_1(g_2)$ – note since $\varepsilon_1, \varepsilon_2$ are bijections, every element of N_1 can be written in this form. Then

$$\begin{aligned} \varepsilon_2 f \varepsilon_1^{-1}(n_1 n_2) &= \varepsilon_2 f \varepsilon_1^{-1}(\varepsilon_1(g_1)\varepsilon_1(g_2)) = \varepsilon_2 \varepsilon_2^{-1}(\varepsilon_2(f(g_1))\varepsilon_2(f(g_2))) \\ &= \varepsilon_2(f(g_1))\varepsilon_2(f(g_2)) = \varepsilon_2(f(\varepsilon_1^{-1}(n_1)))\varepsilon_2(f(\varepsilon_1^{-1}(n_2)) \\ &= \varepsilon_2 f \varepsilon_1^{-1}(n_1)\varepsilon_2 f \varepsilon_1^{-1}(n_2), \end{aligned}$$

so $\varepsilon_2 f \varepsilon_1^{-1}$ is a homomorphism.

Conversely, suppose $\varepsilon_2 f \varepsilon_1^{-1} = \widetilde{f} \in \mathrm{Hom}_{\mathcal{G}r}(N_1, N_2)$, so $f\varepsilon_1^{-1} = \varepsilon_2^{-1}\widetilde{f}$. Then

$$\begin{aligned} f(g_1 \oplus g_2) &= f(\varepsilon_1^{-1}(\varepsilon_1(g_1)\varepsilon_1(g_2))) = \varepsilon_2^{-1}(\widetilde{f}(\varepsilon_1(g_1)\varepsilon_1(g_2))) \\ &= \varepsilon_2^{-1}(\widetilde{f}(\varepsilon_1(g_1))\widetilde{f}(\varepsilon_1(g_2))) = \varepsilon_2^{-1}(\varepsilon_2 f(g_1)\varepsilon_2 f(g_2)) \\ &= f(g_1) \oplus f(g_2) \text{ for all } g_1, g_2 \in G. \end{aligned}$$

so f is a morphism of skew braces. □

Let $G \subseteq \mathrm{Hol}(N)$ be a regular subgroup. Then we have embeddings

$$\mathrm{Aut}_{\mathcal{B}r}(G) \hookrightarrow \mathrm{Aut}_{\mathcal{G}r}(N) \text{ and } \mathrm{Aut}_{\mathcal{B}r}(G) \hookrightarrow \mathrm{Aut}_{\mathcal{G}r}(G).$$

Also recall that by Subsection 2.1.1 the group G has a presentation

$$G = \langle \eta_1, ..., \eta_r, v_1\alpha_1, ..., v_s\alpha_s \rangle \subseteq \mathrm{Hol}(N),$$

where we set $H_1 \overset{\text{def}}{=} G \cap N = \langle \eta_1, ..., \eta_r \rangle$ and $H_2 \overset{\text{def}}{=} \Theta(H) = \langle \alpha_1, ..., \alpha_s \rangle$.

Theorem 2.3.8. *Let $G \subseteq \mathrm{Hol}(N)$ be a regular subgroup. Then we have a natural isomorphism*

$$\mathrm{Aut}_{\mathcal{B}r}(G) \xrightarrow{\sim} \mathrm{Stab}(G).$$

In particular, we have

$$\mathrm{Aut}_{\mathcal{B}r}(G) \subseteq \mathrm{Stab}(H_1) \cap \mathrm{Stab}(H_2),$$

where

$$\mathrm{Stab}(H_1) \stackrel{\text{def}}{=} \{\beta \in \mathrm{Aut}_{\mathcal{G}r}(N) \mid \beta(H_1) = H_1\},$$
$$\mathrm{Stab}(H_2) \stackrel{\text{def}}{=} \left\{\beta \in \mathrm{Aut}_{\mathcal{G}r}(N) \mid \beta H_2 \beta^{-1} = H_2\right\}.$$

Proof. Clearly the map C_β, conjugation by $\beta \in \mathrm{Stab}(G)$ on $\mathrm{Hol}(N)$, restricts to an automorphism on the group G, also note that we have

$$\varepsilon C_\beta \varepsilon^{-1}(N) = \varepsilon C_\beta \varepsilon^{-1}(\langle \eta_1, ..., \eta_r, v_1, ..., v_s\rangle) = \left\langle \eta_1^\beta, ..., \eta_r^\beta, v_1^\beta, ..., v_s^\beta \right\rangle,$$

so $\varepsilon C_\beta \varepsilon^{-1} = \beta \in \mathrm{Aut}_{\mathcal{G}r}(N)$, thus by Lemma 2.3.7, we have $C_\beta \in \mathrm{Aut}_{\mathcal{B}r}(G)$. This gives a homomorphism

$$\mathrm{Stab}(G) \longrightarrow \mathrm{Aut}_{\mathcal{B}r}(G),$$

which is injective since for any $f \in \mathrm{Aut}_{\mathcal{G}r}(G)$ we have $\varepsilon f \varepsilon^{-1} = \mathrm{id}$ if and only if $f = \mathrm{id}$. Conversely, let $f \in \mathrm{Aut}_{\mathcal{B}r}(G)$. Then by Lemma 2.3.7, we have $\varepsilon f \varepsilon^{-1} = \beta \in \mathrm{Aut}_{\mathcal{G}r}(N)$, and so $f = \varepsilon^{-1}\beta\varepsilon$; in fact, by Proposition 2.3.5, we have that f is given by conjugation by β, which shows that the map above is surjective.

The second statement follows since for $\beta \in \mathrm{Aut}_{\mathcal{B}r}(G)$ we need

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

and so we must have $\beta(H_1) \subseteq H_1$ and $\beta H_2 \beta^{-1} \subseteq H_2$. □

2.4 From Hopf-Galois structures to skew braces

In this section we discuss the explicit relationship between Hopf-Galois structures and skew braces and explain how we find our non-isomorphic skew braces. First we recall from Section 2.2, Theorem 2.2.7, that if L/K is a Galois extension of fields with Galois group G, and H is a K-Hopf algebra giving L/K a Hopf-Galois structure, then we must have $H = L[N]^G$ for some $N \subseteq \mathrm{Perm}(G)$ which is a regular subgroup normalised by the image of G as left translations inside $\mathrm{Perm}(G)$. Let us find a skew brace which corresponds to H. The fact that N is a regular subgroup implies that we have a bijection $\phi : N \longrightarrow G$ given by $n \longmapsto n \cdot 1_G$. Now we can define a skew brace B_H, corresponding to H, by setting $(B_H, \oplus) = N$ and defining

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

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 $f_{g,n} \in N$. Note, we have identified G with its image as left translations inside $\mathrm{Perm}(G)$. In particular, we can find $f_{\phi(n_1),n_2} \in N$ so that

$\phi(n_1)n_2 = f_{\phi(n_1),n_2}\phi(n_1)$ for any $n_1, n_2 \in N$. Therefore, for $n_1, n_2, n_3 \in N$, we have

$$\begin{aligned}
&(n_1 \odot n_2) \ominus n_1 \oplus (n_1 \odot n_3) = \phi^{-1}\left(\phi(n_1)\phi(n_2)\right) n_1^{-1}\phi^{-1}\left(\phi(n_1)\phi(n_3)\right)\\
&= \phi^{-1}\phi\left(f_{\phi(n_1),n_2}n_1\right) n_1^{-1}\phi^{-1}\phi\left(f_{\phi(n_1),n_3}n_1\right) = f_{\phi(n_1),n_2}f_{\phi(n_1),n_3}n_1 = f_{\phi(n_1),n_2n_3}n_1\\
&= \phi^{-1}\left(f_{\phi(n_1),n_2n_3}\left(\phi(n_1)\right)\right) = \phi^{-1}\left(\phi(n_1)\phi(n_2n_3)\right) = n_1 \odot (n_2 \oplus n_3)\,;
\end{aligned}$$

thus we have a skew brace $(B_H, \oplus, \odot)$ which is a G-skew brace of type N corresponding to the Hopf-Galois structure arising from H.

Conversely, let $(B, \oplus, \odot)$ be a G-skew brace of type N. Then we find an injective homomorphism $d : (B, \oplus) \longrightarrow \mathrm{Perm}(B, \odot)$ induced by the regular action of $(B, \oplus)$ on $(B, \odot)$ given by $(a, b) \longmapsto a \oplus b$ where $a \in (B, \oplus)$ and $b \in (B, \odot)$. Now, for any $a \in (B, \oplus)$ and $b, c \in (B, \odot)$, using the skew brace property, we have

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

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

Let us now discuss how we find the non-isomorphism skew braces. We shall denote by $B_G^N(m)$ for the isomorphism class of a G-skew brace of type N given by $(B, \oplus, \odot)$, whose size after embedding in $\mathrm{Hol}(B, \oplus)$ and projecting to $\mathrm{Aut}(B, \oplus)$ is m. We further let $\widetilde{e}(G, N, m)$ to be the number of isomorphism classes of G-skew braces of type N given by $(B, \oplus, \odot)$ whose size after embedding in $\mathrm{Hol}(B, \oplus)$ and projecting to $\mathrm{Aut}(B, \oplus)$ is m. We set

$$\widetilde{e}(G, N) \stackrel{\text{def}}{=} \sum_m \widetilde{e}(G, N, m) = \sum_m \sum_{B_G^N(m)} 1,$$

which is the number of isomorphism classes of G-skew braces of type N. Further we denote by

$$S_G^N(m) \stackrel{\text{def}}{=} \{H \subseteq \mathrm{Hol}(N) \mid H \text{ is regular},\ |\Theta(H)| = m,\ H \cong G\ \}.$$

Then conjugation by elements of $\mathrm{Aut}(N)$ on $\mathrm{Hol}(N)$ induces an action of $\mathrm{Aut}(N)$ on $S_G^N(m)$; thus, $S_G^N(m)$ is a disjoint union of orbits; consequently, according to Proposition 2.3.5, the number of distinct orbits is precisely the number of non-isomorphic G-skew braces of type N whose size after embedding in $\mathrm{Hol}(N)$ and projecting to $\mathrm{Aut}(N)$ is m.

Therefore, in order to find the set of non-isomorphic G-skew braces of type N, it suffices to find the set of regular subgroups of $\mathrm{Hol}(N)$ which are isomorphic to

G, and then extract a maximal subset whose elements are not conjugate by any element of $\mathrm{Aut}(N)$. Recall, in Section 2.2, we denoted by $e(G,N)$ the number of Hopf-Galois structures of type N on the field extension L/K whose Galois group is G, and we had

$$e(G,N) \stackrel{\text{def}}{=} \sum_m e(G,N,m).$$

Now we show how $e(G,N,m)$ and $\widetilde{e}(G,N,m)$ are related. Recall, from the formula (2.1), we had that

$$e(G,N,m) \stackrel{\text{def}}{=} \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|} e'(G,N,m),$$

which followed from Theorem 2.2.8, where $e'(G,N,m) = \left|S_G^N(m)\right|$ is the number of regular subgroups of $\mathrm{Hol}(N)$ isomorphic to G whose image under Θ has size m. We have

$$\begin{aligned} e'(G,N,m) = \left|S_G^N(m)\right| &= \sum_{G \in S_G^N(m)/\mathrm{Aut}(N)} |\mathrm{Orb}(G)| \\ &= \sum_{G \in S_G^N(m)/\mathrm{Aut}(N)} \frac{|\mathrm{Aut}(N)|}{|\mathrm{Stab}(G)|}, \end{aligned}$$

where $S_G^N(m)/\mathrm{Aut}(N)$ is the quotient set containing distinct orbits. Since running through elements $G \in S_G^N(m)/\mathrm{Aut}(N)$ corresponds to running through isomorphism classes of G-skew braces of type N, i.e., $B_G^N(m)$, and since using Theorem 2.3.8 we have $|\mathrm{Stab}(G)| = \left|\mathrm{Aut}(B_G^N(m))\right|$, we find

$$e'(G,N,m) = \sum_{B_G^N(m)} \frac{|\mathrm{Aut}(N)|}{|\mathrm{Aut}(B_G^N(m))|}.$$

Therefore, we have

$$e(G,N,m) = \sum_{B_G^N(m)} \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(B_G^N(m))|},$$

from which it follows, since $\mathrm{Aut}(B_G^N(m)) \subseteq \mathrm{Aut}(G)$, that

$$e(G,N,m) = \sum_{B_G^N(m)} \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(B_G^N(m))|} \geq \sum_{B_G^N(m)} 1 = \widetilde{e}(G,N,m).$$

This also implies that if we understand $\mathrm{Aut}(G)$ and the automorphism groups of all G-skew braces of type N, then we can determine the number of Hopf-Galois structures of type N on a Galois extension of fields with Galois group G.

Chapter 3

Preliminaries II: The groups of order p^3

Let p be a prime number. Then, up to isomorphism, there are 3 abelian and 2 nonabelian groups of order p^3. In this chapter we are mainly concerned with studying groups of order p^3 and their automorphisms groups, but in some places we have studied more general p-groups.

3.1 The cyclic group C_{p^n}

For $n \geq 1$ the cyclic group C_{p^n} has a presentation

$$C_{p^n} \stackrel{\text{def}}{=} \left\langle \sigma \mid \sigma^{p^n} = 1 \right\rangle.$$

Note, for all $0 \leq m \leq n$ the group C_{p^n} contains a unique subgroup of order p^{n-m} given by $\left\langle \sigma^{p^m} \right\rangle$.

Lemma 3.1.1. *For $p > 2$ we have $|\mathrm{Aut}(C_{p^n})| = (p-1)p^{n-1}$ and*

$$\mathrm{Aut}(C_{p^n}) \cong C_{p^{n-1}} \times C_{p-1},$$

where $C_{p^{n-1}}$ is generated by $\alpha \in \mathrm{Aut}(C_{p^n})$ with $\sigma^\alpha = \sigma^{p+1}$.

For $p = 2$ and $n > 1$ we have $|\mathrm{Aut}(C_{2^n})| = 2^{n-1}$ and

$$\mathrm{Aut}(C_{2^n}) \cong C_{2^{n-2}} \times C_2 = \langle \alpha_1, \alpha_2 \rangle$$

where $\alpha_1, \alpha_2 \in \mathrm{Aut}(C_{2^n})$ are given by $\sigma^{\alpha_1} = \sigma^5$ and $\sigma^{\alpha_2} = \sigma^{-1}$.

Proof. If $\beta \in \mathrm{Aut}(C_{p^n})$, then β must map the generator σ to another generator, so we must have $\sigma^\beta = \sigma^a$ with $p \nmid a$; in particular $\mathrm{Aut}(C_{p^n})$ is abelian and

$$|\mathrm{Aut}(C_{p^3})| = (p-1)p^{n-1}.$$

Note, for $p > 2$ we may identify

$$\mathrm{Aut}(C_{p^n}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \frac{\mathbb{Z}}{(p-1)p^{n-1}\mathbb{Z}}$$

from which it follows that $\mathrm{Aut}(C_{p^n}) \cong C_{p^{n-1}} \times C_{p-1}$ with the factor $C_{p^{n-1}}$ given by

$$C_{p^{n-1}} = \langle \alpha \rangle \text{ where } \sigma^\alpha = \sigma^{p+1}.$$

The structure of $\mathrm{Aut}(C_{p^n})$ for $p = 2$ and $n = 2$ is clear. For $n > 2$ our claim follows by noting that $\mathrm{Aut}(C_{2^n})$ is not cyclic, the automorphism α_1 with $\sigma^{\alpha_1} = \sigma^5$ has order 2^{n-2}, the automorphism α_2 with $\sigma^{\alpha_2} = \sigma^{-1}$ has order 2, and they commute. □

3.2 The product of cyclic groups $C_{p^{n-1}} \times C_p$

For $n \geq 3$ the group $C_{p^{n-1}} \times C_p$ has a presentation

$$C_{p^{n-1}} \times C_p \stackrel{\text{def}}{=} \left\langle \sigma, \tau \mid \sigma^{p^{n-1}} = \tau^p = 1,\ \tau\sigma = \sigma\tau \right\rangle.$$

Note, when $n = 3$, the group $C_{p^2} \times C_p$ contains $p^2 - 1$ elements of order p of the form $\sigma^{a_1 p}\tau^{a_2}$ for integers a_1 and a_2, not both zero, so it contains $\frac{p^2-1}{p-1} = p + 1$ subgroups of order p which are of the form

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

Further, $C_{p^2} \times C_p$ contains $p + 1$ subgroups of order p^2, of which one subgroup is isomorphic to C_p^2 given by $\langle \sigma^p, \tau \rangle$ and p of them are cyclic which of the form $\langle \sigma\tau^b \rangle$ for $b = 0, ..., p-1$.

Let us denote by

$$\mathrm{L}(\mathbb{F}_p) \stackrel{\text{def}}{=} \left\{ A \in \mathrm{GL}_2(\mathbb{F}_p) \mid A = \begin{pmatrix} a_1 & 0 \\ a_3 & a_4 \end{pmatrix} \right\}$$

the subgroup of lower triangular matrices in $\mathrm{GL}_2(\mathbb{F}_p)$.

Lemma 3.2.1. *We have* $|\mathrm{Aut}(C_{p^{n-1}} \times C_p)| = (p-1)^2 p^n$. *Furthermore, every automorphism of* $C_{p^{n-1}} \times C_p$ *can be written as a matrix* $\left(\begin{smallmatrix} a_1 & b_2 p^{n-2} \\ a_3 & a_4 \end{smallmatrix}\right)$, *with* $a_1 = 0, ..., p^{n-1} - 1$ *and* $b_2, a_3, a_4 = 0, ..., p-1$, *such that if we reduce the entries modulo* p, *then we have an element of* $\mathrm{L}(\mathbb{F}_p)$.

Proof. Let $\alpha \in \mathrm{Aut}(C_{p^{n-1}} \times C_p)$. Then we have

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

for some $a_1, a_2, a_3, a_4 \in \mathbb{Z}$. We shall write

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$$

to represent α, where the first row matters modulo p^{n-1} and the second row modulo p. Now since $\tau^p = 1$, and since α is a homomorphism, we must have $\alpha(\tau^p) = \sigma^{a_2 p} = 1$, so we must have

$$a_2 p \equiv 0 \bmod p^{n-1},$$

i.e., we have $a_2 = b_2 p^{n-2}$ for $b_2 = 0, ..., p-1$. Since α is an automorphism, it must send σ to an element of order p^{n-1}, which implies

$$a_1 \not\equiv 0 \bmod p.$$

Further, for α to be injective, we require

$$\langle \sigma^\alpha \rangle \cap \langle \tau^\alpha \rangle = \langle \sigma^{a_1} \tau^{a_3} \rangle \cap \langle \sigma^{a_2} \tau^{a_4} \rangle = 1,$$

and so we must have

$$a_4 \not\equiv 0 \bmod p.$$

One check that these are all the restriction on α to be an automorphism. This gives $p^{n-1} - p^{n-2}$ choices for a_1, p choices for a_2, p choices for a_3, and $p-1$ choices for a_4.

Therefore, we have

$$|\mathrm{Aut}(C_{p^{n-1}} \times C_p)| = (p-1)^2 p^n,$$

and that every automorphism of $C_{p^{n-1}} \times C_p$ can be written as a matrix $\left(\begin{smallmatrix} a_1 & b_2 p^{n-2} \\ a_3 & a_4 \end{smallmatrix}\right)$ such that if we reduce the entries modulo p, then the matrix is an element of $\mathrm{L}(\mathbb{F}_p)$. □

3.3 The elementary abelian group C_p^3

The elementary abelian group C_p^3 has a presentation

$$C_p^3 \overset{\text{def}}{=} \langle \rho, \sigma, \tau \mid \rho^p = \sigma^p = \tau^p = 1,\ \sigma\rho = \rho\sigma,\ \tau\rho = \rho\tau,\ \tau\sigma = \sigma\tau \rangle .$$

Note, C_p^3 contains $\frac{p^3-1}{p-1} = p^2 + p + 1$ subgroups of order p, which are of the form

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

also C_p^3 contains $\frac{(p^3-1)(p^3-p)}{(p^2-1)(p^2-p)} = p^2 + p + 1$ subgroups of order p^2.

Lemma 3.3.1. *We have* $\left|\mathrm{Aut}(C_p^3)\right| = (p^3-1)(p^2-1)(p-1)p^3$ *and*

$$\mathrm{Aut}(C_p^3) \cong \mathrm{GL}_3(\mathbb{F}_p).$$

Proof. The group C_p^3 can be identified with $\mathbb{F}_p^3$, the 3-dimensional vector space over the finite field $\mathbb{F}_p$, and so the automorphism group of C_p^3 can be identified with the invertible 3×3 matrices over $\mathbb{F}_p$, namely $\mathrm{GL}_3(\mathbb{F}_p)$. Now the lemma follows from standard results relating to $\mathrm{GL}_3(\mathbb{F}_p)$. □

We remark that in general one has $\mathrm{Aut}(C_p^n) \cong \mathrm{GL}_n(\mathbb{F}_p)$, also

$$|\mathrm{GL}_n(\mathbb{F}_p)| = p^{\frac{1}{2}n(n-1)} \prod_{j=1}^{n} (p^j - 1),$$
$$|\mathrm{SL}_n(\mathbb{F}_p)| = p^{\frac{1}{2}n(n-1)} \prod_{j=2}^{n} (p^j - 1).$$

3.4 The nonabelian exponent p group M_1

For $p > 2$ the exponent p group M_1, or otherwise known as the Heisenberg group of order p^3, 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

$$(\sigma^{a_1}\tau^{a_2})^n = \rho^{\frac{1}{2}a_1 a_2 n(n-1)}\sigma^{na_1}\tau^{na_2}. \tag{3.1}$$

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

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

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

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

Lemma 3.4.1. *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 automorphisms* $\beta, \gamma \in \mathrm{Aut}(M_1)$ *given 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 we find

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

so α is bijective if and only if $a_1a_4 - a_2a_3 \not\equiv 0 \bmod p$. Since if $a_1a_4 - a_2a_3 \equiv 0 \bmod p$, then α is not injective. Conversely, if $a_1a_4 - a_2a_3 \not\equiv 0 \bmod p$, then $(\rho^{v_1}\sigma^{v_2}\tau^{v_3})^\alpha = 1$, implies $v_1 = v_2 = v_3 = 0$ and that α is injective, and hence bijective. We shall write

$$\begin{pmatrix} a_1a_4 - a_2a_3 & b_1 & b_2 \\ 0 & a_1 & a_2 \\ 0 & a_3 & a_4 \end{pmatrix}$$

to represent α. This is only a representation, and so composition of automorphisms does not in general correspond to matrix multiplication.

To understand the structure of $\mathrm{Aut}(M_1)$ we work as follows. 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 $\sigma, \tau \in M_1$. Any automorphism of M_1 must map the characteristic subgroup $Z \subseteq M_1$ to itself, and so it induces an automorphism of M_1/Z; 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 automorphism of M_1 is contained in the kernel of Ψ 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 α, which implies that $\mathrm{Inn}(M_1) = \mathrm{Ker}\,\Psi$. We further find $\mathrm{Ker}\,\Psi = \langle \beta, \gamma \rangle$ where

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

Now we shall show the map Ψ is surjective. For any

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

define a map

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

Then we have

$$\sigma^{\alpha_A}\tau^{\alpha_A} = \rho^{\frac{ac+bd}{2}+bc}\sigma^{a+b}\tau^{c+d},$$
$$\tau^{\alpha_A}\sigma^{\alpha_A} = \rho^{\frac{ac+bd}{2}+ad}\sigma^{a+b}\tau^{c+d},$$

so

$$\rho^{\alpha_A} = \tau^{\alpha_A}\sigma^{\alpha_A}\left(\sigma^{\alpha_A}\tau^{\alpha_A}\right)^{-1} = \rho^{ad-bc} = \rho^{\det(A)}.$$

We see that α_A is an automorphism, and so Ψ is surjective. In particular, the map $A \longmapsto \alpha_A$ is a group homomorphism as follows. Let

$$A_1 \stackrel{\text{def}}{=} \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \ A_2 \stackrel{\text{def}}{=} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p).$$

Then

$$\begin{aligned}
(\sigma^{\alpha_{A_1}})^{\alpha_{A_2}} &= \left(\rho^{\frac{a_1c_1}{2}}\sigma^{a_1}\tau^{c_1}\right)^{\alpha_{A_2}} = \rho^{\det(A_2)\frac{a_1c_1}{2}}\left(\rho^{\frac{a_2c_2}{2}}\sigma^{a_2}\tau^{c_2}\right)^{a_1}\left(\rho^{\frac{b_2d_2}{2}}\sigma^{b_2}\tau^{d_2}\right)^{c_1} \\
&= \rho^{k_1}(\sigma^{a_2}\tau^{c_2})^{a_1}(\sigma^{b_2}\tau^{d_2})^{c_1}, \\
\text{where } k_1 &\stackrel{\text{def}}{=} \frac{1}{2}\left(\det(A_2)a_1c_1 + a_1a_2c_2 + c_1b_2d_2\right), \text{ so} \\
(\sigma^{\alpha_{A_1}})^{\alpha_{A_2}} &= \rho^{k_2}\sigma^{a_1a_2}\tau^{a_1c_2}\sigma^{c_1b_2}\tau^{c_1d_2}, \\
\text{where } k_2 &\stackrel{\text{def}}{=} k_1 + \frac{1}{2}\left(a_2c_2a_1\left(a_1-1\right) + b_2d_2c_1\left(c_1-1\right)\right), \text{ so} \\
(\sigma^{\alpha_{A_1}})^{\alpha_{A_2}} &= \rho^{k_3}\sigma^{a_1a_2}\sigma^{c_1b_2}\tau^{a_1c_2}\tau^{c_1d_2}, \\
\text{where } k_3 &\stackrel{\text{def}}{=} k_2 + a_1c_1b_2c_2 = \frac{1}{2}\left(a_2d_2a_1c_1 + b_2d_2c_1^2 + c_2a_2a_1^2 + a_1c_1b_2c_2\right) \\
&= \frac{1}{2}\left(a_2a_1 + b_2c_1\right)\left(d_2c_1 + c_2a_1\right),
\end{aligned}$$

from which one can see that

$$(\sigma^{\alpha_{A_1}})^{\alpha_{A_2}} = \sigma^{\alpha_{A_2A_1}},$$

similarly, one checks that

$$(\tau^{\alpha_{A_1}})^{\alpha_{A_2}} = \tau^{\alpha_{A_2A_1}},$$

so we see that the map $A \longmapsto \alpha_A$ has the property that $A_2A_1 \longmapsto \alpha_{A_2}\alpha_{A_1}$. Therefore, we have a split exact sequence

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

In order to determine the action of $\mathrm{GL}_2(\mathbb{F}_p)$ on the group C_p^2 in the above exact sequence it suffices to determine the action on the elements β, γ. Let

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

Then $A^{-1} = \frac{1}{\det(A)}\left(\begin{smallmatrix} a_4 & -a_2 \\ -a_3 & a_1 \end{smallmatrix}\right)$. Now we have

$$\begin{aligned}
\sigma^{\alpha_A^{-1}\beta\alpha_A} &= \left(\rho^{\frac{a_1a_3}{2}}\sigma^{a_1}\tau^{a_3}\right)^{\alpha_A^{-1}\beta} = \left(\rho^{\frac{a_1a_3}{2}}\sigma^{a_1}\left(\rho\tau\right)^{a_3}\right)^{\alpha_A^{-1}} = \left(\rho^{a_3}\sigma^{\alpha_A}\right)^{\alpha_A^{-1}} = \sigma^{\gamma^{a_3\det(A^{-1})}}, \\
\tau^{\alpha_A^{-1}\beta\alpha_A} &= \left(\rho^{\frac{a_2a_4}{2}}\sigma^{a_2}\tau^{a_4}\right)^{\alpha_A^{-1}\beta} = \left(\rho^{\frac{a_2a_4}{2}}\sigma^{a_2}\left(\rho\tau\right)^{a_4}\right)^{\alpha_A^{-1}} = \left(\rho^{a_4}\tau^{\alpha_A}\right)^{\alpha_A^{-1}} = \tau^{\beta^{a_4\det(A^{-1})}},
\end{aligned}$$

similarly, we also find

$$\begin{aligned}
\sigma^{\alpha_A^{-1}\gamma\alpha_A} &= \sigma^{\gamma^{a_1\det(A^{-1})}}, \\
\tau^{\alpha_A^{-1}\gamma\alpha_A} &= \tau^{\beta^{a_2\det(A^{-1})}},
\end{aligned}$$

thus, we have

$$\alpha_A^{-1}\beta\alpha_A = \beta^{a_4\det(A^{-1})}\gamma^{a_3\det(A^{-1})},$$
$$\alpha_A^{-1}\gamma\alpha_A = \beta^{a_2\det(A^{-1})}\gamma^{a_1\det(A^{-1})}.$$

Note, the above calculation determines a right action, so replacing A with A^{-1} the left action is given by

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

□

3.5 The nonabelian exponent p^2 group M_2

For $p > 2$ the exponent p^2 group M_2, or otherwise known as the Extraspecial group of order p^3, has a presentation [1]

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

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

$$\sigma^{a_1}\tau^{a_2}\sigma^{a_3}\tau^{a_4} = \sigma^{a_1+a_3(p+1)^{a_2}}\tau^{a_2+a_4} = \sigma^{a_2a_3p}\sigma^{a_1+a_3}\tau^{a_2+a_4},$$

from which we obtain the relation

$$(\sigma^{a_1}\tau^{a_2})^n = \sigma^{\frac{1}{2}a_1a_2n(n-1)p}\sigma^{na_1}\tau^{na_2}. \tag{3.2}$$

We note that the group M_2 contains only $p+1$ subgroups of order p, which are of the form

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

Also M_2 contains only $p+1$ subgroups of order p^2, of which one subgroup is isomorphic to C_p^2 given by $\langle\sigma^p, \tau\rangle$, and p of them are cyclic, which are of the form $\langle\sigma\tau^b\rangle$ for $b = 0, ..., p-1$.

Let

$$\mathrm{L}_1(\mathbb{F}_p) \stackrel{\text{def}}{=} \left\{ A \in \mathrm{GL}_2(\mathbb{F}_p) \mid A = \begin{pmatrix} a_1 & 0 \\ a_3 & 1 \end{pmatrix} \right\}$$

be the subgroup of the lower triangular matrices in $\mathrm{GL}_2(\mathbb{F}_p)$ whose bottom right entry is equal to 1.

Lemma 3.5.1. *We have* $|\mathrm{Aut}(M_2)| = (p-1)p^3$. *Furthermore, every automorphism*

[1] for $p = 2$ the groups M_2 and M_1 are isomorphic.

of M_2 can be written as $\left(\begin{smallmatrix} a_1 & b_2 p \\ a_3 & 1 \end{smallmatrix}\right)$, with $a_1 = 0, ..., p^2 - 1$ and $b_2, a_3, a_4 = 0, ..., p - 1$, such that if we reduce the entries modulo p, then we have an element of $\mathrm{L}_1(\mathbb{F}_p)$.

Proof. Let $\alpha \in \mathrm{Aut}(M_2)$. Then we have

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

for some $a_1, a_2, a_3, a_4 \in \mathbb{Z}$. We shall write

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$$

to represent α, where the first row matters modulo p^2 and the second row modulo p. Note with this representation composition of automorphisms does not in general correspond to matrix multiplication. Now since $\tau^p = 1$, we require that

$$(\sigma^{a_2}\tau^{a_4})^p = \sigma^{a_2 p + \frac{1}{2}a_2 a_4 (p-1)p^2}\tau^{a_4 p} = 1,$$

and so we must have

$$a_2 \equiv 0 \bmod p,$$

which implies that for α to be injective we need

$$a_1, a_4 \not\equiv 0 \bmod p.$$

We further need $(\sigma^\alpha)^{p+1}\tau^\alpha = \tau^\alpha\sigma^\alpha$; thus, setting $a_2 = 0$, we need

$$\begin{aligned}(\sigma^\alpha)^{p+1}\tau^\alpha &= (\sigma^{a_1}\tau^{a_3})^{p+1}\sigma^{a_2}\tau^{a_4} = \sigma^{(p+1)a_1 + a_2}\tau^{(p+1)a_3}\tau^{a_4} \\ &= \sigma^{(p+1)a_1 + a_2}\tau^{a_3 + a_4}\end{aligned}$$

to be equal to $\tau^\alpha\sigma^\alpha = \sigma^{a_2}\tau^{a_4}\sigma^{a_1}\tau^{a_3} = \sigma^{a_1 + a_2 + a_1 a_4 p}\tau^{a_3 + a_4}$, so we must have

$$a_1 a_4 \equiv a_1 \bmod p,$$

which implies that $a_4 = 1$. This gives us

$$|\mathrm{Aut}(M_2)| = (p-1)p^3,$$

and that every automorphism of M_2 can be written as $\left(\begin{smallmatrix} a_1 & b_2 p \\ a_3 & 1 \end{smallmatrix}\right)$ such that if we reduce the entries modulo p, then we have a matrix which is an element of $\mathrm{L}_1(\mathbb{F}_p)$. □

3.6 The groups of order p^3 for $p = 2$

For $p = 2$ the abelian groups of order 8 are the same as in Sections 3.1 – 3.3. The nonabelian groups of order 8 are, the dihedral group,

$$D_8 \stackrel{\text{def}}{=} \left\langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1,\ \tau\sigma = \sigma^{-1}\tau \right\rangle,$$

which is isomorphic to the group

$$M_1 \stackrel{\text{def}}{=} \left\langle \rho, \sigma, \tau \mid \rho^2 = \sigma^2 = \tau^2 = 1,\ \sigma\rho = \rho\sigma,\ \tau\rho = \rho\tau,\ \tau\sigma = \rho\sigma\tau \right\rangle,$$

and the quaternion group

$$Q_8 \stackrel{\text{def}}{=} \left\langle \sigma, \tau \mid \sigma^4 = 1,\ \sigma^2 = \tau^2,\ \tau\sigma = \sigma^{-1}\tau \right\rangle.$$

We shall investigate each of these two groups separately.

Let us consider

$$D_8 \stackrel{\text{def}}{=} \left\langle \sigma, \tau : \sigma^4 = \tau^2 = 1,\ \tau\sigma = \sigma^{-1}\tau \right\rangle.$$

Note, the above relations imply that for positive integers b_1, b_2, b_3, b_4 we have

$$\sigma^{b_1}\tau^{b_2}\sigma^{b_3}\tau^{b_4} = \sigma^{2b_2b_3}\sigma^{b_1+b_3}\tau^{b_2+b_4},$$

from which we obtain the relation

$$\left(\sigma^{b_1}\tau^{b_2}\right)^n = \sigma^{b_1b_2n(n-1)+b_1n}\tau^{b_2n}.$$

Note that D_8 contains 5 subgroups of order 2 of the form

$$\left\langle \sigma^2 \right\rangle, \langle \sigma^a\tau \rangle \text{ for } a = 0, 1, 2, 3,$$

also D_8 contains 3 subgroups of order 4, of which 2 are isomorphic to C_2^2 given by $\left\langle \sigma^2, \sigma^b\tau \right\rangle$ for $b = 0, 1$, and one of them is cyclic given by $\langle \sigma \rangle$.

Now we shall determine automorphism group of D_8 similar to Lemma 3.5.1. Let $\alpha \in \mathrm{Aut}(D_8)$. Then

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

for some $a_i \in \mathbb{Z}$ for $i = 1, ..., 4$, where a_1, a_2 matter modulo 4 and a_3, a_4 modulo 2.

Since τ has order 2 and σ order 4 we need

$$a_2(a_4 + 1) \equiv 0 \bmod 2$$

and $a_3 = 0$, so $a_4 = 1$ and $a_1 \not\equiv 0 \bmod 2$. One can check that $\mathrm{Aut}(D_8)$ fits in the exact sequence

$$1 \longrightarrow C_2^2 \longrightarrow \mathrm{Aut}(D_8) \xrightarrow{\Psi} \mathrm{U}(\mathbb{F}_2) \longrightarrow 1,$$

so $|\mathrm{Aut}(D_8)| = 8$, where

$$\mathrm{U}(\mathbb{F}_2) \stackrel{\text{def}}{=} \left\{ A \in \mathrm{GL}_2(\mathbb{F}_2) : A = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \right\},$$

and $\operatorname{Ker}\Psi = \langle \beta, \gamma \rangle \cong C_2^2$ with β and γ given by

$$\begin{aligned} &\sigma^\beta = \sigma,\ \tau^\beta = \sigma^2\tau \text{ and} \\ &\sigma^\gamma = \sigma^2\sigma,\ \tau^\gamma = \tau. \end{aligned}$$

Next we consider the quaternion group

$$Q_8 \stackrel{\text{def}}{=} \left\langle \sigma, \tau \mid \sigma^4 = 1,\ \sigma^2 = \tau^2,\ \sigma^{-1}\tau = \tau\sigma \right\rangle.$$

Note, the above relations imply that for positive integers b_1, b_2, b_3, b_4, we have

$$\sigma^{b_1}\tau^{b_2}\sigma^{b_3}\tau^{b_4} = \sigma^{2b_2b_3}\sigma^{b_1+b_3}\tau^{b_2+b_4},$$

from which we obtain the relation

$$\left(\sigma^{b_1}\tau^{b_2}\right)^n = \sigma^{b_1b_2n(n-1)}\sigma^{b_1n}\tau^{b_2n}.$$

Note that Q_8 contains one subgroups of order 2 of the form $\langle\sigma^2\rangle$, also Q_8 contains 3 subgroups of order 4, which are cyclic, and they are of the form

$$\langle\sigma\rangle, \langle\sigma^a\tau\rangle \text{ for } a = 0, 1.$$

Now we shall determine automorphism group of Q_8 similar to Lemma 3.4.1.

Let $\alpha \in \mathrm{Aut}(Q_8)$. Then

$$\begin{aligned} \sigma^\alpha &= \sigma^{a_1}\tau^{a_3} \\ \tau^\alpha &= \sigma^{a_2}\tau^{a_4} \end{aligned}$$

for some $a_i \in \mathbb{Z}$ for $i = 1, ..., 4$, and they only matter modulo 4.

We need $a_1 \not\equiv 0 \bmod 2$ or $a_3 \not\equiv 0 \bmod 2$, similarly $a_2 \not\equiv 0 \bmod 2$ or $a_4 \not\equiv 0 \bmod 2$.

Since $\sigma^2 = \tau^2$ we need

$$a_1a_3 + a_1 + a_3 \equiv a_2a_4 + a_2 + a_4 \bmod 2,$$

which is always satisfied. Since $\tau = \sigma\tau\sigma$, we need

$$a_1a_4 - a_2a_3 + a_1a_3 + a_1 + a_3 \equiv 0 \bmod 2,$$

which implies that we need $a_1a_4 - a_2a_3 \equiv 1 \bmod 2$. One can check that $\mathrm{Aut}(Q_8)$ fits in the exact sequence

$$1 \longrightarrow C_2^2 \longrightarrow \mathrm{Aut}(Q_8) \xrightarrow{\Psi} \mathrm{GL}_2(\mathbb{F}_2) \longrightarrow 1,$$

so $|\mathrm{Aut}(D_8)| = 24$, where $\operatorname{Ker}\Psi = \langle\beta, \gamma\rangle \cong C_2^2$ and β, γ are given by

$$\sigma^\beta = \sigma,\ \tau^\beta = \sigma^2\tau \text{ and}$$
$$\sigma^\gamma = \sigma^2\sigma,\ \tau^\gamma = \tau.$$

Remark 3.6.1. We have adopted the convention that whenever we use a matrix representation for our automorphisms, we have consistently used the last column to show the effect of the automorphism on τ, which we have denoted consistently to be the generator with smallest order, the one to the last column on σ, which we have taken consistently to be the generator with the largest order, and the other column (wherever there is one) on ρ. We shall keep to this convention throughout.

Part II

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

Chapter 4

Hopf-Galois structures and skew braces for $p > 3$

In this chapter we determine the Hopf-Galois structures and classify, up to isomorphism, the skew braces, of order p^3, mainly for $p > 3$; although, in some places we have study more general p-groups. Let us here once and for all fix an element

$$\delta \in \mathbb{F}_p^\times \setminus \left(\mathbb{F}_p^\times\right)^2, \tag{4.1}$$

i.e., δ is not a square modulo p.

4.1 Regular subgroups in $\mathrm{Hol}(C_{p^n})$

In this section for $p > 2$ we classify the regular subgroups contained in $\mathrm{Hol}(C_{p^n})$, from which we find the number of Hopf-Galois structures and braces of C_{p^n} type. We also determine the automorphism groups of braces of C_{p^n} type. We note that the classification of the regular subgroups contained in $\mathrm{Hol}(C_{p^n})$ can also be found in [Chi00, (8.6) Proposition], so we have provided some of the calculations here mainly for completeness. The main result of this section is the following.

Proposition 4.1.1. *We have*

$$e(C_{p^n}, C_{p^n}) = p^{n-1} \text{ and } e(G, C_{p^n}) = 0 \text{ for } G \ncong C_{p^n}.$$

Furthermore, we have

$$\widetilde{e}(C_{p^n}, C_{p^n}) = n \text{ and } \widetilde{e}(G, C_{p^n}) = 0 \text{ for } G \ncong C_{p^n}.$$

The proof of the proposition above follows from the calculations in the rest of this section. We shall work with primes $p > 2$. First we recall from Section 3.1, that

$$C_{p^n} \stackrel{\text{def}}{=} \left\langle \sigma \mid \sigma^{p^n} = 1 \right\rangle.$$

Now in order to make the notation easier we shall often use the identification

$$C_{p^n} \cong \mathbb{Z}/p^n\mathbb{Z} \text{ given by } \sigma \longrightarrow 1 \bmod p^n,$$

and we consider all natural numbers modulo p^n. By Lemma 3.1.1, we may identify the holomorph of C_{p^n} with

$$\mathrm{Hol}(C_{p^n}) = \{[v, \beta] : v \in \mathbb{Z}/p^n\mathbb{Z},\ \beta \in \mathrm{Aut}(C_{p^n})\} \cong (\mathbb{Z}/p^n\mathbb{Z}) \rtimes (C_{p^{n-1}} \times C_{p-1}).$$

Note, the image of a subgroup of $\mathrm{Hol}(C_{p^n})$ of order p^n in $\mathrm{Aut}(C_{p^n})$ under the natural projection

$$\Theta : \mathrm{Hol}(C_{p^n}) \longrightarrow \mathrm{Aut}(C_{p^n})$$

must lie in $C_{p^{n-1}}$; thus any subgroup of $\mathrm{Hol}(C_{p^n})$ of order p^n lies in

$$(\mathbb{Z}/p^n\mathbb{Z}) \rtimes \langle\alpha\rangle \cong C_{p^n} \rtimes C_{p^{n-1}}, \text{ where } \alpha(1) \equiv 1 + p \bmod p^n.$$

Now suppose G is a subgroup of order p^n in $\mathrm{Hol}(C_{p^n})$. Then we must have $|\Theta(G)| = 1, p, ..., p^{n-1}$. First we consider the case when $n = 3$, then we generalise the procedure to arbitrary n.

Lemma 4.1.2. *There are exactly p^2 regular subgroups contained in $\mathrm{Hol}(C_{p^3})$ given by the cyclic subgroups*

$$\langle[1, \mathrm{id}]\rangle, \langle[v_1, \alpha^p]\rangle, \langle[v_2, \alpha]\rangle$$

for $v_1 = 1, ..., p-1$ and $v_2 = 1, ..., p^2 - 1$ with $p \nmid v_2$.

Furthermore, there are exactly three cyclic braces of degree p^3 all of which are cyclic type given by

$$\langle[1, \mathrm{id}]\rangle, \langle[1, \alpha^p]\rangle, \langle[1, \alpha]\rangle.$$

Proof. Suppose G is a group of order p^3. If $G \subseteq \mathrm{Hol}(C_{p^3})$ with $|\Theta(G)| = 1$, then we must have $G = \langle[1, \mathrm{id}]\rangle$ which is a regular subgroup of $\mathrm{Hol}(C_{p^3})$ since it acts on C_{p^3} by translation. The class of $\langle[1, \mathrm{id}]\rangle$ gives a brace.

If $G \subseteq \mathrm{Hol}(C_{p^3})$ with $|\Theta(G)| = p$, then we must have $\Theta(G) = \langle\alpha^p\rangle$ and $G \cap C_{p^3} = \langle p\rangle$, so

$$G = \langle[p, \mathrm{id}], [v, \alpha^p]\rangle$$

for some $v \in \mathbb{Z}/p^3\mathbb{Z}$, and by multiplying $[v, \alpha^p]$ with a suitable power of $[p, \mathrm{id}]$, we can assume $v = 0, ..., p-1$. We look for condition on v such that G is regular. Note since

$$\alpha^p(1) = (1 + p)^p = 1 + p^2 \bmod p^3,$$

we have

$$[v, \alpha^p][p, \mathrm{id}] = [v + p + p^3, \alpha^p] = [v + p, \alpha^p] = [p, \mathrm{id}][v, \alpha^p],$$

so G is abelian. Now for a natural number a we have

$$\begin{aligned}[v,\alpha^p]^a &= \left[(1+(1+p)^p+\cdots+(1+p)^{(a-1)p})v, \alpha^{ap}\right] \\ &= \left[av + \frac{1}{2}p^2a(a-1)v + \frac{1}{2}p^3\left(\frac{p}{6}a(a-1)(2a-1) - \frac{1}{2}a(a-1)\right)v, \alpha^{ap}\right] \\ &= \left[(a+\frac{1}{2}p^2a(a-1))v, \alpha^{ap}\right].\end{aligned}$$

We see that G has size p^3 and that G is regular if and only if $v \neq 0$, since $(v,\alpha^p)^a(0) = 0$ for $a \neq 0$ and $v = 0$. Conversely, and if $v \neq 0$ and $[v,\alpha^p]^a(0) = 0$, then we must have

$$(a + \frac{1}{2}p^2a(a-1)) \equiv 0 \bmod p^3$$

so $a = 0$. When $v \neq 0$, by above calculation, $[v,\alpha^p]$ has order p^3, and so

$$G = \langle [p,\mathrm{id}], [v,\alpha^p]\rangle = \langle [v,\alpha^p]\rangle \cong C_{p^3}$$

which is a cyclic regular subgroup of Hol(C_{p^3}). Therefore, there are $p-1$ distinct regular subgroups of Hol(C_{p^3}) of the form

$$\langle [v,\alpha^p]\rangle \cong C_{p^3} \text{ for } v = 1,...,p-1.$$

Furthermore, since there exists an automorphism in Aut(C_{p^3}) which takes 1 to any of $\{1,...,p-1\}$, all these regular subgroups are isomorphic as braces, and so the class of $\langle [1,\alpha^p]\rangle$ corresponds to a brace.

If $G \subseteq \mathrm{Hol}(C_{p^3})$ with $|\Theta(G)| = p^2$, then we must have $\Theta(G) = \langle\alpha\rangle$ and $G \cap C_{p^3} = \langle p^2\rangle$; so

$$G = \left\langle [p^2,\mathrm{id}], [u,\alpha]\right\rangle$$

for some $u \in \mathbb{Z}/p^3\mathbb{Z}$, and we can assume $u = 0,...,p^2-1$. Note, since

$$[u,\alpha][p^2,\mathrm{id}] = [u+(1+p)p^2,\alpha] = [u+p^2,\alpha],$$

we find that G is abelian. Now we have

$$\begin{aligned}[u,\alpha]^a &= \left[\left(1+(1+p)+\cdots+(1+p)^{(a-1)}\right)u, \alpha^a\right] \\ &= \left[au + \frac{1}{2}pa(a-1)u + \frac{1}{6}p^2a(a-1)(a-2)u, \alpha^a\right],\end{aligned}$$

so G has size p^3. The group G is regular if and only if $p \nmid u$; since if $u = pu_1$, then

$$[p^2,\mathrm{id}]^{-u_1}[u,\alpha]^p(0) = 0,$$

and if $p \nmid u$, then $[u,\alpha]^a(0) = 0$ implies that $a = 0 \bmod p$. If $p \nmid u$, the element $[u,\alpha]$

has order p^3, so

$$G = \langle [u, \alpha] \rangle \cong C_{p^3}$$

which is a cyclic regular subgroup of $\mathrm{Hol}(C_{p^3})$. Thus, there are $(p-1)p$ distinct regular subgroups of the form

$$\langle [u, \alpha] \rangle \cong C_{p^3} \text{ for } u = 1, ..., p^2 - 1 \text{ with } u \not\equiv 0 \bmod p.$$

Furthermore, since there exists an automorphism in $\mathrm{Aut}(C_{p^3})$ which takes 1 to any of

$$\left\{ u = 1, ..., p^2 - 1 \mid u \not\equiv 0 \bmod p \right\},$$

all these regular subgroups are isomorphic as braces, and so the class of $\langle [1, \alpha] \rangle$ correspond to a brace.

Therefore, all regular subgroups of $\mathrm{Hol}(C_{p^3})$ are cyclic, and there are

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

of them; furthermore, there are 3 cyclic braces all of which of cyclic type. □

Corollary 4.1.3. *We have* $e(C_{p^3}, C_{p^3}, 1) = 1$,

$$e(C_{p^3}, C_{p^3}, p^{3-m}) = (p-1)p^{2-m} \text{ for } m = 1, 2,$$

and $e(G, C_{p^3}, p^{3-m}) = 0$ *if* $G \neq C_{p^3}$.

Furthermore, we have $\widetilde{e}(C_{p^3}, C_{p^3}, 1) = 1$,

$$\widetilde{e}(C_{p^3}, C_{p^3}, p^{3-m}) = 1 \text{ for } m = 1, 2,$$

and $\widetilde{e}(G, C_{p^3}, p^{3-m}) = 0$ *if* $G \neq C_{p^3}$.

Proof. Follows from Lemma 4.1.2, and the formula

$$e(G, C_{p^3}, p^{3-m}) = \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(C_{p^3})|} e'(G, C_{p^3}, p^{3-m}).$$

□

We provide the general version of the theorem above for C_{p^n}. First we note that by explanations in [Rib89, p. 23], one has that for p be a prime and $n > 1$, and if k and ap^{n-1}, for $0 < a \leq p-1$, are positive integers with $1 < k < ap^{n-1}$, then one has

$$\upsilon_p \left(\binom{ap^{n-1}}{k} \right) = \upsilon_p \left(\frac{ap^{n-1}!}{(ap^{n-1} - k)!k!} \right) = n - 1 - \upsilon_p(k).$$

Lemma 4.1.4. *There are exactly p^{n-1} regular subgroups contained in* Hol(C_{p^n}) *given by the cyclic subgroups*

$$\langle [1, \mathrm{id}] \rangle, \langle [v_1, \alpha] \rangle, ..., \left\langle [v_{n-1}, \alpha^{p^{n-2}}] \right\rangle$$

for $v_m = 1, ..., p^{n-m} - 1$ with $p \nmid v_m$ and $m = 1, ..., n-1$.

Furthermore, there are exactly n cyclic braces of order p^n all of which are of cyclic type given by

$$\langle [1, \mathrm{id}] \rangle, \langle [1, \alpha] \rangle, ..., \left\langle [1, \alpha^{p^{n-2}}] \right\rangle.$$

Proof. If $G \subseteq \mathrm{Hol}(C_{p^n})$ with $|\Theta(G)| = 1$, then we must have $G = \langle [1, \mathrm{id}] \rangle$ which is a regular subgroup of Hol(C_{p^n}). The class $\langle [1, \mathrm{id}] \rangle$ corresponds to a brace.

If $G \subseteq \mathrm{Hol}(C_{p^n})$ with $|\Theta(G)| = p^{n-m}$ for $1 \leq m < n$, then we must have $\Theta(G) = \left\langle \alpha^{p^{m-1}} \right\rangle$ and $G \cap C_{p^n} = \langle p^{n-m} \rangle$, so

$$G = \left\langle [p^{n-m}, \mathrm{id}], [v, \alpha^{p^{m-1}}] \right\rangle$$

for some $v \in \mathbb{Z}/p^n\mathbb{Z}$, and we can assume $v = 0, ..., p^{n-m} - 1$. Now, we have

$$\alpha^{p^{m-1}}(1) = (1+p)^{p^{m-1}} = \left(1 + \binom{p^{m-1}}{1} p + \binom{p^{m-1}}{2} p^2 + \cdots + p^{p^{m-1}}\right)$$

$$= 1 + \sum_{k=1}^{p^{m-1}} \binom{p^{m-1}}{k} p^k.$$

Note, the quantity

$$l \stackrel{\mathrm{def}}{=} \sum_{k=1}^{p^{m-1}} \binom{p^{m-1}}{k} p^{k-m}$$

is an integer, which as already mentioned follows from [Rib89, p. 23], and since $k \geq \upsilon_p(k) + 1$ for all k which can be shown by induction on k. Consequently, we find

$$\begin{aligned}
[v, \alpha^{p^{m-1}}][p^{n-m}, \mathrm{id}] &= [v + p^{n-m} + \sum_{k=1}^{p^{m-1}} \binom{p^{m-1}}{k} p^{k+n-m}, \alpha^{p^{m-1}}] \\
&= [v + p^{n-m} + p^n l, \alpha^{p^{m-1}}] = [v + p^{n-m}, \alpha^{p^{m-1}}] \\
&= [p^{n-m}, \mathrm{id}][v, \alpha^{p^{m-1}}],
\end{aligned}$$

so G is abelian. Next, we calculate, for a natural number $i \geq 1$

$$[v, \alpha^{p^{m-1}}]^{p^i} = \left[\left(1 + (1+p)^{p^{m-1}} + \cdots + (1+p)^{(p^i-1)p^{m-1}}\right) v, \alpha^{p^{m-1+i}} \right].$$

Note we have

$$\sum_{j=0}^{p^i-1}(1+p)^{jp^{m-1}} = \frac{(1+p)^{p^{m-1+i}}-1}{(1+p)^{p^{m-1}}-1}$$
$$= \frac{p^{m+i}+\binom{p^{m-1+i}}{2}p^2+\cdots+p^{p^{m-1+i}}}{p^m+\binom{p^{m-1}}{2}p^2+\cdots+p^{p^{m-1}}} = \frac{k_i}{k_m}.$$

Now since $p>2$ we have that $\upsilon_p(k_m)=m$ and $\upsilon_p(k_i)=m+i$, and so if we let $l_m=\frac{k_m}{p^m}$ and $l_i=\frac{k_i}{p^m}$, we have $\upsilon_p(l_i)=i$ and $\upsilon_p(l_m)=0$

$$[v,\alpha^{p^{m-1}}]^{p^i} = [l_i l_m^{-1}v, \alpha^{p^{m-1+i}}],$$

so G has size p^n and the element $[v,\alpha^{p^{m-1}}]$ can have order p^n or a lower power of p depending on v.

If $p \mid v$, then without loss of generality we can assume $v=p^r s$ with $0<r<n-m$ and $p \nmid s$, but in such a case G cannot be a regular subgroup of Hol(C_{p^n}) since we find

$$[v,\alpha^{p^{m-1}}]^{p^{n-m-r}}(0) = [l_{n-m-r}l_m^{-1}v, \alpha^{p^{n-r-1}}](0) = l_{n-m-r}l_m^{-1}v \in \left\langle p^{n-m}\right\rangle$$

If $p \nmid v$, then we see that $v\alpha^{p^{m-1}}$ has order p^n from which it can be deduced that

$$G = \left\langle [v,\alpha^{p^{m-1}}]\right\rangle \cong C_{p^n}$$

is a regular cyclic subgroup of Hol(C_{p^n}). There are $(p-1)p^{n-m-1}$ regular subgroups of the form

$$\left\langle [v_m,\alpha^{p^{m-1}}]\right\rangle \cong C_{p^n} \text{ for } v_m = 1,...,p^{n-m}-1 \text{ with } v_m \not\equiv 0 \bmod p,\ m=1,...,n-1.$$

Furthermore, since there exists an automorphism in Aut(C_{p^n}) taking 1 to any element of

$$\left\{v_m = 1,...,p^{n-m}-1 \mid v_m \not\equiv 0 \bmod p\right\},$$

each class $\left\langle [1,\alpha^{p^{m-1}}]\right\rangle$ corresponds to a brace.

Therefore, for $p>2$, all regular subgroups of Hol(C_{p^n}) are cyclic, and there are

$$1+\sum_{m=1}^{n-1}(p-1)p^{n-m-1} = p^{n-1}$$

of them. Furthermore, there are n cyclic braces of order p^n all of which are of cyclic type. □

Corollary 4.1.5. *We have* $e(C_{p^n}, C_{p^n}, 1) = 1$,

$$e(C_{p^n}, C_{p^n}, p^{n-m}) = (p-1)p^{n-m-1} \text{ for } m = 1, ..., n-1,$$

and $e(G, C_{p^n}, p^{n-m}) = 0$ *for* $G \ncong C_{p^n}$.

Furthermore, we have $\widetilde{e}(C_{p^n}, C_{p^n}, 1) = 1$,

$$\widetilde{e}(C_{p^n}, C_{p^n}, p^{n-m}) = 1 \text{ for } m = 1, ..., n-1,$$

and $\widetilde{e}(G, C_{p^n}, p^{n-m}) = 0$ *for* $G \ncong C_{p^n}$.

Proof. Follows from Lemma 4.1.4, and the formula

$$e(G, C_{p^n}, p^{n-m}) = \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(C_{p^n})|} e'(G, C_{p^n}, p^{n-m}).$$

□

4.1.1 Automorphism groups of braces of C_{p^n} type

Note, by Lemma 4.1.4, the braces of C_{p^n} type are given by

$$\langle [1, \mathrm{id}] \rangle, \langle [1, \alpha] \rangle, ..., \langle [1, \alpha^{p^{n-2}}] \rangle \cong C_{p^n}.$$

Now, using the explanation of Subsection 2.3.1, the automorphism groups of the above braces are given by

$$\mathrm{Aut}_{\mathcal{B}r}(\langle [1, \mathrm{id}] \rangle) = \mathrm{Aut}_{\mathcal{G}r}(\langle [1, \mathrm{id}] \rangle) \cong C_{p^{n-1}} \times C_{p-1},$$
$$\mathrm{Aut}_{\mathcal{B}r}(\langle [1, \alpha^{p^{n-m-1}}] \rangle) = \langle \alpha^{p^{m-1}} \rangle \cong C_{p^{n-m}} \text{ for } m = 1, ..., n-1.$$

4.2 Regular subgroups in Hol($C_{p^2} \times C_p$)

In this section we classify the regular subgroups contained in Hol($C_{p^2} \times C_p$) and the braces of $C_{p^2} \times C_p$ type. The main result of this section is the following.

Proposition 4.2.1. *We have*

$$e(C_{p^2} \times C_p, C_{p^2} \times C_p) = (2p-1)p^2,$$
$$e(M_2, C_{p^2} \times C_p) = (2p-1)p^2,$$

and $e(G, C_{p^2} \times C_p) = 0$ *for* $G \ncong C_{p^2} \times C_p$ *or* M_2.

Furthermore, we have

$$\widetilde{e}(C_{p^2} \times C_p, C_{p^2} \times C_p) = 9,$$
$$\widetilde{e}(M_2, C_{p^2} \times C_p) = 4p + 1,$$

and $\widetilde{e}(G, C_{p^2} \times C_p) = 0$ *for* $G \ncong C_{p^2} \times C_p$ *or* M_2.

The proof of the proposition above follows from the calculations in the rest of this section, particularly by adding relevant quantities in Corollaries 4.2.3 and 4.2.5. First we recall from Section 3.2,

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

To make the notations easier, we shall identify $C_{p^2} \times C_p$ with $\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ via

$$\sigma \longmapsto e_1 \stackrel{\text{def}}{=} \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ \tau \longmapsto e_2 \stackrel{\text{def}}{=} \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

By Lemma 3.2.1, we have $|\mathrm{Aut}(C_{p^2} \times C_p)| = (p-1)^2 p^3$. Note, with notation introduced in Lemma 3.2.1, if $\alpha, \beta \in \mathrm{Aut}(C_{p^2} \times C_p)$, say

$$\alpha = \begin{pmatrix} a_1 & a_2 p \\ a_3 & a_4 \end{pmatrix},\ \beta = \begin{pmatrix} b_1 & b_2 p \\ b_3 & b_4 \end{pmatrix},$$

then the composition $\alpha\beta$ corresponds to the matrix

$$\alpha\beta = \begin{pmatrix} a_1 b_1 + a_2 b_3 p & (a_1 b_2 + a_2 b_4)p \\ a_3 b_1 + a_4 b_3 & a_4 b_4 \end{pmatrix}. \tag{4.2}$$

Now, we let

$$\Theta : \mathrm{Hol}(C_{p^2} \times C_p) \longrightarrow \mathrm{Aut}(C_{p^2} \times C_p)$$

be the natural projection. Further we let

$$\Psi : \mathrm{Aut}(C_{p^2} \times C_p) \longrightarrow \mathrm{L}(\mathbb{F}_p)$$
$$\begin{pmatrix} a_1 & a_2 p \\ a_3 & a_4 \end{pmatrix} \longmapsto \begin{pmatrix} a_1 \bmod p & 0 \\ a_3 & a_4 \end{pmatrix}$$

be the reduction of entries modulo p, where $\mathrm{L}(\mathbb{F}_p)$ was defined just before Lemma 3.2.1 is the lower triangular invertible 2×2 matrices over the finite filed $\mathbb{F}_p$. Then the image of a subgroup

$$G \subseteq \mathrm{Hol}(C_{p^2} \times C_p)$$

of order p^3 in $\mathrm{L}(\mathbb{F}_p)$ under the composition of projections

$$\Psi\Theta : \mathrm{Hol}(C_{p^2} \times C_p) \longrightarrow \mathrm{L}(\mathbb{F}_p)$$

must lie in the unique Sylow p-subgroup of $\mathrm{L}(\mathbb{F}_p)$, which is the subgroup generated by the image of the automorphism $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ under Ψ. Let

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

Note, α_1, α_3 generate $\operatorname{Ker}\Psi$ and the elements $\alpha_1, \alpha_2, \alpha_3 \in \mathrm{Aut}(C_{p^2} \times C_p)$ have order p. They satisfy the relations

$$\alpha_2\alpha_1 = \alpha_1\alpha_2,\ \alpha_3\alpha_1 = \alpha_1\alpha_3,\ \alpha_3\alpha_2 = \alpha_1\alpha_2\alpha_3, \tag{4.3}$$

which implies that

$$\langle \alpha_1, \alpha_2, \alpha_3 \rangle \cong M_1.$$

Therefore, we always have

$$\Theta(G) \subseteq \mathrm{A}(C_{p^2} \times C_p) \stackrel{\text{def}}{=} \langle \alpha_1, \alpha_2, \alpha_3 \rangle,$$

and so any subgroup of $\mathrm{Hol}(C_{p^2} \times C_p)$ of order p^3 lies in

$$(C_{p^2} \times C_p) \rtimes \mathrm{A}(C_{p^2} \times C_p).$$

We have

$$\begin{aligned} e(C_{p^2} \times C_p, C_{p^2} \times C_p, 1) = \widetilde{e}(C_{p^2} \times C_p, C_{p^2} \times C_p, 1) = 1 \text{ and} \\ e(G, C_{p^2} \times C_p, 1) = \widetilde{e}(G, C_{p^2} \times C_p, 1) = 0 \text{ if } G \neq C_{p^2} \times C_p. \end{aligned}$$

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

But before we begin, it will be useful for our calculations to derive the explicit formula for a term of the form $(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r$ for natural numbers r, a_i and an element $v = v_1e_1 + v_2e_2 \in \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. First we note that we have

$$\begin{aligned} \alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3} \cdot v &= \begin{pmatrix} a_1p+1 & a_3p \\ a_2 & 1 \end{pmatrix} \cdot v \\ &= v_1\left(a_1pe_1 + e_1 + a_2e_2\right) + v_2\left(a_3pe_1 + e_2\right) \\ &= v + (a_1v_1 + a_3v_2)pe_1 + a_2v_1e_2. \end{aligned} \tag{4.4}$$

Now,

$$(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r = \left(v + \alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3} \cdot v + \cdots + (\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^{r-1} \cdot v\right)(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r$$

where, using (4.3) and (4.4), we find

$$\begin{aligned}(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^j \cdot v &= \alpha_1^{a_1 j + \frac{1}{2}a_2a_3j(j-1)}\alpha_2^{a_2 j}\alpha_3^{a_3 j} \cdot v \\ &= v + \left(a_1v_1j + \frac{1}{2}a_2a_3v_1j(j-1) + a_3v_2j\right)pe_1 + a_2v_1je_2,\end{aligned}$$

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

Therefore, from above we have

$$\begin{aligned}(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r &= \left(\sum_{j=0}^{r-1}(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^j \cdot v\right)(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r \\ &= (rv + l_1pe_1 + l_2a_2v_1e_2)\,(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r, \end{aligned} \tag{4.5}$$

where

$$\begin{aligned}l_1 = l_1(r) &\stackrel{\text{def}}{=} \sum_{j=1}^{r-1}\left(a_1v_1j + \frac{1}{2}a_2a_3v_1j(j-1) + a_3v_2j\right) \text{ and} \\ l_2 = l_2(r) &\stackrel{\text{def}}{=} \sum_{j=1}^{r-1} j.\end{aligned}$$

Note, l_1 and l_2 are divisible by r for $r > 3$ a prime number, so

$$(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^p = pv = v_1pe_1 \tag{4.6}$$

since $p > 3$, i.e., the element $v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}$ can have order p or p^2 depending on v_1. Furthermore, note for future use that in (4.5), when $a_2 = 0$, for any integer r we have

$$(v\alpha_1^{a_1}\alpha_3^{a_3})^r \in rv\alpha_1^{ra_1}\alpha_3^{ra_3}\langle pe_1\rangle, \tag{4.7}$$

where $\langle pe_1\rangle$ is a normal subgroup of Hol($C_{p^2} \times C_p$) since it is a characteristic subgroup of $C_{p^2} \times C_p$.

It will further be useful, when finding the non-isomorphic braces, to derive the explicit formula for a term of the form $\alpha\,(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})\,\alpha^{-1}$ for an automorphism $\alpha \in \mathrm{Aut}(C_{p^2} \times C_p)$. Note, α can be written as

$$\alpha = \alpha_3^{r_3}\beta \text{ for some } \beta \stackrel{\text{def}}{=} \begin{pmatrix} b_1 & 0 \\ b_3 & b_4 \end{pmatrix} \in \mathrm{Aut}(C_{p^2} \times C_p)$$

and some integer r_3 which matters modulo p. Then we find

$$\alpha^{-1} = \beta^{-1}\alpha_3^{-r_3} = \begin{pmatrix} b_1^{-1} & 0 \\ -b_3 b_1^{-1} b_4^{-1} & b_4^{-1} \end{pmatrix} \alpha_3^{-r_3}.$$

Now, using (4.2), we have

$$\begin{aligned} \beta\alpha_1\beta^{-1} &= \alpha_1, \\ \beta\alpha_2\beta^{-1} &= \alpha_2^{b_1^{-1}b_4}, \\ \beta\alpha_3\beta^{-1} &= \alpha_1^{-b_3 b_4^{-1}} \alpha_3^{b_1 b_4^{-1}}, \end{aligned}$$

so, using (4.3),

$$\begin{aligned} \alpha\alpha_1\alpha^{-1} &= \alpha_1, \\ \alpha\alpha_2\alpha^{-1} &= \alpha_1^{r_3 b_1^{-1} b_4} \alpha_2^{b_1^{-1} b_4}, \\ \alpha\alpha_3\alpha^{-1} &= \alpha_1^{-b_3 b_4^{-1}} \alpha_3^{b_1 b_4^{-1}}. \end{aligned}$$

Therefore, we find

$$\alpha\left(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)\alpha^{-1} = (\alpha \cdot v)\,\alpha_1^{a_1 - a_3 b_3 b_4^{-1} + r_3 a_2 b_1^{-1} b_4} \alpha_2^{a_2 b_1^{-1} b_4} \alpha_3^{a_3 b_1 b_4^{-1}}, \tag{4.8}$$

where

$$\alpha \cdot v = b_1 v_1 e_1 + r_3\left(b_3 v_1 + b_4 v_2\right) p e_1 + \left(b_3 v_1 + b_4 v_2\right) e_2.$$

The above calculations, particularly (4.8), relating to conjugation of automorphisms, are repeatedly used in order to prove when a given set of regular subgroups are conjugate, i.e., as braces they are not isomorphic, in the next two lemmas.

Lemma 4.2.2. *For $|\Theta(G)| = p$ there are exactly*

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

regular subgroups isomorphic to $C_{p^2} \times C_p$ and exactly $2(p-1)p^2$ regular subgroups isomorphic to M_2 contained in Hol($C_{p^2} \times C_p$).

Furthermore, there are three $(C_{p^2} \times C_p)$-braces of $C_{p^2} \times C_p$ type and five M_2-braces of $C_{p^2} \times C_p$ type.

Proof. If $G \subseteq \mathrm{Hol}(C_{p^2} \times C_p)$ with $|\Theta(G)| = p$, then we must have $\Theta(G) \subseteq \langle \alpha_1, \alpha_2, \alpha_3 \rangle$ a subgroup of order p and $G \cap (C_{p^2} \times C_p)$ 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 $G \cap (C_{p^2} \times C_p)$ is one of

$$\langle pe_1, e_2 \rangle, \langle e_1 + de_2 \rangle \text{ for } d = 0, ..., p-1.$$

We shall consider the subgroups of order p^2 in $C_{p^2} \times C_p$ and all ways of pairing them with a subgroup of order p of $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ which results in a regular subgroup according to the procedure described in Subsection 2.1.1. We will give the description of all regular subgroups, with $|\Theta(G)| = p$, in the body of the lemma and count them at the end of the lemma. Thus, there are two main cases to consider.

Case I: We start with the regular subgroups containing the subgroup $\langle pe_1, e_2 \rangle$ of $C_{p^2} \times C_p$. Note, the subgroup $\langle pe_1, e_2 \rangle$ is invariant under the action of $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ as it is the only subgroup of $C_{p^2} \times C_p$ isomorphic to C_p^2, so we must have

$$G = \langle pe_1, e_2, g \rangle \text{ where } g \stackrel{\text{def}}{=} e_1 \alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3}.$$

It follows from (4.6) that $g^p = pe_1$, thus $G = \langle e_2, g \rangle$. Now for $r \neq 0$, using (4.4) and (4.6), we have

$$\begin{aligned} g\,(re_2) = (e_1 \alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3})\,(re_2) &= (ra_3 pe_1 + re_2 + e_1)\,\alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3} \\ &= g^{ra_3 p}\,(re_2)\,g, \end{aligned} \tag{4.9}$$

Thus, G has order p^3. The subgroup G is abelian if and only if $a_3 = 0$, and if $a_3 \neq 0$, choosing r in (4.9) so that $ra_3 \equiv 1 \bmod p$, we have that G is isomorphic to M_2. Furthermore, all these subgroups are regular since they have order p^3 and Orb(0) contains $\langle pe_1, e_2 \rangle \cup \{e_1\}$, that is $p^2 + 1$ elements, which implies that G is transitive.

Therefore, we find regular subgroups isomorphic to $C_{p^2} \times C_p$ for $a_3 = 0$ and isomorphic to M_2 for $a_3 \neq 0$ which are

$$\begin{aligned} &\langle e_2, e_1 \alpha_1^c \rangle, \langle e_2, e_1 \alpha_1^a \alpha_2^c \rangle \cong C_{p^2} \times C_p, \ \langle e_2, e_1 \alpha_1^a \alpha_2^b \alpha_3^c \rangle \cong M_2 \\ &\text{for } a, b = 0, ..., p-1, \ c = 1, ..., p-1. \end{aligned} \tag{4.10}$$

To find the non-isomorphic braces corresponding to the above regular subgroups we work as follows. We let $\alpha \in \mathrm{Aut}(C_{p^2} \times C_p)$ and write

$$\alpha = \alpha_3^{r_3} \beta \text{ for some } \beta \stackrel{\text{def}}{=} \begin{pmatrix} b_1 & 0 \\ b_3 & b_4 \end{pmatrix} \in \mathrm{Aut}(C_{p^2} \times C_p).$$

Now, using (4.8) we have

$$\alpha\,(e_1 \alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3})\,\alpha^{-1} = (\alpha \cdot e_1)\,\alpha_1^{a_1 - a_3 b_3 b_4^{-1} + r_3 a_2 b_1^{-1} b_4} \alpha_2^{a_2 b_1^{-1} b_4} \alpha_3^{a_3 b_1 b_4^{-1}},$$

where

$$\alpha \cdot e_1 = b_1 e_1 + r_3 b_3 p e_1 + b_3 e_2,$$

so

$$\alpha \left(e_1 \alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3}\right)^{b_1^{-1}} \alpha^{-1} \in e_1 \alpha_1^{a_1 b_1^{-1} - a_3 b_1^{-1} b_3 b_4^{-1} + r_3 a_2 b_1^{-2} b_4 + \frac{1}{2} a_2 a_3 b_1^{-1}\left(b_1^{-1}-1\right)} \alpha_2^{a_2 b_1^{-2} b_4} \alpha_3^{a_3 b_4^{-1}} \langle p e_1, e_2 \rangle .$$

Now

$$\alpha \left(e_1 \alpha_1^{c}\right)^{b_1^{-1}} \alpha^{-1} = \left(\alpha \cdot \left(b_1^{-1} e_1\right)\right) \alpha_1^{b_1^{-1} c} \in e_1 \alpha_1^{b_1^{-1} c} \langle p e_1, e_2 \rangle ,$$

so conjugating the subgroup $\langle e_2, e_1\alpha_1 \rangle$ with the automorphism represented by $\left(\begin{smallmatrix} c^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right)$ we get $\langle e_2, e_1\alpha_1^c \rangle$. Next, note we have

$$\alpha \left(e_1 \alpha_1^{a} \alpha_2^{c}\right)^{b_1^{-1}} \alpha^{-1} \in e_1 \alpha_1^{a b_1^{-1} + r_3 c b_1^{-2} b_4} \alpha_2^{c b_1^{-2} b_4} \langle p e_1, e_2 \rangle ,$$

so if we conjugate the subgroup $\langle e_2, e_1\alpha_2 \rangle$ with the automorphism represented by $\alpha_3^{ac^{-1}} \left(\begin{smallmatrix} c^{-1} & 0 \\ 0 & c^{-1} \end{smallmatrix}\right)$, then we get $\langle e_2, e_1\alpha_1^a\alpha_2^c \rangle$, and since α_1 can never be conjugated to α_2 here we only have two abelian type braces $\langle e_2, e_1\alpha_1 \rangle$ and $\langle e_2, e_1\alpha_2 \rangle$.

Next, working similar to above, we have

$$\alpha \left(e_1 \alpha_1^{a} \alpha_3^{c}\right)^{b_1^{-1}} \alpha^{-1} \in e_1 \alpha_1^{a b_1^{-1} - c b_1^{-1} b_3 b_4^{-1}} \alpha_3^{c b_4^{-1}} \langle p e_1, e_2 \rangle ,$$

so if we conjugate the subgroup $\langle e_2, e_1\alpha_3 \rangle$ with the automorphism represented by $\left(\begin{smallmatrix} c^{-1} & 0 \\ -a & c^{-1} \end{smallmatrix}\right)$, then we get $\langle e_2, e_1\alpha_1^a\alpha_3^c \rangle$, also for future use we see that we cannot conjugate $\langle e_2, e_1\alpha_1^a\alpha_3^c \rangle$ to a subgroup involving α_2. Finally, we have

$$\alpha \left(e_1 \alpha_1^{a} \alpha_2^{b} \alpha_3^{c}\right)^{b_1^{-1}} \alpha^{-1} \in e_1 \alpha_1^{a b_1^{-1} - c b_1^{-1} b_3 b_4^{-1} + r_3 b b_1^{-2} b_4 + \frac{1}{2} b c b_1^{-1}\left(b_1^{-1}-1\right)} \alpha_2^{b b_1^{-2} b_4} \alpha_3^{c b_4^{-1}} \langle p e_1, e_2 \rangle ,$$

Now for $\delta \in \mathbb{F}_p^\times$ which is not a square, as fixed in (4.1), and for $b, c \in \mathbb{F}_p^\times$, we can write $bc = s_1^2 s$ where $s_1 \in \mathbb{F}_p^\times$ and $s = 1, \delta$. Now conjugating the subgroup $\langle e_2, e_1\alpha_2^s\alpha_3 \rangle$ with the automorphism represented by $\alpha_3^{ab^{-1} - \frac{1}{2}c\left(1-s_1^{-1}\right)} \left(\begin{smallmatrix} s_1^{-1} & 0 \\ 0 & c^{-1} \end{smallmatrix}\right)$ we get $\left\langle e_2, e_1\alpha_1^a\alpha_2^b\alpha_3^c \right\rangle$, also note that $\langle e_2, e_1\alpha_2^s\alpha_3 \rangle$ for different values of s cannot be conjugate to each other since if we try to conjugate $\langle e_2, e_1\alpha_2\alpha_3 \rangle$ to $\left\langle e_2, e_1\alpha_2^\delta\alpha_3 \right\rangle$ we have

$$\alpha \left(e_1 \alpha_2 \alpha_3\right)^{b_1^{-1}} \alpha^{-1} \in e_1 \alpha_1^{-b_1^{-1} b_3 b_4^{-1} + r_3 b_1^{-2} b_4 + \frac{1}{2} b_1^{-1}\left(b_1^{-1}-1\right)} \alpha_2^{b_1^{-2} b_4} \alpha_3^{b_4^{-1}} \langle p e_1, e_2 \rangle ,$$

which forces us to set $b_4 = 1$, but this implies that we need $b_1^{-2} = \delta$ which is impossible as δ is not a square.

Therefore, from above regular subgroups, by considering (4.8) and above explanations, we see that the only non-isomorphic braces here are

$$\langle e_2, e_1\alpha_1 \rangle , \langle e_2, e_1\alpha_2 \rangle \cong C_{p^2} \times C_p, \ \langle e_2, e_1\alpha_3 \rangle , \langle e_2, e_1\alpha_2^s\alpha_3 \rangle \cong M_2. \tag{4.11}$$

Case II: Finally, we consider the subgroup $\langle e_1 + de_2 \rangle$ of $C_{p^2} \times C_p$ and investigate the possibility of pairing $\langle e_1 + de_2 \rangle$ with a subgroup of the form $\langle \alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3} \rangle$. Note, using (4.4), we need

$$\alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3} \cdot (e_1 + de_2) = (1 + a_1 p + a_3 dp)\, e_1 + (a_2 + d)\, e_2 \in \langle e_1 + de_2 \rangle$$

which implies that we must set $a_2 = 0$. Thus, we must have

$$G = \langle e_1 + de_2, h \rangle \text{ where } h \stackrel{\text{def}}{=} e_2 \alpha_1^{a_1} \alpha_3^{a_3}.$$

Note, for $r \neq 0$ using (4.7) we have

$$h^r = (e_2 \alpha_1^{a_1} \alpha_3^{a_3})^r \in r e_2 \alpha_1^{r a_1} \alpha_3^{r a_3} \langle e_1 + de_2 \rangle,$$

so we see that $r e_2 \alpha_1^{r a_1} \alpha_3^{r a_3} \in G$. Now, using (4.4),

$$\begin{aligned} (r e_2 \alpha_1^{r a_1} \alpha_3^{r a_3})\, (e_1 + de_2) &= (r e_2 + e_1 + de_2 + r\, (a_1 + a_3 d)\, p e_1)\, \alpha_1^{r a_1} \alpha_3^{r a_3} \\ &= (r\, (a_1 + a_3 d)\, p e_1)\, (e_1 + de_2)\, (r e_2 \alpha_1^{r a_1} \alpha_3^{r a_3}). \end{aligned}$$

Thus, G has order p^3, and by considering $|\mathrm{Orb}(0)|$, one can see that G is regular. Furthermore, G is abelian if and only if $a_1 + a_3 d \equiv 0 \bmod p$.

Therefore, we find regular subgroups isomorphic to $C_{p^2} \times C_p$ for $a_1 + a_3 d \equiv 0 \bmod p$ and isomorphic to M_2 for $a_1 + a_3 d \not\equiv 0 \bmod p$ which are

$$\begin{aligned} &\left\langle e_1 + de_2, e_2 \alpha_1^{-cd} \alpha_3^{c} \right\rangle \cong C_{p^2} \times C_p \text{ for } d = 0, ..., p-1,\ c = 1, ..., p-1, \\ &\langle e_1 + d_2 e_2, e_2 \alpha_1^{a_1} \rangle, \langle e_1 + de_2, e_2 \alpha_1^{a} \alpha_3^{c} \rangle \cong M_2 \\ &\text{for } a, d, d_2 = 0, ..., p-1,\ a_1, c = 1, ..., p-1, \text{ with } a + cd \not\equiv 0 \bmod p. \end{aligned} \tag{4.12}$$

To find the non-isomorphic braces corresponding to the above regular subgroups, we note that the automorphism represented by $\left(\begin{smallmatrix} 1 & 0 \\ d & 1 \end{smallmatrix}\right)$ sends e_1 to $e_1 + de_2$, so we may consider orbits of regular subgroups above for $d = 0$ and conjugation by automorphisms which fix the subgroup generated by e_1, i.e, automorphisms of the form $\alpha = \alpha_3^{r_3} \left(\begin{smallmatrix} b_1 & 0 \\ 0 & b_4 \end{smallmatrix}\right)$. Thus, every regular subgroup in (4.12) is conjugate to one of

$$\begin{aligned} &\langle e_1, e_2 \alpha_3^{c} \rangle \cong C_{p^2} \times C_p \text{ for } c = 1, ..., p-1, \\ &\langle e_1, e_2 \alpha_1^{a} \rangle, \langle e_1, e_2 \alpha_1^{a} \alpha_3^{c} \rangle \cong M_2 \\ &\text{for } a, c = 1, ..., p-1. \end{aligned}$$

Now, using (4.8) we have

$$\alpha\, (e_2 \alpha_1^{a_1} \alpha_3^{a_3})\, \alpha^{-1} = (\alpha \cdot e_2)\, \alpha_1^{a_1} \alpha_3^{a_3 b_1 b_4^{-1}},$$

where

$$\alpha \cdot e_2 = r_3 b_4 p e_1 + b_4 e_2,$$

so

$$\alpha \left(e_2 \alpha_1^{a_1} \alpha_3^{a_3}\right)^{b_4^{-1}} \alpha^{-1} \in e_2 \alpha_1^{a_1 b_4^{-1}} \alpha_3^{a_3 b_1 b_4^{-2}} \langle e_1 \rangle .$$

Thus, if we conjugate the subgroup $\langle e_1, e_2\alpha_3\rangle$ with the automorphism represented by $\left(\begin{smallmatrix} c^{-1} & 0 \\ 0 & c^{-1} \end{smallmatrix}\right)$, then we get the subgroup $\langle e_1, e_2\alpha_3^c\rangle$; if we conjugate the subgroup $\langle e_1, e_2\alpha_1\rangle$ with the automorphism represented by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & a_1^{-1} \end{smallmatrix}\right)$, then we get $\langle e_1, e_2\alpha_1^{a_1}\rangle$; and finally if we conjugate the subgroup $\langle e_1, e_2\alpha_1\alpha_3\rangle$ with the automorphism represented by $\left(\begin{smallmatrix} a^{-2}c & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$ for $a \neq 0$, then we get $\langle e_1, e_2\alpha_1^a\alpha_3^c\rangle$.

Therefore, from above regular subgroups, we see that the only non-isomorphic braces here are

$$\langle e_1, e_2\alpha_3\rangle \cong C_{p^2} \times C_p,\ \langle e_1, e_2\alpha_1\rangle, \langle e_1, e_2\alpha_1\alpha_3\rangle \cong M_2, \tag{4.13}$$

since we cannot conjugate an abelian group to a nonabelian group, and we cannot conjugate α_1 to get $\alpha_1\alpha_3$.

In summary: if $G \subseteq \mathrm{Hol}(C_{p^2} \times C_p)$ is a regular subgroup with $|\Theta(G)| = p$, then G is isomorphic to either $C_{p^2} \times C_p$ or M_2. In particular, combining lists (4.10) and (4.12), if G is isomorphic to $C_{p^2} \times C_p$, then the subgroup G is precisely one of

$$\langle e_2, e_1\alpha_1^c\rangle, \langle e_2, e_1\alpha_1^a\alpha_2^c\rangle, \left\langle e_1 + de_2, e_2\alpha_1^{-cd}\alpha_3^c\right\rangle \cong C_{p^2} \times C_p$$

$$\text{for } a, d = 0, ..., p-1,\ c = 1, ..., p-1,$$

and there are (counting the subgroups whose descriptions is directly in the final two lines above)

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

of these; if G is isomorphic to M_2, then G is precisely one of

$$\left\langle e_2, e_1\alpha_1^a\alpha_2^b\alpha_3^c\right\rangle, \langle e_1 + d_2e_2, e_2\alpha_1^{a_1}\rangle, \langle e_1 + de_2, e_2\alpha_1^{a_2}\alpha_3^{c_1}\rangle \cong M_2$$

$$\text{for } a, a_1, a_2, b, d, d_2 = 0, ..., p-1,\ c_1 = 1, ..., p-1 \text{ with } a_2 + c_1 d \not\equiv 0 \bmod p,$$

and there are

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

of these.

The corresponding braces, combining lists (4.11) and (4.13), are

$$\langle e_2, e_1\alpha_1\rangle, \langle e_2, e_1\alpha_2\rangle, \langle e_1, e_2\alpha_3\rangle \cong C_{p^2} \times C_p,$$

$$\langle e_2, e_1\alpha_3\rangle, \langle e_2, e_1\alpha_2^s\alpha_3\rangle, \langle e_1, e_2\alpha_1\rangle, \langle e_1, e_2\alpha_1\alpha_3\rangle \cong M_2 \text{ for } s = 1, \delta.$$

□

Corollary 4.2.3. *We have*

$$e(C_{p^2} \times C_p, C_{p^2} \times C_p, p) = (2p+1)(p-1),$$
$$e(M_2, C_{p^2} \times C_p, p) = 2p^2,$$

and $e(G, C_{p^2} \times C_p, p) = 0$ *for* $G \ncong C_{p^2} \times C_p$ *or* M_2.

Furthermore, we have

$$\widetilde{e}(C_{p^2} \times C_p, C_{p^2} \times C_p, p) = 3,$$
$$\widetilde{e}(M_2, C_{p^2} \times C_p, p) = 5,$$

and $\widetilde{e}(G, C_{p^2} \times C_p, p) = 0$ *for* $G \ncong C_{p^2} \times C_p$ *or* M_2.

Proof. Follows from Lemma 4.2.2, and the calculation

$$\begin{aligned} e(M_2, C_{p^2} \times C_p, p) &\overset{\text{def}}{=} \frac{|\mathrm{Aut}(M_2)|}{|\mathrm{Aut}(C_{p^2} \times C_p)|} e'(M_2, C_{p^2} \times C_p, p) \\ &= \frac{p^3(p-1)}{p^3(p-1)^2} \times 2(p-1)p^2 = 2p^2. \end{aligned}$$

□

Lemma 4.2.4. *For* $|\Theta(G)| = p^2$ *there are exactly*

$$(2p-1)(p-1)p$$

regular subgroups isomorphic to $C_{p^2} \times C_p$ *and exactly*

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

regular subgroups isomorphic to M_2 *contained in* $\mathrm{Hol}(C_{p^2} \times C_p)$.

Furthermore, there are five $(C_{p^2} \times C_p)$*-braces of* $C_{p^2} \times C_p$ *type and* $4(p-1)$ M_2*-braces of* $C_{p^2} \times C_p$ *type.*

Proof. If $G \subseteq \mathrm{Hol}(C_{p^2} \times C_p)$ with $|\Theta(G)| = p^2$, then we must have $\Theta(G) \subseteq \langle \alpha_1, \alpha_2, \alpha_3\rangle$ a subgroup of order p^2 and $G \cap (C_{p^2} \times C_p)$ 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 $G \cap (C_{p^2} \times C_p)$ is one of

$$\langle pe_1\rangle, \langle bpe_1 + e_2\rangle \text{ for } b = 0, ..., p-1.$$

We shall consider all subgroups of order p in $C_{p^2} \times C_p$ and all ways of pairing them with a subgroup of order p^2 of $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ which results is a regular subgroup.

Now there are three cases to consider. We start with the subgroup $\langle pe_1 \rangle$ of $C_{p^2} \times C_p$ on which $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ acts trivially. Thus, we consider subgroups of the form

$$G = \langle pe_1, u\alpha_1, v\alpha_3 \rangle, \langle pe_1, x\alpha_1, y\alpha_2\alpha_3^a \rangle \text{ for } a = 0, ..., p-1$$

for some elements $u, v, x, y \in C_{p^2} \times C_p$ with $u_i, v_i, x_i, y_i = 0, ..., p-1$, where we need $v_1 \neq 0$ or $u_1 \neq 0$, similarly, $x_1 \neq 0$ or $y_1 \neq 0$. This reduces us, using (4.6), to consider the subgroups

$$G = \langle u\alpha_1, v\alpha_3 \rangle, \langle x\alpha_1, y\alpha_2\alpha_3^a \rangle.$$

Case I: Let us consider subgroups of the form

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

Note, for $r \neq 0$, by (4.7) we have $(u\alpha_1)^r \in ru\alpha_1^r \langle pe_1 \rangle$, so $ru\alpha_1^r \in G$. Now we have

$$\begin{aligned} (ru\alpha_1^r)(v\alpha_3) &= (rv_1pe_1)(ru+v)\alpha_1^r\alpha_3 \text{ and} \\ (v\alpha_3)(ru\alpha_1^r) &= (ru_2pe_1)(ru+v)\alpha_1^r\alpha_3. \end{aligned} \tag{4.14}$$

so G has order p^3, and is abelian if and only if $u_2 = v_1$. We can consider two subcases for when $u_1 = 0$ and $u_1 \neq 0$.

Subcase I.1: If $u_1 = 0$, then using (4.6) $u\alpha_1$ has order p, and for G to be regular we need $u_2, v_1 \neq 0$, so using (4.6) the element $v\alpha_3$ has order p^2, and using (4.14) the generators commute if and only if $u_2 = v_1$.

Therefore, for $u_2 = v_1$ we find regular subgroups isomorphic to $C_{p^2} \times C_p$

$$\begin{aligned} &\langle v_1e_2\alpha_1, v\alpha_3 \rangle \cong C_{p^2} \times C_p \\ &\text{for } v_2 = 0, ..., p-1,\ v_1 = 1, ..., p-1, \end{aligned} \tag{4.15}$$

and if $u_2 \neq v_1$, letting $r = (v_1 - u_2)^{-1} v_1$ in (4.14), we find regular subgroups isomorphic to M_2

$$\begin{aligned} &\langle u_2e_2\alpha_1, v\alpha_3 \rangle \cong M_2 \\ &\text{for } v_2 = 0, ..., p-1,\ u_2, v_1 = 1, ..., p-1 \text{ with } u_2 - v_1 \not\equiv 0 \bmod p. \end{aligned} \tag{4.16}$$

To find the non-isomorphic braces corresponding to the above regular subgroups, we note that for an arbitrary automorphism $\alpha = \alpha_3^{r_3}\beta \stackrel{\text{def}}{=} \alpha_3^{r_3}\left(\begin{smallmatrix} b_1 & 0 \\ b_3 & b_4 \end{smallmatrix}\right) \in \text{Aut}(C_{p^2} \times C_p)$,

using (4.8), we have

$$\alpha\left(u_2e_2\alpha_1\right)\alpha^{-1} \in b_4u_2e_2\alpha_1\left\langle pe_1\right\rangle,$$
$$\alpha\left(u_2e_2\alpha_1\right)^{b_1^{-1}b_3}\left(v\alpha_3\right)^{b_1^{-1}b_4}\alpha^{-1} \in \left(b_4v_1e_1 + b_1^{-1}b_4\left(b_3\left(u_2+v_1\right)+b_4v_2\right)e_2\right)\alpha_3\left\langle pe_1\right\rangle,$$

so without loss of generality we can set $r_3 = 0$ and only use β. Furthermore, we observe that $u_2e_2\alpha_1$ cannot be conjugated to $\widetilde{u}\alpha_1$ for $\widetilde{u}_1 \neq 0$ and neither of α_1 of α_3 can be conjugated to an element involving α_2. Now conjugating the subgroup $\langle u_2e_2\alpha_1, v\alpha_3\rangle$, when $u_2 + v_1 \not\equiv 0 \bmod p$, by the automorphism represented by $\begin{pmatrix} u_2^{-1} & 0 \\ -u_2^{-1}v_2(u_2+v_1)^{-1} & u_2^{-1}\end{pmatrix}$ we get $\left\langle e_2\alpha_1, u_2^{-1}v_1e_1\alpha_3\right\rangle$, and, for $u_2 + v_1 \equiv 0 \bmod p$, conjugating the subgroup $\langle -v_1e_1\alpha_1, v\alpha_3\rangle$ with the automorphism represented by $\begin{pmatrix} b_1^{-1}v_1^{-2} & 0 \\ 0 & -v_1^{-1}\end{pmatrix}$ we get $\langle e_2\alpha_1, \left(b_1v_2e_2 - e_1\right)\alpha_3\rangle$, where we can set $b_1 = 1$ if $v_2 = 0$ and $b_1 = v_2^{-1}$ if $v_2 \neq 0$. Note, the first case implies that conjugating the subgroup $\langle v_1e_2\alpha_1, v\alpha_3\rangle$ with the automorphism represented by $\begin{pmatrix} v_1^{-1} & 0 \\ -\frac{1}{2}v_1^{-2}v_2 & v_1^{-1}\end{pmatrix}$ we get $\langle e_2\alpha_1, e_1\alpha_3\rangle$. Now, one can check that the subgroups $\left\langle e_2\alpha_1, u_2^{-1}v_1e_1\alpha_3\right\rangle$, $\langle e_2\alpha_1, -e_1\alpha_3\rangle$, $\langle e_2\alpha_1, \left(e_2 - e_1\right)\alpha_3\rangle$ for $u_2^{-1}v_1 \neq -1$ cannot be conjugate to each other.

Therefore, from above regular subgroups we find the non-isomorphic braces

$$\begin{aligned}&\langle e_2\alpha_1, e_1\alpha_3\rangle \cong C_{p^2} \times C_p,\ \langle e_2\alpha_1, t_1e_1\alpha_3\rangle, \langle e_2\alpha_1, \left(t_2e_2 - e_1\right)\alpha_3\rangle \cong M_2\\ &\text{for } t_1 = 2, ..., p-2,\ t_2 = 0, 1.\end{aligned} \tag{4.17}$$

Subcase I.2: If $u_1 \neq 0$, then since

$$\begin{aligned}\left(u\alpha_1\right)^{-u_1^{-1}v_1}\left(v\alpha_3\right) &= \left(-u_1^{-1}v_1u + \frac{1}{2}u_1^{-1}v_1\left(u_1^{-1}v_1+1\right)u_1pe_1 + v - u_1^{-1}v_1^2pe_1\right)\alpha_1^{-v_1u_1^{-1}}\alpha_3\\ &\in \left(\left(-u_1^{-1}v_1u_2 + v_2\right)e_2\right)\alpha_1^{-v_1u_1^{-1}}\alpha_3\left\langle pe_1\right\rangle,\end{aligned}$$

for G to be regular we further need $u_1v_2 - u_2v_1 \not\equiv 0 \bmod p$, so

$$G = \langle u\alpha_1, v\alpha_3\rangle = \langle u\alpha_1, q_2e_2\alpha_1^q\alpha_3\rangle,$$

where $q_2 \overset{\text{def}}{=} \left(u_1v_2 - u_2v_1\right)u_1^{-1}$ and $q \overset{\text{def}}{=} -v_1u_1^{-1}$. Note, using (4.7) we have

$$rq_2e_2\alpha_1^{rq}\alpha_3^r \in G.$$

Now, we have

$$\begin{aligned}\left(u\alpha_1\right)\left(rq_2e_2\alpha_1^{rq}\alpha_3^r\right) &= \left(u + rq_2e_2\right)\alpha_1^{1+rq}\alpha_3^r \text{ and}\\ \left(rq_2e_2\alpha_1^{rq}\alpha_3^r\right)\left(u\alpha_1\right) &= \left(ru_2pe_1 + rqu_1pe_1\right)\left(u + rq_2e_2\right)\alpha_1^{1+rq}\alpha_3^r,\end{aligned} \tag{4.18}$$

and as before G is abelian if and only if $u_2 = v_1$.

Therefore, for $u_2 = v_1$ we find regular subgroups isomorphic to $C_{p^2} \times C_p$

$$\begin{aligned} &\langle u\alpha_1, (u_2 e_1 + v_2 e_2)\,\alpha_3 \rangle \cong C_{p^2} \times C_p \\ &\text{for } A = \begin{pmatrix} u_1 & u_2 \\ u_2 & v_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \text{ with } u_1 \neq 0. \end{aligned} \tag{4.19}$$

To determine the number of these subgroups we need to the number of triples (u_1, u_2, v_2) with $u_2, v_2 = 0, ..., p-1$ and $u_1 = 1, ..., p-1$ such that $u_1 v_2 - u_2^2 \not\equiv 0 \bmod p$. In total there are $(p-1)p^2$ triples with no constraints, and there are $(p-1)p$ triples with $v_2 = u_2^2 u_1^{-1}$; thus there are

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

of these subgroups. For the case when $u_2 \neq v_1$, letting $r = u_1 (u_2 - v_1)^{-1}$, in (4.18), we find regular subgroups isomorphic to M_2

$$\begin{aligned} &\langle u\alpha_1, v\alpha_3 \rangle \cong M_2 \\ &\text{for } A = \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \text{ with } u_1,\ u_2 - v_1 \not\equiv 0 \bmod p. \end{aligned} \tag{4.20}$$

There are

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

invertible matrices over $\mathbb{F}_p$ of the form $\left(\begin{smallmatrix} u_1 & v_1 \\ u_2 & v_2 \end{smallmatrix}\right)$ with $u_2 \neq v_1$. The explanation for this is as follows. Let us find the number of invertible matrices of the form $\left(\begin{smallmatrix} u_1 & u_2 \\ u_2 & v_2 \end{smallmatrix}\right)$. If $u_2 = 0$, then we have $(p-1)^2$ choices for u_1 and v_2. If $u_2 \neq 0$ and $u_1 = 0$, then there are $(p-1)p$ choices for u_2 and v_2. If $u_2 \neq 0$ and $u_1 \neq 0$, then there are $(p-1)^2 p - (p-1)^2$ choices for u_1, u_2, and v_2. Thus we have exactly

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

of invertible matrices of the form $\left(\begin{smallmatrix} u_1 & u_2 \\ u_2 & v_2 \end{smallmatrix}\right)$, and so there are

$$(p^2-1)(p^2-p) - (p-1)p^2 = (p^2 - p - 1)(p-1)p \tag{4.21}$$

invertible matrices of the form $\left(\begin{smallmatrix} u_1 & v_1 \\ u_2 & v_2 \end{smallmatrix}\right)$ with $u_2 \neq v_1$. Now, subtracting from 4.21 the total number of invertible matrices of the form $\left(\begin{smallmatrix} 0 & v_1 \\ u_2 & v_2 \end{smallmatrix}\right)$ with $u_2 \neq v_1$, there are

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

invertible matrices over $\mathbb{F}_p$ of the form $\left(\begin{smallmatrix} u_1 & v_1 \\ u_2 & v_2 \end{smallmatrix}\right)$ with $u_2 \neq v_1$ and $u_1 \neq 0$.

To find the non-isomorphic braces corresponding to the above regular subgroups, we note that, without loss of generality, we can work with an automorphism of the

form $\beta \stackrel{\text{def}}{=} \left(\begin{smallmatrix} b_1 & 0 \\ b_3 & b_4 \end{smallmatrix}\right) \in \mathrm{Aut}(C_{p^2} \times C_p)$. Now using (4.8) we have

$$\begin{aligned} \beta\left(u\alpha_1\right)\beta^{-1} &= \left(b_1u_1e_1 + \left(b_3u_1 + b_4u_2\right)e_2\right)\alpha_1, \\ \beta\left(u\alpha_1\right)^{b_1^{-1}b_3}\left(v\alpha_3\right)^{b_1^{-1}b_4}\beta^{-1} &= \left(b_1^{-1}b_3\beta\cdot u + b_1^{-1}b_4\beta\cdot v + \kappa p e_1\right)\alpha_3, \end{aligned}$$

for some κ. We let $B_0 \stackrel{\text{def}}{=} \left(\begin{smallmatrix} u_1 & v_1 \\ u_2 & v_2 \end{smallmatrix}\right)$ and write $\det(B_0) = s_1^2 s$ where $s = 1, \delta$ and $s_1 \in \mathbb{F}_p^\times$ for δ which is not a square modulo p as we fixed in (4.1). Then setting $b_3 = -b_4u_1^{-1}u_2$ and $b_1 = u_1^{-1}$ we have

$$\begin{aligned} \beta\left(u\alpha_1\right)\beta^{-1} &= e_1\alpha_1, \\ \beta\left(u\alpha_1\right)^{b_1^{-1}b_3}\left(v\alpha_3\right)^{b_1^{-1}b_4}\beta^{-1} &= \left(-b_4u_2e_1 + \left(u_1v_2 - u_2v_1\right)b_4^2e_2 + b_4v_1e_1 + \kappa p e_1\right)\alpha_3, \end{aligned}$$

so conjugating $\langle u\alpha_1, v\alpha_3\rangle$ by $\left(\begin{smallmatrix} u_1^{-1} & 0 \\ \mp u_1^{-1}s_1^{-1}u_2 & \pm s_1^{-1} \end{smallmatrix}\right)$ gives $\left\langle e_1\alpha_1, \left(\pm s_1^{-1}\left(v_1 - u_2\right)e_1 + se_2\right)\alpha_3\right\rangle$, and none of these subgroups are further conjugate to each other.

Therefore, we find non-isomorphic braces

$$\begin{aligned} &\langle e_1\alpha_1, se_2\alpha_3\rangle \cong C_{p^2} \times C_p,\ \langle e_1\alpha_1, \left(t_3e_1 + se_2\right)\alpha_3\rangle \cong M_2 \\ &\text{for } t_3 = 1, ..., \frac{1}{2}(p-1). \end{aligned} \tag{4.22}$$

Case II: Next we consider subgroups of the form

$$G = \left\langle x\alpha_1, y\alpha_2\alpha_3^a\right\rangle.$$

Note, as before for $r \neq 0$ using (4.7) we have $rx\alpha_1^r \in G$. Now we find

$$\begin{aligned} \left(rx\alpha_1^r\right)\left(y\alpha_2\alpha_3^a\right) &= \left(ry_1pe_1\right)\left(rx + y\right)\alpha_1^r\alpha_2\alpha_3^a, \text{ and} \\ \left(y\alpha_2\alpha_3^a\right)\left(rx\alpha_1^r\right) &= \left(rax_2pe_1 + rx_1e_2\right)\left(rx + y\right)\alpha_1^r\alpha_2\alpha_3^a, \end{aligned} \tag{4.23}$$

so for G to have order p^3 we need

$$\left(y\alpha_2\alpha_3^a\right)\left(rx\alpha_1^r\right)\left(y\alpha_2\alpha_3^a\right)^{-1}\left(rx\alpha_1^r\right)^{-1} = rax_2pe_1 - ry_1pe_1 + rx_1e_2 \in \left\langle pe_2\right\rangle,$$

which implies that we need to set $x_1 = 0$. Then for G to be regular we need $x_2, y_1 \neq 0$, so using (4.6) the element $y\alpha_2\alpha_3^a$ has order p^2, and using 4.23 the group G is abelian if and only if $ax_2 \equiv y_1 \bmod p$.

Therefore, for $ax_2 \equiv y_1 \bmod p$ we find regular subgroups isomorphic to $C_{p^2} \times C_p$

$$\begin{aligned} &\left\langle x_2e_2\alpha_1, \left(ax_2e_1 + y_2e_2\right)\alpha_2\alpha_3^a\right\rangle \cong C_{p^2} \times C_p \\ &\text{for } y_2 = 0, ..., p-1,\ a, x_2 = 1, ..., p-1. \end{aligned} \tag{4.24}$$

If $ax_2 \not\equiv y_1 \bmod p$, then setting $r = y_1\left(y_1 - ax_2\right)^{-1}$ in (4.23), we find regular

subgroups isomorphic to M_2

$$\begin{aligned} &\langle x_2 e_2 \alpha_1, y\alpha_2 \alpha_3^a \rangle \cong M_2 \\ &\text{for } a, y_2 = 0, ..., p-1,\ y_1, x_2 = 1, ..., p-1 \text{ with } \ ax_2 - y_1 \not\equiv 0 \bmod p, \end{aligned} \tag{4.25}$$

and we note that there are

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

of these.

To find the non-isomorphic braces corresponding to the above regular subgroups we note that for an arbitrary automorphism of the form $\beta \stackrel{\text{def}}{=} \left(\begin{smallmatrix} b_1 & 0 \\ b_3 & b_4 \end{smallmatrix}\right) \in \text{Aut}(C_{p^2} \times C_p)$ using (4.8) we have

$$\begin{aligned} &\left(\alpha_3^{r_3}\beta\right)\left(x_2 e_2 \alpha_1\right)\left(\alpha_3^{r_3}\beta\right)^{-1} = \left(b_4 x_2 e_2 + b_4 r_3 p e_1\right)\alpha_1 \text{ and} \\ &\left(\alpha_3^{r_3}\beta\right)\left(x_2 e_2 \alpha_1\right)^{ab_1 b_3 b_4^{-2} - r_3 - \frac{1}{2}ab_1 b_4^{-1}\left(b_1 b_4^{-1}-1\right)}\left(y\alpha_2\alpha_3^a\right)^{b_1 b_4^{-1}}\left(\alpha_3^{r_3}\beta\right)^{-1} = \\ &\left(\left(ab_1 b_3 b_4^{-1} - b_4 r_3 - \frac{1}{2}ab_1\left(b_1 b_4^{-1}-1\right)\right)x_2 e_2 + b_1 b_4^{-1}\beta\cdot y + \frac{1}{2}b_1\left(b_1 b_4^{-1}-1\right)y_1 e_2 + \kappa p e_1\right)\alpha_2 \alpha_3^{ab_1^2 b_4^{-2}}, \end{aligned}$$

for some κ and r_3. Let us write $x_2 y_1 = s_1^{-2} s$ where $s = 1, \delta$ and $s_1 \in \mathbb{F}_p^\times$. Then conjugating the subgroup $\langle x_2 e_2 \alpha_1, y\alpha_2\alpha_3^a\rangle$ with the automorphism represented by $\alpha_3^{r_3}\left(\begin{smallmatrix} s_1 & 0 \\ 0 & x_2^{-1} \end{smallmatrix}\right)$, where

$$r_3 = -\frac{1}{2}as_1\left(x_2 s_1 - 1\right) + s_1 y_2 + \frac{1}{2}s_1\left(x_2 s_1 - 1\right)y_1,$$

gives $\left\langle e_2\alpha_1, se_1\alpha_2\alpha_3^{ax_2 y_1^{-1} s}\right\rangle$ and none of these subgroups are further conjugate to each other.

Therefore, we find non-isomorphic braces

$$\begin{aligned} &\langle e_2\alpha_1, se_1\alpha_2\alpha_3^s\rangle \cong C_{p^2}\times C_p,\ \left\langle e_2\alpha_1, se_1\alpha_2\alpha_3^{t_4 s}\right\rangle \cong M_2 \\ &\text{for } t_4 = 0, 2, ..., p-1. \end{aligned} \tag{4.26}$$

Case III: Finally, we consider the subgroup $\langle bpe_1 + e_2\rangle$ of $C_{p^2}\times C_p$ and investigate the possibility of pairing this subgroup with the subgroups $\langle\alpha_1, \alpha_3\rangle, \langle\alpha_1, \alpha_2\alpha_3^a\rangle$. We consider a pairing of the form

$$G = \langle bpe_1 + e_2, u\alpha_1, v\alpha_2^{a_2}\alpha_3^{a_3}\rangle \ \text{ for } \ (a_2, a_3) \neq (0,0),$$

but for G to have order p^3 we need $u_1 \equiv v_1 \equiv 0 \bmod p$, which implies that G cannot be regular since we find $e_1 \notin \text{Orb}(0)$.

In summary: if $G \subseteq \text{Hol}(C_{p^2}\times C_p)$ is a regular subgroup with $|\Theta(G)| = p^2$, then G is isomorphic to either $C_{p^2}\times C_p$ or M_2. In particular, if G is isomorphic to

$C_{p^2} \times C_p$, then, combining (4.15), (4.19), and (4.24), the subgroup G is exactly one of

$$\begin{aligned}
&\langle v_1 e_2 \alpha_1, v\alpha_3 \rangle \text{ for } v_2 = 0, ..., p-1,\ v_1 = 1, ..., p-1,\\
&\langle u\alpha_1, (u_2 e_1 + v_2 e_2)\, \alpha_3 \rangle \text{ for } A = \begin{pmatrix} u_1 & u_2 \\ u_2 & v_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p), \text{ with } u_1 \neq 0,\\
&\langle x_2 e_2 \alpha_1, (a x_2 e_1 + y_2 e_2)\, \alpha_2 \alpha_3^a \rangle \text{ for } y_2 = 0, ..., p-1,\ a, x_2 = 1, ..., p-1,
\end{aligned}$$

and there are exactly

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

of them, and if G is isomorphic to M_2, then, combining (4.16), (4.20), and (4.25), the subgroup G is exactly one of

$$\begin{aligned}
&\langle u_2 e_2 \alpha_1, v\alpha_3 \rangle \text{ for } v_2 = 0, ..., p-1,\ u_2, v_1 = 1, ..., p-1 \text{ with } u_2 - v_1 \not\equiv 0 \bmod p,\\
&\langle u\alpha_1, v\alpha_3 \rangle \text{ for } A = \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \text{ with } u_1,\ u_2 - v_1 \not\equiv 0 \bmod p,\\
&\langle x_2 e_2 \alpha_1, y\alpha_2 \alpha_3^a \rangle \text{ for } a, y_2 = 0, ..., p-1,\ y_1, x_2 = 1, ..., p-1 \text{ with } a x_2 - y_1 \not\equiv 0 \bmod p,
\end{aligned}$$

and there are

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

of them.

The corresponding braces, combining (4.17), (4.22), and (4.26), are

$$\langle e_2\alpha_1, e_1\alpha_3 \rangle, \langle e_1\alpha_1, s e_2 \alpha_3 \rangle, \langle e_2\alpha_1, s e_1 \alpha_2 \alpha_3^s \rangle \cong C_{p^2} \times C_p,$$

$$\langle e_2\alpha_1, t_1 e_1 \alpha_3 \rangle, \langle e_2\alpha_1, (t_2 e_2 - e_1)\, \alpha_3 \rangle, \langle e_1\alpha_1, (t_3 e_1 + s e_2)\, \alpha_3 \rangle, \left\langle e_2\alpha_1, s e_1 \alpha_2 \alpha_3^{t_4 s} \right\rangle \cong M_2$$

$$\text{for } s = 1, \delta,\ t_1 = 2, ..., p-2,\ t_2 = 0, 1,\ t_3 = 1, ..., \frac{1}{2}(p-1),\ t_4 = 0, 2, ..., p-1;$$

therefore there are five $(C_{p^2} \times C_p)$-braces of $C_{p^2} \times C_p$ type and

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

M_2-braces of $C_{p^2} \times C_p$ type. □

Corollary 4.2.5. *We have*

$$\begin{aligned}
e(C_{p^2} \times C_p, C_{p^2} \times C_p, p^2) &= (2p-1)(p-1)p,\\
e(M_2, C_{p^2} \times C_p, p^2) &= (2p-3)p^2,
\end{aligned}$$

and $e(G, C_{p^2} \times C_p, p^2) = 0$ *for* $G \ncong C_{p^2} \times C_p$ *or* M_2.

Furthermore, we have

$$\widetilde{e}(C_{p^2} \times C_p, C_{p^2} \times C_p, p^2) = 5,$$
$$\widetilde{e}(M_2, C_{p^2} \times C_p, p^2) = 4(p-1),$$

and $\widetilde{e}(G, C_{p^2} \times C_p, p^2) = 0$ *for* $G \ncong C_{p^2} \times C_p$ *or* M_2

Proof. Follows from Lemma 4.2.4, and calculation similar to Corollary 4.2.3. □

Lastly, if $G \subseteq \mathrm{Hol}(C_{p^2} \times C_p)$ with $|\Theta(G)| = p^3$, then we must have $\Theta(G) = \langle \alpha_1, \alpha_2, \alpha_3 \rangle$, and so

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

Now, for G to have size p^3 we require $u_1, v_1, w_1 \equiv 0 \bmod p$, but this will imply that G cannot be regular.

4.3 Regular subgroups in $\mathrm{Hol}(C_p^3)$

In this section we classify the regular subgroups contained in $\mathrm{Hol}(C_p^3)$ and the braces of C_p^3 type. The main result of this section is the following.

Proposition 4.3.1. *We have*

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

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

Furthermore, we have

$$\widetilde{e}(C_p^3, C_p^3) = 5,$$
$$\widetilde{e}(M_1, C_p^3) = 2p + 1,$$

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

The proof of the proposition above follows from the calculation in the rest of this section, particularly by adding the relevant numbers in Corollaries 4.3.3 and 4.3.5. Recall, from Section 3.3 we have

$$C_p^3 \overset{\text{def}}{=} \langle \rho, \sigma, \tau \mid \rho^p = \sigma^p = \tau^p = 1,\ \rho\sigma = \sigma\rho,\ \tau\rho = \rho\tau,\ \tau\sigma = \sigma\tau \rangle .$$

To make the notations easier we shall often use the identification $C_p^3 \cong \mathbb{F}_p^3$ by

$$\rho \longmapsto e_1 \stackrel{\text{def}}{=} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \ \sigma \longmapsto e_2 \stackrel{\text{def}}{=} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \ \tau \longmapsto e_3 \stackrel{\text{def}}{=} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Now, the holomorph of C_p^3 can be identified with the affine transformations of $\mathbb{F}_p^3$, thus we work with

$$\mathrm{Hol}(C_p^3) \cong \left\{ [t, A] \mid t \in \mathbb{F}_p^3, \ A \in \mathrm{GL}_3(\mathbb{F}_p) \right\}.$$

Note, we have a surjective group homomorphism

$$\det : \mathrm{GL}_3(\mathbb{F}_p) \longrightarrow \mathbb{F}_p^\times$$

whose kernel is $\operatorname{Ker} \det = \mathrm{SL}_3(\mathbb{F}_p)$, the 3×3 matrices over $\mathbb{F}_p$ whose determinant is one. Now the image of a subgroup of $\mathrm{Hol}(C_p^3)$ of order p^3 in $\mathrm{Aut}(C_p^3)$ under the natural projection

$$\Theta : \mathrm{Hol}(C_p^3) \longrightarrow \mathrm{Aut}(C_p^3)$$

must lie in $\mathrm{SL}_3(\mathbb{F}_p)$; thus any subgroup of $\mathrm{Hol}(C_p^3)$ of order p^3 lies in

$$C_p^3 \rtimes \mathrm{SL}_3(\mathbb{F}_p).$$

If G is a subgroup of order p^3 in $\mathrm{Hol}(C_p^3)$, then we can have $|\Theta(G)| = 1, p, p^2$, or p^3. In particular, $\Theta(G)$ lies in a conjugate, by an element of $\mathrm{SL}_3(\mathbb{F}_p)$, of the Sylow p-subgroup of $\mathrm{SL}_3(\mathbb{F}_p)$

$$B(C_p^3) \stackrel{\text{def}}{=} \langle A_1, A_2, A_3 \rangle \cong M_1$$

[cf. Rob96, p. 39, 1.6.16 (Sylow's Theorem)] where

$$A_1 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ A_2 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \ A_3 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{4.27}$$

Note the matrices A_1, A_2, and A_3 have order p, and they satisfy

$$A_2 A_1 = A_1 A_2, \ A_1 A_3 = A_3 A_1, \ A_3 A_2 = A_1 A_2 A_3.$$

We have

$$e(C_p^3, C_p^3, 1) = \widetilde{e}(C_p^3, C_p^3, 1) = 1,$$

$$e(G, C_p^3, 1) = \widetilde{e}(G, C_p^3, 1) = 0 \text{ if } G \neq C_p^3.$$

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

But before we begin, we note that if $A \in \mathrm{SL}_3(\mathbb{F}_p)$ is an element of order p, then as mentioned above, A is conjugate to an element of the form

$$B = \begin{pmatrix} b_1 & b_2 & b_3 \\ b_4 & b_5 & b_6 \\ 0 & 0 & b_7 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p).$$

Let $B_1 \overset{\text{def}}{=} \left(\begin{smallmatrix} b_1 & b_2 \\ b_4 & b_5 \end{smallmatrix}\right)$ and $y \overset{\text{def}}{=} \left(\begin{smallmatrix} b_3 \\ b_6 \end{smallmatrix}\right)$. Then we can write $B = \left(\begin{smallmatrix} B_1 & y \\ 0 & b_7 \end{smallmatrix}\right)$, and for $r \geq 1$ we have

$$B^r = \begin{pmatrix} B_1^r & \left(B_1^{r-1} + B_1^{r-2} b_7 + \cdots + b_7^{r-1}\right) y \\ 0 & b_7^r \end{pmatrix},$$

so if B has order p i.e., $B^p = I$ and $B \neq I$, then $b_7^p = b_7 = 1$ and $B_1^p = I$. Note, in such case for any $v \in \mathbb{F}_p^3$ we have

$$[v, B]^p = \left[\left(I + B + \cdots + B^{p-1}\right)(v), B^p\right] = \left[\left(I + B + \cdots + B^{p-1}\right)(v), I\right],$$

where

$$\begin{aligned} & I + B + \cdots + B^{p-1} \\ &= \begin{pmatrix} B_1^{p-1} + \cdots + I & \left(\left(B_1^{p-2} + \cdots + I\right) + \left(B_1^{p-3} + \cdots + I\right) + I\right) y \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} \sum_{j=0}^{p-1} B_1^j & \left(B_1^{p-2} + 2B_1^{p-3} + 3B_1^{p-4} + \cdots + (p-2) B_1 + (p-1) I\right) y \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} \sum_{j=0}^{p-1} B_1^j & \left(\sum_{j=1}^{p-1} j B_1^{p-1-j}\right) y \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

Now, since $B_1^p = I$, we have that B_1 is conjugate to a matrix of the form $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ which implies that $\sum_{j=0}^{p-1} B_1^j = 0$ since $p > 2$, also

$$\begin{aligned} \sum_{j=1}^{p-1} j \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{p-1-j} &= \begin{pmatrix} \sum_{j=1}^{p-1} j & \sum_{j=1}^{p-1} j\,(p-j-1)\,b \\ 0 & \sum_{j=1}^{p-1} j \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{2}(p-1)\,p & \frac{1}{2} b\,(p-1)^2\,p - \frac{1}{6} bp\,(p-1)\,(2p-1) \\ 0 & \frac{1}{2}(p-1)\,p \end{pmatrix}, \end{aligned}$$

so

$$\sum_{j=1}^{p-1} j B_1^{p-1-j} = 0 \text{ since } p > 3,$$

which implies that

$$I + B + \cdots + B^{p-1} = 0.$$

Thus it follows that, when $p > 3$, we have

$$[v, B]^p = 1 \text{ for any } B \text{ such that } B^p = I \text{ and } v \in \mathbb{F}_p^3. \tag{4.28}$$

Let us further note that if

$$B = \begin{pmatrix} B_1 & y \\ 0 & b_7 \end{pmatrix}, \ \widetilde{B} = \begin{pmatrix} \widetilde{B}_1 C & \widetilde{y} \\ 0 & \widetilde{b}_7 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p)$$

are 3×3 matrices, where $B_1, \widetilde{B}_1$ are 2×2 matrices and $y, \widetilde{y}$ are column vectors, and $CB_1C^{-1} = B_1$, then we have a conjugation formula:

$$\begin{aligned} \left[1, \widetilde{B}\right][v, B]\left[1, \widetilde{B}^{-1}\right] &= \left[\widetilde{B}(v), \begin{pmatrix} \widetilde{B}_1 C & \widetilde{y} \\ 0 & \widetilde{b}_7 \end{pmatrix}\begin{pmatrix} B_1 & y \\ 0 & b_7 \end{pmatrix}\begin{pmatrix} C^{-1}\widetilde{B}_1^{-1} & -\widetilde{b}_7^{-1}C^{-1}\widetilde{B}_1^{-1}\widetilde{y} \\ 0 & \widetilde{b}_7^{-1} \end{pmatrix}\right] \\ &= \left[\widetilde{B}(v), \begin{pmatrix} \widetilde{B}_1 B_1 \widetilde{B}_1^{-1} & \widetilde{b}_7^{-1} b_7 \widetilde{y} - \widetilde{b}_7^{-1}\widetilde{B}_1 B_1 \widetilde{B}_1^{-1}\widetilde{y} + \widetilde{b}_7^{-1}\widetilde{B}_1 C y \\ 0 & b_7 \end{pmatrix}\right]. \end{aligned} \tag{4.29}$$

This conjugation formula we shall use when finding non-isomorphic braces. From now on to simplify the notation we shall use our alternative notation and simply write tA to denote the element $[t, A] \in \mathrm{Hol}(C_p^3)$, also we identify C_p^3 with its image inside $\mathrm{Hol}(C_p^3)$ i.e., write t for the element $[t, I] \in \mathrm{Hol}(C_p^3)$.

Lemma 4.3.2. *For $|\Theta(G)| = p$ there are exactly*

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

regular subgroups isomorphic to C_p^3 and exactly

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

regular subgroups isomorphic to M_1 contained in $\mathrm{Hol}(C_p^3)$.

Furthermore, there is one C_p^3-brace of C_p^3 type and two M_1-braces of C_p^3 type.

Proof. If $G \subseteq \mathrm{Hol}(C_p^3)$ with $|\Theta(G)| = p$, then we must have $\Theta(G) \subseteq \mathrm{SL}_3(\mathbb{F}_p)$ a subgroup of order p and $G \cap C_p^3$ a subgroup of order p^2, so

$$G = \langle u, v, wA \rangle$$

for some $A \in \mathrm{SL}_3(\mathbb{F}_p)$ which has order p, and $u, v, w \in \mathbb{F}_p^3$ such that

$$U \stackrel{\text{def}}{=} \langle u, v \rangle \cong \mathbb{F}_p^2 \subseteq \mathbb{F}_p^3 \text{ and } A \cdot U \subseteq U.$$

Now there are

$$\frac{(p^3 - 1)(p^3 - p)}{(p^2 - 1)(p^2 - p)} = \frac{p^3 - 1}{p - 1} \tag{4.30}$$

distinct subgroups of order p^2 in $\mathbb{F}_p^3$, and if $U = \langle u_1, u_2 \rangle$ is any arbitrary subgroup of $\mathbb{F}_p^3$ of order p^2 and $x \notin U$, via the automorphism that takes e_1, e_2, e_3 to u_1, u_2, x respectively, we can always assume that $U = \langle e_1, e_2 \rangle$. In what follows we shall find the number of regular subgroups which contain $\langle e_1, e_2 \rangle$ and then multiply this by the number of distinct subgroups of order p^2 in $\mathbb{F}_p^3$. Thus, first we fix the subspace $\langle e_1, e_2 \rangle$ and find all subgroups of order p in $\mathrm{SL}_3(\mathbb{F}_p)$ and all possible ways of pairing these groups with $\langle e_1, e_2 \rangle$ to give a regular subgroup of Hol(C_p^3).

Therefore, let $U \stackrel{\text{def}}{=} \langle e_1, e_2 \rangle \subseteq \mathbb{F}_p^3$. Then the set of matrices of the form

$$B = \begin{pmatrix} b_1 & b_2 & b_3 \\ b_4 & b_5 & b_6 \\ 0 & 0 & b_7 \end{pmatrix} \in \mathrm{SL}_3(\mathbb{F}_p)$$

is the largest subgroup of $\mathrm{SL}_3(\mathbb{F}_p)$ whose elements fix U, and we let

$$\mathrm{SL}_3(\mathbb{F}_p)_U \stackrel{\text{def}}{=} \{B \in \mathrm{SL}_3(\mathbb{F}_p) \mid B \cdot U \subseteq U\}.$$

We need to find distinct subgroups of order p in $\mathrm{SL}_3(\mathbb{F}_p)_U$ so we can pair them with U to have a chance of obtaining a subgroup of order p^3. We shall first find elements of order p in $\mathrm{SL}_3(\mathbb{F}_p)_U$. For any $B \in \mathrm{SL}_3(\mathbb{F}_p)_U$ as given above, we let $B_1 = \left(\begin{smallmatrix} b_1 & b_2 \\ b_4 & b_5 \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} b_3 \\ b_6 \end{smallmatrix}\right)$. Then we can write $B = \left(\begin{smallmatrix} B_1 & y \\ 0 & b_7 \end{smallmatrix}\right)$, so if B has order p i.e., $B^p = I$ and $B \neq I$, then $b_7 = 1$ and $B_1^p = I$. Note in such case we have already calculated that $(vB)^p = 1$ for all $v \in \mathbb{F}_p^3$ by (4.28). Now for $B \in \mathrm{SL}_3(\mathbb{F}_p)_U$ which has order p we shall consider two cases when $B_1 = I$ and $B_1 \neq I$.

Case I: If $B_1 = I$, then we consider subgroups of the form

$$G = \langle e_1, e_2, e_3 B \rangle.$$

Now G is abelian and is isomorphic to C_p^3 since it is generated by elements of order p and

$$e_1 + e_2 = e_2 + e_1, \ (e_3B)e_1 = e_1(e_3B), \ (e_3B)e_2 = e_2(e_3B).$$

The group G is regular since it has size p^3 and acts on $\mathbb{F}_p^3$ transitively, i.e., since $|\mathrm{Orb}(0)| > p^2$. We count the number of these subgroups. There are $p^2 - 1$ choices for y, and since $B_1 = I$, we find

$$p^2 - 1 \tag{4.31}$$

regular subgroups of the form

$$\langle e_1, e_2, e_3 B \rangle \cong C_p^3 \text{ for } B_1 = I.$$

To find the braces corresponding to the above regular subgroups, we note that

for a matrix

$$\widetilde{B} = \begin{pmatrix} \widetilde{B}_1 C & \widetilde{y} \\ 0 & \widetilde{b}_7 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p)$$

using (4.29), we have

$$\widetilde{B}(e_3 B)\widetilde{B}^{-1} \in \widetilde{b}_7 e_3 \begin{pmatrix} B_1 & \widetilde{b}_7^{-1}\widetilde{B}_1 C y \\ 0 & 1 \end{pmatrix} \langle e_1, e_2 \rangle ,$$

so conjugating the subgroup $\left\langle e_1, e_2, e_3 \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right) \right\rangle$ with the matrix $\left(\begin{smallmatrix} x_1 & b_3 & 0 \\ x_2 & b_6 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, where x_1 and x_2 are such that $x_1 b_6 - x_2 b_3 \neq 0$, we get G.

Therefore, we find a C_p^3-brace of C_p^3 type

$$\langle e_1, e_2, e_3 A_2 \rangle \cong C_p^3. \tag{4.32}$$

Case II: If $B_1 \neq I$, then B_1 is conjugate to $B_2 = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ with $b \neq 0$ by some element of $\mathrm{SL}_2(\mathbb{F}_p)$. Note, the set of matrices of the form

$$\begin{pmatrix} a_0 & b_0 \\ 0 & a_0^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_p)$$

is the normaliser of $\langle B_2 \rangle$ in $\mathrm{SL}_2(\mathbb{F}_p)$ and has size $(p-1)p$; thus there are

$$\frac{|\mathrm{SL}_2(\mathbb{F}_p)|}{(p-1)p} = \frac{(p^2-1)p}{(p-1)p} = p+1$$

subgroups of order p in $\mathrm{SL}_2(\mathbb{F}_p)$. Hence, there are

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

elements of order p in $\mathrm{SL}_2(\mathbb{F}_p)$. Since there are p^2 choices for y, we find $(p^2-1)p^2$ matrices $B \in \mathrm{SL}_3(\mathbb{F}_p)$ of order p such that $B \cdot U \subseteq U$ and $B_1 \neq I$; consequently there are $(p+1)p^2$ subgroups of order p generated by such elements. Without loss of generality, we can take a matrix

$$B = \begin{pmatrix} 1 & 1 & b_3 \\ 0 & 1 & b_6 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_3(\mathbb{F}_p)$$

and consider subgroups of the holomorph of the form

$$G = \langle e_1, e_2, v_3 e_3 B \rangle \text{ for } v_3 \neq 0.$$

Note, G is generated by elements of order p, and we have

$$e_1 + e_2 = e_2 + e_1,\ (vB)e_1 = e_1(vB),\ (vB)e_2 = (e_2 + e_1)(vB),$$

where $v = v_3e_3$, also if we replace $B_1 = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ by one of its conjugates, by say $A_0 \in \mathrm{SL}_2(\mathbb{F}_p)$, then we can replace e_1 by $\left(\begin{smallmatrix}A_0 & 0\\ 0 & 1\end{smallmatrix}\right)\cdot e_1$ and e_2 by $\left(\begin{smallmatrix}A_0 & 0\\ 0 & 1\end{smallmatrix}\right)\cdot e_2$ and we still keep the above relations. We further see that G is regular since $v_3 \neq 0$.

Now there are $p-1$ values for v, and as already mentioned since we have $(p+1)p^2$ choices for B, we have

$$(p+1)(p-1)p^2 = (p^2-1)p^2 \tag{4.33}$$

regular subgroups of the form

$$\langle e_1, e_2, v_3e_3B\rangle \cong M_1 \text{ for } v_3 = 1, ..., p-1 \text{ and } B_1 \neq I.$$

To find the braces corresponding to the above regular subgroups we note that for a matrix

$$\widetilde{B} = \begin{pmatrix} \widetilde{B}_1C & \widetilde{y}\\ 0 & \widetilde{b}_7\end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p)$$

and B as above, i.e., which fixes U and has order p with $B_1 \neq I$, and C such that $CB_1C^{-1} = B_1$, using (4.29), we have

$$\widetilde{B}(e_3B)\widetilde{B}^{-1} = \widetilde{b}_7e_3\begin{pmatrix}\widetilde{B}_1B_1\widetilde{B}_1^{-1} & \widetilde{b}_7^{-1}\widetilde{y} - \widetilde{b}_7^{-1}\widetilde{B}_1B_1\widetilde{B}_1^{-1}\widetilde{y} + \widetilde{b}_7^{-1}\widetilde{B}_1Cy\\ 0 & 1\end{pmatrix}.$$

This means that we can conjugate G to a subgroup of the form

$$\left\langle e_1, e_2, e_3\left(\begin{smallmatrix}1 & 1 & b_3\\ 0 & 1 & b_6\\ 0 & 0 & 1\end{smallmatrix}\right)\right\rangle \cong M_1 \text{ for } b_3, b_6 = 0, ..., p-1.$$

Now by choosing suitable C and $\widetilde{y}$ we see that if $b_6 = 0$, then G is conjugate to $\left\langle e_1, e_2, e_3\left(\begin{smallmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{smallmatrix}\right)\right\rangle$, and if $b_6 \neq 0$, then G is conjugate to $\left\langle e_1, e_2, e_3\left(\begin{smallmatrix}1 & 1 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{smallmatrix}\right)\right\rangle$, and these two subgroups cannot be conjugate to each other or to the brace found in 4.32.

Therefore, we find two M_1-braces of C_p^3 type

$$\langle e_1, e_2, e_3A_3\rangle, \langle e_1, e_2, e_3A_2A_3\rangle \cong M_1. \tag{4.34}$$

Conclusion: Therefore, to find the total number of regular subgroups, we multiply the numbers in the (4.31) and (4.33) by the number of distinct subgroups of

order p^2 in $\mathbb{F}_p^3$ given in (4.30); thus there are exactly

$$\frac{p^3-1}{p-1} \times (p^2-1) = (p^3-1)(p+1)$$

regular subgroups isomorphic to C_p^3 and exactly

$$\frac{p^3-1}{p-1} \times (p^2-1)p^2 = (p^3-1)(p+1)p^2,$$

regular subgroups isomorphic to M_1 contained in Hol(C_p^3) with $|\Theta(G)| = p$.

The corresponding braces, combining (4.32) and (4.34), are

$$\langle e_1, e_2, e_3 A_2 \rangle \cong C_p^3, \ \langle e_1, e_2, e_3 A_3 \rangle, \langle e_1, e_2, e_3 A_2 A_3 \rangle \cong M_1.$$

□

Corollary 4.3.3. *We have*

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

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

Furthermore, we have

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

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

Proof. Follows from Lemma 4.3.2, and the computation of

$$\begin{aligned} e(M_1, C_p^3, p) &\overset{\text{def}}{=} \frac{|\mathrm{Aut}(M_1)|}{\left|\mathrm{Aut}(C_p^3)\right|} e'(G, C_p^3, p) \\ &= \frac{p^2(p^2-1)(p^2-p)}{(p^3-1)(p^3-p)(p^3-p^2)} \times (p^3-1)(p+1)p^2 = (p+1)p^2. \end{aligned}$$

□

Lemma 4.3.4. *For* $|\Theta(G)| = p^2$ *there are exactly*

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

regular subgroups isomorphic to C_p^3 *and exactly*

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

regular subgroups isomorphic to M_1 contained in $\mathrm{Hol}(C_p^3)$.

Furthermore, there are three C_p^3-braces of C_p^3 type and $2p-1$ M_1-braces of C_p^3 type.

Proof. If $G \subseteq \mathrm{Hol}(C_p^3)$ with $|\Theta(G)| = p^2$, then we must have $\Theta(G) \subseteq \mathrm{SL}_3(\mathbb{F}_p)$ a subgroup of order p^2 and $G \cap C_p^3$ a subgroup of order p. Thus,

$$G = \left\langle u, vA, w\widetilde{A} \right\rangle,$$

where $\left\langle A, \widetilde{A} \right\rangle \cong C_p^2$ and $u, v, w \in \mathbb{F}_p^3$ with $u \neq 0$ and $\langle u \rangle$ is a subspace of $\mathbb{F}_p^3$ fixed under A and $\widetilde{A}$. We shall find the number of regular subgroups which contain $\langle e_1 \rangle$ and then multiply this by the number of distinct subgroups of order p in $\mathbb{F}_p^3$ which is

$$\frac{p^3-1}{p-1}. \tag{4.35}$$

Therefore, we fix the subspace $\langle e_1 \rangle$, find all subgroups of order p^2 in $\mathrm{SL}_3(\mathbb{F}_p)$ which fix $\langle e_1 \rangle$, and find all possible ways of pairing these subgroups with $\langle e_1 \rangle$ to give a regular subgroup of $\mathrm{Hol}(C_p^3)$.

Let $U \stackrel{\text{def}}{=} \langle e_1 \rangle \subseteq \mathbb{F}_p^3$. Then the set of matrices of the form

$$B = \begin{pmatrix} b_1 & b_2 & b_3 \\ 0 & b_4 & b_5 \\ 0 & b_6 & b_7 \end{pmatrix} \in \mathrm{SL}_3(\mathbb{F}_p)$$

is the largest subgroup of $\mathrm{SL}_3(\mathbb{F}_p)$ whose elements fix U, and we let

$$\mathrm{SL}_3(\mathbb{F}_p)_U \stackrel{\text{def}}{=} \{B \in \mathrm{SL}_3(\mathbb{F}_p) \mid B \cdot U \subseteq U\}.$$

Note,

$$|\mathrm{SL}_3(\mathbb{F}_p)_U| = (p^2-1)(p-1)p^3.$$

Now we need to find subgroups of order p^2 in $\mathrm{SL}_3(\mathbb{F}_p)_U$ so we can pair them with the subspace U to have a chance of obtaining a subgroup of order p^3 in $\mathrm{Hol}(C_p^3)$. Recall we denoted by

$$B(C_p^3) \stackrel{\text{def}}{=} \langle A_1, A_2, A_3 \rangle \cong M_1,$$

with A_1, A_2, and A_3 as given in (4.27). We observe $B(C_p^3) \subseteq \mathrm{SL}_3(\mathbb{F}_p)_U$ is a Sylow p-subgroup. Note, the group $B(C_p^3)$ contains $p+1$ distinct subgroups of order p^2 which are of the form

$$\langle A_1, A_3 \rangle, \left\langle A_1, A_2 A_3^d \right\rangle \text{ for } d = 0, ..., p-1.$$

We shall first count the number of Sylow p-subgroups in $\mathrm{SL}_3(\mathbb{F}_p)_U$ which is the index

of the normaliser of $B(C_p^3)$ in $\mathrm{SL}_3(\mathbb{F}_p)_U$. We find that the set of matrices of the form

$$A = \begin{pmatrix} a_1 & a_2 & a_3 \\ 0 & a_4 & a_5 \\ 0 & 0 & a_1^{-1}a_4^{-1} \end{pmatrix} \in \mathrm{SL}_3(\mathbb{F}_p)_U$$

is the normaliser of $B(C_p^3)$ in $\mathrm{SL}_3(\mathbb{F}_p)_U$ and has size $(p-1)^2p^3$; thus the number of Sylow p-subgroups of $\mathrm{SL}_3(\mathbb{F}_p)_U$ is

$$\frac{(p^2-1)(p-1)p^3}{(p-1)^2p^3} = p+1,$$

and they are all isomorphic to $B(C_p^3)$.

Therefore, there can be at most $(p+1)^2$ distinct subgroups of order p^2 in $\mathrm{SL}_3(\mathbb{F}_p)_U$. Note, for any matrix

$$B = \begin{pmatrix} b_1 & b_2 & b_3 \\ 0 & b_4 & b_5 \\ 0 & b_6 & b_7 \end{pmatrix} \in \mathrm{SL}_3(\mathbb{F}_p)_U,$$

by a matrix calculation (it can be verified by hand, by using a matrix calculator, or using a conjugation formula similar to 4.29) one can see that

$$BA_1B^{-1} \in \langle A_1, A_3\rangle \text{ and } BA_3B^{-1} \in \langle A_1, A_3\rangle,$$

but $BA_2B^{-1} \in B(C_p^3)$ if and only if $b_6 = 0$. When $b_6 = 0$ we find that

$$\begin{aligned} BA_1B^{-1} &= A_1^{b_4^{-1}b_7^{-2}}, \\ BA_2B^{-1} &= A_1^{b_2b_7^{-1}}A_2^{b_4b_7^{-1}}, \\ BA_3B^{-1} &= A_1^{-b_5(b_4b_7)^{-2}}A_3^{b_4^{-2}b_7^{-1}}; \end{aligned}$$

thus we have

$$(BA_2A_3^dB^{-1})^{b_4^{-1}b_7} = \left(A_1^{b_2b_7^{-1}}A_2^{b_4b_7^{-1}}A_1^{-b_5(b_4b_7)^{-2}d}A_3^{b_4^{-2}b_7^{-1}d}\right)^{b_4^{-1}b_7} = A_1^kA_2A_3^{b_4^{-3}d}$$

for some k. This implies that, when $b_6 = 0$, we have

$$\begin{aligned} &B\langle A_1, A_2\rangle B^{-1} \subseteq \langle A_1, A_2\rangle, \\ &B\langle A_1, A_3\rangle B^{-1} \subseteq \langle A_1, A_3\rangle, \\ &B\left\langle A_1, A_2A_3^d\right\rangle B^{-1} \subseteq \left\langle A_1, A_2A_3^{b_4^{-3}d}\right\rangle \text{ for } d = 1, ..., p-1. \end{aligned}$$

Now let S_{p^2} denote the set of subgroups of order p^2 in $\mathrm{SL}_3(\mathbb{F}_p)_U$. Then the action by conjugation by elements of $\mathrm{SL}_3(\mathbb{F}_p)_U$ on $\mathrm{SL}_3(\mathbb{F}_p)_U$ induces an action on S_{p^2} which

makes S_{p^2} into a disjoint union of orbits. There can be at most $p+1$ orbits and each orbit can have at most $p+1$ elements; we are interested in the cardinality $|S_{p^2}|$ which is hence bounded by

$$p+1 \leq |S_{p^2}| \leq (p+1)^2.$$

As seen above, all matrices of $\mathrm{SL}_3(\mathbb{F}_p)_U$ fix $\langle A_1, A_3\rangle \in S_{p^2}$, and so

$$|\mathrm{Orb}(\langle A_1, A_3\rangle)| = 1.$$

The set of matrices which fix $\langle A_1, A_2\rangle$ is exactly the normaliser of $B(C_p^3)$ in $\mathrm{SL}_3(\mathbb{F}_p)_U$ so $|\mathrm{Stab}(\langle A_1, A_2\rangle)| = (p-1)^2p^3$; thus

$$|\mathrm{Orb}(\langle A_1, A_2\rangle)| = \frac{(p^2-1)(p-1)p^3}{(p-1)^2p^3} = p+1.$$

Now, for the orbits $\mathrm{Orb}(\langle A_1, A_2A_3^d\rangle)$, for $d = 1, ..., p-1$, since we have

$$B\left\langle A_1, A_2A_3^d\right\rangle B^{-1} \subseteq \left\langle A_1, A_2A_3^{b_4^{-3}d}\right\rangle \text{ for } d = 1, ..., p-1,$$

one can consider, although it will lead to the same results, two cases when $3 \nmid p-1$ and $3 \mid p-1$. If $3 \nmid p-1$, then raising to the power of 3 and inversion are bijections of $\mathbb{F}_p^\times$ onto itself, and so b_4^{-3} takes all values in $\mathbb{F}_p^\times$ as b_4 runs through all values of $\mathbb{F}_p^\times$; thus there remains only one further orbit, which we can take to be $\mathrm{Orb}(\langle A_1, A_2A_3\rangle)$. Then the subgroup $\langle A_1, A_2A_3\rangle$ has as stabiliser the set of matrices of the form

$$B = \begin{pmatrix} b_1 & b_2 & b_3 \\ 0 & 1 & b_5 \\ 0 & 0 & b_1^{-1} \end{pmatrix} \in \mathrm{SL}_3(\mathbb{F}_p)_U,$$

which has size $(p-1)p^3$; thus we have

$$|\mathrm{Orb}(\langle A_1, A_2A_3\rangle)| = \frac{(p^2-1)(p-1)p^3}{(p-1)p^3} = p^2-1;$$

hence, when $3 \nmid p-1$, we have

$$|S_{p^2}| = 1+p+1+p^2-1 = p^2+p+1.$$

If $3 \mid p-1$, then there are precisely $\frac{1}{3}(p-1)$ cubic residues modulo p. Taking three representative from the classes of non-cubic residues in $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^3$ we find three orbits of the form $\mathrm{Orb}(\langle A_1, A_2A_3^d\rangle)$ for three values of d, they each have as stabiliser

the set of matrices of the form

$$B = \begin{pmatrix} b_1 & b_2 & b_3 \\ 0 & b_4 & b_5 \\ 0 & 0 & b_1^{-1}b_4^{-1} \end{pmatrix} \in \mathrm{SL}_3(\mathbb{F}_p)_U \text{ with } b_4^3 = 1$$

which has size $3(p-1)p^3$, and so

$$\left|\mathrm{Orb}(\left\langle A_1, A_2A_3^d \right\rangle)\right| = \frac{(p^2-1)(p-1)p^3}{3(p-1)p^3} = \frac{1}{3}(p^2-1),$$

and again we find

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

Next, we shall classify all regular subgroups $G \subseteq \mathrm{Hol}(C_p^3)$ with $|\Theta(G)| = p^2$ which contain $\langle e_1 \rangle$. By above arguments we can consider three cases according to the classes

$$\mathrm{Orb}(\langle A_1, A_2 \rangle),\ \mathrm{Orb}(\langle A_1, A_3 \rangle),\ \mathrm{Orb}(\left\langle A_1, A_2A_3^d \right\rangle).$$

Case I: Let us consider subgroups of the form

$$G = \langle e_1, uA_1, vA_2 \rangle$$

for some vectors u, v, and we may assume $u_1 = v_1 = 0$. Note, by (4.28) we have $(uA_1)^p = (vA_2)^p = 1$, also we have

$$\begin{aligned} (uA_1)(vA_2) &= (u + v + v_3e_1)A_1A_2 \text{ and} \\ (vA_2)(uA_1) &= (u + v + u_3e_2)A_1A_2, \end{aligned}$$

and so

$$\begin{aligned} (uA_1)(vA_2)(uA_1)^{-1}(vA_2)^{-1} &= ((u + v + v_3e_1)A_1A_2)\left((u + v + u_3e_2)A_1A_2\right)^{-1} \\ &= ((v_3e_1((u+v)A_1A_2))\left(((u+v)A_1A_2)^{-1}\right)(-u_3e_2) \\ &= v_3e_1 - u_3e_2, \end{aligned}$$

which implies that for G to have order p^3 we need to set $u_3 = 0$. Further, note

$$(vA_2)^{r_2} = (r_2v + k_2e_2)A_2^{r_2},$$

where

$$k_2 \stackrel{\text{def}}{=} \frac{1}{2}r_2(r_2-1)v_3.$$

Then, for any r_1 and r_2, we have

$$(uA_1)^{r_1}(vA_2)^{r_2} = (r_1u + r_2v + r_1r_2v_3e_1 + k_2e_2)\, A_1^{r_1}A_2^{r_2},$$

and so for G to be regular we need $u_2, v_3 \neq 0$. Note, that we have

$$(uA_1)v_3e_1 = v_3e_1(uA_1),\ (vA_2)v_3e_1 = v_3e_1(vA_2);$$

we also calculate

$$\begin{aligned}(uA_1)(vA_2) &= (u + v + v_3e_1)A_1A_2 \text{ and}\\ (vA_2)(uA_1) &= (u + v)A_1A_2,\end{aligned}$$

so, replacing e_1 with v_3e_1 if necessary, we find regular subgroups

$$\langle e_1, u_2e_2A_1, vA_2\rangle \cong M_1 \text{ for } u_2, v_3 = 1, ..., p-1,\ v_2 = 0, ..., p-1.$$

Recall we had $|\mathrm{Orb}(\langle A_1, A_2\rangle)| = p + 1$.

Therefore, we have

$$(p+1)(p-1)^2p \tag{4.36}$$

subgroups of the form $\left\langle e_1, uA, v\widetilde{A}\right\rangle \cong M_1$, where A, and $\widetilde{A}$ are conjugates of A_1 and A_2 in $\mathrm{SL}_3(\mathbb{F}_p)_U$.

To find the braces corresponding to the above regular subgroups we note that for a matrix

$$B = \begin{pmatrix} b_1 & b_2 & b_3\\ 0 & b_4 & b_5\\ 0 & 0 & b_7\end{pmatrix} = \begin{pmatrix} b_1 & y\\ 0 & B_1\end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p)_U,$$

with $y = \begin{pmatrix} b_2 & b_3\end{pmatrix}$ and $B_1 = \left(\begin{smallmatrix} b_4 & b_5\\ 0 & b_7\end{smallmatrix}\right)$, by a matrix calculation we find

$$\begin{aligned}BA_1^{b_1^{-1}b_7}B^{-1} &= A_1,\\ BA_1^{-b_1^{-1}b_2b_4^{-1}b_7}A_2^{b_4^{-1}b_7}B^{-1} &= A_2,\end{aligned}$$

so we find

$$B(u_2e_2A_1)^{b_1^{-1}b_7}B^{-1} = (b_1^{-1}b_4b_7u_2e_2)A_1$$

and

$$\begin{aligned}&B(u_2e_2A_1)^{-b_1^{-1}b_2b_4^{-1}b_7}(vA_2)^{b_4^{-1}b_7}B^{-1} =\\ &\left(\left(\frac{1}{2}(b_4^{-1}b_7 - 1)v_3 - b_1^{-1}b_2u_2\right)b_7e_2 + b_4^{-1}b_7B_1\cdot v + \kappa e_1\right)A_2\end{aligned}$$

for some κ.

Therefore, if we conjugate the subgroup

$$\langle e_1, e_2A_1, e_3A_2\rangle \cong M_1 \tag{4.37}$$

by the matrix

$$B = \begin{pmatrix} v_3^2u_2^{-1} & 0 & 0 \\ 0 & v_3 & v_2 \\ 0 & 0 & v_3 \end{pmatrix}$$

we get the subgroup $\langle e_1, u_2e_2A_1, vA_2\rangle$, and so we find one C_p^3-brace of M_1 type.

Case II: Next, we consider subgroups of the form

$$G = \langle e_1, uA_1, vA_3\rangle$$

for some vectors u, v with $u_1 = v_1 = 0$. Then, using (4.28), we have $(uA_1)^p = (vA_3)^p = 1$. Note that we have

$$(uA_1)e_1 = e_1(uA_1),\ (vA_3)e_1 = e_1(vA_3);$$

we also calculate

$$\begin{aligned}(uA_1)(vA_3) &= (u + v + v_3e_1)\, A_1A_3 \text{ and}\\ (vA_3)(uA_1) &= (u + v + u_2e_1)\, A_1A_3,\end{aligned}$$

so G has order p^3, and is abelian if and only if $u_2 = v_3$. We shall count the cases when G is regular. First we may assume $u, v \neq 0$ otherwise G is not regular. Now note we have

$$\begin{aligned}(uA_1)^{r_1} &= \left(r_1u + \frac{1}{2}u_3r_1\,(r_1 - 1)\, e_1\right) A_1^{r_1} \text{ and}\\ (vA_3)^{r_3} &= \left(r_3v + \frac{1}{2}v_2r_3\,(r_3 - 1)\, e_1\right) A_3^{r_3},\end{aligned}$$

thus, we have

$$(uA_1)^{r_1}(vA_3)^{r_3} = (r_1u + r_3v + k_1e_1)A_1^{r_1}A_3^{r_3},$$

where

$$k_1 \stackrel{\text{def}}{=} \frac{1}{2}v_2r_3(r_3 - 1) + \frac{1}{2}u_3r_1(r_1 - 1) + r_3r_1v_3,$$

we see that G is regular if and only if u and v are linearly independent. Recall, if $u_2 = v_3$, then G is abelian. To count these subgroups we need find the number of invertible matrices of the form $\left(\begin{smallmatrix} u_2 & v_2 \\ u_3 & u_2 \end{smallmatrix}\right)$. We do this as follows. If $u_2 = 0$, then we have $(p - 1)^2$ choices for u_3 and v_2. If $u_2 \neq 0$ and $u_3 = 0$, then there are $(p - 1)p$ choices for u_2 and v_2. Finally, if $u_2 \neq 0$ and $u_3 \neq 0$, then there are $(p-1)^2p-(p-1)^2$

choices for u_2, u_3, and v_2.

Therefore, we have exactly

$$(p-1)^2 + (p-1)p + (p-1)^2 p - (p-1)^2 = (p-1)p^2 \tag{4.38}$$

regular subgroups of the form

$$\langle e_1, uA_1, vA_3 \rangle \cong C_p^3 \text{ with } u_2 = v_3,$$

and since there are

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

invertible matrices of the form $\left(\begin{smallmatrix} u_2 & v_2 \\ u_3 & v_3 \end{smallmatrix}\right)$ with $u_2 \neq v_3$, we have exactly

$$(p^2-p-1)(p-1)p \tag{4.39}$$

regular subgroups of the form

$$\langle e_1, uA_1, vA_3 \rangle \cong M_1 \text{ with } u_2 \neq v_3.$$

To find the non-isomorphic braces corresponding to the above regular subgroups we note that for a matrix

$$B = \begin{pmatrix} b_1 & b_2 & b_3 \\ 0 & b_4 & b_5 \\ 0 & b_6 & b_7 \end{pmatrix} = \begin{pmatrix} b_1 & y \\ 0 & B_1 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p)_U,$$

with $y \stackrel{\text{def}}{=} \left(\begin{smallmatrix} b_2 & b_3 \end{smallmatrix}\right)$ and $B_1 \stackrel{\text{def}}{=} \left(\begin{smallmatrix} b_4 & b_5 \\ b_6 & b_7 \end{smallmatrix}\right)$, we have

$$\begin{aligned} &B\left(uA_1\right)^{r_1}\left(vA_2^{d_2}A_3^{d_3}\right)^{r_2}B^{-1} \in \\ &\left(r_1\left(\begin{smallmatrix} 1 & 0 \\ 0 & B_1 \end{smallmatrix}\right)\cdot u + r_2\left(\begin{smallmatrix} 1 & 0 \\ 0 & B_1 \end{smallmatrix}\right)\cdot v + k_2\left(\begin{smallmatrix} 1 & 0 \\ 0 & B_1 \end{smallmatrix}\right)\cdot e_2\right) BA_1^{r_1}\left(A_2^{d_2}A_3^{d_3}\right)^{r_2}B^{-1}\langle e_1\rangle, \end{aligned}$$

where

$$k_2 \stackrel{\text{def}}{=} \frac{1}{2}d_2 r_2\left(r_2-1\right)v_3.$$

Now by a matrix calculation (again quicker to use a matrix calculator) we have

$$\begin{aligned} BA_1^{b_1^{-1}b_7}A_3^{b_1^{-1}b_6}B^{-1} &= A_1, \\ BA_1^{b_1^{-1}b_5}A_3^{b_1^{-1}b_4}B^{-1} &= A_3, \end{aligned}$$

so we find

$$B\,(uA_1)^{b_1^{-1}b_7}\,(vA_3)^{b_1^{-1}b_6}\,B^{-1} = \left(b_1^{-1}\left(\begin{smallmatrix}1 & 0\\ 0 & B_1\end{smallmatrix}\right)\cdot(b_7u+b_6v)+ke_1\right)A_1,$$
$$B(uA_1)^{b_1^{-1}b_5}\,(vA_3)^{b_1^{-1}b_4}\,B^{-1} = \left(b_1^{-1}\left(\begin{smallmatrix}1 & 0\\ 0 & B_1\end{smallmatrix}\right)\cdot(b_5u+b_4v)+k'e_1\right)A_3$$

for some integers k and k'. We let $B_0 = \left(\begin{smallmatrix}v_2 & u_2\\ v_3 & u_3\end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_p)$. Then we have $\left(\begin{smallmatrix}1 & 0\\ 0 & B_0\end{smallmatrix}\right)\cdot e_2 = v$ and $\left(\begin{smallmatrix}1 & 0\\ 0 & B_0\end{smallmatrix}\right)\cdot e_3 = u$, so we have

$$\begin{aligned}
B\,(uA_1)^{b_1^{-1}b_7}\,(vA_3)^{b_1^{-1}b_6}\,B^{-1} &= \left(b_1^{-1}\left(\begin{smallmatrix}1 & 0\\ 0 & B_1\end{smallmatrix}\right)\cdot\left(b_7\left(\begin{smallmatrix}1 & 0\\ 0 & B_0\end{smallmatrix}\right)\cdot e_3+b_6\left(\begin{smallmatrix}1 & 0\\ 0 & B_0\end{smallmatrix}\right)\cdot e_2\right)+ke_1\right)A_1\\
&= \left(b_1^{-1}\left(\begin{smallmatrix}1 & 0\\ 0 & B_1B_0B_1^T\end{smallmatrix}\right)\cdot e_3+ke_1\right)A_1,\\
B\,(uA_1)^{b_1^{-1}b_5}\,(vA_3)^{b_1^{-1}b_4}\,B^{-1} &= \left(b_1^{-1}\left(\begin{smallmatrix}1 & 0\\ 0 & B_1\end{smallmatrix}\right)\cdot\left(b_5\left(\begin{smallmatrix}1 & 0\\ 0 & B_0\end{smallmatrix}\right)\cdot e_3+b_4\left(\begin{smallmatrix}1 & 0\\ 0 & B_0\end{smallmatrix}\right)\cdot e_2\right)+k'e_1\right)A_3\\
&= \left(b_1^{-1}\left(\begin{smallmatrix}1 & 0\\ 0 & B_1B_0B_1^T\end{smallmatrix}\right)\cdot e_2+k'e_1\right)A_3,
\end{aligned}$$

where superscript T on a matrix denotes its transpose. Note, the product group $\mathcal{H} \stackrel{\text{def}}{=} \mathbb{F}_p^\times \times \mathrm{GL}_2(\mathbb{F}_p)$ acts on $\mathrm{GL}_2(\mathbb{F}_p)$ as follows: for $(b_1, B_1) \in \mathcal{H}$ and $B_0 \in \mathrm{GL}_2(\mathbb{F}_p)$ we set

$$(b_1, B_1)\cdot B_0 \stackrel{\text{def}}{=} b_1^{-1}B_1B_0B_1^T.$$

Then the elements of the quotient space $\mathrm{GL}_2(\mathbb{F}_p)/\mathcal{H}$ give rise to non-isomorphic braces. We shall find a set of representatives for these elements. Let us write $\det(B_0) = s_1^2 s$ where $s = 1, \delta$ and $s_1 \in \mathbb{F}_p^\times$.

Note if $v_2 \neq 0$, then

$$\left(v_2, \begin{pmatrix} 1 & 0 \\ \pm v_3 s_1^{-1} & \mp v_2 s_1^{-1}\end{pmatrix}\right)\cdot\begin{pmatrix} v_2 & u_2\\ v_3 & u_3\end{pmatrix} = \begin{pmatrix} 1 & \pm(v_3-u_2)s_1^{-1}\\ 0 & s\end{pmatrix},$$

if $u_3 \neq 0$, then

$$\left(u_3, \begin{pmatrix} 0 & 1 \\ \pm u_3 s_1^{-1} & \mp u_2 s_1^{-1}\end{pmatrix}\right)\cdot\begin{pmatrix} v_2 & u_2\\ v_3 & u_3\end{pmatrix} = \begin{pmatrix} 1 & \pm(v_3-u_2)s_1^{-1}\\ 0 & s\end{pmatrix},$$

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

$$\left(u_2+v_3, \begin{pmatrix} 1 & 1 \\ \pm v_3 s_1^{-1} & \mp u_2 s_1^{-1}\end{pmatrix}\right)\cdot\begin{pmatrix} v_2 & u_2\\ v_3 & u_3\end{pmatrix} = \begin{pmatrix} 1 & \pm(v_3-u_2)s_1^{-1}\\ 0 & s\end{pmatrix},$$

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

$$(u_2, I)\cdot B_0 = \begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix}.$$

Therefore, when $u_2 = v_3$, we find two non-isomorphic braces

$$\langle e_1, se_3A_1, e_2A_3\rangle \cong C_p^3, \tag{4.40}$$

and for $u_2 \neq v_3$ we find non-isomorphic braces

$$\begin{aligned}&\langle e_1, (te_2 + se_3)A_1, e_2A_3\rangle, \langle e_1, e_2A_1, -e_3A_3\rangle \cong M_1\\ &\text{for } t = 1, ..., \frac{1}{2}(p-1).\end{aligned} \tag{4.41}$$

Case III: Finally, we consider subgroups of the from

$$G = \left\langle e_1, uA_1, vA_2A_3^d\right\rangle$$

for a fixed $d = 1, ..., p-1$. Then, using (4.28), we have $(uA_1)^p = (vA_2A_3^d)^p = 1$. We further have

$$(uA_1)e_1 = e_1(uA_1),\ (vA_2A_3^d)e_1 = e_1(vA_2A_3^d).$$

We calculate

$$\begin{aligned}(uA_1)(vA_2A_3^d) &= (u + v + v_3e_1)A_1A_2A_3^d \text{ and}\\ (vA_2A_3^d)(uA_1) &= (u + v + du_2e_1 + u_3e_2)A_1A_2A_3^d.\end{aligned}$$

Thus for G to have order p^3 we need to set $u_3 = 0$. Then for G to be regular we need $u_2, v_3 \neq 0$. The groups G is abelian when $du_2 = v_3$ and isomorphic to M_1 when $du_2 \neq v_3$.

Therefore, we find regular subgroups

$$\left\langle e_1, v_3d^{-1}e_2A_1, vA_2A_3^d\right\rangle \cong C_p^3 \text{ for } v_3 = 1, ..., p-1,\ v_2 = 0, ..., p-1;$$

there are $(p-1)p$ of them, and

$$\left\langle e_1, u_2e_2A_1, vA_2A_3^d\right\rangle \cong M_1$$

$$\text{for } u_2, v_3 = 1, ..., p-1,\ v_2 = 0, ..., p-1 \text{ with } du_2 \neq v_3,$$

there are

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

of them. Recall, in either case if $3 \mid p-1$ or not, we have $p^2 - 1$ conjugates for groups of the from $\left\langle A_1, A_2A_3^d\right\rangle$; therefore we have exactly

$$(p^2-1)(p-1)p \tag{4.42}$$

regular subgroups of the form $\left\langle e_1, uA, v\widetilde{A}'\widetilde{A}^d \right\rangle \cong C_p^3$, and we have exactly

$$(p^2-1)(p-1)(p-2)p \tag{4.43}$$

regular subgroups of the form $\left\langle e_1, uA, v\widetilde{A}'\widetilde{A}^d \right\rangle \cong M_1$, where A, $\widetilde{A}$, and $\widetilde{A}'$ are conjugates of A_1, A_2, and A_3 in $\mathrm{SL}_3(\mathbb{F}_p)_U$.

To find the braces corresponding to the above regular subgroups we note that for a matrix

$$B = \begin{pmatrix} b_1 & b_2 & b_3 \\ 0 & b_4 & b_5 \\ 0 & 0 & b_7 \end{pmatrix} = \begin{pmatrix} b_1 & y \\ 0 & B_1 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p)_U,$$

with $y \stackrel{\text{def}}{=} \left(\begin{smallmatrix} b_2 & b_3 \end{smallmatrix}\right)$ and $B_1 \stackrel{\text{def}}{=} \left(\begin{smallmatrix} b_4 & b_5 \\ 0 & b_7 \end{smallmatrix}\right)$, by a matrix calculation we find

$$\begin{aligned} BA_1^{b_1^{-1}b_7}B^{-1} &= A_1, \\ BA_1^{l_3}\left(A_2A_3^d\right)^{b_4^{-1}b_7}B^{-1} &= A_2A_3^{b_1b_4^{-2}b_7d}, \end{aligned}$$

for some integer l_3, so we find

$$\begin{aligned} &B\left(u_2e_2A_1\right)^{b_1^{-1}b_7}B^{-1} = \left(b_1^{-1}b_4b_7u_2e_2\right)A_1 \text{ and} \\ &B\left(u_2e_2A_1\right)^{l_3}\left(vA_2A_3^d\right)^{b_4^{-1}b_7}B^{-1} = \\ &\left(\left(\frac{1}{2}db_7\left(b_4^{-1}b_7-1\right)v_3 + b_4l_3u_2\right)e_2 + b_4^{-1}b_7\left(\begin{smallmatrix} 1 & 0 \\ 0 & B_1 \end{smallmatrix}\right)\cdot v + \kappa e_1\right)A_2A_3^{b_1b_4^{-2}b_7d}. \end{aligned}$$

for some κ. Note, if we set $b_1 = b_4^2$ and $b_7 = d$, then we find

$$B\left\langle A_1, A_2A_3\right\rangle B^{-1} = \left\langle A_1, A_2A_3^d\right\rangle.$$

Thus, we may consider conjugates of $\langle e_1, u_2e_2A_1, vA_2A_3\rangle$ by a matrix

$$\begin{pmatrix} b_4^2b_7^{-1} & b_2 & b_3 \\ 0 & b_4 & b_5 \\ 0 & 0 & b_7 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p)_U.$$

Now conjugating the subgroup

$$\langle e_1, e_2A_1, e_3A_2A_3\rangle \cong C_p^3 \tag{4.44}$$

by the matrix

$$\begin{pmatrix} v_3 & -v_2 & 0 \\ 0 & v_3 & 0 \\ 0 & 0 & v_3 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p)_U$$

we get $\langle e_1, v_3 e_2 A_1, v A_2 A_3 \rangle$, and conjugating the subgroup

$$\langle e_1, e_2 A_1, b e_3 A_2 A_3 \rangle \cong M_1 \text{ for } b = v_3 u_2^{-1} \neq 1 \tag{4.45}$$

by the matrix

$$\begin{pmatrix} u_2 & -v_2 & 0 \\ 0 & u_2 & 0 \\ 0 & 0 & u_2 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p)_U$$

we get

$$\langle e_1, u_2 e_2 A_1, v A_2 A_3 \rangle \text{ with } u_2 \neq v_3,$$

and one can check that none of these regular subgroups are further conjugate to each other. Therefore, we find one C_p^3-brace of C_p^3 type and $p-2$ M_1-braces of C_p^3 type.

Conclusion: Now we sum all the cases to find the total number of regular subgroups isomorphic to C_p^3 and isomorphic to M_1 which contain $\langle e_1 \rangle$. Hence, for the fix subspace $\langle e_1 \rangle$ we find, by adding the numbers in (4.38) and (4.42),

$$(p-1)p^2 + (p^2-1)(p-1)p = (p^2+p-1)(p-1)p \tag{4.46}$$

regular subgroups isomorphic to C_p^3 and, by adding numbers in (4.39), (4.36), and (4.43), we find

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

$$(p^2-2)(p-1)p^2 \tag{4.47}$$

regular subgroups isomorphic to M_1. Now we multiply the numbers in (4.46) and (4.47) by the number of distinct subgroups of order p in C_p^3 which is $\frac{p^3-1}{p-1}$ to find the total number of regular subgroups with $|\Theta(G)| = p^2$, so we have exactly

$$\frac{p^3-1}{p-1} \times (p^2+p-1)(p-1)p = (p^3-1)(p^2+p-1)p$$

regular subgroups isomorphic to C_p^3 and

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

isomorphic to M_1.

The corresponding non-isomorphic braces combining (4.40), (4.44), (4.41), (4.37),

and (4.45) are

$$\langle e_1, se_3A_1, e_2A_3\rangle, \langle e_1, e_2A_1, e_3A_2A_3\rangle \cong C_p^3, \langle e_1, (t_2e_2+se_3)A_1, e_2A_3\rangle,$$

$$\langle e_1, e_2A_1, -e_3A_3\rangle, \langle e_1, e_2A_1, e_3A_2\rangle, \langle e_1, e_2A_1, t_3e_3A_2A_3\rangle \cong M_1$$
$$\text{for } s=1,\delta,\ t_2=1,...,\frac{1}{2}(p-1),\ t_3=2,...,p-1;$$

therefore, there are three C_p^3-braces of C_p^3 type and

$$2\times\frac{1}{2}(p-1)+1+1+(p-2)=2p-1$$

M_1-braces of C_p^3 type. □

Corollary 4.3.5. *We have*

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

and $e(G, C_p^3, p^2) = 0$ *for* $G \ncong C_p^3$ *or* M_1.

Furthermore, we have

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

and $\widetilde{e}(G, C_p^3, p^2) = 0$ *for* $G \ncong C_p^3$ *or* M_1.

Proof. Follows from Lemma 4.3.4, and calculation similar to Corollary 4.3.3. □

Lemma 4.3.6. *For* $|\Theta(G)| = p^3$ *there are no regular subgroups contained in* $\mathrm{Hol}(C_p^3)$.

Proof. If $G \subseteq \mathrm{Hol}(C_p^3)$ with $|\Theta(G)| = p^3$, then we must have $\Theta(G) \subseteq \mathrm{SL}_3(\mathbb{F}_p)$ a subgroup of order p^3, so $\Theta(G)$ is conjugate to

$$B(C_p^3) \stackrel{\text{def}}{=} \langle A_1, A_2, A_3\rangle \cong M_1$$

by an element of $\mathrm{SL}_3(\mathbb{F}_p)$, and G is isomorphic to $\Theta(G)$. Thus we can assume, without loss of generality, that

$$G = \langle uA_1, vA_2, wA_3\rangle$$

for some vectors

$$u = v_1e_1+u_2e_2+u_3e_3,\ v = v_1e_1+v_2e_2+v_3e_3,\ w = w_1e_1+w_2e_2+w_3e_3.$$

Then, finding the relations between the generators of G, we see

$$(uA_1)(vA_2) = (u + v + v_3e_1)A_1A_2 \text{ and}$$
$$(vA_2)(uA_1) = (u + v + u_3e_2)A_1A_2,$$

so (vA_1) and (wA_2) commute if and only if $u_3 = v_3 = 0$. We have

$$(uA_1)(wA_3) = (u + w + w_3e_1)A_1A_3 \text{ and}$$
$$(wA_3)(uA_1) = (u + w + u_2e_1)A_1A_3$$

so (wA_3) and (uA_1) commute if and only if $u_2 = w_3$. Finally, we have

$$(uA_1)(vA_2)(wA_3) = (u + v + w + v_3e_1 + w_3e_1 + w_3e_2)A_1A_2A_3 \text{ and}$$
$$(wA_3)(vA_2) = (v + w + v_2e_1)A_3A_2,$$

so $(uA_1)(vA_2)(wA_3) = (wA_3)(vA_2)$ if and only if

$$u = (v_2 - v_3 - w_3)e_1 - w_3e_2,$$

which implies that $u_1 = v_2 - v_3 - w_3$ and $u_2 = -w_3$. Thus, gathering all the conditions together, for G to be isomorphic to M_1, we need (note we have $u_2 = -w_3$ and $u_2 = w_3$ and $p \neq 2$)

$$u_2 = u_3 = v_3 = w_3 = 0,\ u_1 = v_2.$$

Therefore, we must have

$$u = v_2e_1,\ v = v_1e_1 + v_2e_2,\ w = w_1e_1 + w_2e_2.$$

In this case G can never be regular since A_1, A_2, and A_3 fix the subspace $\langle e_1, e_2\rangle$, so the subgroup G will fail to be transitive. □

4.4 Regular subgroups in Hol(M_1)

In this section we classify the regular subgroups contained in Hol(M_1) and the skew braces of M_1 type. The main result of this section is the following.

Proposition 4.4.1. *We have*

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

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

Furthermore, 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.

The proof of the proposition above follows from the calculation in the rest of this section, particularly by adding the relevant numbers from Corollaries 4.4.3, 4.4.5, and 4.4.7. First we recall from Section 3.4, that we have

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

Note in Lemma 3.4.1, we set the notation that any automorphism $\alpha \in \mathrm{Aut}(M_1)$ can be represented as

$$\alpha \stackrel{\text{def}}{=} \begin{pmatrix} a_1a_4 - a_2a_3 & b_1 & b_2 \\ 0 & a_1 & a_2 \\ 0 & a_3 & a_4 \end{pmatrix},$$

where we had

$$\rho^\alpha = \rho^{a_1a_4 - a_2a_3},\ \sigma^\alpha = \rho^{b_1}\sigma^{a_1}\tau^{a_3},\ \tau^\alpha = \rho^{b_2}\sigma^{a_2}\tau^{a_4}.$$

Here we only use matrices as a convenient way to represent the automorphisms; consequently the composition of two automorphisms may not in general coincide with the matrix multiplication of their representatives.

Let us denote by

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

Note in Lemma 3.4.1, we had $\alpha_1 = \gamma$ and $\alpha_3 = \beta$, also we had $|\mathrm{Aut}(M_1)| = (p^2 - 1)(p - 1)p^3$. 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

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \alpha_1 = \alpha_1^{a_4}\alpha_3^{-a_2},\ \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \alpha_3 = \alpha_1^{-a_3}\alpha_3^{a_1}. \tag{4.48}$$

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

$$\alpha_2\alpha_1 = \alpha_1\alpha_2,\ \alpha_3\alpha_1 = \alpha_1\alpha_3,\ \alpha_3\alpha_2 = \alpha_1\alpha_2\alpha_3. \tag{4.49}$$

Thus, we have $\langle \alpha_1, \alpha_2, \alpha_3 \rangle \cong M_1$ 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. 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.

Bute before we begin, 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 and an element $v = \rho^{v_1}\sigma^{v_2}\tau^{v_3} \in M_1$. For this we first note that we have

$$\begin{aligned} \alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3} \cdot v &= \begin{pmatrix} 1 & a_1 & a_3 \\ 0 & 1 & 0 \\ 0 & a_2 & 1 \end{pmatrix} \cdot v \\ &= \rho^{v_1} \left(\rho^{a_1}\sigma\tau^{a_2}\right)^{v_2} \left(\rho^{a_3}\tau\right)^{v_3} \\ &= \rho^{v_1}\rho^{a_1v_2}\rho^{\frac{1}{2}a_2v_2(v_2-1)}\sigma^{v_2}\tau^{a_2v_2}\rho^{a_3v_3}\tau^{v_3} \\ &= \rho^{a_1v_2+\frac{1}{2}a_2v_2(v_2-1)+a_3v_3}v\tau^{a_2v_2}. \end{aligned} \tag{4.50}$$

Now we have

$$(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r = \left(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\cdot v\cdots(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^{r-1}\cdot v\right)(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r,$$

where by using (4.49) and (4.50) we find

$$\begin{aligned}(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^j\cdot v &= \alpha_1^{a_1 j+\frac{1}{2}a_2a_3j(j-1)}\alpha_2^{a_2 j}\alpha_3^{a_3 j}\cdot v\\ &= \rho^{k_j}v\tau^{a_2v_2j},\end{aligned}$$

with

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

for $j=0,...,r-1$. Thus we have

$$\begin{aligned}(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r &= \left(\prod_{j=0}^{r-1}\rho^{k_j}v\tau^{a_2v_2j}\right)(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r\\ &= \rho^{l_1}v^r\tau^{l_2a_2v_2}\,(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r,\end{aligned}\tag{4.51}$$

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

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

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

$$(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^p = 1\tag{4.52}$$

for every $v\in M_1$ since $p>3$. Note, further that in (4.51), when $a_2=0$, we have

$$(v\alpha_1^{a_1}\alpha_3^{a_3})^r \in v^r\alpha_1^{ra_1}\alpha_3^{ra_3}\langle\rho\rangle,\tag{4.53}$$

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

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

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

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

then, using (4.48), we have

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

where using the section of the exact sequence in Lemma 3.4.1, 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

$$\alpha\cdot v = \rho^{\det(\beta)v_1+\frac{1}{2}\left(b_3b_1v_2^2+b_4b_2v_3^2\right)+b_2b_3v_2v_3+r_1(b_1v_2+b_2v_3)+r_3(b_3v_2+b_4v_3)}\sigma^{b_1v_2+b_2v_3}\tau^{b_3v_2+b_4v_3}. \tag{4.54}$$

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

$$\alpha\left(v\alpha_1^{a_1}\alpha_3^{a_3}\right)\alpha^{-1} = (\alpha\cdot v)\,\alpha_1^{a_1b_4-a_3b_3}\alpha_3^{a_3b_1-a_1b_2}, \tag{4.55}$$

with $\alpha\cdot v$ as given in (4.54), 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

$$\alpha\left(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)\alpha^{-1} = (\alpha\cdot v)\,\alpha_1^{a_1b_4-a_3b_3+r_3a_2b_1^{-1}b_4+\frac{1}{2}a_2b_4\left(b_1^{-1}-1\right)}\alpha_2^{a_2b_1^{-1}b_4}\alpha_3^{a_3b_1}, \tag{4.56}$$

where $\alpha\cdot v$ can be calculation using (4.54).

Lemma 4.4.2. *For $|\Theta(G)| = p$ there are exactly*

$$p^4 - p^2 - p - 1$$

regular subgroups isomorphic to M_1 and exactly $(p+1)p^2$ regular subgroups isomorphic to C_p^3 contained in Hol(M_1).

Furthermore, there are $2(p-1)$ 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 $|\Theta(G)| = p$, 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 $G \cap M_1$ 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

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

We shall consider all subgroups of order p^2 in M_1 and all ways of pairing them with a subgroup of order p of $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ and then multiply our findings by $p+1$ whenever a pairing involves α_2 to take account for $p+1$ distinct conjugates of α_2. There are two main cases to consider.

Case I: We start with the subgroup $\langle \rho, \tau \rangle$ of M_1. Hence, 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 (4.50), 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 paring is possible. Further, it follows by (4.52) that $g^p = 1$. Now, for $r \neq 0$, using (4.50), we have

$$g\tau^r = \left(\sigma\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)\tau^r = \rho^{ra_3}\sigma\tau^r\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3} = \rho^{r(a_3-1)}\tau^r g, \tag{4.57}$$

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

$$\begin{aligned} &\langle \rho, \tau, \sigma\alpha_1^a\alpha_3 \rangle, \left\langle \rho, \tau, \sigma\alpha_1^a\alpha_2^b\alpha_3 \right\rangle \cong C_p^3 \\ &\text{for } a = 0, ..., p-1,\ b = 1, ..., p-1, \end{aligned} \tag{4.58}$$

and for $a_3 \neq 1$, setting $r = (1-a_3)^{-1}$ in (4.57), we find regular subgroups isomorphic to M_1 of the form

$$\begin{aligned} &\left\langle \rho, \tau, \sigma\alpha_1^b \right\rangle, \left\langle \rho, \tau, \sigma\alpha_1^a\alpha_2^b \right\rangle, \langle \rho, \tau, \sigma\alpha_1^a\alpha_3^c \rangle, \left\langle \rho, \tau, \sigma\alpha_1^a\alpha_2^b\alpha_3^c \right\rangle \cong M_1 \\ &\text{for } a = 0, ..., p-1,\ b, c = 1, ..., p-1 \text{ with } c \neq 1. \end{aligned} \tag{4.59}$$

Case II: Next, we consider the subgroups $\left\langle \rho, \sigma\tau^d \right\rangle$ of M_1 for some $d = 0, ..., p-1$, and investigate the possibility of pairing these subgroups with subgroups of the form $\langle \alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3} \rangle$. Thus, we can consider subgroups of the form

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

Note, using (4.50), we must have

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

and since for a natural number r we have

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

for the pairing to be possible, we need $a_2 = 0$. Therefore, we consider subgroups of the form

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

Now, using (4.50), we have

$$h\left(\sigma\tau^d\right) = \rho^{a_3d+a_1+1}\sigma\tau^d\tau\alpha_1^{a_1}\alpha_3^{a_3} = \rho^{a_3d+a_1+1}\left(\sigma\tau^d\right)h,$$

so G is abelian if and only if $a_3d + a_1 + 1 \equiv 0 \bmod p$.

Therefore, for $da_3 + a_1 + 1 \equiv 0 \bmod p$ we find regular subgroups isomorphic to C_p^3 of the form

$$\left\langle \rho, \sigma\tau^d, \tau\alpha_1^{-(cd+1)}\alpha_3^c\right\rangle \cong C_p^3 \text{ for } c, d = 0, ..., p-1, \tag{4.60}$$

and for $da_3 + a_1 + 1 \not\equiv 0 \bmod p$ we find regular subgroups isomorphic to M_1 of the form

$$\left\langle \rho, \sigma\tau^d, \tau\alpha_1^b\right\rangle, \left\langle \rho, \sigma\tau^d, \tau\alpha_1^a\alpha_3^c\right\rangle \cong M_1 \tag{4.61}$$
$$\text{for } a, d = 0, ..., p-1,\ b, c = 1, ..., p-1 \text{ with } b \neq p-1,\ a + cd + 1 \not\equiv 0 \bmod p.$$

To find the non-isomorphic skew braces corresponding to the above regular subgroups we work as follows. Let

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

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

First note that 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 $\langle \rho, \tau\rangle$; thus we can assume every skew brace is isomorphic

to one of the subgroups in (4.58) and (4.59), i.e., to one of

$$\begin{aligned}
&\langle \rho, \tau, \sigma\alpha_1^a\alpha_3 \rangle , \langle \rho, \tau, \sigma\alpha_1^a\alpha_2^b\alpha_3 \rangle \cong C_p^3 \\
&\text{for } a = 0, ..., p-1,\ b = 1, ..., p-1, \\
&\langle \rho, \tau, \sigma\alpha_1^b \rangle , \langle \rho, \tau, \sigma\alpha_1^a\alpha_2^b \rangle , \langle \rho, \tau, \sigma\alpha_1^a\alpha_3^c \rangle , \langle \rho, \tau, \sigma\alpha_1^a\alpha_2^b\alpha_3^c \rangle \cong M_1 \\
&\text{for } a = 0, ..., p-1,\ b, c = 1, ..., p-1 \text{ with } c \neq 1,
\end{aligned}$$

and now we work with automorphisms which fix the subgroup $\langle \rho, \tau \rangle$, i.e., when $b_2 = 0$. In such case, using (4.56), we have

$$\alpha \left(\sigma\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)\alpha^{-1} = (\alpha \cdot \sigma)\, \alpha_1^{a_1 b_4 - a_3 b_3 + r_3 a_2 b_1^{-1} b_4 + \frac{1}{2} a_2 b_4 \left(b_1^{-1}-1\right)} \alpha_2^{a_2 b_1^{-1} b_4} \alpha_3^{a_3 b_1},$$

where using (4.54)

$$\alpha \cdot \sigma = \rho^{\frac{1}{2} b_1 b_3 - r_1 b_1 + r_3 b_3} \sigma^{b_1} \tau^{b_3}.$$

Now since

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

we have

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

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

$$\alpha \left(\sigma\alpha_1^a\alpha_2^b\alpha_3^c\right)^{b_1^{-1}}\alpha^{-1} \in \sigma\alpha_1^{ab_1^{-1}b_4 - cb_1^{-1}b_3 + r_3 b b_1^{-2} b_4 + \frac{1}{2} b b_1^{-1} b_4 \left(b_1^{-1}-1\right)(c+1)} \alpha_2^{b b_1^{-2} b_4}\alpha_3^c \langle \rho, \tau \rangle .$$

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 $\langle \rho, \tau, \sigma\alpha_1^a\alpha_2^b\alpha_3^c \rangle$, 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

$$\alpha \left(\sigma\alpha_1^a\alpha_2^b\right)^{b_1^{-1}}\alpha^{-1} \in \sigma\alpha_1^{ab_1^{-1}b_4 + r_3 b b_1^{-2} b_4 + \frac{1}{2} b b_1^{-1} b_4 \left(b_1^{-1}-1\right)} \alpha_2^{b b_1^{-2} b_4} \langle \rho, \tau \rangle ,$$

so

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

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 $\langle \rho, \tau, \sigma\alpha_1^b \rangle$, 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 $\langle \rho, \tau, \sigma\alpha_1^a\alpha_2^b \rangle$.

Therefore, we have non-isomorphic skew braces

$$\begin{aligned}&\langle \rho, \tau, \sigma\alpha_3\rangle, \langle \rho, \tau, \sigma\alpha_2\alpha_3\rangle \cong C_p^3,\ \langle \rho, \tau, \sigma\alpha_1\rangle, \langle \rho, \tau, \sigma\alpha_2\rangle,\\ &\langle \rho, \tau, \sigma\alpha_3^c\rangle, \langle \rho, \tau, \sigma\alpha_2\alpha_3^c\rangle \cong M_1 \text{ for } c = 2, ..., p-1.\end{aligned} \tag{4.62}$$

In summary: if $G \subseteq \mathrm{Hol}(M_1)$ is a regular subgroup with $|\Theta(G)| = p$, then G is isomorphic to either M_1 or C_p^3. In particular, if G is isomorphic to M_1, then combining lists (4.59) and (4.61), the subgroup G is conjugate to precisely one of

$$\left\langle \rho, \tau, \sigma\alpha_1^b\right\rangle, \left\langle \rho, \tau, \sigma\alpha_1^a\alpha_2^b\right\rangle, \langle \rho, \tau, \sigma\alpha_1^a\alpha_3^c\rangle, \left\langle \rho, \tau, \sigma\alpha_1^a\alpha_2^b\alpha_3^c\right\rangle$$

$$\text{for } a = 0, ..., p-1,\ b, c = 1, ..., p-1, \text{with } c \neq 1,$$

$$\left\langle \rho, \sigma\tau^d, \tau\alpha_1^b\right\rangle, \left\langle \rho, \sigma\tau^d, \tau\alpha_1^a\alpha_3^c\right\rangle$$

$$\text{for } a, d = 0, ..., p-1,\ b, c = 1, ..., p-1 \text{ with } b \neq p-1,\ a + cd + 1 \not\equiv 0 \bmod p,$$

and there are (we shall multiply by $p+1$ appropriately wherever a subgroup involves α_2)

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

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

of them; if G is isomorphic to C_p^3, then combining lists (4.58) and (4.60), the subgroup G is conjugate to precisely one of

$$\langle \rho, \tau, \sigma\alpha_1^a\alpha_3\rangle, \left\langle \rho, \tau, \sigma\alpha_1^a\alpha_2^b\alpha_3\right\rangle, \left\langle \rho, \sigma\tau^d, \tau\alpha_1^{-(cd+1)}\alpha_3^c\right\rangle$$

$$\text{for } a, c, d = 0, ..., p-1,\ b = 1, ..., p-1,$$

and there are

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

of them.

The corresponding skew braces are given in (4.62), 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. □

Corollary 4.4.3. *We have*

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

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

Furthermore, we have

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

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

Proof. Follows from Lemma 4.4.2, and the calculation

$$\begin{aligned} e(C_p^3, M_1, p) &\overset{\text{def}}{=} \frac{\left|\mathrm{Aut}(C_p^3)\right|}{|\mathrm{Aut}(M_1)|} e'(C_p^3, M_1, p) \\ &= \frac{(p^3-1)(p^2-1)(p-1)p^3}{(p^2-1)(p-1)p^3} \times (p+1)p^2 = (p^3-1)(p+1)p^2. \end{aligned}$$

□

Lemma 4.4.4. *For* $|\Theta(G)| = p^2$ *there are exactly*

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

regular subgroups isomorphic to M_1 *and exactly*

$$(p^2-2)p^2$$

regular subgroups isomorphic to C_p^3 *contained in* Hol(M_1).

Furthermore, there are $(2p-3)p$ 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 $|\Theta(G)| = p^2$, 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 all ways of pairing them with a subgroup of order p^2 of $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ and then multiply our findings by $p+1$ whenever a pairing involves α_2.

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.

$$(v\alpha_1)\, u\, (v\alpha_1)^{-1} = v\,(\alpha_1 \cdot u)\, v^{-1}u^{-1} = \rho^{u_2+u_2v_3-u_3v_2} \in \langle u \rangle\,, \tag{4.63}$$

$$(w\alpha_2^{a_2}\alpha_3^{a_3})\, u\, (w\alpha_2^{a_2}\alpha_3^{a_3})^{-1} = w\,(\alpha_2^{a_2}\alpha_3^{a_3} \cdot u)\, w^{-1}u^{-1} = \rho^{\frac{1}{2}a_2u_2(u_2-1)+a_3u_3+u_2w_3-u_3w_2-a_2u_2w_2-a_2u_2^2}\tau^{a_2u_2} \in \langle u \rangle\,, \tag{4.64}$$

$$\begin{aligned}&(v\alpha_1)\,(w\alpha_2^{a_2}\alpha_3^{a_3})\,((w\alpha_2^{a_2}\alpha_3^{a_3})\,(v\alpha_1))^{-1} = \\ &(\rho^{w_2}vw\alpha_1\alpha_2^{a_2}\alpha_3^{a_3})\left(\rho^{\frac{1}{2}a_2v_2(v_2-1)+a_3v_1-a_2v_2^2+v_2w_1-v_1w_2}\tau^{a_2v_2}vw\alpha_1\alpha_2^{a_2}\alpha_3^{a_3}\right)^{-1} \\ &= \rho^{w_2-\frac{1}{2}a_2v_2(v_2-1)-a_3v_1+a_2v_2^2-v_2w_1+v_1w_2}\tau^{-a_2v_2} \in \langle u \rangle\,.\end{aligned} \tag{4.65}$$

Now 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 (4.63) implies that $u_2 = v_2$ and (4.64) 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 (4.65) 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 (4.63) gives $v_3 = -1$, also (4.64) gives $a_2 = 0$, and (4.65) gives $a_3 = 0$ which is not possible.

Therefore, we can 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

$$\begin{aligned}&(u\alpha_1)\,(v\alpha_3) = \rho^{v_2}uv\alpha_1\alpha_3 \text{ and} \\ &(v\alpha_3)\,(u\alpha_1) = \rho^{u_3}vu\alpha_1\alpha_3 = \rho^{u_3+u_2v_3-u_3v_2}uv\alpha_1\alpha_3,\end{aligned} \tag{4.66}$$

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

$$\begin{aligned} &\langle \rho, u\alpha_1, v\alpha_3 \rangle \cong C_p^3 \\ &\text{for } A = \begin{pmatrix} u_2 & v_2 \\ u_3 & v_3 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \text{ with } v_2 = u_3 + \det(A). \end{aligned} \tag{4.67}$$

We count these by considering the cases when $u_2 = 0$ and $u_2 \neq 0$, and we find that there are

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

of these. 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

$$\begin{aligned} &\langle \rho, u\alpha_1, v\alpha_3 \rangle \cong M_1 \\ &\text{for } A = \begin{pmatrix} u_2 & v_2 \\ u_3 & v_3 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \text{ with } v_2 - u_3 - \det(A) \not\equiv 0 \bmod p, \end{aligned} \tag{4.68}$$

and there are

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

of these.

To find the non-isomorphic skew braces corresponding to the above regular subgroups, we let $\beta_0 \stackrel{\text{def}}{=} \left(\begin{smallmatrix} u_2 & v_2 \\ u_3 & v_3 \end{smallmatrix}\right)$ and note that considering (4.54) and (4.56), it suffices to work with an automorphism corresponding to $\beta \stackrel{\text{def}}{=} \left(\begin{smallmatrix} b_1 & b_2 \\ b_3 & b_4 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_p)$ with $b \stackrel{\text{def}}{=} \det(\beta)^{-1}$, and we find

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

for some κ_1, κ_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

$$b\beta\beta_0\beta^T = \beta_0.$$

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

$$\begin{aligned}&\left\langle \rho, \sigma\alpha_1, \sigma^{u_2}\tau^{u_2}\alpha_3\right\rangle, \left\langle \rho, \tau^{-2}\alpha_1, \sigma^2\alpha_3\right\rangle \cong C_p^3,\\ &\left\langle \rho, \sigma\alpha_1, \sigma^{u_3}\tau^{u_4}\alpha_3\right\rangle, \left\langle \rho, \tau^{-u_5}\alpha_1, \sigma^{u_5}\alpha_3\right\rangle \cong M_1\\ &\text{for } u_4 = 0, ..., p-1,\ u_2, u_3, u_5 = 1, ..., p-1 \text{ with } u_5 \neq 2,\ u_3 - u_4 \not\equiv 0 \bmod p.\end{aligned} \tag{4.69}$$

Case II: Next, we consider subgroups of the form

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

Note, we have

$$\begin{aligned}(x\alpha_1)\left(y\alpha_2\alpha_3^a\right) &= \rho^{y_2}xy\alpha_1\alpha_2\alpha_3^a \text{ and}\\ \left(y\alpha_2\alpha_3^a\right)(x\alpha_1) &= \rho^{ax_3-x_3y_2}xy\alpha_1\alpha_2\alpha_3^a,\end{aligned} \tag{4.70}$$

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

$$\begin{aligned}&\left\langle \rho, \tau^{x_3}\alpha_1, \sigma^{y_2}\tau^{y_3}\alpha_2\alpha_3^{(1+x_3)y_2x_3^{-1}}\right\rangle \cong C_p^3\\ &\text{for } y_3 = 0, ..., p-1,\ y_2, x_3 = 1, ..., p-1,\end{aligned} \tag{4.71}$$

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

$$\begin{aligned}&\left\langle \rho, \tau^{x_3}\alpha_1, y\alpha_2\alpha_3^a\right\rangle \cong M_1\\ &\text{for } a, y_3 = 0, ..., p-1,\ x_3, y_2 = 1, ..., p-1 \text{ with } ax_3 - y_2 - x_3y_2 \not\equiv 0 \bmod p.\end{aligned} \tag{4.72}$$

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 $\beta \stackrel{\text{def}}{=} \left(\begin{smallmatrix} b_1 & 0 \\ b_3 & b_4 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_p)$. Then, using (4.54) and (4.56), we have

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

for some κ_1, κ_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

$$
\begin{aligned}
&\left\langle \rho, \tau^{x_3}\alpha_1, \sigma\alpha_2\alpha_3^{(1+x_3)x_3^{-1}}\right\rangle \cong C_p^3,\ \langle \rho, \tau^{x_3}\alpha_1, \sigma\alpha_2\alpha_3^{a}\rangle \cong M_1 \qquad (4.73)\\
&\text{for } a = 0, ..., p-1,\ x_3 = 1, ..., p-1 \text{ with } a-(1+x_3)x_3^{-1} \not\equiv 0 \bmod p.
\end{aligned}
$$

In summary: if $G \subseteq \mathrm{Hol}(M_1)$ is a regular subgroup with $|\Theta(G)| = p^2$, then G is isomorphic to either M_1 or C_p^3. In particular, if G is isomorphic to M_1, then, combining (4.68) and (4.72), the subgroup G is conjugate to exactly one of

$$
\begin{aligned}
&\langle \rho, u\alpha_1, v\alpha_3\rangle \text{ for } A = \left(\begin{smallmatrix} u_2 & v_2 \\ u_3 & v_3 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_p) \text{ with } v_2 - u_3 - \det(A) \not\equiv 0 \bmod p,\\
&\langle \rho, \tau^{x_3}\alpha_1, y\alpha_2\alpha_3^{a}\rangle \text{ for } a, y_3 = 0, ..., p-1,\ y_2, x_3 = 1, ..., p-1\\
&\text{with } y_2 - ax_3 + x_3y_2 \not\equiv 0 \bmod p,
\end{aligned}
$$

and so there are (we shall multiply by $p+1$ appropriately whenever a subgroup involves α_2)

$$
\begin{aligned}
&(p^2-1)(p^2-p) - (p-2)p - (p-1)^2p + (p+1)((p-1)^2p^2 - (p-1)^2p)\\
&= (p^4 - p^3 - 2p^2 + 2p + 1)p
\end{aligned}
$$

of them, and if G is isomorphic to C_p^3, then, combining (4.67) and (4.71), the subgroup G is conjugate to exactly one of the following

$$
\begin{aligned}
&\langle \rho, u\alpha_1, v\alpha_3\rangle \text{ for } A = \left(\begin{smallmatrix} u_2 & v_2 \\ u_3 & v_3 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_p) \text{ with } v_2 = u_3 + \det(A),\\
&\left\langle \rho, \tau^{x_3}\alpha_1, \sigma^{y_2}\tau^{y_3}\alpha_2\alpha_3^{(1+x_3)y_2x_3^{-1}}\right\rangle \text{ for } y_3 = 0, ..., p-1,\ y_2, x_3 = 1, ..., p-1,
\end{aligned}
$$

and there are

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

of them.

The corresponding non-isomorphic skew braces, combining (4.69) and (4.73), are

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

$$\langle \rho, \sigma\alpha_1, \sigma^{u_2}\tau^{u_2}\alpha_3 \rangle, \langle \rho, \tau^{-2}\alpha_1, \sigma^2\alpha_3 \rangle, \left\langle \rho, \tau^{x_3}\alpha_1, \sigma\alpha_2\alpha_3^{(1+x_3)x_3^{-1}} \right\rangle \cong C_p^3 \text{ for}$$

$$a, u_3 = 0, ..., p-1,\ u_2, u_4, u_5, x_3, = 1, ..., p-1$$

$$\text{with } u_5 \neq 2,\ u_3 - u_4,\ ax_3 - (1+x_3) \not\equiv 0 \bmod p.$$

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. □

Corollary 4.4.5. *We have*

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

and $e(G, M_1, p^2) = 0$ *for* $G \ncong M_1$ *or* C_p^3.

Furthermore, we have

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

and $\widetilde{e}(G, M_1, p^2) = 0$ *for* $G \ncong M_1$ *or* C_p^3.

Proof. Follows from Lemma 4.4.4, and calculations similar to Corollary 4.4.3. □

Lemma 4.4.6. *For* $|\Theta(G)| = p^3$ *there are exactly*

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

regular subgroups isomorphic to M_1 *contained in* Hol(M_1) *and no other if* $G \ncong M_1$.

Furthermore, there are four M_1*-skew braces of* M_1 *type.*

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

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

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

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

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,

$$\begin{aligned}&u_2 = 0,\ v_2 = -u_3v_2,\ w_2 = u_3 - u_3w_2,\ u_3 = -w_2,\\ &u_1 - v_2(w_2-1) - \frac{1}{2}w_2(w_2-1) = v_3 + w_3v_2 - v_3w_2. \qquad (4.74)\end{aligned}$$

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 (4.74) 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 $\alpha \stackrel{\text{def}}{=} \beta\gamma \in \mathrm{Aut}(M_1)$, where $\beta \stackrel{\text{def}}{=} \left(\begin{smallmatrix} b_1 & 0 \\ b_3 & b_4 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_p)$ and $\gamma \stackrel{\text{def}}{=} \alpha_1^{r_1}\alpha_3^{r_3} \in C_p^2$. Now using (4.54) and (4.56) we have

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

so we have

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

Note that we have

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

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

$$\begin{aligned}
&\alpha \cdot u^{b_4^{-1}} = \rho^{u_1b_1-2r_3}\tau^{-2},\\
&\alpha\cdot\left(u^{-r_3b_4^{-1}-\frac{1}{2}b_4^{-1}(1-b_1)}v^{b_1b_4^{-1}}\right) = \rho^{r_3(2r_3+1)+v_1b_1^2+\frac{1}{2}u_1b_1(b_1-1)-2r_3u_1b_1}\tau^{1+2r_3-u_1b_1},\\
&\left(\alpha\cdot u^{b_1^{-1}b_3b_4^{-1}}\right)\left(\alpha\alpha_1^{b_1^{-1}b_3b_4^{-1}}\cdot\left(\rho^{\frac{1}{2}w_3b_1^{-1}\left(b_1^{-1}-1\right)}w^{b_1^{-1}}\right)\right) = \rho^{b_3u_1-2r_3b_1^{-1}b_3}\tau^{-2b_1^{-1}b_3}\\
&\rho^{\frac{3}{2}w_3b_4\left(b_1^{-1}-1\right)+b_4w_1+2b_1^{-1}b_3+2b_1^{-1}b_5+b_3(2b_1^{-1}-1)}\sigma^2\tau^{2b_1^{-1}b_3+w_3b_1^{-1}b_4}\\
&= \rho^{2r_1+\frac{3}{2}w_3b_4\left(b_1^{-1}-1\right)+b_4w_1+u_1b_3}\sigma^2\tau^{w_3b_1^{-1}b_4}.
\end{aligned}$$

We let

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

which gives us

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

Next, for $\delta \in \mathbb{F}_p^\times$ which is not a square, as fixed in (4.1), 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

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

Therefore, every such regular subgroup is conjugate to

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

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

Corollary 4.4.7. *We have*

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

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

Furthermore, we have

$$\widetilde{e}(M_1, M_1, p^3) = 4$$

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

Proof. Follows from Lemma 4.4.6. □

4.5 Regular subgroups in Hol(M_2)

In this section we classify the regular subgroups contained in Hol(M_2) and the skew braces of M_2 type. The main result of this section is the following. This section shares some similarities with Sections 4.2 and 4.4.

Proposition 4.5.1. *We have*

$$e(M_2, M_2) = (2p-1)(p-1)p^2,$$
$$e(C_{p^2} \times C_p, M_2) = (2p-1)(p-1)p^2,$$

and $e(G, M_2) = 0$ *for* $G \ncong M_2$ *or* $C_{p^2} \times C_p$.

Furthermore, we have

$$\widetilde{e}(M_2, M_2) = 4p^2 - 3p - 1,$$
$$\widetilde{e}(C_{p^2} \times C_p, M_2) = 4p + 1,$$

and $\widetilde{e}(G, M_2) = 0$ *for* $G \ncong M_2$ *or* $C_{p^2} \times C_p$.

The proof of the proposition above follows from the calculation in the rest of this section, particularly by adding the relevant numbers from Corollaries 4.5.3 and 4.5.5. First we recall from Section 3.5

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

In Lemma 3.5.1, we set the notation to represent an automorphism $\alpha \in \mathrm{Aut}(M_2)$ by

$$\alpha \stackrel{\text{def}}{=} \begin{pmatrix} a_1 & a_2 p \\ a_3 & 1 \end{pmatrix},$$

where

$$\sigma^\alpha = \sigma^{a_1}\tau^{a_3},\ \tau^\alpha = \sigma^{a_2 p}\tau.$$

Now by Lemma 3.5.1, we have $|\mathrm{Aut}(M_2)| = (p-1)p^3$. Note, with notation introduced in Lemma 3.5.1, if $\alpha, \beta \in \mathrm{Aut}(M_2)$, say $\alpha = \left(\begin{smallmatrix} a_1 & a_2 p \\ a_3 & 1 \end{smallmatrix}\right)$ and $\beta = \left(\begin{smallmatrix} b_1 & b_2 p \\ b_3 & 1 \end{smallmatrix}\right)$, then the

composition $\alpha\beta$ corresponds to

$$\alpha\beta = \begin{pmatrix} a_1b_1 + \left(a_2b_3 + \frac{1}{2}a_1a_3b_1\left(b_1-1\right)\right)p & \left(a_1b_2+a_2\right)p \\ a_3b_1 + b_3 & 1 \end{pmatrix}. \tag{4.75}$$

Let

$$\Theta : \mathrm{Hol}(M_2) \longrightarrow \mathrm{Aut}(M_2)$$

be the natural projection. Further, let

$$\begin{gathered} \Psi : \mathrm{Aut}(M_2) \longrightarrow \mathrm{L}_1(\mathbb{F}_p) \\ \begin{pmatrix} a_1 & a_2p \\ a_3 & 1 \end{pmatrix} \longmapsto \begin{pmatrix} a_1 \bmod p & 0 \\ a_3 & 1 \end{pmatrix} \end{gathered}$$

be the reduction of entries modulo p, where $\mathrm{L}_1(\mathbb{F}_p)$ was defined just before Lemma 3.5.1 as the set of invertible 2×2 lower triangular matrices whose bottom right hand entry is 1. Then the image of a subgroup of $G \subseteq \mathrm{Hol}(M_2)$ of order p^3 in $\mathrm{L}_1(\mathbb{F}_p)$ under the composition of projections

$$\Psi\Theta : \mathrm{Hol}(M_2) \longrightarrow \mathrm{L}_1(\mathbb{F}_p)$$

must lie in the unique Sylow p-subgroup of $\mathrm{L}_1(\mathbb{F}_p)$ which is the subgroup generated by the image of the automorphism $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ under Ψ. Let

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

Note, the elements α_1, α_3 generate $\mathrm{Ker}\,\Psi$, and the elements $\alpha_1, \alpha_2, \alpha_3 \in \mathrm{Aut}(M_2)$ have order p. They satisfy

$$\alpha_2\alpha_1 = \alpha_1\alpha_2,\ \alpha_3\alpha_1 = \alpha_1\alpha_3,\ \alpha_3\alpha_2 = \alpha_1\alpha_2\alpha_3, \tag{4.76}$$

which implies that

$$\langle \alpha_1, \alpha_2, \alpha_3 \rangle \cong M_1.$$

Therefore, we always have

$$\Theta(G) \subseteq \mathrm{A}(M_2) \stackrel{\text{def}}{=} \langle \alpha_1, \alpha_2, \alpha_3 \rangle,$$

and so any subgroup of $\mathrm{Hol}(M_2)$ of order p^3 lies in

$$M_2 \rtimes \mathrm{A}(M_2).$$

We have

$$e(M_2, M_2, 1) = \widetilde{e}(M_2, M_2, 1) = 1 \text{ and}$$
$$e(G, M_2, 1) = \widetilde{e}(G, M_2, 1) = 0 \text{ if } G \neq M_2.$$

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

But before we begin, it will be useful for our calculations to derive the explicit formula for a term of the form $(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r$ for natural numbers r, a_i and an element $v = \sigma^{v_1}\tau^{v_2} \in M_2$. First note that we have

$$\begin{aligned}\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3} \cdot v &= \begin{pmatrix} a_1p+1 & a_3p \\ a_2 & 1 \end{pmatrix} \cdot v \\ &= \left(\sigma^{a_1p+1}\tau^{a_2}\right)^{v_1} \left(\sigma^{a_3p}\tau\right)^{v_2} \\ &= \sigma^{a_1v_1p+\frac{1}{2}a_2v_1(v_1-1)+v_1}\tau^{a_2v_1}\sigma^{a_3v_2p}\tau^{v_2} \\ &= \sigma^{a_1v_1p+\frac{1}{2}a_2v_1(v_1-1)p+a_3v_2p}v\tau^{a_2v_1}. \end{aligned} \tag{4.77}$$

Now, similar to the previous section, we have

$$(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r = \left(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3} \cdot v \cdots (\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^{r-1} \cdot v\right)(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r$$

where, using (4.76) and (4.77), we find

$$\begin{aligned}(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^j \cdot v &= \alpha_1^{a_1j+\frac{1}{2}a_2a_3j(j-1)}\alpha_2^{a_2j}\alpha_3^{a_3j} \cdot v \\ &= \sigma^{k_jp}v\tau^{a_2v_1j},\end{aligned}$$

with

$$k_j \stackrel{\text{def}}{=} a_1v_1j + \frac{1}{2}a_2a_3v_1j\,(j-1) + \frac{1}{2}a_2v_1\,(v_1-1)\,j + a_3v_2j,$$

for $j = 0, ..., r-1$; thus we find

$$\begin{aligned}(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r &= \left(\prod_{j=0}^{r-1}\sigma^{k_jp}v\tau^{a_2v_1j}\right)(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^r \\ &= \sigma^{l_1p}v^r\tau^{l_2a_2v_1}\left(\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)^r, \end{aligned} \tag{4.78}$$

(note order of the product below matters and is in increasing j) where

$$l_1 = l_1(r) = \sum_{j=1}^{r-1} k_j + \frac{a_2v_1^2}{2}\sum_{j=1}^{r-2} j\,(j+1) \text{ and}$$
$$l_2 = l_2(r) = \sum_{j=1}^{r-1} j.$$

Similar, to the previous section the second summation in l_1 arises by gathering the

terms $\tau^{a_2 v_1 j}$ in one place using the rule $\tau\sigma = \sigma^{p+1}\tau$. Further we note, l_1 and l_2 are divisible by r for $r > 3$ a prime number, so

$$(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^p = v^p = \sigma^{v_1 p} \tag{4.79}$$

since $p > 3$, i.e., the element $v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}$ has order p or p^2 depending on v_1. Note, for future use that in (4.78), when $a_2 = 0$, we have

$$(v\alpha_1^{a_1}\alpha_3^{a_3})^r \in v^r \alpha_1^{ra_1}\alpha_3^{ra_3} \langle\sigma^p\rangle, \tag{4.80}$$

where $\langle\sigma^p\rangle$ is a normal subgroup of Hol(M_2) since it is a characteristic subgroup of M_2.

It will further be useful, when finding the non-isomorphic 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 $\alpha \in \mathrm{Aut}(M_2)$. Now every $\alpha \in \mathrm{Aut}(M_2)$ can be written as

$$\alpha = \alpha_3^{r_3}\beta \text{ for some } \beta \stackrel{\text{def}}{=} \begin{pmatrix} b_1 & 0 \\ b_3 & 1 \end{pmatrix} \in \mathrm{Aut}(M_2)$$

and some integer r_3 which matters modulo p. Then we find

$$\alpha^{-1} = \beta^{-1}\alpha_3^{-r_3} = \begin{pmatrix} b_1^{-1} - \frac{1}{2}b_3 b_1^{-1}\left(b_1^{-1}-1\right)p & 0 \\ -b_3 b_1^{-1} & 1 \end{pmatrix}\alpha_3^{-r_3}.$$

Now, using (4.75), we find

$$\begin{aligned} \beta\alpha_1\beta^{-1} &= \alpha_1, \\ \beta\alpha_2\beta^{-1} &= \alpha_1^{\frac{1}{2}\left(b_1^{-1}-1\right)}\alpha_2^{b_1^{-1}}, \\ \beta\alpha_3\beta^{-1} &= \alpha_1^{-b_3}\alpha_3^{b_1}, \end{aligned}$$

so we have

$$\begin{aligned} \alpha\alpha_1\alpha^{-1} &= \alpha_1, \\ \alpha\alpha_2\alpha^{-1} &= \alpha_1^{r_3 b_1^{-1}+\frac{1}{2}\left(b_1^{-1}-1\right)}\alpha_2^{b_1^{-1}}, \\ \alpha\alpha_3\alpha^{-1} &= \alpha_1^{-b_3}\alpha_3^{b_1}. \end{aligned}$$

Therefore, we find

$$\alpha\left(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)\alpha^{-1} = (\alpha\cdot v)\,\alpha_1^{a_1 - a_3 b_3 + r_3 a_2 b_1^{-1} + \frac{1}{2}a_2\left(b_1^{-1}-1\right)}\alpha_2^{a_2 b_1^{-1}}\alpha_3^{a_3 b_1}, \tag{4.81}$$

where

$$\alpha\cdot v = \sigma^{\left(\frac{1}{2}b_1 b_3 v_1(v_1-1)+r_3(b_3 v_1+v_2)\right)p}\sigma^{b_1 v_1}\tau^{b_3 v_1+v_2}.$$

Lemma 4.5.2. *For $|\Theta(G)| = p$ there are exactly*

$$2p^3 - 2p^2 - p - 1$$

regular subgroups isomorphic to M_2 and exactly $2p^2$ regular subgroups isomorphic to $C_{p^2} \times C_p$ contained in Hol(M_2).

Furthermore, there are $5p-6$ M_2-skew braces of M_2 type and five $(C_{p^2} \times C_p)$-skew braces of M_2 type.

Proof. If $G \subseteq \mathrm{Hol}(M_2)$ with $|\Theta(G)| = p$, then we must have $\Theta(G) \subseteq \langle \alpha_1, \alpha_2, \alpha_3 \rangle$ a subgroup of order p and $G \cap M_2$ 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 $G \cap M_2$ is one of

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

We shall consider all subgroups of order p^2 in M_2 and all ways of pairing them with a subgroup of order p of $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$. We divide our investigations into two main cases.

Case I: We start with the subgroup $\langle \sigma^p, \tau \rangle$ of M_2. Then we must have

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

Note using (4.77) we find

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

so the paring is possible. Furthermore, it follows from (4.79) that $g^p = \sigma^p$, thus $G = \langle \tau, g \rangle$. Now for $r \neq 0$ and using (4.77), we have

$$g\tau^r = \sigma^{ra_3 p} \sigma \tau^r \alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3} = \sigma^{ra_3 p - rp} \tau^r g = g^{r(a_3-1)p} \tau^r g, \tag{4.82}$$

so G is abelian if and only if $a_3 = 1$. Furthermore, all these subgroups are regular since they have size p^3 and $\langle \sigma^p, \tau \rangle \cup \{\sigma\} \subseteq \mathrm{Orb}(1)$.

Therefore, for $a_3 = 1$ we have regular subgroups isomorphic to $C_{p^2} \times C_p$ of the form

$$\left\langle \tau, \sigma \alpha_1^a \alpha_2^b \alpha_3 \right\rangle \cong C_{p^2} \times C_p \text{ for } a, b = 0, ..., p-1, \tag{4.83}$$

and if $a_3 \neq 1$, then letting $r = (1 - a_3)^{-1}$ in (4.82), we find regular subgroups

isomorphic to M_2 of the form

$$\begin{aligned}&\left\langle \tau, \sigma\alpha_1^{a_1}\right\rangle, \left\langle \tau, \sigma\alpha_1^{a}\alpha_2^{a_1}\right\rangle, \left\langle \tau, \sigma\alpha_1^{a}\alpha_2^{b}\alpha_3^{c}\right\rangle \cong M_2\\ &\text{for } a,b=0,...,p-1,\ a_1=1,...,p-1,\ c=2,...,p-1.\end{aligned} \tag{4.84}$$

To find the non-isomorphic skew braces corresponding to the above regular subgroups we work as follows. We let $\alpha \in \mathrm{Aut}(M_2)$ and write

$$\alpha = \alpha_3^{r_3}\beta \text{ for some } \beta \stackrel{\text{def}}{=} \begin{pmatrix} b_1 & 0\\ b_3 & 1\end{pmatrix} \in \mathrm{Aut}(M_2).$$

Now recall by (4.81) we have

$$\alpha\left(\sigma\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)\alpha^{-1} = \sigma^{r_3b_3p}\sigma^{b_1}\tau^{b_3}\alpha_1^{a_1-a_3b_3+r_3a_2b_1^{-1}+\frac{1}{2}a_2\left(b_1^{-1}-1\right)}\alpha_2^{a_2b_1^{-1}}\alpha_3^{a_3b_1},$$

so

$$\alpha\left(\sigma\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\right)^{b_1^{-1}}\alpha^{-1} \in \sigma\alpha_1^{a_1b_1^{-1}-a_3b_1^{-1}b_3+r_3a_2b_1^{-2}+\frac{1}{2}a_2b_1^{-1}\left(b_1^{-1}-1\right)(a_3+1)}\alpha_2^{a_2b_1^{-2}}\alpha_3^{a_3}\left\langle\sigma^p,\tau\right\rangle.$$

Now if $a_2=0$, we have

$$\alpha\left(\sigma\alpha_1^{a_1}\alpha_3^{a_3}\right)^{b_1^{-1}}\alpha^{-1} \in \sigma\alpha_1^{a_1b_1^{-1}-a_3b_1^{-1}b_3}\alpha_3^{a_3}\left\langle\sigma^p,\tau\right\rangle,$$

which implies that conjugating a subgroup of the form $\langle\tau,\sigma\alpha_3^c\rangle$ with the automorphism represented by $\left(\begin{smallmatrix}1 & 0\\ -ac^{-1} & 1\end{smallmatrix}\right)$ we get $\langle\tau,\sigma\alpha_1^a\alpha_3^c\rangle$, and the subgroups $\langle\tau,\sigma\alpha_3^c\rangle$ for different values of c cannot be conjugate. If $a_2\neq 0$ for $s=1,\delta$, we have

$$\alpha\left(\sigma\alpha_2^{s}\alpha_3^{c}\right)^{b_1^{-1}}\alpha^{-1} \in \sigma\alpha_1^{-cb_1^{-1}b_3+r_3sb_1^{-2}+\frac{1}{2}sb_1^{-1}\left(b_1^{-1}-1\right)(c+1)}\alpha_2^{sb_1^{-2}}\alpha_3^{c}\left\langle\sigma^p,\tau\right\rangle,$$

which implies that, if for any integer $b\neq 0$ considered as an element of $\mathbb{F}_p^\times$ we write $b=s_1^2s$ for some $s_1\in\mathbb{F}_p^\times$, then conjugating subgroups of the form $\langle\tau,\sigma\alpha_2^s\alpha_3^c\rangle$ with the automorphism represented by $\alpha_3^{ab^{-1}-\frac{1}{2}\left(1-s_1^{-1}\right)(c+1)\left(\begin{smallmatrix}s_1^{-1} & 0\\ 0 & 1\end{smallmatrix}\right)}$ we get $\left\langle\tau,\sigma\alpha_1^a\alpha_2^b\alpha_3^c\right\rangle$. Finally, conjugating the subgroup $\langle\tau,\sigma\alpha_1\rangle$ with the automorphism represented by $\left(\begin{smallmatrix}a_1^{-1} & 0\\ 0 & 1\end{smallmatrix}\right)$ we get $\langle\tau,\sigma\alpha_1^{a_1}\rangle$.

Therefore, we have non-isomorphic skew braces

$$\begin{aligned}&\left\langle\tau,\sigma\alpha_3\right\rangle, \left\langle\tau,\sigma\alpha_2^s\alpha_3\right\rangle \cong C_p\times C_{p^2},\ \left\langle\tau,\sigma\alpha_1\right\rangle, \left\langle\tau,\sigma\alpha_2^s\right\rangle,\\ &\left\langle\tau,\sigma\alpha_3^c\right\rangle, \left\langle\tau,\sigma\alpha_2^s\alpha_3^c\right\rangle \cong M_2 \text{ for } c=2,...,p-1,\ s=1,\delta.\end{aligned} \tag{4.85}$$

Case II: Finally, we consider the subgroups $\left\langle\sigma\tau^d\right\rangle$ of M_2 for $d=0,...,p-1$ and investigate the possibility of pairing these subgroups with a subgroup of the form

$\langle \alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}\rangle$. Thus, we consider subgroups of the form

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

Note we must have

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

and since we have

$$\left(\sigma\tau^d\right)^{(a_3d+a_1+1)p+1} = \sigma^{(a_3d+a_1+1)p+1}\tau^d,$$

for the pairing to be possible, we need $a_2 = 0$, hence we can consider the following subgroups

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

Note by (4.78) and (4.80), we have $h^p = 1$, and for $r \neq 0$, we have

$$h^r = (\tau\alpha_1^{a_1}\alpha_3^{a_3})^r \in \tau^r\alpha_1^{ra_1}\alpha_3^{ra_3}\left\langle \sigma\tau^d \right\rangle.$$

Now

$$(\tau^r\alpha_1^{ra_1}\alpha_3^{ra_3})\left(\sigma\tau^d\right) = \sigma^{ra_3dp+ra_1p+rp}\sigma\tau^r\tau^d\alpha_1^{ra_1}\alpha_3^{ra_3} = \left(\sigma\tau^d\right)^{r(a_3d+a_1+1)p+1}(\tau^r\alpha_1^{ra_1}\alpha_3^{ra_3}),$$

so G is abelian if and only if $a_3d + a_1 + 1 \equiv 0 \bmod p$, and all these subgroups are regular.

Therefore, for $a_3d + a_1 + 1 \equiv 0 \bmod p$ we find regular subgroups isomorphic to $C_{p^2} \times C_p$ of the form

$$\left\langle \sigma\tau^d, \tau\alpha_1^{-(cd+1)}\alpha_3^c \right\rangle \cong C_{p^2} \times C_p \text{ for } c, d = 0, ..., p-1, \tag{4.86}$$

and for $da_3 + a_1 + 1 \not\equiv 0 \bmod p$ we find regular subgroups isomorphic to M_2 of the form

$$\begin{aligned} &\left\langle \sigma\tau^d, \tau\alpha_1^b \right\rangle, \left\langle \sigma\tau^d, \tau\alpha_1^a\alpha_3^c \right\rangle \cong M_2 \qquad (4.87)\\ &\text{for } a, d = 0, ..., p-1,\ b, c = 1, ..., p-1 \text{ with } b \neq p-1,\ a + cd + 1 \not\equiv 0 \bmod p. \end{aligned}$$

To find the non-isomorphic skew braces corresponding to the above regular subgroups, we note that the automorphism represented by $\left(\begin{smallmatrix} 1 & 0 \\ d & 1 \end{smallmatrix}\right)$ sends σ to $\sigma\tau^d$, so we may consider orbits of regular subgroups when $d = 0$ and conjugation by automorphisms which fix $\langle\sigma\rangle$, i.e., we only consider automorphisms of the form $\alpha = \alpha_3^{r_3}\left(\begin{smallmatrix} b_1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Now by (4.81) we have

$$\alpha\left(\tau\alpha_1^{a_1}\alpha_3^{a_3}\right)\alpha^{-1} = \sigma^{r_3p}\tau\alpha_1^{a_1}\alpha_3^{a_3b_1}.$$

For each fixed b conjugation by any automorphism which fixes $\langle\sigma\rangle$ will fix $\left\langle\sigma,\tau\alpha_1^b\right\rangle$, and conjugating the subgroup $\langle\sigma,\tau\alpha_1^a\alpha_3\rangle$ with an automorphism represented by $\left(\begin{smallmatrix} c & 0 \\ 0 & 1 \end{smallmatrix}\right)$ we get $\langle\sigma,\tau\alpha_1^a\alpha_3^c\rangle$.

Therefore, we find non-isomorphic skew braces

$$\begin{aligned}&\left\langle\sigma,\tau\alpha_1^{-1}\right\rangle,\left\langle\sigma,\tau\alpha_1^{-1}\alpha_3\right\rangle\cong C_{p^2}\times C_p,\\&\left\langle\sigma,\tau\alpha_1^{b}\right\rangle,\langle\sigma,\tau\alpha_1^{a}\alpha_3\rangle\cong M_2 \text{ for } a=0,...,p-2,\ b=1,...,p-2.\end{aligned}\tag{4.88}$$

In summary: if $G\subseteq\mathrm{Hol}(M_2)$ is a regular subgroup with $|\Theta(G)|=p$, then G is isomorphic to either M_2 or $C_{p^2}\times C_p$. In particular, if G is isomorphic to M_2, then combining lists (4.84) and (4.87), the subgroup G is precisely one of

$$\langle\tau,\sigma\alpha_1^{a_1}\rangle,\langle\tau,\sigma\alpha_1^a\alpha_2^{a_1}\rangle,\left\langle\tau,\sigma\alpha_1^a\alpha_2^b\alpha_3^c\right\rangle$$

$$\text{for } a,b=0,...,p-1,\ a_1=1,...,p-1,\ c=2,...,p-1,$$

$$\left\langle\sigma\tau^d,\tau\alpha_1^b\right\rangle,\left\langle\sigma\tau^d,\tau\alpha_1^a\alpha_3^c\right\rangle$$

$$\text{for } a,d=0,...,p-1,\ b,c=1,...,p-1 \text{ with } b\neq p-1,\ a\neq-(cd+1),$$

and there are

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

$$=2p^3-2p^2-p-1$$

of them; if G is isomorphic to $C_{p^2}\times C_p$, then combining lists (4.83) and (4.86), the subgroup G is precisely one of

$$\left\langle\tau,\sigma\alpha_1^a\alpha_2^b\alpha_3\right\rangle,\left\langle\sigma\tau^d,\tau\alpha_1^{-(cd+1)}\alpha_3^c\right\rangle \text{ for } a,b,c,d=0,...,p-1,$$

and there are $2p^2$ of them.

The corresponding skew braces, combining lists (4.85) and (4.88) are

$$\langle\tau,\sigma\alpha_1\rangle,\langle\tau,\sigma\alpha_2^s\rangle,\langle\tau,\sigma\alpha_3^c\rangle,\langle\tau,\sigma\alpha_2^s\alpha_3^c\rangle,\left\langle\sigma,\tau\alpha_1^b\right\rangle,\langle\sigma,\tau\alpha_1^a\alpha_3\rangle\cong M_2$$

$$\langle\tau,\sigma\alpha_3\rangle,\langle\tau,\sigma\alpha_2^s\alpha_3\rangle,\left\langle\sigma,\tau\alpha_1^{-1}\right\rangle,\left\langle\sigma,\tau\alpha_1^{-1}\alpha_3\right\rangle\cong C_{p^2}\times C_p$$

$$\text{for } a=0,...,p-2,\ b=1,...,p-2,\ c=2,...,p-1,\ s=1,\delta;$$

therefore there are

$$1+2+(p-2)+2(p-2)+(p-2)+p-1=5p-6$$

M_2-skew braces of M_2 type and five $(C_{p^2}\times C_p)$-skew braces of M_2 type. □

Corollary 4.5.3. *We have*

$$e(M_2, M_2, p) = 2p^3 - 2p^2 - p - 1,$$
$$e(C_{p^2} \times C_p, M_2, p) = 2(p-1)p^2,$$

and $e(G, M_2, p) = 0$ *for* $G \ncong M_2$ *or* $C_{p^2} \times C_p$.

Furthermore, we have

$$\widetilde{e}(M_2, M_2, p) = 5p - 6,$$
$$\widetilde{e}(C_{p^2} \times C_p, M_2, p) = 5,$$

and $\widetilde{e}(G, M_2, p) = 0$ *for* $G \ncong M_2$ *or* $C_{p^2} \times C_p$.

Proof. Follows from Lemma 4.5.2, and the calculation

$$\begin{aligned} e(C_{p^2} \times C_p, M_2, p) &\overset{\text{def}}{=} \frac{|\mathrm{Aut}(C_{p^2} \times C_p)|}{|\mathrm{Aut}(M_2)|} e'(C_{p^2} \times C_p, M_2, p) \\ &= \frac{p^3(p-1)^2}{p^3(p-1)} \times 2p^2 = 2(p-1)p^2. \end{aligned}$$

□

Lemma 4.5.4. *For* $|\Theta(G)| = p^2$ *there are exactly*

$$(2p^3 - 5p^2 + 3p + 1)p$$

regular subgroups isomorphic to M_2 *and exactly* $(2p-3)p^2$ *regular subgroups isomorphic to* $C_{p^2} \times C_p$ *contained in* Hol(M_2).

Furthermore, there are $4(p-1)^2$ M_2*-skew braces of* M_2 *type and* $4(p-1)$ $(C_{p^2} \times C_p)$*-skew braces of* M_2 *type.*

Proof. If $G \subseteq \mathrm{Hol}(M_2)$ with $|\Theta(G)| = p^2$, then we must have $\Theta(G) \subseteq \langle \alpha_1, \alpha_2, \alpha_3 \rangle$ a subgroup of order p^2 and $G \cap M_2$ 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 $G \cap M_2$ is one of

$$\langle \sigma^p \rangle, \left\langle \tau \sigma^{bp} \right\rangle \text{ for } b = 0, ..., p-1.$$

We shall consider all subgroups of order p in M_2 and all ways of pairing them with a subgroup of order p^2 of $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$.

We can divide our investigation into three main cases. We start with the subgroup $\langle \sigma^p \rangle$ of M_2 which is a characteristic subgroup; thus to obtain regular subgroups we need to consider subgroups of the form

$$G = \langle \sigma^p, u\alpha_1, v\alpha_3 \rangle, \langle \sigma^p, x\alpha_1, y\alpha_2 \alpha_3^a \rangle$$

for $u=\sigma^{u_1}\tau^{u_2},\ v=\sigma^{v_1}\tau^{v_2},\ x=\sigma^{x_1}\tau^{x_2},\ y=\sigma^{y_1}\tau^{y_2},$ with $a,u_i,v_i,x_i,y_i=0,...,p-1$

where either $u_1\neq 0$ or $v_1\neq 0$, similarly, either $x_1\neq 0$ or $y_1\neq 0$, this reduces us to consider subgroups of the form

$$G=\left\langle u\alpha_1, v\alpha_3\right\rangle, \left\langle x\alpha_1, y\alpha_2\alpha_3^a\right\rangle.$$

Case I: Let us consider the subgroups of the form

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

Note, using (4.80) we have $(u\alpha_1)^r\in u^r\alpha_1^r\left\langle\sigma^p\right\rangle$, so $u^r\alpha_1^r\in G$, and we have

$$\begin{aligned}(u^r\alpha_1^r)(v\alpha_3)&=\sigma^{rv_1p}u^rv\alpha_3\alpha_1^r \text{ and}\\ (v\alpha_3)(u^r\alpha_1^r)&=\sigma^{ru_2p+ru_1v_2p-ru_2v_1p}u^rv\alpha_3\alpha_1^r.\end{aligned}\tag{4.89}$$

Now we consider two subcases when $u_1=0$ and $u_1\neq 0$.

Subcase I.1: If $u_1=0$, then for $r\neq 0$, the element $u^r\alpha_1^r\in G$ has order p, and we need $u_2,v_1\neq 0$ for G to be regular. The element $v\alpha_3$ has order p^2, and the group G is abelian if and only if $v_1\equiv u_2-u_2v_1 \bmod p$.

Therefore, for $v_1\equiv u_2-u_2v_1 \bmod p$ we have regular subgroups of the form

$$\begin{aligned}&\left\langle\tau^{u_2}\alpha_1,\sigma^{u_2(1+u_2)^{-1}}\tau^{v_2}\alpha_3\right\rangle\cong C_{p^2}\times C_p\\ &\text{for } v_2=0,...,p-1,\ u_2=1,...,p-2,\end{aligned}\tag{4.90}$$

and for $v_1\not\equiv u_2-u_2v_1 \bmod p$, setting $r=v_1(v_1-u_2+u_2v_1)^{-1}$ in (4.89) we find regular subgroups of the form

$$\begin{aligned}&\left\langle\tau^{u_2}\alpha_1,\sigma^{v_1}\tau^{v_2}\alpha_3\right\rangle\cong M_2\\ &\text{for } v_2=0,...,p-1,\ u_2,v_1=1,...,p-1, \text{ with } v_1-u_2+u_2v_1\not\equiv 0 \bmod p.\end{aligned}\tag{4.91}$$

To find the non-isomorphic skew braces corresponding to the above regular subgroups, we note that considering (4.81), it suffices to work with automorphisms of the form $\beta\overset{\text{def}}{=}\left(\begin{smallmatrix}b_1 & 0\\ b_3 & 1\end{smallmatrix}\right)\in\text{Aut}(M_2)$, and using (4.81) we find

$$\begin{aligned}\beta(\tau^{u_2}\alpha_1)\beta^{-1}&=\tau^{u_2}\alpha_1,\\ \beta(\tau^{u_2}\alpha_1)^{b_1^{-1}b_3}(v\alpha_3)^{b_1^{-1}}\beta^{-1}&=\sigma^{\kappa p}\sigma^{v_1}\tau^{b_1^{-1}(b_3(u_2+v_1)+v_2)}\alpha_3,\end{aligned}$$

for some κ. Now conjugating the subgroup $\left\langle\tau^{u_2}\alpha_1,\sigma^{v_1}\tau^{v_2}\alpha_3\right\rangle$, when $u_2+v_1\not\equiv 0 \bmod p$ with the automorphism represented by $\left(\begin{smallmatrix}1 & 0\\ -v_2(u_2+v_1)^{-1} & 1\end{smallmatrix}\right)$ we get $\left\langle\tau^{u_2}\alpha_1,\sigma^{v_1}\alpha_3\right\rangle$, and when $u_2+v_1\equiv 0 \bmod p$ conjugating the subgroup $\left\langle\tau^{-v_1}\alpha_1,\sigma^{v_1}\tau^{v_2}\alpha_3\right\rangle$ with the automorphism represented by $\left(\begin{smallmatrix}b_1 & 0\\ 0 & 1\end{smallmatrix}\right)$ we get $\left\langle\tau^{-v_1}\alpha_1,\sigma^{v_1}\tau^{b_1^{-1}v_2}\alpha_3\right\rangle$. Furthermore,

the subgroups $\langle \tau^{u_2}\alpha_1, \sigma^{v_1}\alpha_3\rangle$ and $\left\langle \tau^{-v_1}\alpha_1, \sigma^{v_1}\tau^{b_1^{-1}v_2}\alpha_3\right\rangle$ for different values are not conjugate to each other.

Therefore, we find non-isomorphic skew braces

$$\left\langle \tau^{u_2}\alpha_1, \sigma^{u_2(1+u_2)^{-1}}\alpha_3\right\rangle, \left\langle \tau^{-2}\alpha_1, \sigma^2\tau^{t_2}\alpha_3\right\rangle \cong C_{p^2}\times C_p \tag{4.92}$$

for $u_2 = 1, ..., p-3,\ t_2 = 0, 1,$

$\langle \tau^{u_2}\alpha_1, \sigma^{v_1}\alpha_3\rangle, \left\langle \tau^{-t_1}\alpha_1, \sigma^{t_1}\tau^{t_2}\alpha_3\right\rangle \cong M_2$

for $u_2, v_1, t_1 = 1, ..., p-1,\ t_2 = 0, 1$ with $t_1 \neq 2,\ v_1 - u_2 + u_2v_1,\ u_2 + v_1 \not\equiv 0 \bmod p.$

Subcase I.2: If $u_1 \neq 0$, then $u\alpha_1$ has order p^2, and since

$$\left(\sigma^{u_1}\tau^{u_2}\alpha_1\right)^{-u_1^{-1}v_1}\left(\sigma^{v_1}\tau^{v_2}\alpha_3\right) \in \tau^{u_1^{-1}(u_1v_2-u_2v_1)}\alpha_1^{-u_1^{-1}v_1}\alpha_3\left\langle\sigma^p\right\rangle,$$

we can assume

$$G = \langle u\alpha_1, \tau^{q_2}\alpha_1^q\alpha_3\rangle$$

where $q_2 \overset{\text{def}}{=} u_1^{-1}(u_1v_2 - u_2v_1)$ and $q \overset{\text{def}}{=} -u_1^{-1}v_1$, and we need $(u_1v_2 - u_2v_1) \not\equiv 0 \bmod p$ for G to be regular. Now

$$\left(\tau^{q_2}\alpha_1^q\alpha_3\right)^r = \sigma^{(rqu_1+ru_2)p}\tau^{rq_2}\alpha_1^{rq}\alpha_3^r \in \tau^{rq_1}\alpha_1^{rq}\alpha_3^r\left\langle\sigma^p\right\rangle,$$

so $\tau^{rq_2}\alpha_1^{rq}\alpha_3^r \in G$, and we have

$$\begin{aligned}(u\alpha_1)\left(\tau^{rq_2}\alpha_1^{rq}\alpha_3^r\right) &= u\tau^{rq_2}\alpha_1^{1+rq}\alpha_3^r \text{ and}\\ \left(\tau^{rq_2}\alpha_1^{rq}\alpha_3^r\right)(u\alpha_1) &= \sigma^{ru_2p-rv_1p+r(u_1v_2-u_2v_1)p}u\tau^{rq_2}\alpha_1^{1+rq}\alpha_3^r,\end{aligned} \tag{4.93}$$

so the group G is abelian if and only if $v_1 \equiv u_2 + (u_1v_2 - u_2v_1) \bmod p$.

Therefore, for $v_1 \equiv u_2 + (u_1v_2 - u_2v_1) \bmod p$ we have regular subgroups of the form

$$\begin{aligned}&\langle u\alpha_1, v\alpha_3\rangle \cong C_{p^2}\times C_p\\ &\text{for } A = \begin{pmatrix} u_1 & v_1\\ u_2 & v_2\end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \text{ with } u_1 \neq 0,\ v_1 = u_2 + \det(A).\end{aligned} \tag{4.94}$$

To determine the number of these subgroups, we need to determine the number of matrices

$$A = \begin{pmatrix} u_1 & v_1\\ u_2 & u_1^{-1}(u_2v_1 - u_2 + v_1)\end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p),$$

so we need to determine the number of triples (u_1, u_2, v_1) with $u_2, v_1 = 0, ..., p-1$ and $u_1 = 1, ..., p-1$ such that $u_2 \neq v_1$, which is

$$(p-1)p^2 - (p-1)p = (p-1)^2p.$$

For $v_1 \not\equiv u_2 + u_1 v_2 - u_2 v_1 \bmod p$ we have the regular subgroups of the form

$$\begin{aligned} &\langle u\alpha_1, v\alpha_3\rangle \cong M_2 \\ &\text{for } A = \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \text{ with } u_1,\ v_1 - u_2 - \det(A) \not\equiv 0 \bmod p; \end{aligned} \tag{4.95}$$

the number of these matrices is given by the difference between the total number of invertible matrices with $u_1 \neq 0$ and the number of matrices with $v_1 - u_2 = \det(A)$ and $u_1 \neq 0$ which is

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

To find the non-isomorphic skew braces corresponding to the above regular subgroups, it suffices to work with automorphisms of the form $\beta \overset{\text{def}}{=} \left(\begin{smallmatrix} b_1 & 0 \\ b_3 & 1 \end{smallmatrix}\right) \in \mathrm{Aut}(M_2)$, and using (4.81) we have

$$\begin{aligned} \beta\,(u\alpha_1)\,\beta^{-1} &= \sigma^{\kappa_1 p}\sigma^{b_1 u_1}\tau^{b_3 u_1 + u_2}\alpha_1, \\ \beta\,(u\alpha_1)^{b_1^{-1}b_3}\,(v\alpha_3)^{b_1^{-1}}\,\beta^{-1} &= \sigma^{\kappa_2 p}\beta\cdot u^{b_1^{-1}b_3}\beta\cdot v^{b_1^{-1}}\alpha_3, \end{aligned}$$

for some κ_1, κ_2. Then conjugating $\langle u\alpha_1, v\alpha_3\rangle$ by $\left(\begin{smallmatrix} u_1^{-1} & 0 \\ -u_1^{-1}u_2 & 1 \end{smallmatrix}\right)$ gives $\langle \sigma\alpha_1, \sigma^{v_1-u_2}\tau^{u_1 v_2 - u_2 v_1}\alpha_3\rangle$ and these subgroups cannot further be conjugate to each other.

Therefore, we find non-isomorphic skew braces

$$\begin{aligned} &\langle \sigma\alpha_1, \sigma^{u_2}\tau^{u_2}\alpha_3\rangle \cong C_{p^2}\times C_p,\ \langle \sigma\alpha_1, \sigma^{v_1}\tau^{v_2}\alpha_3\rangle \cong M_2 \\ &\text{for } v_1 = 0,\ldots,p-1,\ u_2, v_2 = 1,\ldots,p-1 \text{ with } v_2 - v_1 \not\equiv 0 \bmod p. \end{aligned} \tag{4.96}$$

Case II: Next we consider subgroups of the form

$$G = \langle x\alpha_1, y\alpha_2\alpha_3^a\rangle\,.$$

Note for $r \neq 0$ we have $x^r\alpha_1^r \in G$. Now we have

$$\begin{aligned} (x^r\alpha_1^r)\,(y\alpha_2\alpha_3^a) &= \sigma^{r y_1 p} x^r y \alpha_2 \alpha_3^a \alpha_1^r \text{ and} \\ (y\alpha_2\alpha_3^a)\,(x^r\alpha_1^r) &= \sigma^{r a x_2 p + r x_1 y_2 p - r x_2 y_1 p} x^r y \tau^{r x_1}\alpha_2\alpha_3^a\alpha_1^r \end{aligned} \tag{4.97}$$

so for G to have size p^3, we must set $x_1 = 0$. Than for G to be regular, we need $x_2, y_1 \neq 0$. Now G is abelian if and only if $y_1 \equiv a x_2 - x_2 y_1 \bmod p$.

Therefore, for $y_1 \equiv a x_2 - x_2 y_1 \bmod p$ we have regular subgroups of the form

$$\begin{aligned} &\left\langle \tau^{x_2}\alpha_1, \sigma^{y_1}\tau^{y_2}\alpha_2\alpha_3^{y_1(1+x_2)x_2^{-1}}\right\rangle \cong C_{p^2}\times C_p \\ &\text{for } y_2 = 0,\ldots,p-1\ x_2, y_1 = 1,\ldots,p-1, \end{aligned} \tag{4.98}$$

and for $y_1 \not\equiv ax_2 - x_2y_1 \bmod p$, letting $r = y_1 \left(y_1 + x_2y_1 - ax_2\right)^{-1}$ in (4.97), we have regular subgroups

$$\begin{aligned} &\langle \tau^{x_2}\alpha_1, \sigma^{y_1}\tau^{y_2}\alpha_2\alpha_3^a\rangle \cong M_2 \qquad (4.99)\\ &\text{for } a, y_2 = 0, ..., p-1,\ x_2, y_1 = 1, ..., p-1 \text{ with } ax_2 - y_1 - x_2y_1 \not\equiv 0 \bmod p. \end{aligned}$$

To find the non-isomorphic skew braces corresponding to the above regular subgroups, we note that for an automorphism $\alpha_3^{r_3}\beta \stackrel{\text{def}}{=} \alpha_3^{r_3}\left(\begin{smallmatrix} b_1 & 0 \\ b_3 & 1 \end{smallmatrix}\right) \in \mathrm{Aut}(M_2)$, using (4.81) we have

$$\begin{aligned} &\left(\alpha_3^{r_3}\beta\right)\left(\tau^{x_2}\alpha_1\right)\left(\alpha_3^{r_3}\beta\right)^{-1} = \sigma^{\kappa_1 p}\tau^{x_2}\alpha_1 \text{ and}\\ &\left(\alpha_3^{r_3}\beta\right)\left(\tau^{x_2}\alpha_1\right)^{ab_1b_3 - r_3 - \frac{1}{2}ab_1(b_1-1) - \frac{1}{2}(1-b_1)}\left(y\alpha_2\alpha_3^a\right)^{b_1}\left(\alpha_3^{r_3}\beta\right)^{-1} =\\ &\sigma^{\kappa_2 p}\sigma^{y_1b_1^2}\tau^{\left(ab_1b_3 - r_3 - \frac{1}{2}ab_1(b_1-1) - \frac{1}{2}(1-b_1)\right)x_2 + b_1y_2 + \frac{1}{2}b_1(b_1-1)y_1}\alpha_2\alpha_3^{ab_1^2}, \end{aligned}$$

for some κ_1, κ_2. Let us write $y_1 = s_1^{-2}s$ where $s = 1, \delta$ and $s_1 \in \mathbb{F}_p^\times$. Then conjugating the subgroup $\langle \tau^{x_2}\alpha_1, y\alpha_2\alpha_3^a\rangle$ with the automorphism represented by $\alpha_3^{r_3}\left(\begin{smallmatrix} s_1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, where

$$r_3 = -\frac{1}{2}as_1\left(s_1 - 1\right) - \frac{1}{2}\left(1 - s_1\right) + x_2^{-1}s_1y_2 + \frac{1}{2}x_2^{-1}s_1\left(s_1 - 1\right)y_1,$$

gives $\left\langle \tau^{x_2}\alpha_1, \sigma^s\alpha_2\alpha_3^{asy_1^{-1}}\right\rangle$.

Therefore, we find non-isomorphic skew braces

$$\begin{aligned} &\left\langle \tau^{x_2}\alpha_1, \sigma^s\alpha_2\alpha_3^{s(1+x_2)x_2^{-1}}\right\rangle \cong C_{p^2} \times C_p,\ \langle \tau^{x_2}\alpha_1, \sigma^s\alpha_2\alpha_3^a\rangle \cong M_2\\ &\text{with } ax_2 \neq s + x_2s. \qquad (4.100) \end{aligned}$$

Case III: Finally, we consider the subgroup $\left\langle \tau\sigma^{bp}\right\rangle$ of M_2 for $b = 0, ..., p-1$, and investigate pairing this subgroup with the subgroups $\langle \alpha_1, \alpha_3\rangle, \langle \alpha_1, \alpha_2\alpha_3^a\rangle$. Let us consider a subgroup

$$G = \left\langle \tau\sigma^{bp}, \sigma^{u_1}\tau^{u_2}\alpha_1, \sigma^{v_1}\tau^{v_2}\alpha_2^{a_3}\alpha_3^{a_2}\right\rangle \text{ for } (a_2, a_3) \neq (0, 0).$$

For this to be a group of order p^3 we need $u_1, v_1 \equiv 0 \bmod p$, but such a subgroup cannot be regular.

In summary: if $G \subseteq \mathrm{Hol}(M_2)$ is a regular subgroup with $|\Theta(G)| = p^2$, then G is isomorphic to either M_2 or $C_{p^2} \times C_p$. In particular, if G is isomorphic to M_2, then

combining lists (4.91), (4.95), and (4.99), the subgroup G is exactly one of

$\langle \tau^{u_2}\alpha_1, \sigma^{v_1}\tau^{v_2}\alpha_3\rangle$ for $v_2 = 0, ..., p-1,\ u_2, v_1 = 1, ..., p-1$ with $v_1 - u_2 + u_2v_1 \not\equiv 0 \bmod p$,

$\langle u\alpha_1, v\alpha_3\rangle$ for $A = \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$ with $u_1, v_1 - u_2 - \det(A) \not\equiv 0 \bmod p$,

$\langle \tau^{x_2}\alpha_1, \sigma^{y_1}\tau^{y_2}\alpha_2\alpha_3^a\rangle$ for $a, y_2 = 0, ..., p-1,\ x_2, y_1 = 1, ..., p-1$
with $ax_2 - y_1 - x_2y_1 \not\equiv 0 \bmod p$;

there are

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

$$= (2p^3 - 5p^2 + 3p + 1)p$$

of them, and if G is isomorphic to $C_{p^2} \times C_p$, then combining lists (4.90), (4.94), and (4.98), the subgroup G is exactly one of

$\left\langle \tau^{u_2}\alpha_1, \sigma^{u_2(1+u_2)^{-1}}\tau^{v_2}\alpha_3\right\rangle$ for $v_2 = 0, ..., p-1,\ u_2 = 1, ..., p-2$,

$\langle u\alpha_1, v\alpha_3\rangle$ for $A = \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$ with $u_1 \neq 0,\ v_1 = u_2 + \det(A)$,

$\left\langle \tau^{x_2}\alpha_1, \sigma^{y_1}\tau^{y_2}\alpha_2\alpha_3^{y_1(1+x_2)x_2^{-1}}\right\rangle \cong C_{p^2} \times C_p$ for $y_2 = 0, ..., p-1,\ y_1, x_2 = 1, ..., p-1$;

and there are

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

of them.

The corresponding skew braces, combining lists (4.92), (4.96), and (4.100), are

$$\langle \tau^{u_2}\alpha_1, \sigma^{v_1}\alpha_3\rangle, \left\langle \tau^{-t_1}\alpha_1, \sigma^{t_1}\tau^{t_2}\alpha_3\right\rangle, \left\langle \sigma\alpha_1, \sigma^{t_3}\tau^{t_4}\alpha_3\right\rangle, \langle \tau^{x_2}\alpha_1, \sigma^s\alpha_2\alpha_3^a\rangle \cong M_2,$$

$$\left\langle \tau^{u_4}\alpha_1, \sigma^{u_4(1+u_4)^{-1}}\alpha_3\right\rangle, \left\langle \tau^{-2}\alpha_1, \sigma^2\tau\alpha_3\right\rangle, \langle \sigma\alpha_1, \sigma^{u_3}\tau^{u_3}\alpha_3\rangle, \left\langle \tau^{x_2}\alpha_1, \sigma^s\alpha_2\alpha_3^{s(1+x_2)x_2^{-1}}\right\rangle \cong C_{p^2} \times C_p$$

for $a, t_3 = 0, ..., p-1,\ u_2, v_1, t_1, t_4, x_2, u_3, u_4 = 1, ..., p-1,\ t_2 = 0, 1,\ s = 1, \delta$

with $v_1 \neq u_2 - u_2v_1,\ u_2 + v_1 \neq 0,\ t_1 \neq 2,\ t_3 \neq t_4,\ ax_2 \neq s + x_2s,\ u_4 \neq p-1$;

therefore there are

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

$$= 4(p-1)^2$$

M_2-skew braces of M_2 type and

$$p - 2 + 1 + p - 1 + 2(p-1) = 4(p-1)$$

$(C_{p^2} \times C_p)$-skew braces of M_2 type. □

Corollary 4.5.5. *We have*

$$e(M_2, M_2, p^2) = (2p^3 - 5p^2 + 3p + 1)p,$$
$$e(C_{p^2} \times C_p, M_2, p^2) = (2p-3)(p-1)p^2,$$

and $e(G, M_2, p^2) = 0$ *for* $G \ncong M_2$ *or* $C_{p^2} \times C_p$.

Furthermore, we have

$$\widetilde{e}(M_2, M_2, p^2) = 4(p-1)^2,$$
$$\widetilde{e}(C_{p^2} \times C_p, M_2, p^2) = 4(p-1),$$

and $\widetilde{e}(G, M_2, p^2) = 0$ *for* $G \ncong M_2$ *or* $C_{p^2} \times C_p$.

Proof. Follows from Lemma 4.5.4, and calculation similar to Corollary 4.5.3. □

Lastly, if $G \subseteq \mathrm{Hol}(M_2)$ with $|\Theta(G)| = p^3$, then we must have $\Theta(G) = \langle \alpha_1, \alpha_2, \alpha_3 \rangle$ and so

$$G = \langle \sigma^{u_1}\tau^{u_2}\alpha_1, \sigma^{v_1}\tau^{v_2}\alpha_2, \sigma^{w_1}\tau^{w_2}\alpha_3 \rangle,$$

where for G to have size p^3, we require $u_1, v_1, w_1 \equiv 0 \bmod p$, but in such case G cannot be regular. Now we have enough information to state our main theorems.

4.6 Main results I: Hopf-Galois structures and skew braces for $p > 3$

In this section we add the contributions from Sections 4.1 – 4.5 and give the number of Hopf-Galois structures on a Galois field extension of degree p^3. We further provide a list of all non-isomorphic skew braces of order p^3 as regular subgroups inside holomorphs. We discuss the patterns revealed by these results, point to how to explain some of them, and mention a few further research ideas. The main results are as follows (we shall consider all congruences modulo p, unless stated otherwise). We first state our theorems relating to Hopf-Galois structures.

Theorem 4.6.1. *Let L/K be a cyclic extension of fields of degree p^3 for a prime $p > 2$. Then L/K admits precisely p^2 Hopf-Galois structures all of which are of cyclic type.*

Proof. Follows from Lemma 4.1.2, and Sections 4.1 – 4.5. □

Theorem 4.6.2. *Let L/K be a $C_{p^2} \times C_p$ extension of fields for a prime $p > 3$. Then L/K admits precisely the following Hopf-Galois structures:*

$$e(C_{p^2} \times C_p, C_{p^2} \times C_p) = (2p-1)p^2$$

of $C_{p^2} \times C_p$ type and

$$e(C_{p^2} \times C_p, M_2) = (2p-1)(p-1)p^2$$

of M_2 type.

Proof. Follows from Sections 4.1 – 4.5. For $e(C_{p^2} \times C_p, N) \neq 0$ see Sections 4.2 and 4.5. □

Theorem 4.6.3. *Let L/K be a C_{p^3} extension of fields for a prime $p > 3$. Then L/K admits precisely the following Hopf-Galois structures:*

$$e(C_p^3, C_p^3) = (p^4 + p^3 - 1)p^2$$

of C_{p^3} type and

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

of M_1 type.

Proof. Follows from Sections 4.1 – 4.5. For $e(C_p^3, N) \neq 0$ see Sections 4.3 and 4.4. □

Theorem 4.6.4. *Let L/K be an M_1 extension of fields for a prime $p > 3$. Then L/K admits precisely the following Hopf-Galois structures:*

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

of M_1 type and

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

of C_p^3 type.

Proof. Follows from Sections 4.1 – 4.5. For $e(M_1, N) \neq 0$ see Sections 4.3 and 4.4. □

Theorem 4.6.5. *Let L/K be an M_2 extension of fields a prime $p > 3$. Then L/K admits precisely the following Hopf-Galois structures:*

$$e(M_2, M_2) = (2p-1)(p-1)p^2$$

of M_2 type and

$$e(M_2, C_{p^2} \times C_p) = (2p-1)p^2$$

of $C_{p^2} \times C_p$ type.

Proof. Follows from Sections 4.1 – 4.5. For $e(M_2, N) \neq 0$ see Sections 4.2 and 4.5. □

Now we state our results for skew braces. In all theorems we assume that $p > 3$. We also recall that

$$\delta \in \mathbb{F}_p^\times \setminus \left(\mathbb{F}_p^\times\right)^2.$$

Theorem 4.6.6. *There precisely are*

$$\widetilde{e}(C_{p^3}, C_{p^3}) = 3$$

braces of cyclic type all of which are cyclic given, as regular subgroups of the holomorph, by

$$\langle \sigma \rangle, \langle \sigma\alpha^p \rangle, \langle \sigma\alpha \rangle,$$

where $C_{p^3} = \langle \sigma \rangle$ and $\sigma^\alpha = \sigma^{p+1}$.

Follows from Section 4.1, Lemma 4.1.2.

Theorem 4.6.7. *The braces of $C_{p^2} \times C_p$ type are precisely*

$$\widetilde{e}(C_{p^2} \times C_p, C_{p^2} \times C_p) = 9$$

$(C_{p^2} \times C_p)$-braces given, as regular subgroups of the holomorph, by

$$\langle \sigma, \tau \rangle, \langle \tau, \sigma\alpha_1 \rangle, \langle \tau, \sigma\alpha_2 \rangle, \langle \sigma, \tau\alpha_3 \rangle,$$

$$\langle \tau\alpha_1, \sigma\alpha_3 \rangle, \langle \sigma\alpha_1, \tau^s\alpha_3 \rangle, \langle \tau\alpha_1, \sigma^s\alpha_2\alpha_3^s \rangle$$

for $s = 1, \delta$ and

$$\widetilde{e}(M_2, C_{p^2} \times C_p) = 4p + 1$$

M_2-braces given by

$$\langle \tau, \sigma\alpha_3 \rangle, \langle \tau, \sigma\alpha_2^s\alpha_3 \rangle, \langle \sigma, \tau\alpha_1 \rangle, \langle \sigma, \tau\alpha_1\alpha_3 \rangle, \left\langle \tau\alpha_1, \sigma^{t_1}\alpha_3 \right\rangle,$$

$$\left\langle \tau\alpha_1, \sigma^{-1}\tau^{t_2}\alpha_3 \right\rangle, \left\langle \sigma\alpha_1, \sigma^{t_3}\tau^s\alpha_3 \right\rangle, \left\langle \tau\alpha_1, \sigma^s\alpha_2\alpha_3^{t_4 s} \right\rangle$$

for $s = 1, \delta$, $t_1 = 2, .., p-2$, $t_2 = 0, 1$, $t_3 = 1, ..., \frac{1}{2}(p-1)$, $t_4 = 0, 2, ..., p-1$, where $C_{p^2} \times C_p = \langle \sigma, \tau \rangle$, and $\alpha_1, \alpha_2, \alpha_3$ as given in Section 4.2.

Proof. Follows from Section 4.2. □

Theorem 4.6.8. *The braces of C_p^3 type are precisely*

$$\widetilde{e}(C_p^3, C_p^3) = 5$$

C_p^3-braces given, as regular subgroups of the holomorph, by

$$\langle \rho, \sigma, \tau \rangle, \langle \rho, \sigma, \tau A_2 \rangle, \langle \rho, \tau^s A_1, \sigma A_3 \rangle, \langle \rho, \sigma A_1, \tau A_2 A_3 \rangle$$

for $s = 1, \delta$ and

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

M_1-braces given by

$$\langle \rho, \sigma, \tau A_3 \rangle, \langle \rho, \sigma, \tau A_2 A_3 \rangle, \left\langle \rho, \sigma^{t_2} \tau^s A_1, \sigma A_3 \right\rangle,$$

$$\left\langle \rho, \sigma A_1, \tau^{-1} A_3 \right\rangle, \langle \rho, \sigma A_1, \tau A_2 \rangle, \left\langle \rho, \sigma A_1, \tau^{t_3} A_2 A_3 \right\rangle$$

for $s = 1, \delta,\ t_2 = 1, ..., \frac{1}{2}(p-1)$, $t_3 = 2, ..., p-1$, where $C_p^3 = \langle \tau, \sigma, \rho \rangle$ and A_1, A_2, A_3 given as in Section 4.3.

Proof. Follows from Section 4.3. □

Theorem 4.6.9. *The skew braces of M_1 type are precisely*

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

M_1-braces given, as regular subgroups of the holomorph, by

$$\langle \rho, \sigma, \tau \rangle, \langle \rho, \tau, \sigma \alpha_1 \rangle, \langle \rho, \tau, \sigma \alpha_2 \rangle, \langle \rho, \tau, \sigma \alpha_3^c \rangle, \langle \rho, \tau, \sigma \alpha_2 \alpha_3^c \rangle,$$

$$\langle \rho, \sigma \alpha_1, \sigma^{u_3} \tau^{u_4} \alpha_3 \rangle, \left\langle \rho, \tau^{-u_5} \alpha_1, \sigma^{u_5} \alpha_3 \right\rangle, \langle \rho, \tau^{x_3} \alpha_1, \sigma \alpha_2 \alpha_3^a \rangle, \left\langle \tau^{-2} \alpha_1, \rho^s \tau \alpha_2, \sigma^2 \tau^{t_3} \alpha_3 \right\rangle$$

for $c = 2, ..., p-1$, $a, u_4 = 0, ..., p-1$, $u_2, u_3, u_4, x_3 = 1, ..., p-1$, $t_3 = 0, 1$, $s = 1, \delta$, with $u_5 \neq 2$, $u_3 \not\equiv -u_4$, $ax_3 \not\equiv (1 + x_3)$ and

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

C_p^3-braces given by

$$\langle \rho, \tau, \sigma \alpha_3 \rangle, \langle \rho, \tau, \sigma \alpha_2 \alpha_3 \rangle$$

$$\langle \rho, \sigma \alpha_1, \sigma^{u_2} \tau^{u_2} \alpha_3 \rangle, \left\langle \rho, \tau^{-2} \alpha_1, \sigma^2 \alpha_3 \right\rangle, \left\langle \rho, \tau^{x_3} \alpha_1, \sigma \alpha_2 \alpha_3^{(1+x_3)x_3^{-1}} \right\rangle$$

for $s = 1, \delta$, $u_2, x_3 = 1, ..., p-1$, where $M_1 = \langle \rho, \sigma, \tau \rangle$ and $\alpha_1, \alpha_2, \alpha_3$ as given in Section 4.4.

Proof. Follows from Section 4.4. □

Theorem 4.6.10. *The skew braces of M_2 type are precisely*

$$\widetilde{e}(M_2, M_2) = 4p^2 - 3p - 1$$

M_2-braces given, as regular subgroups of the holomorph, by

$$\langle \sigma, \tau \rangle, \langle \tau, \sigma\alpha_1 \rangle, \langle \tau, \sigma\alpha_2^s \rangle, \langle \tau, \sigma\alpha_3^c \rangle, \langle \tau, \sigma\alpha_2^s\alpha_3^c \rangle, \left\langle \sigma, \tau\alpha_1^b \right\rangle, \langle \sigma, \tau\alpha_1^a\alpha_3 \rangle,$$

$$\langle \tau^{u_2}\alpha_1, \sigma^{v_1}\alpha_3 \rangle, \left\langle \tau^{-t_1}\alpha_1, \sigma^{t_1}\tau^{t_2}\alpha_3 \right\rangle, \left\langle \sigma\alpha_1, \sigma^{t_3}\tau^{t_4}\alpha_3 \right\rangle, \left\langle \tau^{x_2}\alpha_1, \sigma^s\alpha_2\alpha_3^d \right\rangle$$

for $s = 1, \delta$, $a = 0, ..., p-2$, $b = 1, ..., p-2$, $c = 2, ..., p-1$, $d, t_3 = 0, ..., p-1$, $u_2, v_1, v_4, t_1, t_4, x_2 = 1, ..., p-1$, $t_2 = 0, 1$ with $u_2 \not\equiv -v_1$, $u_2 \not\equiv v_1(1+u_2)$, $t_3 \not\equiv t_4$, $dx_2 \not\equiv s(1+x_2)$, $t_1 \neq 2$ and

$$\widetilde{e}(C_{p^2} \times C_p, M_2) = 4p + 1$$

$(C_{p^2} \times C_p)$-braces given by

$$\langle \tau, \sigma\alpha_3 \rangle, \langle \tau, \sigma\alpha_2^s\alpha_3 \rangle, \left\langle \sigma, \tau\alpha_1^{-1} \right\rangle, \left\langle \sigma, \tau\alpha_1^{-1}\alpha_3 \right\rangle,$$

$$\left\langle \tau^{u_4}\alpha_1, \sigma^{u_4(1+u_4)^{-1}}\alpha_3 \right\rangle, \left\langle \tau^{-2}\alpha_1, \sigma^2\tau\alpha_3 \right\rangle, \langle \sigma\alpha_1, \sigma^{u_3}\tau^{u_3}\alpha_3 \rangle, \left\langle \tau^{x_2}\alpha_1, \sigma^s\alpha_2\alpha_3^{s(1+x_2)x_2^{-1}} \right\rangle$$

for $s = 1, \delta$, $u_3, x_2, u_4 = 1, ..., p-1$ with $u_4 \neq p-1$, where $M_2 = \langle \sigma, \tau \rangle$ and $\alpha_1, \alpha_2, \alpha_3$ as given in Section 4.5.

Proof. Follows from Section 4.5. □

In the next subsection we shall provide a summary of our results and discuss the patterns revealed by them.

4.6.1 Discussion on the results and further questions

Our theorems can be summarised in the following two tables

$e(G,N)$	C_{p^3}	$C_{p^2} \times C_p$	C_p^3	M_1	M_2
C_{p^3}	p^2				
$C_{p^2} \times C_p$		$(2p-1)p^2$			$(2p-1)(p-1)p^2$
C_p^3			$(p^4+p^3-1)p^2$	$(p^3-1)(p^2+p-1)p^2$	
M_1			$(p^2+p-1)p^2$	$(2p^3-3p^2+1)p^2$	
M_2		$(2p-1)p^2$			$(2p-1)(p-1)p^2$

Table 4.1: Number of Hopf-Galois structures of order p^3 for $p > 3$

$\widetilde{e}(G,N)$	C_{p^3}	$C_{p^2} \times C_p$	C_p^3	M_1	M_2
C_{p^3}	3				
$C_{p^2} \times C_p$		9			$4p+1$
C_p^3			5	$2p+1$	
M_1			$2p+1$	$2p^2-p-3$	
M_2		$4p+1$			$4p^2-3p-1$

Table 4.2: Number of skew braces of order p^3 for $p > 3$

where rows correspond to G and columns to N. Note, immediately we observe that the number of Hopf-Galois structures are all divisible by p^2, and that the number of skew braces are symmetric along the diagonal. Furthermore, for the groups with two generators, i.e., $C_{p^2} \times C_p$ and M_2, we have

$$\begin{aligned} e(C_{p^2} \times C_p, C_{p^2} \times C_p) &= e(M_2, C_{p^2} \times C_p) \text{ and} \\ e(C_{p^2} \times C_p, M_2) &= e(M_2, M_2). \end{aligned} \tag{4.101}$$

In fact we observe the same patterns when looking at values of $e(G, N, m)$ and $\widetilde{e}(G, N, m)$ for $m = 1, p, p^2, p^3$, and we have the following. First we observe

$$e(G, G, 1) = \widetilde{e}(G, G, 1) = 1 \text{ and } e(G, N, 1) = \widetilde{e}(G, N, 1) = 0 \text{ if } G \neq N,$$

also

$$e(G, N, p^3) = \widetilde{e}(G, N, p^3) = 0 \text{ if } G \neq M_1 \text{ or } N \neq M_1,$$

and we have

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

Next, we find a relationship between $e(G, N, m)$ and $e(N, G, m)$, which is

$$e(G, N, m) = \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|} e(N, G, m); \tag{4.102}$$

and furthermore, for skew braces we have

$$\widetilde{e}(G, N, m) = \widetilde{e}(N, G, m). \tag{4.103}$$

Therefore, one may wish to ask the following questions

1. To what extent the pattern of (4.101) holds for p-groups generated by two elements?
2. To what extent the formula of (4.102) holds for p-groups?
3. To what extent the duality of (4.103) is valid for p-skew braces?

The following subsection gives some explanations for (4.103).

4.6.2 Skew braces of semi-direct product type

Here we provide some reasons as to why our table containing the number of skew braces is symmetric along the diagonal and investigate this for more general settings.

First we note that according to [SV17, Example 1.6], if H and N are groups, and

$$\beta : H \longrightarrow \mathrm{Aut}\,(N)$$

is a group homomorphism, then the set $N \times H$ with

$$\begin{aligned}(n_1, h_1) \oplus (n_2, h_2) &\stackrel{\text{def}}{=} (n_1 n_2, h_1 h_2)\,,\\ (n_1, h_1) \odot (n_2, h_2) &\stackrel{\text{def}}{=} (n_1 \beta_{h_1}(n_2), h_1 h_2)\end{aligned}$$

is a skew brace; furthermore, the set $N \times H$ with

$$\begin{aligned}(n_1, h_1) \oplus (n_2, h_2) &\stackrel{\text{def}}{=} (n_1 \beta_{h_1}(n_2), h_1 h_2)\,,\\ (n_1, h_1) \odot (n_2, h_2) &\stackrel{\text{def}}{=} (n_1 n_2, h_2 h_1)\end{aligned}$$

is a skew brace. Therefore, the set $N \times H$ can be made into a skew braces in two different ways: first is when $(N \times H, \oplus) \cong N \times H$ and $(N \times H, \odot) \cong N \rtimes_\beta H$, and second is when $(N \times H, \oplus) \cong N \rtimes_\beta H$ and $(N \times H, \odot) \cong N \times H$, i.e., through β we get a $(N \rtimes_\beta H)$-skew brace of type $N \times H$ and a $(N \times H)$-skew brace of type $N \rtimes_\beta H$. This fact may explain why our table for the number of skew braces is symmetric along the diagonal since we investigate groups of the form $C_p^2 \rtimes C_p$ and $C_{p^2} \rtimes C_p$. However, we shall show that a more general statement to above holds, where instead of using one group homomorphism we can use two.

We shall show that for two groups H and N together with two group homomorphisms $\alpha, \beta : H \longrightarrow \mathrm{Aut}\,(N)$, if α and β satisfy certain properties, we can make $N \times H$ into two different skew braces using α, β, similar to the above (note in the above example α is the trivial homomorphism). This shows that in some situations one can swap the skew brace structure with the skew brace type. More precisely, we prove that if H and N are groups, $\alpha, \beta : H \longrightarrow \mathrm{Aut}\,(N)$ are group homomorphisms such that $\mathrm{Im}\,\alpha$ is an abelian group, and $[\mathrm{Im}\,\alpha, \mathrm{Im}\,\beta] = 1$, then the set $N \times H$ together with the operations

$$\begin{aligned}(n_1, h_1) \oplus (n_2, h_2) &\stackrel{\text{def}}{=} (n_1 \alpha_{h_1}(n_2), h_1 h_2)\,,\\ (n_1, h_1) \odot (n_2, h_2) &\stackrel{\text{def}}{=} (n_1 \beta_{h_1}(n_2), h_1 h_2)\end{aligned}$$

is a skew brace; furthermore, the set $N \times H$ together with the operations

$$\begin{aligned}(n_1, h_1) \oplus (n_2, h_2) &\stackrel{\text{def}}{=} (n_1 \beta_{h_1}(n_2), h_1 h_2)\,,\\ (n_1, h_1) \odot (n_2, h_2) &\stackrel{\text{def}}{=} (n_1 \alpha_{h_1}(n_2), h_2 h_1)\,.\end{aligned}$$

We show that we simultaneously find a $(N \rtimes_\beta H)$-skew brace of type $N \rtimes_\alpha H$ and a $(N \rtimes_\alpha H^{\mathrm{op}})$-skew brace of type $N \rtimes_\beta H$. Let us proceed with the proof of this. Thus,

we fix two groups H and N and two group homomorphisms $\alpha, \beta : H \longrightarrow \mathrm{Aut}\,(N)$. First we note the following.

Lemma 4.6.11. *The set $N \times H$ together with the operation $\odot$ given by*

$$(n_1, h_1) \odot (n_2, h_2) \stackrel{\text{def}}{=} (n_1 \alpha_{h_1}(n_2), h_2 h_1)$$

is a group if and only if $\mathrm{Im}\,\alpha$*, the image of α, is an abelian group. Furthermore, in the case that* $\mathrm{Im}\,\alpha$ *is an abelian group, we have*

$$(N \times H, \odot) \cong N \rtimes_{\alpha} H^{\mathrm{op}};$$

also the map

$$\Psi : N \rtimes_{\alpha} H \longrightarrow (N \times H, \odot) \text{ given by } (n, h) \longrightarrow \left(n, h^{-1}\right)$$

is a homomorphism if and only if $\mathrm{Im}\,\alpha$ *has exponent 2.*

Proof. Let us check the associativity of $\odot$. After this it will be easy to see under what conditions $(N \times H, \odot)$ is a group since the identity and inverses exist. Therefore, let $(n_1, h_1), (n_2, h_2), (n_3, h_3) \in N \times H$ be arbitrary elements. Then we have

$$\begin{aligned}
(n_1, h_1) \odot ((n_2, h_2) \odot (n_3, h_3)) &= (n_1, h_1) \odot (n_2 \alpha_{h_2}(n_3), h_3 h_2) \\
&= (n_1 \alpha_{h_1}(n_2) \alpha_{h_1 h_2}(n_3), h_3 h_2 h_1) \text{ while} \\
((n_1, h_1) \odot (n_2, h_2)) \odot (n_3, h_3) &= (n_1 \alpha_{h_1}(n_2), h_2 h_1) \odot (n_3, h_3) \\
&= (n_1 \alpha_{h_1}(n_2) \alpha_{h_2 h_1}(n_3), h_3 h_2 h_1)\,;
\end{aligned}$$

thus, $(N \times H, \odot)$ is associative if and only if

$$\alpha_{h_1 h_2}(n_3) = \alpha_{h_2 h_1}(n_3) \text{ for all } h_1, h_2 \in H \text{ and } n_3 \in N,$$

which is true if and only if

$$\alpha_{h_1 h_2} = \alpha_{h_1} \alpha_{h_2} = \alpha_{h_2} \alpha_{h_1} = \alpha_{h_2 h_1} \text{ for all } h_1, h_2 \in H,$$

which is true if and only if $\mathrm{Im}\,\alpha$ is an abelian group. This proves the first statement.

To prove the second statement let us suppose that $\mathrm{Im}\,\alpha$ is an abelian group. Let $(n_1, h_1), (n_2, h_2) \in N \times H$ be arbitrary elements. To prove the first part we note that N is a normal subgroup of $(N \times H, \odot)$, which gives rise to the exact sequence

$$1 \longrightarrow N \longrightarrow (N \times H, \odot) \longrightarrow H^{\mathrm{op}} \longrightarrow 1.$$

This exact sequence is a split by the homomorphism $H^{\mathrm{op}} \longrightarrow (N \times H, \odot)$ which maps $h \longmapsto (1, h)$, so we have $(N \times H, \odot) \cong N \rtimes H^{\mathrm{op}}$. One can check that the

action of H^{op} on N is given by α.

Finally, the map Ψ is a group homomorphism if and only if

$$\begin{aligned}\Psi\left(n_1\alpha_{h_1}(n_2), h_1h_2\right) &= \left(n_1\alpha_{h_1}(n_2), (h_1h_2)^{-1}\right) = \\ \Psi\left(n_1, h_1\right) \odot \Psi\left(n_2, h_2\right) &= \left(n_1\alpha_{h_1^{-1}}(n_2), (h_1h_2)^{-1}\right),\end{aligned}$$

so the second statement is proved if and only if

$$\alpha_{h_1}(n_2) = \alpha_{h_1^{-1}}(n_2) \text{ for all } h_1 \in H \text{ and } n_2 \in N,$$

which is true if and only if

$$\alpha_{h_1} = \alpha_{h_1^{-1}} \text{ for all } h_1 \in H$$

which is true if and only if $\operatorname{Im}\alpha$ has exponent 2. □

For the rest of our calculations we shall assume that $\operatorname{Im}\alpha$ is an abelian group, and so by Lemma 4.6.11, the set $N \times H$ together with the operation $\odot$ given by

$$(n_1, h_1) \odot (n_2, h_2) \stackrel{\text{def}}{=} (n_1\alpha_{h_1}(n_2), h_2h_1)$$

is a group. Now we have the following proposition.

Proposition 4.6.12. *The set $N \times H$ together with the operations*

$$\begin{aligned}(n_1, h_1) \oplus (n_2, h_2) &\stackrel{\text{def}}{=} (n_1\alpha_{h_1}(n_2), h_1h_2), \\ (n_1, h_1) \odot (n_2, h_2) &\stackrel{\text{def}}{=} (n_1\beta_{h_1}(n_2), h_1h_2)\end{aligned}$$

is a skew brace, furthermore, the set $N \times H$ together with the operations

$$\begin{aligned}(n_1, h_1) \oplus (n_2, h_2) &\stackrel{\text{def}}{=} (n_1\beta_{h_1}(n_2), h_1h_2), \\ (n_1, h_1) \odot (n_2, h_2) &\stackrel{\text{def}}{=} (n_1\alpha_{h_1}(n_2), h_2h_1)\end{aligned}$$

is a skew brace, if and only if $[\operatorname{Im}\alpha, \operatorname{Im}\beta] = 1$.

Proof. Let use prove the first part. It is clear that

$$(N \times H, \oplus) = N \rtimes_\alpha H \text{ and } (N \times H, \odot) = N \rtimes_\beta H.$$

Now let $(n_1, h_1), (n_2, h_2), (n_3, h_3) \in N \times H$ be arbitrary elements. Then we have

$$\begin{aligned}(n_1, h_1) \odot ((n_2, h_2) \oplus (n_3, h_3)) &= (n_1, h_1) \odot (n_2\alpha_{h_2}(n_3), h_2h_3) \\ &= (n_1\beta_{h_1}(n_2)\beta_{h_1}\left(\alpha_{h_2}(n_3)\right), h_1h_2h_3),\end{aligned}$$

on the other hand we have

$$\begin{aligned}
&((n_1,h_1)\odot(n_2,h_2))\ominus(n_1,h_1)\oplus((n_1,h_1)\odot(n_3,h_3))\\
&=(n_1\beta_{h_1}(n_2),h_1h_2)\oplus\left(\alpha_{h_1^{-1}}(n_1^{-1}),h_1^{-1}\right)\oplus(n_1\beta_{h_1}(n_3),h_1h_3)\\
&=\left(n_1\beta_{h_1}(n_2)\alpha_{h_1h_2}(\alpha_{h_1^{-1}}(n_1^{-1})),h_1h_2h_1^{-1}\right)\oplus(n_1\beta_{h_1}(n_3),h_1h_3)\\
&=\left(n_1\beta_{h_1}(n_2)\alpha_{h_1h_2h_1^{-1}}(n_1^{-1})\alpha_{h_1h_2h_1^{-1}}(n_1\beta_{h_1}(n_3)),h_1h_2h_1^{-1}h_1h_3\right)\\
&=(n_1\beta_{h_1}(n_2)\alpha_{h_2}(\beta_{h_1}(n_3)),h_1h_2h_3)\,,
\end{aligned}$$

thus the first set of operations make $N\times H$ into a skew braces if and only if

$$\beta_{h_1}\left(\alpha_{h_2}(n_3)\right)=\alpha_{h_2}(\beta_{h_1}(n_3))\text{ for all }h_1,h_2\in H\text{ and }n_3\in N,$$

i.e., if and only if

$$\beta_{h_1}\alpha_{h_2}=\alpha_{h_2}\beta_{h_1}\text{ for all }h_1,h_2\in H,$$

which is true if and only if $[\operatorname{Im}\alpha,\operatorname{Im}\beta]=1$.

Similarly, let us consider the second set of operations. It is clear that $(N\times H,\oplus)=N\rtimes_\beta H$, and by Lemma 4.6.11, we know that $(N\times H,\odot)$ is a group, which is isomorphic to $N\rtimes_\alpha H^{\mathrm{op}}$. Now we have

$$\begin{aligned}
(n_1,h_1)\odot((n_2,h_2)\oplus(n_3,h_3))&=(n_1,h_1)\odot(n_2\beta_{h_2}(n_3),h_2h_3)\\
&=(n_1\alpha_{h_1}(n_2)\alpha_{h_1}\left(\beta_{h_2}(n_3)\right),h_2h_3h_1)\,,
\end{aligned}$$

on the other hand we have

$$\begin{aligned}
&((n_1,h_1)\odot(n_2,h_2))\ominus(n_1,h_1)\oplus((n_1,h_1)\odot(n_3,h_3))\\
&=(n_1\alpha_{h_1}(n_2),h_2h_1)\oplus\left(\beta_{h_1^{-1}}(n_1^{-1}),h_1^{-1}\right)\oplus(n_1\alpha_{h_1}(n_3),h_3h_1)\\
&=\left(n_1\alpha_{h_1}(n_2)\beta_{h_2h_1}(\beta_{h_1^{-1}}(n_1^{-1})),h_2h_1h_1^{-1}\right)\oplus(n_1\alpha_{h_1}(n_3),h_3h_1)\\
&=\left(n_1\alpha_{h_1}(n_2)\beta_{h_2}(n_1^{-1})\beta_{h_2}(n_1\alpha_{h_1}(n_3)),h_2h_3h_1\right)\\
&=(n_1\alpha_{h_1}(n_2)\beta_{h_2}(\alpha_{h_1}(n_3)),h_2h_3h_1)\,,
\end{aligned}$$

thus the second set of operations make $N\times H$ into a skew braces if and only if

$$\alpha_{h_1}\left(\beta_{h_2}(n_3)\right)=\beta_{h_2}(\alpha_{h_1}(n_3))\text{ for all }h_1,h_2\in H\text{ and }n_3\in N,$$

i.e., if and only if

$$\alpha_{h_1}\beta_{h_2}=\beta_{h_2}\alpha_{h_1}\text{ for all }h_1,h_2\in H,$$

which is again true if and only if $[\operatorname{Im}\alpha,\operatorname{Im}\beta]=1$. □

4.6.3 A future research plan

One of our future research plans is to establish to what extent the patterns observed in our results are general and to expand our current results, by studying, initially, certain Hopf-Galois structures and skew braces of order p^n, for some prime $p > 2$, whose type has at most three generators. More precisely, we would like to study Hopf-Galois structures and skew braces whose type is given as a semi-direct product of the cyclic group of order p acting on an abelian group of order some power of p which has at most two generators. This we deem possible since in our thesis, for a prime p, we have studied Hopf-Galois structures and skew braces whose type is given as

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

subject to $e + f \leq 2$, where $e \geq 0$ and $f \geq 0$ are integers, and we aim to generalise these results by relaxing the restrictions on e and f.

We believe that the outcome of above proposed plans will advance our understanding of the classification of Hopf-Galois structures and p-skew braces, and also shed light on how one might approach when aiming to understand semi-direct type skew braces, at least for simple cases. If successful, our goal is to continue studying more complex p-skew braces, in particular how one can create skew braces via extension of smaller skew braces, at least for p-skew braces.

Chapter 5

Hopf-Galois structures and skew braces of order p^2 and p^3: special cases

In this chapter we study Hopf-Galois structures and skew braces of order p^2, 8, and 27.

5.1 Main results II: special cases

The main results, some which are known, but we have reproduced here for completeness, are the following.

Theorem 5.1.1. *Let L/K be a cyclic extension of fields of degree p^2 for a prime p. Then for $p > 2$ the extension L/K admits precisely p Hopf-Galois structures all of which are of cyclic type.*

For $p = 2$ the extension L/K admits precisely one Hopf-Galois structure of cyclic type and one Hopf-Galois structure of elementary abelian type.

Theorem 5.1.2. *Let L/K be an elementary abelian extension of fields of degree p^2 for a prime p. Then for $p > 2$ the extension L/K admits precisely p^2 Hopf-Galois structures all of which are of elementary abelian type.*

For $p = 2$ the extension L/K admits precisely one Hopf-Galois structure of elementary abelian type and three Hopf-Galois structures of cyclic type.

We remark that these two theorems were originally proved by Byott in [Byo96].

Theorem 5.1.3. *Let L/K be a Galois extension of fields of degree 27 with Galois group G. Then $e(G,N)$ is given by the table*

$e(G,N)$	C_{27}	$C_9 \times C_3$	C_3^3	M_1	M_2
C_{27}	9				
$C_9 \times C_3$		39	6	12	78
C_3^3		624	339	1300	1248
M_1		48	51	317	96
M_2		39	6	12	78

Table 5.1: Number of Hopf-Galois structures of order 27

where rows correspond to G and columns to N.

The results corresponding to the classification of skew braces of order 27 are the following.

Theorem 5.1.4. *Let G be a group of order 27. Then $\widetilde{e}(G,N)$ is given by the table*

$\widetilde{e}(G,N)$	C_{27}	$C_9 \times C_3$	C_3^3	M_1	M_2
C_{27}	3				
$C_9 \times C_3$		8	1	2	11
C_3^3		1	4	5	2
M_1		2	5	14	4
M_2		11	2	4	22

Table 5.2: Number of skew braces of order 27

where rows correspond to G and columns to N.

In the table in Theorem 5.1.4, results in the first three columns also follow from [Bac15, Theorem 3.2]. The final two columns are new results in the classification of skew braces. However we remark that we noticed two errors in [Bac15, Theorem 3.2, 2]: first one is in [Bac15, Theorem 3.2, 2, Socle of order p^2] where for $p = 3$ the final brace should be, using Bachiller's notation, $M(p)$ brace (or M_1 brace) rather than $M_3(p)$ brace (or M_2 brace), and second one is in [Bac15, Theorem 3.2, 2, Socle of order p^3] the brace should be, using Bachiller's notation, $\mathbb{Z}/(p) \times \mathbb{Z}/(p^2)$ rather than $M_3(p)$. For $p = 2$ we have the following theorems on the next page.

Theorem 5.1.5. *Let L/K be a Galois extension of fields of degree 8 with Galois group G. Then $e(G,N)$ is given by the table*

$e(G,N)$	C_8	$C_4 \times C_2$	C_2^3	D_8	Q_8
C_8	2			2	2
$C_4 \times C_2$	4	10	4	6	2
C_2^3		42	8	42	14
D_8	2	14	6	6	2
Q_8	6	6	2	6	2

Table 5.3: Number of Hopf-Galois structures of order 8

where rows correspond to G and columns to N.

In the table in Theorem 5.1.5 results in the first row also follows from [Byo07, Theorem 5.1]. The rest of the four rows are new results. The results corresponding to the classification of skew braces of order 8 are the following.

Theorem 5.1.6. *Let G be a group of order 8. Then $\widetilde{e}(G,N)$ is given by the table*

$\widetilde{e}(G,N)$	C_8	$C_4 \times C_2$	C_2^3	D_8	Q_8
C_8	2			2	2
$C_4 \times C_2$	1	6	3	3	1
C_2^3		2	2	1	1
D_8	1	5	2	4	2
Q_8	1	1	1	2	2

Table 5.4: Number of skew braces of order 8

where rows correspond to G and columns to N.

The rest of the sections through to the end of the document are dedicated to proving the above theorems. In Section 5.2, we determine Hopf-Galois structures and skew braces of C_{2^n} for $n = 2, 3$. In Section 5.3, we determine Hopf-Galois structures and skew braces of type C_p^2, C_3^3 and C_2^3. In Section 5.4, we determine Hopf-Galois structures and skew braces of type $C_9 \times C_3$ and $C_4 \times C_2$. In Section 5.5, we determine Hopf-Galois structures and skew braces of type M_1 for $p = 3$. In Section 5.6, we determine Hopf-Galois structures and skew braces of type M_2 for $p = 3$. In Section 5.7, we determine Hopf-Galois structures and skew braces of type D_8. Finally, In Section 5.8, we determine Hopf-Galois structures and skew braces of type Q_8 for $p = 3$.

5.2 Regular subgroups in Hol(C_{2^n})

In this section we find the regular subgroups contained in Hol(C_{2^n}) for $n = 2, 3$ and the corresponding braces. The main result of this section is the following.

Proposition 5.2.1. *For $n = 2$ we have*

$$e(C_4, C_4) = 1 \text{ and } e(C_2^2, C_4) = 3.$$

Furthermore, we have

$$\widetilde{e}(C_4, C_4) = 1 \text{ and } \widetilde{e}(C_2^2, C_4) = 1.$$

For $n = 3$ we have $e(C_8, C_8) = 2$,

$$e(C_{2^2} \times C_2, C_8) = 4,\ e(D_8, C_8) = 2,\ e(Q_8, C_8) = 6,$$

and $e(G, C_8) = 0$ otherwise. Furthermore, we have $\widetilde{e}(C_8, C_8) = 2$,

$$\widetilde{e}(C_4 \times C_2, C_8) = 1,\ \widetilde{e}(D_8, C_8) = 1,\ \widetilde{e}(Q_8, C_8) = 1,$$

and $\widetilde{e}(G, C_8) = 0$ otherwise.

The proof of the proposition above follows from calculations in the rest of this section. We use the identification

$$C_{2^n} \cong \mathbb{Z}/2^n\mathbb{Z} \text{ given by } \sigma \longrightarrow 1 \bmod 2^n.$$

By Lemma 3.1.1, we may identify the holomorph of C_{p^n} with

$$\mathrm{Hol}(C_{2^n}) = \{[t, \beta] : t \in \mathbb{Z}/2^n\mathbb{Z},\ \beta \in \mathrm{Aut}(C_{2^n})\} \cong (\mathbb{Z}/2^n\mathbb{Z}) \rtimes (C_{2^{n-2}} \times C_2).$$

Note, the image of a subgroup of Hol(C_{2^n}) of order 2^n in Aut(C_{2^n}) under the natural projection

$$\Theta : \mathrm{Hol}(C_{2^n}) \longrightarrow \mathrm{Aut}(C_{2^n})$$

must lie in

$$\langle \alpha_1, \alpha_2 \rangle \cong C_{2^{n-2}} \times C_2, \text{ where } \alpha_1(1) = 5 \text{ and } \alpha_2(1) = -1.$$

Note if $n = 2$ and G is a regular subgroup contained in Hol(C_4), then G must be one of the

$$\langle [1, \mathrm{id}] \rangle \cong C_4,\ \langle [2, \mathrm{id}], [1, \alpha_2] \rangle \cong C_2^2$$

and from this follows the first part of Proposition 5.2.1.

Lemma 5.2.2. *For $n = 3$ inside* Hol(C_8) *there are two cyclic regular subgroups, two isomorphic to $C_4 \times C_2$, one isomorphic to D_8 and one isomorphic to Q_8 given by*

$$\langle [1, \mathrm{id}] \rangle, \langle [2, \mathrm{id}], [1, \alpha_1] \rangle \cong C_8,\ \langle [2, \mathrm{id}], [1, \alpha_2] \rangle \cong D_8,$$

$$\langle [2,\mathrm{id}],[1,\alpha_1\alpha_2]\rangle \cong D_8,\ \langle [v_1,\alpha_1],[-v_1,\alpha_2]\rangle \cong C_4\times C_2 \text{ for } v_1=1,3.$$

Furthermore, there are two C_8, one $C_4\times C_2$, one D_8, and one Q_8-braces of C_8 type.

Proof. If $G\subseteq \mathrm{Hol}(C_8)$ with $|\Theta(G)|=1$, then we must have $G=\langle [1,\mathrm{id}]\rangle$.

If $G\subseteq \mathrm{Hol}(C_8)$ with $|\Theta(G)|=2$, then we must have that G is one of the following

$$\langle [2,\mathrm{id}],[1,\alpha_1]\rangle \cong C_8,\ \langle [2,\mathrm{id}],[1,\alpha_2]\rangle \cong D_8, \langle [2,\mathrm{id}],[1,\alpha_1\alpha_2]\rangle \cong Q_8.$$

If $G\subseteq \mathrm{Hol}(C_8)$ with $|\Theta(G)|=4$, then we must have that

$$G=\langle [4,\mathrm{id}],[v_1,\alpha_1],[v_2,\alpha_2]\rangle$$

and for G to be regular it must be one of the following

$$\langle [v_1,\alpha_1],[-v_1,\alpha_2]\rangle \cong C_4\times C_2 \text{ for } v_1=1,3.$$

Therefore, there are two cyclic regular subgroups, two isomorphic to $C_4\times C_2$, one isomorphic to Q_8, and one isomorphic to D_8. The corresponding non-isomorphic braces are easily found. □

Corollary 5.2.3. *For $p=2$ we have $e(C_8,C_8,1)=1$,*

$$\begin{aligned} e(C_8,C_8,2)&=1,\\ e(C_4\times C_2,C_8,4)&=4,\\ e(D_8,C_8,2)&=2,\\ e(Q_8,C_8,2)&=6, \end{aligned}$$

and $e(G,C_8,2^{n-m})=0$ otherwise.

Furthermore, we have $\widetilde{e}(C_8,C_8,1)=1$,

$$\begin{aligned} \widetilde{e}(C_8,C_8,2)&=1,\\ \widetilde{e}(C_4\times C_2,C_8,4)&=1,\\ \widetilde{e}(D_8,C_8,2)&=1,\\ \widetilde{e}(Q_8,C_8,2)&=1, \end{aligned}$$

and $\widetilde{e}(G,C_8,2^{n-m})=0$ otherwise.

Proof. Follows from Lemma 5.2.2, and the formula

$$e(G,C_8,2^{3-m}) \overset{\text{def}}{=} \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(C_8)|}e'(G,C_8,2^{3-m}).$$

□

5.3 Regular subgroups in $\mathrm{Hol}(C_{p^2} \times C_p)$ for special cases

In this section we find the regular subgroups contained in $\mathrm{Hol}(C_{p^2} \times C_p)$, for $p = 2, 3$, and the corresponding braces of $C_{p^2} \times C_p$ type. The main result of this section is the following.

Proposition 5.3.1. *For $p = 3$ we have*

$$\begin{aligned} e(C_{p^2} \times C_p, C_{p^2} \times C_p) &= 39, \\ e(M_2, C_{p^2} \times C_p) &= 39, \\ e(C_p^3, C_{p^2} \times C_p) &= 624, \\ e(M_1, C_{p^2} \times C_p) &= 48, \end{aligned}$$

and $e(C_{p^3}, C_p^3) = 0$. Furthermore, we have

$$\begin{aligned} \widetilde{e}(C_{p^2} \times C_p, C_{p^2} \times C_p) &= 8, \\ \widetilde{e}(M_2, C_{p^2} \times C_p) &= 11, \\ \widetilde{e}(C_p^3, C_{p^2} \times C_p) &= 1, \\ \widetilde{e}(M_1, C_{p^2} \times C_p) &= 2, \end{aligned}$$

and $\widetilde{e}(C_{p^3}, C_p^3) = 0$.

For $p = 2$ we have

$$\begin{aligned} e(C_{p^2} \times C_p, C_{p^2} \times C_p) &= 10, \\ e(D_8, C_{p^2} \times C_p) &= 14, \\ e(C_p^3, C_{p^2} \times C_p) &= 42, \\ e(Q_8, C_{p^2} \times C_p) &= 6, \end{aligned}$$

and $e(C_{p^3}, C_p^3) = 0$. Furthermore, we have

$$\begin{aligned} \widetilde{e}(C_{p^2} \times C_p, C_{p^2} \times C_p) &= 6, \\ \widetilde{e}(D_8, C_{p^2} \times C_p) &= 5, \\ \widetilde{e}(C_p^3, C_{p^2} \times C_p) &= 2, \\ \widetilde{e}(Q_8, C_{p^2} \times C_p) &= 1, \end{aligned}$$

and $\widetilde{e}(C_{p^3}, C_p^3) = 0$.

The proof of proposition above follows from calculations in the rest of this section. We shall use the notation of Section 4.2. Recall a subgroup of $\mathrm{Hol}(C_{p^2} \times C_p)$ of order

p^3 lies in

$$(C_{p^2} \times C_p) \rtimes \langle \alpha_1, \alpha_2, \alpha_3 \rangle \cong (C_{p^2} \times C_p) \rtimes M_1.$$

Note, $M_1 \cong M_2 = D_8$ for $p = 2$.

We have

$$\begin{aligned} e(C_{p^2} \times C_p, C_{p^2} \times C_p, 1) = \widetilde{e}(C_{p^2} \times C_p, C_{p^2} \times C_p, 1) = 1 \text{ and} \\ e(G, C_{p^2} \times C_p, 1) = \widetilde{e}(G, C_{p^2} \times C_p, 1) = 0 \text{ if } G \neq C_{p^2} \times C_p. \end{aligned}$$

We shall deal with the cases $|\Theta(G)| = p, p^2, p^3$ in the following lemmas. Note, for natural numbers a_i and an element $v = v_1 e_1 + v_2 e_2 \in \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, we have

$$(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^p = \begin{cases} (1 + a_2 a_3)\, v_1 p e_1, & \text{if } p = 3 \\ (((1 + a_1)\, v_1 + a_3 v_2)\, p e_1 + a_2 v_1 e_2)\, \alpha_1^{a_2 a_3}, & \text{if } p = 2, \end{cases} \tag{5.1}$$

so the element $v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}$ can have order p or p^2 depending on various configurations, and this is the main difference in comparison to Section 4.2.

We further recall that any automorphism $\alpha \in \mathrm{Aut}(C_{p^2} \times C_p)$ can be written as

$$\alpha = \alpha_3^{r_3}\beta \text{ for some } \beta \stackrel{\text{def}}{=} \begin{pmatrix} b_1 & 0 \\ b_3 & b_4 \end{pmatrix} \in \mathrm{Aut}(C_{p^2} \times C_p)$$

and some integer r_3 which matters modulo p.

Now, for $p = 3$, we have

$$\alpha\,(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})\,\alpha^{-1} = \alpha \cdot v\alpha_1^{a_1 - a_3 b_3 b_4^{-1} + r_2 a_2 b_1^{-1} b_4} \alpha_2^{a_2 b_1^{-1} b_4} \alpha_3^{a_3 b_1 b_4^{-1}}, \text{ where}$$

$$\alpha \cdot v = b_1 v_1 e_1 + r_3\,(b_3 v_1 + b_4 v_2)\, p e_1 + (b_3 v_1 + b_4 v_2)\, e_2.$$

Similarly, for $p = 2$ we have

$$\alpha\,(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})\,\alpha^{-1} = \alpha \cdot v\alpha_1^{a_1 - a_3 b_3 + r_3 a_2}\alpha_2^{a_2}\alpha_3^{a_3}, \text{ where}$$

$$\alpha \cdot v = v_1 e_1 + r_3\,(b_3 v_1 + v_2)\, p e_1 + (b_3 v_1 + v_2)\, e_2.$$

Lemma 5.3.2. *For $p = 3$ and $|\Theta(G)| = p$ there are exactly*

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

regular subgroups isomorphic to $C_{p^2} \times C_p$,

$$(2p - 1)(p - 1)p$$

isomorphic to M_2, and $(p - 1)p$ isomorphic to M_1 contained in Hol($C_{p^2} \times C_p$). *Furthermore, there are three $C_{p^2} \times C_p$, four M_2, and one M_1-braces of $C_{p^2} \times C_p$ type.*

For $p = 2$ and $|\Theta(G)| = p$ there are exactly p^2 regular subgroups isomorphic to $C_{p^2} \times C_p$, p^2 isomorphic to D_8, one isomorphic to C_p^3, and p isomorphic to Q_8 contained in $\mathrm{Hol}(C_{p^2} \times C_p)$*. Furthermore, there are two $C_{p^2} \times C_p$, two D_8, one C_p^3, and one Q_8-braces of $C_{p^2} \times C_p$ type.*

Proof. If $G \subseteq \mathrm{Hol}(C_{p^2} \times C_p)$ with $|\Theta(G)| = p$, then we must have $\Theta(G) \subseteq \langle \alpha_1, \alpha_3, \alpha_2 \rangle$ a subgroup of order p and $G \cap (C_{p^2} \times C_p)$ a subgroup of order p^2. We classify the regular subgroups for $p = 3$ first and then do the same for $p = 2$. We also note that in places some of the calculations are similar to that of Lemma 4.2.2, where we have avoided repetitions of those calculations as much as possible.

Now for $p = 3$, we have that $\Theta(G)$ is one of

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

and $G \cap (C_{p^2} \times C_p)$ is one of

$$\langle pe_1, e_2 \rangle, \langle e_1 + de_2 \rangle \text{ for } d = 0, ..., p-1.$$

Let us consider a subgroup of the form

$$G = \langle pe_1, e_2, g \rangle \text{ where } g \stackrel{\text{def}}{=} e_1 \alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3}.$$

Using (5.1) we have $g^p = (1 + a_2 a_3)\, pe_1$, which implies that G has exponent p^2 if and only if $1 + a_2 a_3 \not\equiv 0 \bmod p$. Now for $r \neq 0$ we have

$$(e_1 \alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3})\,(re_2) = (ra_3 pe_1)\,(re_2)\,(e_1 \alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3}),$$

so G is abelian if and only if $a_3 = 0$.

Therefore, we find regular subgroups

$$\begin{aligned} &\langle e_2, e_1 \alpha_1^c \rangle, \langle e_2, e_1 \alpha_1^a \alpha_2^c \rangle \cong C_{p^2} \times C_p, \\ &\left\langle e_2, e_1 \alpha_1^a \alpha_2^b \alpha_3^c \right\rangle \cong M_2, \ \left\langle pe_1, e_2, e_1 \alpha_1^a \alpha_2^{-c^{-1}} \alpha_3^c \right\rangle \cong M_1 \\ &\text{for } a, b = 0, ..., p-1, \ c = 1, ..., p-1 \text{ with } b \neq -c^{-1}. \end{aligned}$$

Finally, we consider the subgroup $\langle e_1 + de_2 \rangle$ of $C_{p^2} \times C_p$ and investigate the possibility of pairing $\langle e_1 + de_2 \rangle$ with the groups $\langle \alpha_1 \rangle, \langle \alpha_1^a \alpha_2 \rangle, \left\langle \alpha_1^c \alpha_2^b \alpha_3 \right\rangle$. Note we need

$$\alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3} \cdot (e_1 + de_2) = (1 + a_1 p + a_3 dp)\, e_1 + (d + a_2)\, e_2 \in \langle e_1 + de_2 \rangle$$

which implies that we need $a_2 = 0$.

Therefore, we find regular subgroups

$$\left\langle e_1 + de_2, e_2\alpha_1^{-cd}\alpha_3^c \right\rangle \cong C_{p^2} \times C_p \text{ for } d = 0, ..., p-1,\ c = 1, ..., p-1,$$
$$\left\langle e_1 + d_1e_2, e_2\alpha_1^{a_1} \right\rangle, \left\langle e_1 + de_2, e_2\alpha_1^a\alpha_3^c \right\rangle \cong M_2$$
$$\text{for } a, d, d_1 = 0, ..., p-1,\ a_1, c = 1, ..., p-1, \text{ with } a + cd \not\equiv 0 \bmod p.$$

Therefore, if $G \subseteq \mathrm{Hol}(C_{p^2} \times C_p)$ is a regular subgroup with $|\Theta(G)| = p$ and $p = 3$, then G is isomorphic to either $C_{p^2} \times C_p$, M_2, or M_1. In particular, there are $(2p+1)(p-1)$ regular subgroups isomorphic to $C_{p^2} \times C_p$,

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

isomorphic to M_2, and $(p-1)p$ isomorphic to M_1.

The corresponding non-isomorphic braces for $p = 3$ are

$$\left\langle e_2, e_1\alpha_1 \right\rangle, \left\langle e_2, e_1\alpha_2 \right\rangle, \left\langle e_1, e_2\alpha_3 \right\rangle \cong C_{p^2} \times C_p,$$

$$\left\langle e_2, e_1\alpha_3 \right\rangle, \left\langle e_2, e_1\alpha_2\alpha_3 \right\rangle, \left\langle e_1, e_2\alpha_1 \right\rangle, \left\langle e_1, e_2\alpha_1\alpha_3 \right\rangle \cong M_2,\ \left\langle pe_1, e_2, e_1\alpha_2^2\alpha_3 \right\rangle \cong M_1.$$

For $p = 2$, we have that $\Theta(G)$ is one of

$$\langle \alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3} \rangle \text{ with } a_2a_3 = 0$$

and $G \cap (C_{p^2} \times C_p)$ is one of

$$\left\langle pe_1, e_2 \right\rangle, \left\langle e_1 + de_2 \right\rangle \text{ for } d = 0, 1.$$

Let us consider

$$G = \left\langle pe_1, e_2, g \right\rangle \text{ where } g \stackrel{\text{def}}{=} e_1\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3}.$$

Then using (5.1) we have $g^p = (1 + a_1)\, pe_1 + a_2e_2$. We also have

$$ge_2 = (a_3pe_1)\,(e_2)\,g,$$

so G is abelian if and only if $a_3 = 0$.

Therefore, we find regular subgroups

$$\left\langle pe_1, e_2, e_1\alpha_1^a\alpha_2 \right\rangle \cong C_{p^2} \times C_p,\ \left\langle pe_1, e_2, e_1\alpha_1 \right\rangle \cong C_p^3,\ \left\langle pe_1, e_2, e_1\alpha_1^a\alpha_3 \right\rangle \cong D_8.$$

Next, we can consider

$$G = \left\langle e_1 + de_2, e_2\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3} \right\rangle,$$

and as before we find that we need to set $a_2 = 0$. Then using (5.1) we have

$(e_2\alpha_1^{a_1}\alpha_3^{a_3})^p = a_3 p e_1$. We also have

$$(e_2\alpha_1^{a_1}\alpha_3^{a_3})\,(e_1 + de_2) = ((a_1 + a_3 d)\,pe_1)\,(e_1 + de_2)\,(e_2\alpha_1^{a_1}\alpha_3^{a_3})\,,$$

so G is abelian if and only $a_1 + a_3 d \equiv 0 \bmod p$.

Therefore, we find regular subgroups

$$\left\langle e_1 + de_2, e_2\alpha_1^d\alpha_3 \right\rangle \cong C_{p^2} \times C_p,\ \left\langle e_1 + de_2, e_2\alpha_1 \right\rangle \cong D_8,\ \left\langle e_1 + de_2, e_2\alpha_1^{d+1}\alpha_3 \right\rangle \cong Q_8.$$

The corresponding non-isomorphic braces for $p = 2$ are

$$\langle e_2, e_1\alpha_2 \rangle\,, \langle e_1, e_2\alpha_3 \rangle \cong C_{p^2} \times C_p,\ \langle pe_1, e_2, e_1\alpha_1 \rangle \cong C_p^3,$$

$$\langle e_2, e_1\alpha_3 \rangle\,, \langle e_1, e_2\alpha_1 \rangle \cong D_8,\ \langle e_1, e_2\alpha_1\alpha_3 \rangle \cong Q_8.$$

□

Corollary 5.3.3. *For $p = 3$ we have*

$$\begin{aligned} e(C_{p^2} \times C_p, C_{p^2} \times C_p, p) &= (2p+1)(p-1), \\ e(M_2, C_{p^2} \times C_p, p) &= (2p-1)p, \\ e(M_1, C_{p^2} \times C_p, p) &= (p-1)^3 p, \end{aligned}$$

and $e(G, C_{p^2} \times C_p, p) = 0$ otherwise. Furthermore, we have

$$\begin{aligned} \widetilde{e}(C_{p^2} \times C_p, C_{p^2} \times C_p, p) &= 3, \\ \widetilde{e}(M_2, C_{p^2} \times C_p, p) &= 4, \\ \widetilde{e}(M_1, C_{p^2} \times C_p, p) &= 1, \end{aligned}$$

and $\widetilde{e}(G, C_{p^2} \times C_p, p) = 0$ otherwise.

For $p = 2$ we have

$$\begin{aligned} e(C_{p^2} \times C_p, C_{p^2} \times C_p, p) &= p^2, \\ e(D_8, C_{p^2} \times C_p, p) &= p^2, \\ e(C_p^3, C_{p^2} \times C_p, p) &= (p^3-1)(p+1), \\ e(Q_8, C_{p^2} \times C_p, p) &= (p+1)p, \end{aligned}$$

and $e(C_{p^3}, C_{p^2} \times C_p, p) = 0$. *Furthermore, we have*

$$\begin{aligned}\widetilde{e}(C_{p^2} \times C_p, C_{p^2} \times C_p, p) &= 2,\\ \widetilde{e}(D_8, C_{p^2} \times C_p, p) &= 2,\\ \widetilde{e}(C_p^3, C_{p^2} \times C_p, p) &= 1,\\ \widetilde{e}(Q_8, C_{p^2} \times C_p, p) &= 1,\end{aligned}$$

and $\widetilde{e}(C_{p^3}, C_{p^2} \times C_p, p) = 0$.

Proof. Follows from Lemma 5.3.2. □

Remark 5.3.4. Comparing our results in the above lemma with [Bac15], we seem to find an error in [Bac15], which we have explained below. For $p = 3$, let us consider the subgroup

$$G = \left\langle pe_1, e_2, e_1\alpha_2^2\alpha_3 \right\rangle \subseteq \mathrm{Hol}(C_{p^2} \times C_p),$$

where

$$\alpha_2 \overset{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},\ \alpha_3 \overset{\text{def}}{=} \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \in \mathrm{Aut}(C_{p^2} \times C_p).$$

Note,

$$\begin{aligned}\alpha_2^2\alpha_3 \cdot e_2 &= \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & p \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} p \\ 1 \end{pmatrix} = \begin{pmatrix} p \\ 1 \end{pmatrix} = pe_1 + e_2,\\ \alpha_2^2\alpha_3 \cdot e_1 &= \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} = e_1 + 2e_2.\end{aligned}$$

The elements $pe_1, e_2 \in G$ have order p and

$$\begin{aligned}\left(e_1\alpha_2^2\alpha_3\right)^p &= \left(e_1\alpha_2^2\alpha_3\right)\left(e_1\alpha_2^2\alpha_3\right)\left(e_1\alpha_2^2\alpha_3\right)\\ &= \left(e_1\alpha_2^2\alpha_3\right)\left(\left(2e_2 + 2e_1\right)\left(\alpha_2^2\alpha_3\right)^2\right)\\ &= \left(e_1 + 2e_1 + 2pe_1\right)\left(\alpha_2^2\alpha_3\right)^3 = \left(pe_1 + 2pe_1\right) = 3pe_1 = 1,\end{aligned}$$

so the element $e_1\alpha_2^2\alpha_3 \in G$ also has order p; we further have

$$\left(e_1\alpha_2^2\alpha_3\right)e_2 = \left(e_2 + e_1 + pe_1\right)\alpha_2^2\alpha_3 = \left(pe_1\right)\left(e_2\right)\left(e_1\alpha_2^2\right);$$

thus $G \cong M_1$, and G is regular since $|\mathrm{Orb}(0)| > p^2$; but this is different to results obtained in [Bac15, Theorem 3.2, 2, Socle of order p^2] i.e., M_2. Hence, we verified that there is an inaccuracy in [Bac15, Theorem 3.2, 2, Socle of order p^2] for the final brace.

Lemma 5.3.5. *For* $p = 3$ *and* $|\Theta(G)| = p^2$ *there are exactly* $(p-1)^3p$ *regular subgroups isomorphic to* $C_{p^2} \times C_p$, $(p-1)^4p$ *isomorphic to* M_2, $(p-1)p$ *isomorphic*

to C_p^3, and $(p-1)p$ isomorphic to M_1 contained in $\mathrm{Hol}(C_{p^2} \times C_p)$. Furthermore, there are four $C_{p^2} \times C_p$, seven M_2, one C_p^3, and one M_1-braces of $C_{p^2} \times C_p$ type.

For $p = 2$ and $|\Theta(G)| = p^2$ there are exactly $p^2 + 1$ regular subgroups isomorphic to $C_{p^2} \times C_p$, $(p+1)p$ isomorphic to D_8, and one isomorphic to C_p^3 contained in $\mathrm{Hol}(C_{p^2} \times C_p)$. Furthermore, there are three $C_{p^2} \times C_p$, two D_8, and one C_p^3-braces of $C_{p^2} \times C_p$ type.

Proof. If $G \subseteq \mathrm{Hol}(C_{p^2} \times C_p)$ with $|\Theta(G)| = p^2$, then we must have $\Theta(G) \subseteq \langle \alpha_1, \alpha_2, \alpha_3 \rangle$ a subgroup of order p^2 and $G \cap (C_{p^2} \times C_p)$ a subgroup of order p.

For $p = 3$ we have that $\Theta(G)$ 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 $G \cap (C_{p^2} \times C_p)$ is one of

$$\langle pe_1 \rangle, \langle bpe_1 + e_2 \rangle \text{ for } b = 0, ..., p-1.$$

We start with the subgroup $\langle pe_1 \rangle$ of $C_{p^2} \times C_p$ on which $\langle \alpha_1, \alpha_3, \alpha_2 \rangle$ acts trivially. Thus, to obtain regular subgroups we need to consider subgroups of the form

$$G = \langle pe_1, v\alpha_1, u\alpha_3 \rangle, \langle pe_1, x\alpha_1, y\alpha_2 \alpha_3^a \rangle \text{ for } a, v_i, u_i, x_i, y_i = 0, ..., p-1$$

where $v, u, x, y \in C_{p^2} \times C_p$. Note

$$(v\alpha_1)^p = pv_1 e_1, \ (u\alpha_3)^p = pu_1 e_1, \ (y\alpha_2 \alpha_3^a)^p = (1+a)\, py_1 e_1.$$

Now calculation identical to that of Lemma 4.2.4 shows that considering subgroups of the form

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

we find regular subgroups

$\langle v_1 e_2 \alpha_1, v\alpha_3 \rangle \cong C_{p^2} \times C_p$ for $v_2 = 0, ..., p-1, \ v_1 = 1, ..., p-1$,

$\langle u_2 e_2 \alpha_1, v\alpha_3 \rangle \cong M_2$ for $v_2 = 0, ..., p-1, \ u_2, v_1 = 1, ..., p-1$ with $u_2 - v_1 \not\equiv 0 \bmod p$,

$\langle u\alpha_1, (u_2 e_1 + v_2 e_2)\, \alpha_3 \rangle \cong C_{p^2} \times C_p$ for $A = \begin{pmatrix} u_1 & v_1 \\ u_2 & u_1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$ with $u_1 \neq 0$,

$\langle u\alpha_1, v\alpha_3 \rangle \cong M_2$ for $A = \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$ with $u_1, \ u_2 - v_1 \not\equiv 0 \bmod p$.

Next, we consider subgroups of the form

$$G = \langle pe_1, x\alpha_1, y\alpha_2 \alpha_3^a \rangle.$$

For G to have order p^3 we must set $x_1 = 0$. Then for G to be regular we need $x_2, y_1 \neq 0$, so $y\alpha_2\alpha_3^a$ has order p^2 if $a = 0, 1$ and has order p if $a = 2$; we find regular subgroups

$$\langle x_2e_2\alpha_1, (x_2e_1 + y_2e_2)\alpha_2\alpha_3\rangle \cong C_{p^2} \times C_p \text{ for } y_2 = 0, ..., p-1,\ x_2 = 1, ..., p-1,$$
$$\left\langle pe_1, x_2e_2\alpha_1, (y_2e_2 - x_2e_1)\alpha_2\alpha_3^{-1}\right\rangle \cong C_p^3 \text{ for } y_2 = 0, ..., p-1,\ x_2 = 1, ..., p-1,$$
$$\langle x_2e_2\alpha_1, y\alpha_2\alpha_3^a\rangle \cong M_2 \text{ for } y_2 = 0, ..., p-1,\ a = 0, 1,\ y_1, x_2 = 1, ..., p-1 \text{ with } ax_2 \neq y_1,$$
$$\left\langle pe_1, x_2e_2\alpha_1, y\alpha_2\alpha_3^{-1}\right\rangle \cong M_1 \text{ for } y_2 = 0, ..., p-1,\ y_1, x_2 = 1, ..., p-1 \text{ with } 2x_2 \neq y_1.$$

Finally, there cannot be any pairing between subgroups of the form $\langle bpe_1 + e_2\rangle$ of $C_{p^2} \times C_p$ for $b = 0, ..., p-1$ with any subgroups of the form

$$\langle\alpha_1, \alpha_3\rangle, \langle\alpha_1, \alpha_2\alpha_3^a\rangle$$

which results in a regular subgroup.

In summary, we have that if $G \subseteq \text{Hol}(C_{p^2} \times C_p)$ is a regular subgroup with $|\Theta(G)| = p^2$ and $p = 3$, then G is isomorphic to either $C_{p^2} \times C_p$, M_2, C_p^3, or M_1. In particular, there are

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

regular subgroups isomorphic to $C_{p^2} \times C_p$,

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

isomorphic to M_2,

$$(p-1)p$$

isomorphic to C_p^3, and

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

isomorphic to M_1.

The corresponding non-isomorphic braces for $p = 3$ are

$$\langle e_2\alpha_1, e_1\alpha_3\rangle, \langle e_1\alpha_1, se_2\alpha_3\rangle, \langle e_2\alpha_1, e_1\alpha_2\alpha_3\rangle \cong C_{p^2} \times C_p,$$

$$\left\langle pe_1, e_2\alpha_1, -e_1\alpha_2\alpha_3^{-1}\right\rangle \cong C_p^3,\ \langle e_2\alpha_1, (t_2e_2 - e_1)\alpha_3\rangle, \langle e_1\alpha_1, (se_2 + e_1)\alpha_3\rangle,$$

$$\langle e_2\alpha_1, se_1\alpha_2\rangle, \langle e_2\alpha_1, -e_1\alpha_2\alpha_3\rangle \cong M_2,\ \left\langle pe_1e_2\alpha_1, e_1\alpha_2\alpha_3^{-1}\right\rangle \cong M_1 \text{ for } s \in \mathbb{F}_p^\times,\ t_2 = 0, 1.$$

For $p = 2$ we have that $\Theta(G)$ is one of

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

and $G \cap (C_{p^2} \times C_p)$ is one of

$$\langle pe_1 \rangle, \langle bpe_1 + e_2 \rangle \text{ for } b = 0, 1.$$

Let us consider pairing of $\langle \alpha_1, \alpha_2^{a_2}\alpha_3^{a_3} \rangle$ and $\langle b_1 pe_1 + b_2 e_2 \rangle$. Suppose

$$G = \langle b_1 pe_1 + b_2 e_2, u\alpha_1, v\alpha_2^{a_2}\alpha_3^{a_3} \rangle .$$

Then we need

$$\begin{aligned} \alpha_1 \cdot (b_1 pe_1 + b_2 e_2) &= b_1 pe_1 + b_2 e_2 \in \langle b_1 pe_1 + b_2 e_2 \rangle , \\ \alpha_2^{a_2}\alpha_3^{a_3} \cdot (b_1 pe_1 + b_2 e_2) &= (b_1 + a_3 b_2)\, pe_1 + b_2 e_2 \in \langle b_1 pe_1 + b_2 e_2 \rangle , \end{aligned} \tag{5.2}$$

so we need $a_3 b_2 \equiv 0 \bmod p$. Further, note we have $(u\alpha_1)^p = 1$ and

$$(v\alpha_2^{a_2}\alpha_3^{a_3})^p = ((v_1 + a_3 v_2)\, pe_1 + a_2 v_1 e_2)\, \alpha_1^{a_2 a_3}. \tag{5.3}$$

We also have

$$\begin{aligned} (u\alpha_1)\,(v\alpha_2^{a_2}\alpha_3^{a_3}) &= (u + v + pv)\, \alpha_1\alpha_2^{a_2}\alpha_3^{a_3} \text{ and} \\ (v\alpha_2^{a_2}\alpha_3^{a_3})\,(u\alpha_1) &= (u + v + a_3 u_2 pe_1 + a_2 u_1 e_2)\, \alpha_1\alpha_2^{a_2}\alpha_3^{a_3}; \end{aligned}$$

thus we need

$$(u\alpha_1)\,(v\alpha_2^{a_2}\alpha_3^{a_3})\,(u\alpha_1)^{-1}\,(v\alpha_2^{a_2}\alpha_3^{a_3})^{-1} = (a_3 u_2 - v_1)\, pe_1 + a_2 u_1 e_2 \in \langle b_1 pe_1 + b_2 e_2 \rangle , \tag{5.4}$$

Note for G to be regular we need at least $u+v+pv \neq 0$ and $u+v+a_3u_2pe_1+a_2u_1e_2 \neq 0$. Now we consider two cases for $b_2 = 0$ and 1.

If $b_2 = 0$, then (5.4) implies that we need $a_2 u_1 = 0$, and the subgroup G is abelian if and only if $a_3 u_2 = v_1$. Therefore, when $a_2 = 0$ considering subgroups of the form $\langle pe_1, u\alpha_1, v\alpha_3 \rangle$ case by case, we find regular subgroups

$$\langle e_1\alpha_1, e_2\alpha_3 \rangle , \langle (u_1 e_1 + e_2)\, \alpha_1, e_1\alpha_3 \rangle \cong C_{p^2} \times C_p \text{ for } u_1 = 0, 1,$$

$$\langle pe_1, e_2\alpha_1, (e_1 + e_2)\, \alpha_3 \rangle \cong C_p^3,$$

$$\langle pe_1, (e_1 + e_2)\, \alpha_1, e_2\alpha_3 \rangle , \langle pe_1, e_1\alpha_1, (e_1 + e_2)\, \alpha_3 \rangle \cong D_8,$$

and when $a_2 = 1$ considering subgroups of the form $\langle pe_1, x\alpha_1, y\alpha_2\alpha_3^a \rangle$, first we need to set $x_1 = 0$, and we find regular subgroups

$$\langle pe_1, e_2\alpha_1, (e_1 + y_2 e_2)\, \alpha_2\alpha_3 \rangle \cong C_{p^2} \times C_p \text{ for } y_2 = 0, 1.$$

Finally, if $b_2 = 1$, by (5.2) we must set $a_3 = 0$, so $a_2 = 1$. Considering that cases for $v_1 = 1, 2, 3$, we find regular subgroups

$$\langle e_2, u_1 e_1 \alpha_1, p e_1 \alpha_2 \rangle, \langle p e_1 + e_2, u_1 e_1 \alpha_1, -u_1 e_1 \alpha_2 \rangle \cong D_8 \text{ for } u_1 = 1, 3.$$

In summary, if $G \subseteq \mathrm{Hol}(C_{p^2} \times C_p)$ is a regular subgroup with $|\Theta(G)| = p^2$ and $p = 2$, then G is isomorphic to either $C_{p^2} \times C_p$, D_8, or C_p^3. In particular, there are $p^2 + 1$ regular subgroups isomorphic to $C_{p^2} \times C_p$, there are $(p+1)p$ isomorphic to D_8, and one isomorphic to C_p^3.

The corresponding non-isomorphic braces for $p = 2$ are

$$\langle p e_1, e_1 \alpha_1, e_2 \alpha_3 \rangle, \langle p e_1, e_2 \alpha_1, e_1 \alpha_3 \rangle, \langle p e_1, e_2 \alpha_1, e_1 \alpha_2 \alpha_3 \rangle \cong C_{p^2} \times C_p,$$

$$\langle p e_1, (e_1 + e_2)\, \alpha_1, e_2 \alpha_3 \rangle, \langle e_2, e_1 \alpha_1, p e_1 \alpha_2 \rangle \cong D_8,$$

$$\langle p e_1, e_2 \alpha_1, (e_1 + e_2)\, \alpha_3 \rangle \cong C_p^3.$$

□

Corollary 5.3.6. *For $p = 3$ we have*

$$\begin{aligned} e(C_{p^2} \times C_p, C_{p^2} \times C_p, p^2) &= (p-1)^3 p, \\ e(M_2, C_{p^2} \times C_p, p^2) &= (p-1)^3 p, \\ e(C_p^3, C_{p^2} \times C_p, p^2) &= (p^3 - 1)(p-1)^3 p, \\ e(M_1, C_{p^2} \times C_p, p^2) &= (p-1)^3 p, \end{aligned}$$

and $e(C_{p^3}, C_{p^2} \times C_p, p^2) = 0$. Furthermore, we have

$$\begin{aligned} \widetilde{e}(C_{p^2} \times C_p, C_{p^2} \times C_p, p^2) &= 4, \\ \widetilde{e}(M_2, C_{p^2} \times C_p, p^2) &= 7, \\ \widetilde{e}(C_p^3, C_{p^2} \times C_p, p^2) &= 1, \\ \widetilde{e}(M_1, C_{p^2} \times C_p, p^2) &= 1, \end{aligned}$$

and $\widetilde{e}(C_{p^2}, C_{p^2} \times C_p, p^2) = 0$.

For $p = 2$ we have

$$\begin{aligned} e(C_{p^2} \times C_p, C_{p^2} \times C_p, p^2) &= p^2 + 1, \\ e(D_8, C_{p^2} \times C_p, p^2) &= (p+1)p, \\ e(C_p^3, C_{p^2} \times C_p, p^2) &= (p^3 - 1)(p+1), \end{aligned}$$

and $e(G, C_{p^2} \times C_p, p^2) = 0$ *otherwise. Furthermore, we have*

$$\begin{aligned}\widetilde{e}(C_{p^2} \times C_p, C_{p^2} \times C_p, p^2) &= 3,\\ \widetilde{e}(D_8, C_{p^2} \times C_p, p^2) &= 2,\\ \widetilde{e}(C_p^3, C_{p^2} \times C_p, p^2) &= 1,\end{aligned}$$

and $\widetilde{e}(G, C_{p^2} \times C_p, p^2) = 0$ *otherwise.*

Proof. Follows from Lemma 5.3.5. □

Lemma 5.3.7. *For* $p = 3$ *and* $|\Theta(G)| = p^3$ *there are no regular subgroups contained in* Hol($C_{p^2} \times C_p$).

For $p = 2$ *and* $|\Theta(G)| = p^3$ *there are exactly* p^2 *regular subgroups isomorphic to* D_8 *contained in* Hol($C_{p^2} \times C_p$). *These regular subgroups correspond to one brace.*

Proof. If $G \subseteq \mathrm{Hol}(C_{p^2} \times C_p)$ with $|\Theta(G)| = p^3$, then we must have $\Theta(G) = \langle \alpha_1, \alpha_2, \alpha_3 \rangle$, and so

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

where for $p = 3$ for G to have size p^3 we require $pu_1 = pv_1 = pw_1 \equiv 0 \bmod p$, but in such case G cannot be regular.

For $p = 2$, note that we have

$$(u\alpha_1)^p = 1,\ (v\alpha_2)^p = v_1 p e_1 + v_1 e_2,\ (w\alpha_3)^p = w_1 p e_1 + w_2 p e_1,$$

which implies that we need

$$\begin{aligned}v_1 &\equiv 0 \bmod p,\\ w_1 &\equiv w_2 \bmod p.\end{aligned}$$

Note, G maps isomorphically onto $\Theta(G)$, and we have

$$\begin{aligned}(u\alpha_1)\,(v\alpha_2) &= (u+v)\,\alpha_1\alpha_2 \text{ and}\\ (v\alpha_2)\,(u\alpha_1) &= (u+v+u_1e_2)\,\alpha_1\alpha_2,\end{aligned}$$

so we need $u_1 \equiv 0 \bmod p$, thus $u_1 = ape_1 + u_2e_2$ for some $a = 0, 1$. This implies that for G to be regular we need $w_1 \equiv 1 \bmod p$, so $w = e_1 + bpe_1 + e_2$ for some $b = 0, 1$. We also have

$$\begin{aligned}(u\alpha_1)\,(w\alpha_3) &= (u+w+pe_1)\,\alpha_1\alpha_3 \text{ and}\\ (w\alpha_3)\,(u\alpha_1) &= (u+w+u_2pe_1)\,\alpha_1\alpha_3,\end{aligned}$$

so we need $u_2 \equiv 1 \bmod p$. Finally, we have

$$(w\alpha_3)(v\alpha_2) = (w + v + v_2 pe_1)\,\alpha_3\alpha_2 \text{ and}$$
$$(u\alpha_1)(v\alpha_2)(w\alpha_3) = (w + v + ape_1 + pe_1)\,\alpha_1\alpha_2\alpha_3,$$

so we need $v_2 \equiv a + 1 \bmod p$. Thus, we see that we must have

$$u = ape_1 + e_2,\ v = cpe_1 + (a+1)e_2,\ w = e_1 + bpe_1 + e_2 \text{ for } a, b, c = 0, 1.$$

We further need

$$u + v = (a + c)\,pe_1 + ae_2 \neq 0,$$
$$v = cpe_1 + (a+1)e_2 \neq 0,$$

so $c = 1$.

Therefore, we only have regular subgroups, isomorphic to D_8, given by

$$\langle (ape_1 + e_2)\alpha_1, (pe_1 + (a+1)\,e_2)\,\alpha_2, (e_1 + bpe_1 + e_2)\,\alpha_3 \rangle \text{ for } a, b = 0, 1,$$

The corresponding brace is $\langle e_2\alpha_1, (pe_1 + e_2)\,\alpha_2, (e_1 + e_2)\,\alpha_3, \rangle \cong D_8$. □

Corollary 5.3.8. *For $p = 3$ we have $e(G, C_{p^2} \times C_p, p^3) = 0$. Furthermore, we have $\widetilde{e}(G, C_{p^2} \times C_p, p^3) = 0$ for any group G.*

For $p = 2$ we have

$$e(D_8, C_{p^2} \times C_p, p^3) = p^2$$

and $e(G, C_{p^2} \times C_p, p^3) = 0$ otherwise. Furthermore, we have

$$\widetilde{e}(D_8, C_{p^2} \times C_p, p^3) = 1$$

and $\widetilde{e}(G, C_{p^2} \times C_p, p^3) = 0$ otherwise.

Proof. Follows from Lemma 5.3.7. □

5.4 Regular subgroups in $\mathrm{Hol}(C_p^2)$ and special cases for $\mathrm{Hol}(C_p^3)$

In this section we find the regular subgroup contained in $\mathrm{Hol}(C_p^2)$ for all prime p and regular subgroups contained in $\mathrm{Hol}(C_p^3)$ for $p = 2, 3$. We also find the corresponding braces. We note that the results for $\mathrm{Hol}(C_p^2)$ were originally found in [Byo96], we reproduce them here again for completeness. The main results of this section are the following.

Proposition 5.4.1. *For $p > 2$ we have*

$$e(C_p^2, C_p^2) = p^2$$

and $e(C_{p^2}, C_p^2) = 0$. Furthermore, we have

$$\widetilde{e}(C_p^2, C_p^2) = 2$$

and $\widetilde{e}(C_{p^2}, C_p^2) = 0$.

For $p = 2$ we have

$$\begin{aligned} e(C_p^2, C_p^2) &= 1, \\ e(C_{p^2}, C_p^2) &= 1. \end{aligned}$$

Furthermore, we have

$$\begin{aligned} \widetilde{e}(C_p^2, C_p^2) &= 1, \\ \widetilde{e}(C_{p^2}, C_p^2) &= 1. \end{aligned}$$

Proposition 5.4.2. *For $p = 3$ we have*

$$\begin{aligned} e(C_p^3, C_p^3) &= 339, \\ e(M_1, C_p^3) &= 51, \\ e(C_{p^2} \times C_p, C_p^3) &= 6, \\ e(M_2, C_p^3) &= 6, \end{aligned}$$

and $e(C_{p^3}, C_p^3) = 0$. Furthermore, we have

$$\begin{aligned} \widetilde{e}(C_p^3, C_p^3) &= 4, \\ \widetilde{e}(M_1, C_p^3) &= 5, \\ \widetilde{e}(C_{p^2} \times C_p, C_p^3) &= 1, \\ \widetilde{e}(M_2, C_p^3) &= 2, \end{aligned}$$

and $\widetilde{e}(C_{p^3}, C_p^3) = 0$.

For $p = 2$ we have

$$\begin{aligned} e(C_p^3, C_p^3) &= 8, \\ e(D_8, C_p^3) &= 6, \\ e(C_{p^2} \times C_p, C_p^3) &= 4, \\ e(Q_8, C_p^3) &= 2, \end{aligned}$$

and $e(C_{p^3}, C_p^3) = 0$. *Furthermore, we have*

$$\begin{aligned}\widetilde{e}(C_p^3, C_p^3) &= 2,\\ \widetilde{e}(D_8, C_p^3) &= 2,\\ \widetilde{e}(C_{p^2} \times C_p, C_p^3) &= 3,\\ \widetilde{e}(Q_8, C_p^3) &= 1,\end{aligned}$$

and $\widetilde{e}(C_{p^3}, C_p^3) = 0$.

Note, the findings in Proposition 5.4.2 are different to the case where $p > 3$ in that for the later case we only find C_p^3 or M_1 Hopf-Galois structures (or skew braces) of type C_p^3, but when $p = 2$ or 3 we find the numbers for C_p^3 or M_1 Hopf-Galois structures (or skew braces) of type C_p^3 splits to give others; for example, when $p = 3$ we have $C_{p^2} \times C_p$ or M_2 Hopf-Galois structures (or skew braces) of type C_p^3 as well. The proof of propositions above follows from calculations in the rest of this section. First we find the regular subgroups contained in Hol(C_p^2). Note, we define

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

To make the notations easier, we shall often use the identification $C_p^2 \cong \mathbb{F}_p^2$ by

$$\sigma \longmapsto e_1 \stackrel{\text{def}}{=} \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ \tau \longmapsto e_2 \stackrel{\text{def}}{=} \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Therefore, the holomorph of C_p^2 can be identified with the affine transformations of $\mathbb{F}_p^2$ i.e.,

$$\mathrm{Hol}(C_p^2) \cong \left\{ tA : t \in \mathbb{F}_p^2,\ A \in \mathrm{GL}_2(\mathbb{F}_p) \right\}.$$

Now the image of a subgroup of Hol(C_p^2) of order p^2 in Aut(C_p^2) under the natural projection

$$\Theta : \mathrm{Hol}(C_p^2) \longrightarrow \mathrm{Aut}(C_p^2)$$

must lie in $\mathrm{SL}_2(\mathbb{F}_p)$; thus any subgroup of Hol(C_p^2) of order p^2 lies in

$$C_p^2 \rtimes \mathrm{SL}_2(\mathbb{F}_p).$$

If G is a subgroup of order p^2 in Hol(C_p^2), then we can have $|\Theta(G)| = 1, p$ or p^2. In particular, $\Theta(G)$ lies in one of the $p + 1$ Sylow p-subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$. These are all conjugate in $\mathrm{SL}_2(\mathbb{F}_p)$ to

$$B(C_p^2) \stackrel{\text{def}}{=} \langle A_1 \rangle \cong C_p$$

where $A_1 \stackrel{\text{def}}{=} \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, so in fact we can only have $|\Theta(G)| = 1$ or p.

Before we begin, it is worth noting that if $A \in \mathrm{SL}_2(\mathbb{F}_p)$ is an element of order p,

then since as mentioned above A is conjugate to $B = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ for some b, we find

$$\begin{aligned} I + B + \cdots + B^{p-1} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} + \cdots + \begin{pmatrix} 1 & (p-1)b \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & \frac{1}{2}p(p-1)b \\ 0 & 0 \end{pmatrix}; \end{aligned}$$

thus we have

$$I + B + \cdots + B^{p-1} = \begin{cases} 0, & \text{if } p > 2 \\ I + B, & \text{if } p = 2. \end{cases}$$

Therefore, for all $v \in \mathbb{F}_p^2$, we have

$$[v, A]^p = \begin{cases} 1, & \text{if } p > 2 \\ [(I + A)(v), I], & \text{if } p = 2. \end{cases} \tag{5.5}$$

We have

$$\begin{aligned} e(C_p^2, C_p^2, 1) = \widetilde{e}(C_p^2, C_p^2, 1) = 1 \text{ and} \\ e(C_{p^2}, C_p^2, 1) = \widetilde{e}(C_{p^2}, C_p^2, 1) = 0. \end{aligned}$$

We shall deal with the cases $|\Theta(G)| = p$ in the following lemma.

Lemma 5.4.3. *For $p > 2$ and $|\Theta(G)| = p$ there are exactly $p^2 - 1$ regular subgroups isomorphic to C_p^2 contained in* Hol(C_p^2). *Furthermore, there is one C_p^2-brace of C_p^2 type.*

For $p = 2$ there are exactly $p^2 - 1$ regular subgroups isomorphic to C_{p^2} contained in Hol(C_p^2). *Furthermore, there is one C_{p^2}-brace of C_p^2 type.*

Proof. If $G \subseteq \mathrm{Hol}(C_p^2)$ with $|\Theta(G)| = p$, then we must have $\Theta(G) \subseteq \mathrm{SL}_2(\mathbb{F}_p)$ a subgroup of order p and $G \cap C_p^2$ a subgroup of order p. Therefore, we must have

$$G = \langle u, vA \rangle$$

for some $A \in \mathrm{SL}_2(\mathbb{F}_p)$ which has order p, and $v \in \mathbb{F}_p^2$ such that

$$U \stackrel{\text{def}}{=} \langle u \rangle \cong \mathbb{F}_p^1 \subseteq \mathbb{F}_p^2 \text{ and } A \cdot U \subseteq U.$$

Now there are $p + 1$ distinct subgroups of order p in $\mathbb{F}_p^2$. We shall find the number of regular subgroups which contain $\langle e_1 \rangle$ and then multiply this by the number of distinct subgroups of order p in $\mathbb{F}_p^2$ which is $p + 1$.

Therefore, we consider subgroups of the form

$$G = \langle e_1, v_2 e_2 A_1 \rangle$$

where for G to be regular we need $v_2 \neq 0$. Note

$$(v_2 e_2 A_3)\, e_1 = (e_1 + v_2 e_2)\, A_3,$$

so G is either isomorphic to C_{p^2} or C_p^2. Now if $p > 2$, then $(vA_3)^p = 1$, so we have regular subgroups

$$\langle e_1, v_2 e_2 A_3 \rangle \cong C_p \times C_p \text{ for } v_2 = 1, ..., p-1$$

and taking into account the $p+1$ conjugates there are $p^2 - 1$ of these. If $p = 2$, then $(e_2 A_3)^p = (A_3 - I) \cdot e_2 = e_1$, so we have a regular subgroup

$$\langle e_1, e_2 A_3 \rangle = \langle e_2 A_3 \rangle \cong C_{p^2}.$$

and there are $p + 1$ of these.

To find the corresponding braces note that conjugating the subgroup $\langle e_1, e_2 A_3 \rangle$ with the automorphism $\left(\begin{smallmatrix} v_2 & 0 \\ 0 & v_2 \end{smallmatrix}\right)$ we get $\langle e_1, v_2 e_2 A_3 \rangle$.

Therefore for $p > 2$ we have one C_p^2-brace of C_p^2 type, and for $p = 2$ we have one C_{p^2}-brace of C_p^2 type. □

Corollary 5.4.4. *For $p > 2$ we have*

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

and $e(C_{p^2}, C_p^2, p) = 0$. Furthermore, we have

$$\widetilde{e}(C_p^2, C_p^2, p) = 1,$$

and $\widetilde{e}(C_{p^2}, C_p^2, p) = 0$.

For $p = 2$ we have

$$e(C_{p^2}, C_p^2, p) = 1,$$

and $e(C_p^2, C_p^2, p) = 0$. Furthermore, we have

$$\widetilde{e}(C_{p^2}, C_p^2, p) = 1,$$

and $\widetilde{e}(C_p^2, C_p^2, p) = 0$.

Proof. Follows from Lemma 5.4.3. □

Next, we find the regular subgroups contained in $\mathrm{Hol}(C_p^3)$ for $p = 2, 3$. We shall use the notation of Section 4.3. Recall, for any subgroup $G \subseteq \mathrm{Hol}(C_p^3)$ of order p^3, we have that $\Theta(G)$ lies in a conjugate, by an element of $\mathrm{SL}_3(\mathbb{F}_p)$, of the Sylow p-subgroup of $\mathrm{SL}_3(\mathbb{F}_p)$

$$B(C_p^3) \stackrel{\text{def}}{=} \langle A_1, A_2, A_3 \rangle \cong M_1.$$

Before we begin, note that if $A \in \mathrm{SL}_3(\mathbb{F}_p)$ is an element of order p, then, as before, A is conjugate to an element of the form

$$B = \begin{pmatrix} b_1 & b_2 & b_3 \\ b_4 & b_5 & b_6 \\ 0 & 0 & b_7 \end{pmatrix} \in \mathrm{SL}_3(\mathbb{F}_p).$$

Let $B_1 = \left(\begin{smallmatrix} b_1 & b_2 \\ b_4 & b_5 \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} b_3 \\ b_6 \end{smallmatrix}\right)$. Then we can write $B = \left(\begin{smallmatrix} B_1 & y \\ 0 & b_7 \end{smallmatrix}\right)$, and for $r \geq 1$ we have

$$B^r = \begin{pmatrix} B_1^r & (B_1^{r-1} + B_1^{r-2} b_7 + \cdots + b_7^{r-1})(y) \\ 0 & b_7^r \end{pmatrix},$$

so if B has order p i.e., $B^p = I$ and $B \neq I$, then $b_7^p = b_7 = 1$ and $B_1^p = I$, furthermore if $p = 2$, we need $(B_1 - I)(y) = 0$.

Now, when B has order p, we have

$$[v, B]^p = \left[\left(I + B + \cdots + B^{p-1}\right)(v), I\right]$$

and

$$I + B + \cdots + B^{p-1} = \begin{pmatrix} \sum_{j=0}^{p-1} B_1^j & (\sum_{j=1}^{p-1} j B_1^{p-1-j})(y) \\ 0 & 0 \end{pmatrix}.$$

Since $B_1^p = I$, we have that B_1 is conjugate to a matrix of the form $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$, so $\sum_{j=0}^{p-1} B_1^j = 0$ if $p > 2$, and $\sum_{j=0}^{p-1} B_1^j = I + B_1$ if $p = 2$, also

$$\sum_{j=1}^{p-1} j B_1^{p-1-j} = \begin{cases} B_1 - I, & \text{if } p = 3 \\ B_1, & \text{if } p = 2. \end{cases}$$

This implies that

$$I + B + \cdots + B^{p-1} = \begin{cases} \begin{pmatrix} 0 & (B_1 - I)(y) \\ 0 & 0 \end{pmatrix}, & \text{if } p = 3 \\ \begin{pmatrix} I + B_1 & y \\ 0 & 0 \end{pmatrix}, & \text{if } p = 2, \end{cases}$$

and so it follows that

$$[v, B]^p = \begin{cases} [v_3 (B_1 - I)(y), I], & \text{if } p = 3 \\ [v, B]^p = [(I + B_1)(v_1 e_1 + v_2 e_2) + v_3 y, I], & \text{if } p = 2, \end{cases} \tag{5.6}$$

where $y = b_3 e_1 + b_6 e_2$ for all $v = v_1 e_1 + v_2 e_2 + v_3 e_3 \in \mathbb{F}_p^3$.

We have

$$e(C_p^3, C_p^3, 1) = \widetilde{e}(C_p^3, C_p^3, 1) = 1,$$
$$e(G, C_p^3, 1) = \widetilde{e}(G, C_p^3, 1) = 0 \text{ if } G \neq C_p^3.$$

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

Lemma 5.4.5. *For $p = 3$ and $|\Theta(G)| = p$ there are exactly*

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

regular subgroups isomorphic to C_p^3,

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

isomorphic to M_1, and

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

isomorphic to M_2 contained in $\mathrm{Hol}(C_p^3)$. Furthermore, there is one C_p^3, one M_1, and one M_2-brace of C_p^3 type.

For $p = 2$ and $|\Theta(G)| = p$ there are exactly

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

regular subgroups isomorphic to $C_{p^2} \times C_p$ and

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

isomorphic to D_8 contained in $\mathrm{Hol}(C_p^3)$. Furthermore, there is one $C_{p^2} \times C_p$ and one D_8-brace of C_p^3 type.

Proof. Similar to Lemma 4.3.2, we shall find the number of regular subgroups which contain $\langle e_1, e_2 \rangle$ and then multiply this by the number of distinct subgroups of order p^2 in $\mathbb{F}_p^3$.

Thus let $U \stackrel{\text{def}}{=} \langle e_1, e_2 \rangle \subseteq \mathbb{F}_p^3$. Then the set of matrices of the form

$$B = \begin{pmatrix} b_1 & b_2 & b_3 \\ b_4 & b_5 & b_6 \\ 0 & 0 & b_7 \end{pmatrix} \in \mathrm{SL}_3(\mathbb{F}_p)$$

is the largest subgroup of $\mathrm{SL}_3(\mathbb{F}_p)$ whose elements fix U, and we let

$$\mathrm{SL}_3(\mathbb{F}_p)_U \stackrel{\text{def}}{=} \{B \in \mathrm{SL}_3(\mathbb{F}_p) : B \cdot U \subseteq U\}.$$

We need to find distinct subgroups of order p in $\mathrm{SL}_3(\mathbb{F}_p)_U$, so we can pair them with U to have a chance of obtaining a subgroup of order p^3. For any $B \in \mathrm{SL}_3(\mathbb{F}_p)_U$ as given above which has order p, let $B_1 = \left(\begin{smallmatrix} b_1 & b_2 \\ b_4 & b_5 \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} b_3 \\ b_6 \end{smallmatrix}\right)$. Then we can write $B = \left(\begin{smallmatrix} B_1 & y \\ 0 & 1 \end{smallmatrix}\right)$ where $B_1^p = I$, with $(B_1 - I) \cdot y = 0$ for $p = 2$. Note in such case we have already calculated the values of $(vB)^p$ in (5.6). Now consider two cases when $B_1 = I$ and $B_1 \neq I$.

If $B_1 = I$, then we consider subgroups of the form

$$G = \langle e_1, e_2, e_3 B \rangle .$$

For $p = 3$, we have that G is regular and isomorphic to C_p^3, and for $p = 2$, we have that G is regular and isomorphic to $C_{p^2} \times C_p$; in either case there are $p^2 - 1$ choices for y.

Therefore, we have $p^2 - 1$ regular subgroups of the form

$$\langle e_1, e_2, e_3 B \rangle \cong C_p^3$$

similarly, for $p = 2$ we have $p^2 - 1$ distinct regular subgroups of the form

$$\langle e_1, e_2, e_3 B \rangle \cong C_{p^2} \times C_p.$$

The above correspond to the brace

$$\left\langle e_1, e_2, e_3 \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix} \right) \right\rangle .$$

If $B_1 \neq I$, then B_1 is conjugate to $B_2 = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix} \right)$, by some element of $\mathrm{SL}_2(\mathbb{F}_p)$, with $b \neq 0$, but for $p = 2$ we also need $(B_1 - I) \cdot y = 0$.

Suppose

$$B = \begin{pmatrix} 1 & 1 & b_3 \\ 0 & 1 & b_6 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_3(\mathbb{F}_p),$$

where for $p = 2$ we set $b_6 = 0$. We can consider the subgroups

$$G = \langle e_1, e_2, v_3 e_3 B \rangle \text{ for } v_3 \neq 0.$$

Now we have

$$e_1 + e_2 = e_2 + e_1, \ (vB)(e_1) = (e_1)(vB), \text{ and } (vB)\, e_2 = (e_2 + e_1)(vB),$$

and we have

$$(vB)^p = \begin{cases} v_3 (B_1 - I) \cdot y = v_3 b_6 e_1, & \text{if } p = 3 \\ v_3 b_3 e_1, & \text{if } p = 2, \end{cases}$$

also if we replace $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix} \right)$ by one of its conjugates, by say $A_0 \in \mathrm{SL}_2(\mathbb{F}_p)$, then we can replace e_1 by $\left(\begin{smallmatrix} A_0 & 0 \\ 0 & 1 \end{smallmatrix} \right) \cdot e_1$ and e_2 by $\left(\begin{smallmatrix} A_0 & 0 \\ 0 & 1 \end{smallmatrix} \right) \cdot e_2$ and we still have the above relationship, where for $p = 2$ we need to replace y with $A_0 \cdot y$ too.

For $p = 3$ we have to consider the cases when $b_6 = 0$ and $b_6 \neq 0$. If $b_6 = 0$, we have regular subgroups

$$\langle e_1, e_2, v_3 e_3 B \rangle \cong M_1,$$

and there are $(p^2-1)p$ of them; if $b_6 \neq 0$, we have regular subgroups

$$\langle e_1, e_2, v_3 e_3 B\rangle \cong M_2,$$

and there are $(p^2-1)(p-1)p$ of them.

The above correspond to the non-isomorphic braces

$$\left\langle e_1, e_2, e_3 \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle \cong M_1, \ \left\langle e_1, e_2, e_3 \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle \cong M_2.$$

For $p = 2$ we need $b_6 = 0$ and we get subgroup isomorphic to D_8 when $b_3 = 0, 1$, and so there are $(p+1)p$ of these, which correspond to the brace

$$\left\langle e_1, e_2, e_3 \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle \cong D_8.$$

Now we shall multiply the numbers above by the number of distinct subgroups of order p^2 in $\mathbb{F}_p^3$. Note, as already mentioned, there are

$$\frac{(p^3-1)(p^3-p)}{(p^2-1)(p^2-p)} = \frac{p^3-1}{p-1}$$

distinct subgroups of order p^2 in $\mathbb{F}_p^3$.

Therefore, for $p = 3$, there are

$$\frac{p^3-1}{p-1} \times (p^2-1) = (p^3-1)(p+1),$$

regular subgroups isomorphic to C_p^3,

$$\frac{p^3-1}{p-1} \times (p^2-1)p = (p^3-1)(p+1)p$$

regular subgroups isomorphic to M_1, and

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

regular subgroups isomorphic to M_2 contained in Hol(C_p^3) with $|\Theta(G)| = p$.

The corresponding non-isomorphic braces for $p = 3$ are

$$\langle e_1, e_2, e_3 A_2\rangle \cong C_p^3, \ \langle e_1, e_2, e_3 A_3\rangle \cong M_1, \ \langle e_1, e_2, e_3 A_2 A_3\rangle \cong M_2.$$

For $p = 2$, there are

$$\frac{p^3-1}{p-1} \times (p^2-1) = (p^3-1)(p+1)$$

regular subgroups isomorphic to $C_{p^2} \times C_p$ and

$$\frac{p^3-1}{p-1} \times (p+1)p = (p^3-1)(p+1)p$$

regular subgroups isomorphic to D_8 contained in $\mathrm{Hol}(C_p^3)$ with $|\Theta(G)| = p$.

The corresponding non-isomorphic braces for $p = 2$ are

$$\langle e_1, e_2, e_3 A_2 \rangle \cong C_{p^2} \times C_p, \ \langle e_1, e_2, e_3 A_3 \rangle \cong D_8.$$

□

Corollary 5.4.6. *For $p = 3$ we have*

$$\begin{aligned} e(C_p^3, C_p^3, p) &= (p^3-1)(p+1), \\ e(M_1, C_p^3, p) &= (p+1)p, \\ e(M_2, C_p^3, p) &= p, \end{aligned}$$

and $e(G, C_p^3, p) = 0$ otherwise. Furthermore, we have

$$\begin{aligned} \widetilde{e}(C_p^3, C_p^3, p) &= 1, \\ \widetilde{e}(M_1, C_p^3, p) &= 1, \\ \widetilde{e}(M_2, C_p^3, p) &= 1, \end{aligned}$$

and $\widetilde{e}(G, C_p^3, p) = 0$ otherwise.

For $p = 2$ we have

$$\begin{aligned} e(C_{p^2} \times C_p, C_p^3, p) &= 1, \\ e(D_8, C_p^3, p) &= p, \end{aligned}$$

and $e(G, C_p^3, p) = 0$ otherwise. Furthermore, we have

$$\begin{aligned} \widetilde{e}(C_{p^2} \times C_p, C_p^3, p) &= 1, \\ \widetilde{e}(D_8, C_p^3, p) &= 1, \end{aligned}$$

and $\widetilde{e}(G, C_p^3, p) = 0$ otherwise.

Proof. Follows from Lemma 5.4.5. □

Lemma 5.4.7. *For $p = 3$ and $|\Theta(G)| = p^2$ there are exactly $(p^3-1)p^2$ regular subgroups isomorphic to C_p^3,*

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

isomorphic to M_1,

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

isomorphic to $C_{p^2}\times C_p$, *and*

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

isomorphic to M_2 *contained in* $\mathrm{Hol}(C_p^3)$. *Furthermore, there are two* C_p^3, *four* M_1, *one* $C_{p^2}\times C_p$, *and one* M_2*-braces of* C_p^3 *type.*

For $p=2$ *and* $|\Theta(G)|=p^2$ *there are exactly* p^3-1 *regular subgroups isomorphic to* C_p^3,

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

isomorphic to $C_{p^2}\times C_p$, *and* $(p^3-1)p$ *isomorphic to* Q_8 *contained in* $\mathrm{Hol}(C_p^3)$. *Furthermore, there is one* C_p^3, *two* $C_{p^2}\times C_p$, *and one* Q_8*-braces of* C_p^3 *type.*

Proof. Without loss of generality we may consider the regular subgroups which contain $\langle e_1\rangle$. The set of matrices of the form

$$B=\begin{pmatrix} b_1 & b_2 & b_3\\ 0 & b_4 & b_5\\ 0 & b_6 & b_7\end{pmatrix}\in \mathrm{SL}_3(\mathbb{F}_p)$$

is the largest subgroup of $\mathrm{SL}_3(\mathbb{F}_p)$ whose elements fix $\langle e_1\rangle$, and we let

$$\mathrm{SL}_3(\mathbb{F}_p)_U \stackrel{\text{def}}{=} \{B\in \mathrm{SL}_3(\mathbb{F}_p) : B\cdot U\subseteq U\}.$$

As before we have $B(C_p^3)\subseteq \mathrm{SL}_3(\mathbb{F}_p)_U$ which is a Sylow p-subgroup.

We shall deal with the case for $p=3$ first. In this case the group $B(C_p^3)$ contains $p+1$ distinct subgroups of order p^2 which are of the form

$$\langle A_1,A_3\rangle, \langle A_1,A_2A_3^d\rangle \text{ for } d=0,..,p-1.$$

Calculation of Lemma 4.3.4 showed that $\langle A_1,A_3\rangle$ has conjugacy class of size one, $\langle A_1,A_2\rangle$ has conjugacy class of size $p+1$, and $\langle A_1,A_2A_3\rangle$ has conjugacy class of size p^2-1; the union of these classes is the set of all subgroups of order p^2 in $\mathrm{SL}_3(\mathbb{F}_p)_U$. Note, when $p=3$, for positive integers a_1,a_2,a_3 and $v\in\mathbb{F}_p^3$ we have

$$(vA_1^{a_1}A_2^{a_2}A_3^{a_3})^p = v_3a_2a_3e_1.$$

Let us consider a subgroup of the form

$$G=\langle e_1, uA_1, vA_2\rangle$$

and we may assume $u_1=v_1=0$. Note, we have $(uA_1)^p=(vA_2)^p=1$. Now we are

back to the situation of Lemma 4.3.4, which gives regular subgroups

$$\langle e_1, u_2 e_2 A_1, v A_2 \rangle \cong M_1 \text{ for } u_2, v_3 = 1, ..., p-1,\ v_2 = 0, ..., p-1.$$

Recall we had $|\mathrm{Orb}(\langle A_1, A_2 \rangle)| = p+1$.

Therefore, we have

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

subgroups of the form $\left\langle e_1, uA, v\widetilde{A} \right\rangle \cong M_1$, where A, and $\widetilde{A}$ are conjugates of A_1 and A_2 in $\mathrm{SL}_3(\mathbb{F}_p)_U$. The corresponding brace is $\langle e_1, e_2 A_1, e_3 A_2 \rangle$.

Next, we consider subgroups of the form

$$G = \langle e_1, uA_1, vA_3 \rangle$$

for some vectors $u, v \in \mathbb{F}_p^3$ where we can assume $u_1 = v_1 = 0$. Again we find $(uA_1)^p = (vA_3)^p = 1$, which is similar to Lemma 4.3.4.

Therefore, we have

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

regular subgroups of the form

$$\langle e_1, uA_1, vA_3 \rangle \cong C_p^3 \text{ with } v_3 = u_2$$

and

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

regular subgroups of the form

$$\langle e_1, uA_1, vA_3 \rangle \cong M_1 \text{ with } v_3 \neq u_2.$$

The above correspond to non-isomorphic braces

$$\langle e_1, u_3 e_3 A_1, e_2 A_3 \rangle \cong C_p^3,\ \langle e_1, (e_2 + u_3 e_3) A_1, e_2 A_3 \rangle, \langle e_1, e_2 A_1, -e_3 A_3 \rangle \cong M_1$$

where $u_3 \in \mathbb{F}_p^\times$.

Finally, we consider subgroups of the from

$$G = \left\langle e_1, uA_1, vA_2 A_3^d \right\rangle$$

for a fixed $d = 1, ..., p-1$. Then we have $(uA_1)^p = 1$ and $\left(vA_2 A_3^d\right)^p = v_3 d e_1$, we further have

$$(uA_1)\, e_1 = e_1\, (uA_1),\ \left(vA_2 A_3^d\right) e_1 = e_1 \left(vA_2 A_3^d\right).$$

We also calculate

$$(uA_1)\left(vA_2A_3^d\right) = (u+v+v_3e_1)\,A_1A_2A_3^d \text{ and}$$
$$\left(vA_2A_3^d\right)(uA_1) = (u+v+du_2e_1+u_3e_2)\,A_1A_2A_3^d.$$

For G to have order p^3 we need to set $u_3 = 0$. Then for G to be regular we need $u_2, v_3 \neq 0$, also G is abelian when $du_2 = v_3$ and isomorphic to M_2 when $du_2 \neq v_3$, so we find regular subgroups

$$\left\langle e_1, v_3d^{-1}e_2A_1, vA_2A_3^d\right\rangle \cong C_{p^2} \times C_p \text{ for } v_3 = 1,...,p-1,\ v_2 = 0,...,p-1,$$

there are $(p-1)p$ of them, and

$$G = \left\langle e_1, u_2e_2A_1, vA_2A_3^d\right\rangle \cong M_2$$

$$\text{for } u_2, v_3 = 1,...,p-1,\ v_2 = 0,...,p-1 \text{ with } du_2 \neq v_3,$$

there are

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

of them, as we have p^2-1 conjugates for subgroups of the from $\left\langle A_1, A_2A_3^d\right\rangle$, we have exactly

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

regular subgroups of the form $\left\langle e_1, uA, v\widetilde{A}'\widetilde{A}^d\right\rangle \cong C_{p^2} \times C_p$, and we have exactly

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

regular subgroups of the form $\left\langle e_1, uA, v\widetilde{A}'\widetilde{A}^d\right\rangle \cong M_2$, where A, $\widetilde{A}$, and $\widetilde{A}'$ are conjugates of A_1, A_2, and A_3 in $\mathrm{SL}_3(\mathbb{F}_p)_U$.

The corresponding non-isomorphic braces are

$$\langle e_1, e_2A_1, e_3A_2A_3\rangle \cong C_{p^2} \times C_p,$$

$$\langle e_1, e_2A_1, be_3A_2A_3\rangle \cong M_2 \text{ where } b = v_3u_2^{-1} \neq 1.$$

Therefore, multiplying by the number of subgroups of order p in $\mathbb{F}_p^3$, we find

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

regular subgroups isomorphic to C_p^3,

$$\frac{p^3-1}{p-1} \times ((p^2-p-1)(p-1)p + (p-1)^2(p+1)p) = (p^3-1)(p^2+p+1)p$$

isomorphic to M_1,

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

isomorphic to $C_{p^2} \times C_p$, and

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

isomorphic to M_2 contained in Hol(C_p^3) with $|\Theta(G)| = p^2$.

The corresponding non-isomorphic braces for $p = 3$ are

$$\langle e_1, u_3e_3A_1, e_2A_3\rangle \cong C_p^3,\ \langle e_1, (e_2+u_3e_3)A_1, e_2A_3\rangle, \langle e_1, e_2A_1, -e_3A_3\rangle,$$

$$\langle e_1, e_2A_1, e_3A_2\rangle \cong M_1,\ \langle e_1, e_2A_1, e_3A_2A_3\rangle \cong C_{p^2} \times C_p,\ \langle e_1, e_2A_1, -e_3A_2A_3\rangle \cong M_2$$

for $u_3 \in \mathbb{F}_p^\times$.

For $p = 2$ the group $B(C_p^3)$ also has $p+1$ distinct subgroups of order p^2, which are of the form

$$\langle A_1, A_2\rangle, \langle A_1, A_3\rangle, \langle A_2A_3\rangle.$$

Calculation similar to Lemma 4.3.4 shows that $\langle A_1, A_3\rangle$ has conjugacy class of size one, $\langle A_1, A_2\rangle$ has conjugacy class of size $p+1$, and $\langle A_2A_3\rangle$ has conjugacy class of size p^2-1; the union of these classes is the set of all subgroups of order p^2 in $\mathrm{SL}_3(\mathbb{F}_p)_U$. Note for positive integers a_1, a_2, a_3 and $u \in \mathbb{F}_p^3$ we have

$$(uA_1^{a_1}A_2^{a_2}A_3^{a_3})^p = ((I + A_1^{a_1}A_2^{a_2}A_3^{a_3}) \cdot u)\,(A_1^{a_1}A_2^{a_2}A_3^{a_3})^p$$

$$= ((a_3u_2 + a_1u_3)\,e_1 + a_2u_3e_2)\,A_1^{a_1a_2}.$$

Let us consider a subgroup of the form

$$G = \langle e_1, uA_1, vA_2\rangle$$

for some vectors $u, v \in \mathbb{F}_p^3$ where we can assume $u_1 = v_1 = 0$. Note since $(vA_2)^p = v_3e_2$, for G to have order p^3, we need to set $v_3 = 0$. Now, we have

$$(uA_1)\,(vA_2) = (u+v)\,A_1A_2 \text{ and}$$
$$(vA_2)\,(uA_1) = (v+u+u_3e_2)\,A_1A_2,$$

so for G to have order p^3 we must set $u_3 = 0$, but in such case G can never be regular.

Next, we consider subgroups of the form

$$G = \langle e_1, uA_1, vA_3\rangle$$

for some vectors $u, v \in \mathbb{F}_p^3$ where we can assume $u_1 = v_1 = 0$. Calculation above shows that $(uA_1)^p = u_3 e_1$ and $(vA_3)^p = v_2 e_1$. We have

$$\begin{aligned}(uA_1)(vA_3) &= (u + v + v_3 e_1) A_1 A_3 \text{ and} \\ (vA_3)(uA_1) &= (v + u + u_2 e_1) A_1 A_3,\end{aligned}$$

thus G is abelian if and only if $u_2 = v_3$.

Therefore, for $u_2 = v_3$ we have regular subgroups

$$\langle e_1, e_3 A_1, e_2 A_3 \rangle, \langle e_1, (e_3 + e_2) A_1, e_3 A_3 \rangle, \langle e_1, e_3 A_1, (e_3 + e_2) A_3 \rangle \cong C_{p^2} \times C_p,$$

$$\langle e_1, e_2 A_1, e_3 A_3 \rangle \cong C_p^3,$$

and for $u_2 \neq v_3$ we have nonabelian regular subgroups

$$\langle e_1, (e_2 + e_3) A_1, e_2 A_3 \rangle, \langle e_1, e_3 A_1, (e_2 + e_3) A_3 \rangle \cong Q_8.$$

Finally, we consider

$$G = \langle e_1, uA_1, vA_2 A_3 \rangle$$

for some vectors $u, v \in \mathbb{F}_p^3$, where we can assume $u_1 = v_1 = 0$. Note,

$$(vA_2 A_3)^p = (v_2 e_1 + v_3 e_2) A_1$$

so for G to be regular we need $v_3 \neq 0$. Now we have

$$\begin{aligned}(uA_1)(vA_2 A_3) &= (u + v + v_3 e_1) A_1 A_2 A_3 \text{ and} \\ (vA_2 A_3)(uA_1) &= (v + u + u_2 e_1 + u_3 e_2) A_1 A_2 A_3,\end{aligned}$$

so for G to have size p^3 we need to set $u_3 = 0$, and so we need $u_2 = 1$ for G to be regular.

Therefore, we find a regular subgroups

$$\langle e_1, e_2 A_1, e_3 A_2 A_3 \rangle, \langle e_1, e_2 A_1, (e_2 + e_3) A_2 A_3 \rangle \cong C_{p^2} \times C_p.$$

Therefore, we find

$$\frac{p^3 - 1}{p - 1}$$

regular subgroups isomorphic to C_p^3,

$$\frac{p^3 - 1}{p - 1} \times (p + 1 + (p^2 - 1)p) = (p^3 - 1)(p + 1)^2$$

isomorphic to $C_{p^2} \times C_p$, and

$$\frac{p^3-1}{p-1} \times p$$

isomorphic to Q_8 contained in Hol(C_p^3) with $|\Theta(G)| = p^2$.

The corresponding non-isomorphic braces for $p = 2$ are

$$\langle e_1, e_3A_1, e_2A_3\rangle, \langle e_1, e_2A_1, e_3A_2A_3\rangle \cong C_{p^2} \times C_p,\ \langle e_1, e_2A_1, e_3A_3\rangle \cong C_p^3,$$

$$\langle e_1, (e_2+e_3)\,A_1, e_2A_3\rangle \cong Q_8.$$

□

Corollary 5.4.8. *For $p = 3$ we have*

$$\begin{aligned} e(C_p^3, C_p^3, p^2) &= (p^3-1)p^2, \\ e(M_1, C_p^3, p^2) &= (p^2+p+1)p, \\ e(C_{p^2} \times C_p, C_p^3, p^2) &= (p-1)p, \\ e(M_2, C_p^3, p^2) &= p, \end{aligned}$$

and $e(C_{p^3}, C_p^3, p^2) = 0$. Furthermore, we have

$$\begin{aligned} \widetilde{e}(C_p^3, C_p^3, p^2) &= 2, \\ \widetilde{e}(M_1, C_p^3, p^2) &= 4, \\ \widetilde{e}(C_{p^2} \times C_p, C_p^3, p^2) &= 1, \\ \widetilde{e}(M_2, C_p^3, p^2) &= 1, \end{aligned}$$

and $\widetilde{e}(C_{p^3}, C_p^3, p^2) = 0$.

For $p = 2$ we have

$$\begin{aligned} e(C_p^3, C_p^3, p^2) &= p^3-1, \\ e(C_{p^2} \times C_p, C_p^3, p^2) &= (p+1), \\ e(Q_8, C_p^3, p^2) &= p, \end{aligned}$$

and $e(G, C_p^3, p^2) = 0$ otherwise. Furthermore, we have

$$\begin{aligned} \widetilde{e}(C_p^3, C_p^3, p^2) &= 1, \\ \widetilde{e}(C_{p^2} \times C_p, C_p^3, p^2) &= 2, \\ \widetilde{e}(Q_8, C_p^3, p^2) &= 1, \end{aligned}$$

and $\widetilde{e}(G, C_p^3, p^2) = 0$ otherwise.

Proof. Follows from Lemma 5.4.7. □

Lemma 5.4.9. *For $p = 3$ and $|\Theta(G)| = p^3$ there are no regular subgroups contained in* $\mathrm{Hol}(C_p^3)$.

For $p = 2$ and $|\Theta(G)| = p^3$ there are exactly

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

regular subgroups isomorphic to D_8 contained in $\mathrm{Hol}(C_p^3)$. *The above corresponds to one brace.*

Proof. The result for $p = 3$ and $|\Theta(G)| = p^3$ follows from Lemma 4.3.6.

For $p = 2$ and $|\Theta(G)| = p^3$, we must have that $\Theta(G)$ is conjugate to

$$B(C_p^3) \stackrel{\text{def}}{=} \langle A_1, A_2, A_3 \rangle \cong M_1 \cong D_8$$

by an element of $\mathrm{SL}_3(\mathbb{F}_p)$ and G is isomorphic to $\Theta(G)$, so we can assume, without loss of generality, that

$$G = \langle uA_1, vA_2, wA_3 \rangle$$

for some vectors

$$u = u_1e_1 + u_2e_2 + u_3e_3,\ v = v_1e_1 + v_2e_2 + v_3e_3,\ w = w_1e_1 + w_2e_2 + w_3e_3.$$

Now

$$(uA_1)^p = u_3e_1,\ (vA_2)^p = v_3e_2,\ (wA_3)^p = w_2e_1,$$

so for G to have order p^3 we need to set

$$u_3 = v_3 = w_2 = 0.$$

Note,

$$\begin{aligned}(uA_1)\,(vA_2) &= (u + v + v_3e_1)\,A_1A_2 \text{ and}\\ (vA_2)\,(uA_1) &= (u + v + u_3e_2)\,A_2A_1,\end{aligned}$$

so uA_1 and vA_2 commute since $u_3 = v_3 = w_2 = 0$ and for G to be regular we need $u + v \neq 0$. We have

$$\begin{aligned}(uA_1)\,(wA_3) &= (u + w + w_3e_1)\,A_1A_3 \text{ and}\\ (wA_3)\,(uA_1) &= (u + w + u_2e_1)\,A_1A_2,\end{aligned}$$

so vA_1 and wA_2 commute if and only if $w_3 = u_2$, again for G to be regular we need

$u + w \neq 0$, and we finally have

$$(wA_3)(vA_2) = (w + v + v_2e_1)A_3A_2 \text{ and}$$
$$(uA_1)(vA_2)(wA_3) = (w + v + u + w_3e_1 + w_3e_2)A_1A_2A_3,$$

so $(uA_1)(vA_2)(wA_3) = (wA_3)(vA_2)$ if and only if

$$u = (v_2 - w_3)e_1 - w_3e_2,$$

which implies that $u_2 = -w_3 = w_3$ and $u_1 = v_2 - w_3$.

Therefore, gathering all the conditions together, for G to be isomorphic to M_1, we need

$$u_2 = w_3,\ u_3 = v_3 = w_2 = 0,\ u_1 = v_2 - w_3;$$

so we must have

$$u = (v_2 - w_3)e_1 + w_3e_2,\ v = v_1e_1 + v_2e_2,\ w = w_1e_1 + w_3e_3.$$

Now for G to act transitively we need $w_3 = 1$, so we have

$$u = (v_2 - 1)e_1 + e_2,\ v = v_1e_1 + v_2e_2,\ w = w_1e_1 + e_3,$$

and for G to act freely, we need to have

$$u + v = (v_1 + v_2 + 1)e_1 + (v_2 + 1)e_2 \neq 0,$$

so we need $v_1 = 1$.

Therefore, we have

$$u = (v_2 - 1)e_1 + e_2,\ v = e_1 + v_2e_2,\ w = w_1e_1 + e_3.$$

This gives us p^2 subgroups of the form $\langle uA_1, vA_2, wA_3\rangle \cong D_8$. Note, the set of upper triangular matrices is the normaliser of the set of upper triangular matrices with 1 on the diagonals, so $\mathrm{SL}_3(\mathbb{F}_p)$ contains

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

Sylow p-subgroups, and thus we have

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

regular subgroups isomorphic to D_8 contained in Hol(C_p^3) with $|\Theta(G)| = p^3$.

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

note that for

$$B = \begin{pmatrix} 1 & b_2 & b_3 \\ 0 & 1 & b_5 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p),$$

we have

$$BA_1B^{-1} = A_1,\ BA_2B^{-1} = A_1^{b_2}A_2,\ BA_3B^{-1} = A_1^{b_5}A_3;$$

thus we find

$$\begin{aligned} B\left(uA_1\right)B^{-1} &= \left(\left(v_2 - 1 + b_2\right)e_1 + e_2\right)A_1, \\ B\left(uA_1\right)^{b_2}\left(vA_2\right)B^{-1} &= \left(e_1 + \left(b_2 + v_2\right)e_2\right)A_2, \\ B\left(uA_1\right)^{b_5}\left(wA_3\right)B^{-1} &= \left(\left(b_5\left(v_2 - 1\right) + w_1 + b_2b_5 + b_3 + b_5\right)e_1 + e_3\right)A_3. \end{aligned}$$

Now, conjugating the regular subgroup $\langle uA_1, vA_2, wA_3\rangle$ as given above with B for $b_2 = v_2 - 1$, $b_3 = w_1$, and $b_5 = 0$, we get

$$\langle e_2A_1, \left(e_1 + e_2\right)A_2, e_3A_3, \rangle \cong D_8.$$

□

Corollary 5.4.10. *For $p = 3$ we have $e(G, C_p^3, p^3) = 0$ also $\widetilde{e}(G, C_p^3, p^3) = 0$ for any group G.*

For $p = 2$ we have

$$e(D_8, C_p^3, p^3) = p^2$$

and $e(G, C_p^3, p^3) = 0$ if $G \neq D_8$. Furthermore, we have

$$\widetilde{e}(D_8, C_p^3, p^3) = 1$$

and $\widetilde{e}(G, C_p^3, p^3) = 0$ if $G \neq D_8$.

Proof. Follows from Lemma 5.4.9. □

5.5 Regular subgroups contained in Hol(M_1) for $p = 3$

In this section we find the regular subgroups contained in Hol(M_1) for $p = 3$ and the corresponding skew braces. The main results of this section is the following.

Proposition 5.5.1. *For $p = 3$ we have*

$$\begin{aligned} e(M_1, M_1) &= 317, \\ e(C_p^3, M_1) &= 1300, \\ e(M_2, M_1) &= 12, \\ e(C_{p^2} \times C_p, M_1) &= 12, \end{aligned}$$

and $e(C_{p^3}, M_1) = 0$.

Furthermore, we have

$$\begin{aligned} \widetilde{e}(M_1, M_1) &= 14, \\ \widetilde{e}(C_p^3, M_1) &= 5, \\ \widetilde{e}(M_2, M_1) &= 4 \\ \widetilde{e}(C_{p^2} \times C_p, M_1) &= 2, \end{aligned}$$

and $\widetilde{e}(C_{p^3}, M_1) = 0$.

The proof of proposition above follows from calculation in the rest of this section. We shall use the notation of Section 4.4. Recall a subgroup of Hol(M_1) of order p^3 lies in one of $p + 1$ conjugates of

$$M_1 \rtimes \langle \alpha_1, \alpha_2, \alpha_3 \rangle \cong M_1 \rtimes M_1.$$

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. First, we note for natural numbers r, a_i and an element $v = \rho^{v_1}\sigma^{v_2}\tau^{v_3} \in M_2$, we have

$$(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^p = \rho^{(a_3+v_2)a_2v_2}, \tag{5.7}$$

so the element $v\alpha_1^{a_1}\alpha_2^{a_3}\alpha_3^{a_2}$ can have order p or p^2 depending on various configurations, and this is the main difference in comparison to Section 4.4 where the element $v\alpha_1^{a_1}\alpha_2^{a_3}\alpha_3^{a_2}$ could only have order p.

Lemma 5.5.2. *For $p = 3$ and $|\Theta(G)| = p$ there are exactly*

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

regular subgroups isomorphic to M_1*,*

$$p^2 + p - 1$$

isomorphic to C_p^3*,* $(p-1)^3 p$ *isomorphic to* M_2*, and* $(p-1)^3 p$ *isomorphic to* $C_{p^2} \times C_p$ *contained in* Hol(M_1)*.*

Furthermore, there are three M_1*, one* C_p^3*, one* M_2*, and one* $C_{p^2} \times C_p$*-skew braces of* M_1 *type.*

Proof. Most procedures are similar to Lemma 4.4.2, so in some places we avoid unnecessary repetitions. If $G \subseteq \mathrm{Hol}(M_1)$ with $|\Theta(G)| = p$, then we can assume $\Theta(G)$ is one of

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

and $G \cap M_1$ is one of

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

We shall consider all subgroups of order p^2 in M_1 and all ways of pairing them with a subgroup of order p of $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$ and then multiply our findings by $p+1$ whenever a pairing involves α_2.

We start with the subgroup $\langle \rho, \tau \rangle$ of M_1. Hence, we must have

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

Now

$$g^p = (\sigma \alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3})^p = \rho^{(a_3+1)a_2}.$$

Further, for $r \neq 0$ we have

$$\begin{aligned} (\sigma \alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3})\, \tau^r &= \rho^{a_3 r} \sigma \tau^r \alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3}, \\ \tau^r\, (\sigma \alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3}) &= \rho^r \sigma \tau^r \alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3}. \end{aligned}$$

Now if $a_2 = 0$, then we find regular subgroups

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

if $a_2 \neq 0$ and $a_3 = -1$, then we find regular subgroups

$$\langle \rho, \tau, \sigma \alpha_1^c \alpha_2^b \alpha_3^{-1} \rangle \cong M_1 \text{ for } c = 0, ..., p-1,\ b = 1, ..., p-1;$$

and if $a_2 \neq 0$ and $a_3 \neq -1$, then we find regular subgroups

$$\left\langle \rho, \tau, \sigma\alpha_1^c\alpha_2^b \right\rangle \cong M_2,\ \left\langle \rho, \tau, \sigma\alpha_1^c\alpha_2^b\alpha_3 \right\rangle \cong C_{p^2} \times C_p \text{ for } c = 0, ..., p-1,\ b = 1, ..., p-1.$$

Next, we consider the subgroups $\left\langle \rho, \sigma\tau^d \right\rangle$ of M_1 for some $d = 0, ..., p-1$, and investigate the possibility of pairing these subgroups with subgroups of the from $\langle \alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3} \rangle$. Thus, we can consider subgroups of the form

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

Note, we have

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

and for r a natural number we have

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

so for the pairing to be possible we need $a_2 = 0$.

Therefore, similar to Lemma 4.4.2, for $da_3 + a_1 + 1 \equiv 0 \bmod p$, we find regular subgroups

$$\left\langle \rho, \sigma\tau^d, \tau\alpha_1^{-(cd+1)}\alpha_3^c \right\rangle \cong C_p^3 \text{ for } c, d = 0, ..., p-1,$$

and for $da_3 + a_1 + 1 \not\equiv 0 \bmod p$, we find regular subgroups

$$\begin{aligned} &\left\langle \rho, \sigma\tau^d, \tau\alpha_1 \right\rangle, \left\langle \rho, \sigma\tau^d, \tau\alpha_1^a\alpha_3^c \right\rangle \cong M_1 \\ &\text{for } a, d = 0, ..., p-1,\ c = 1, ..., p-1 \text{ with } a + cd + 1 \not\equiv 0 \bmod p. \end{aligned}$$

Therefore, we have that if $G \subseteq \text{Hol}(M_1)$ is a regular subgroup with $|\Theta(G)| = p$ and $p = 3$, then G is isomorphic to either M_1, C_p^3, M_2, or $C_{p^2} \times C_p$. In particular, there are (we shall multiply by $p+1$ appropriately wherever a subgroup involves α_2)

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

regular subgroups isomorphic to M_1,

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

regular subgroups isomorphic to C_p^3,

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

regular subgroups isomorphic to M_2, and

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

isomorphic to $C_{p^2} \times C_p$.

The corresponding non-isomorphic skew braces are

$$\langle \rho, \tau, \sigma\alpha_1 \rangle, \langle \rho, \tau, \sigma\alpha_3^{-1} \rangle, \langle \rho, \tau, \sigma\alpha_2\alpha_3^{-1} \rangle \cong M_1,$$

$$\langle \rho, \tau, \sigma\alpha_3 \rangle \cong C_p^3,\ \langle \rho, \tau, \sigma\alpha_2 \rangle \cong M_2,\ \langle \rho, \tau, \sigma\alpha_2\alpha_3 \rangle \cong C_{p^2} \times C_p;$$

therefore there are three M_1, one C_p^3, one M_2, and one $C_{p^2} \times C_p$-skew braces of M_1 type. □

Corollary 5.5.3. *For $p = 3$ we have*

$$\begin{aligned} e(M_1, M_1, p) &= p^4 - p^3 - p^2 - p + 1, \\ e(C_p^3, M_1, p) &= (p^3 - 1)(p^2 + p - 1), \\ e(M_2, M_1, p) &= p, \\ e(C_{p^2} \times C_p, M_1, p) &= (p-1)p, \end{aligned}$$

and $e(C_{p^3}, M_1, p) = 0$.

Furthermore, we have

$$\begin{aligned} \widetilde{e}(M_1, M_1, p) &= 3, \\ \widetilde{e}(C_p^3, M_1, p) &= 1, \\ \widetilde{e}(M_2, M_1, p) &= 1, \\ \widetilde{e}(C_{p^2} \times C_p, M_1, p) &= 1, \end{aligned}$$

and $\widetilde{e}(C_{p^3}, M_1, p) = 0$.

Proof. Follows from Lemma 5.5.2. □

Lemma 5.5.4. *For $p = 3$ and $|\Theta(G)| = p^2$ there are exactly*

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

regular subgroups isomorphic to M_1,

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

isomorphic to C_p^3 ,

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

isomorphic to M_2, and $(p-1)^3 p$ isomorphic to $C_{p^2} \times C_p$ contained in Hol(M_1).

Furthermore, there are six M_1, four C_p^3 , three M_2, and one $C_{p^2} \times C_p$-skew braces of M_1 type.

Proof. If $G \subseteq \mathrm{Hol}(M_1)$ with $|\Theta(G)| = p^2$ and $p = 3$, then we can assume that we have $\Theta(G) \subseteq \langle \alpha_1, \alpha_2, \alpha_3 \rangle$ a subgroup of order p^2 and $G \cap M_1$ a subgroup of order p.

By calculation similar to that of Lemma 4.4.4, we can consider subgroups of the form

$$G = \langle \rho, u\alpha_1, v\alpha_3 \rangle , \langle \rho, x\alpha_1, y\alpha_2\alpha_3^a \rangle .$$

Let us consider

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

Then identically to Lemma 4.4.4, we have regular subgroups

$$\begin{aligned} &\langle \rho, u\alpha_1, v\alpha_3 \rangle \cong C_p^3 \\ &\text{for } A = \begin{pmatrix} u_2 & v_2 \\ u_3 & v_3 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \text{ with } v_2 = u_3 + \det(A). \end{aligned} \tag{5.8}$$

There are

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

of these. We also find regular subgroups

$$\begin{aligned} &\langle \rho, u\alpha_1, v\alpha_3 \rangle \cong M_1 \\ &\text{for } A = \begin{pmatrix} u_2 & v_2 \\ u_3 & v_3 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \text{ with } v_2 - u_3 - \det(A) \not\equiv 0 \bmod p, \end{aligned} \tag{5.9}$$

and there are

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

of these.

Next, we consider the 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

$$(y\alpha_2\alpha_3^a)^p = \rho^{(a+y_2)y_2},$$

we also have

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

so G is abelian if and only if $y_2 = ax_3 - x_3y_2$, also G is of exponent p if $a + y_2 = 0$ and exponent p^2 otherwise.

Therefore, we have regular subgroups

$$\left\langle \rho, \tau\alpha_1, \sigma^{y_2}\tau^{y_3}\alpha_2\alpha_3^{-y_2} \right\rangle \cong C_p^3 \text{ for } y_3 = 0, ..., p-1,\ y_2 = 1, ..., p-1,$$
$$\left\langle \rho, \tau^2\alpha_1, \sigma^{y_2}\tau^{y_3}\alpha_2 \right\rangle \cong C_{p^2} \times C_p \text{ for } y_3 = 0, ..., p-1,\ y_2 = 1, ..., p-1,$$

and if $y_2 \neq ax_3 - x_3y_2$, then we find regular subgroups

$$\left\langle \rho, \tau^2\alpha_1, y\alpha_2\alpha_3^{-y_2} \right\rangle \cong M_1 \text{ for } y_1 = 0, ..., p-1,\ y_2 = 1, ..., p-1,$$
$$\langle \rho, \tau^{x_3}\alpha_1, y\alpha_2\alpha_3^{a} \rangle \cong M_2 \text{ for } a, y_3 = 0, ..., p-1,\ x_3, y_2 = 1, ..., p-1$$
$$\text{with } y_2 \neq ax_3 - x_3y_2,\ a \neq -y_2.$$

In summary, we have that if $G \subseteq \mathrm{Hol}(M_1)$ is a regular subgroup with $|\Theta(G)| = p^2$ and $p = 3$, then G is isomorphism to either M_1, C_p^3, M_2, or $C_{p^2} \times C_p$. In particular (note we have to multiply by $p + 1 = (p-1)^2$ whenever a subgroup contains α_2), there are

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

isomorphic to M_1,

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

isomorphic to C_p^3,

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

isomorphic to M_2, and $(p-1)^3p$ isomorphic to $C_{p^2} \times C_p$.

The corresponding non-isomorphic skew braces are

$$\langle \rho, \sigma\alpha_1, \sigma^{u_3}\tau^{u_4}\alpha_3 \rangle, \left\langle \rho, \tau^{-1}\alpha_1, \sigma\alpha_3 \right\rangle, \left\langle \rho, \tau^2\alpha_1, \sigma\alpha_2\alpha_3^2 \right\rangle \cong M_1,\ \langle \rho, \tau^{x_3}\alpha_1, \sigma\alpha_2\alpha_3^a \rangle \cong M_2,$$

$$\left\langle \rho, \sigma^{u_2}\tau^{-u_2}\alpha_1, \tau\alpha_3 \right\rangle, \left\langle \rho, \tau^{-2}\alpha_1, \sigma^2\alpha_3 \right\rangle, \left\langle \rho, \tau\alpha_1, \sigma\alpha_2\alpha_3^2 \right\rangle \cong C_p^3,$$
$$\left\langle \rho, \tau^2\alpha_1, \sigma\alpha_2 \right\rangle \cong C_{p^2} \times C_p \text{ for } a = 0, 1,\ u_4 = 0, ..., p-1,\ u_2, u_3, x_3 = 1, ..., p-1$$
$$\text{with } u_3 \neq v_4,\ ax_3 \neq (1 + x_3);$$

therefore there are

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

of M_1,

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

of C_p^3, three M_2, and one $C_{p^2} \times C_p$-skew braces of M_1 type. □

Corollary 5.5.5. *For $p = 3$ we have*

$$\begin{aligned} e(M_1, M_1, p^2) &= (p^3 - p^2 + 1)p, \\ e(C_p^3, M_1, p^2) &= (p^3 - 1)(p^2 + p + 1)p, \\ e(M_2, M_1, p^2) &= p^2, \\ e(C_{p^2} \times C_p, M_1, p^2) &= (p - 1)p, \end{aligned}$$

and $e(C_{p^3}, M_2, p^2) = 0$.

Furthermore, we have

$$\begin{aligned} \widetilde{e}(M_1, M_1, p^2) &= 6, \\ \widetilde{e}(C_p^3, M_1, p^2) &= 4, \\ \widetilde{e}(M_2, M_1, p^2) &= 3, \\ \widetilde{e}(C_{p^2} \times C_p, M_1, p^2) &= 1, \end{aligned}$$

and $\widetilde{e}(C_{p^3}, M_2, p^2) = 0$.

Proof. Follows from Lemma 5.5.4. □

Lastly, if $G \subseteq \mathrm{Hol}(M_1)$ with $|\Theta(G)| = p^3$ and $p = 3$, then calculation identical to that of Lemma 4.4.6 and Corollary 4.4.7 will show that we only have

$$e(M_1, M_1, p^3) = (p + 1)(p - 1)p^3 \text{ and } \widetilde{e}(M_1, M_1, p^3) = 4.$$

5.6 Regular subgroups contained in $\mathrm{Hol}(M_2)$ for $p = 3$

In this section we find the regular subgroups contained in Hol(M_2) for $p = 3$ and the corresponding skew braces. The main results of this section is the following.

Proposition 5.6.1. *For $p = 3$ we have*

$$\begin{aligned} e(M_2, M_2) &= 78, \\ e(C_{p^2} \times C_p, M_2) &= 78, \\ e(M_1, M_2) &= 96, \\ e(C_p^3, M_2) &= 1248, \end{aligned}$$

and $e(C_{p^3}, C_p^3) = 0$.

Furthermore, we have

$$\begin{aligned}\widetilde{e}(M_2, M_2) &= 22,\\ \widetilde{e}(C_{p^2} \times C_p, M_2) &= 11,\\ \widetilde{e}(M_1, M_2) &= 4,\\ \widetilde{e}(C_p^3, M_2) &= 2,\end{aligned}$$

and $\widetilde{e}(C_{p^3}, C_p^3) = 0$.

The proof of proposition above follows from the calculations in rest of this section. We shall use the notation of Section 4.5. Recall a subgroup of Hol(M_2) of order p^3 lies in

$$M_2 \rtimes \langle \alpha_1, \alpha_2, \alpha_3 \rangle \cong M_2 \rtimes M_1.$$

We have

$$\begin{aligned}e(M_2, M_2, 1) = \widetilde{e}(M_2, M_2, 1) = 1,\\ e(G, M_2, 1) = \widetilde{e}(G, M_2, 1) = 0 \text{ if } G \neq M_2.\end{aligned}$$

We shall deal with the cases $|\Theta(G)| = p, p^2, p^3$ in the following lemmas. First we note that for natural numbers r, a_i and an element $v = \sigma^{v_1}\tau^{v_2} \in M_2$, we have

$$(v\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3})^p = v^{(a_2a_3+a_2v_1+1)p} = \sigma^{v_1(a_2a_3+a_2v_1+1)p}, \tag{5.10}$$

so the element $v\alpha_1^{a_1}\alpha_2^{a_3}\alpha_3^{a_2}$ can have order p or p^2 depending on various configurations, and this is the main difference in comparison to Section 4.5.

Lemma 5.6.2. *For $p = 3$ and $|\Theta(G)| = p$ there are exactly*

$$p^3 + p - 1$$

regular subgroups isomorphic to M_2,

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

isomorphic to $C_{p^2} \times C_p$, p isomorphic to M_1, and p isomorphic to C_p^3 contained in Hol(M_2).

Furthermore, there are eight M_2, four $C_{p^2} \times C_p$, one M_1, and one C_p^3-skew braces of M_2 type.

Proof. Most procedures are similar to Lemma 4.5.2. If $G \subseteq \mathrm{Hol}(M_2)$ with $|\Theta(G)| = p$ and $p = 3$, then $\Theta(G)$ is one of

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

and $G \cap M_2$ is one of

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

We shall consider all subgroups of order p^2 in M_2 and all ways of pairing them with a subgroup of order p of $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$.

We start with the subgroup $\langle \sigma^p, \tau \rangle$ of M_2. Then we must have

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

Note,

$$g^p = \sigma^{(a_2a_3+a_2+1)p},$$

so G has exponent p if and only if $a_2a_3 + a_2 + 1 = 0$. Now for $r \neq 0$ we have

$$g\tau^r = \sigma^{ra_3p}\sigma\tau^r\alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3} = \sigma^{ra_3p-rp}\tau^r g = g^{r(a_3-1)p}\tau^r g,$$

so G is abelian if and only if $a_3 = 1$.

Therefore, when $a_3 = 1$ we find regular subgroups

$$\left\langle \tau, \sigma\alpha_1^a\alpha_2^b\alpha_3 \right\rangle \cong C_{p^2} \times C_p, \ \langle \sigma^p, \tau, \sigma\alpha_1^a\alpha_2\alpha_3 \rangle \cong C_p^3 \text{ for } a = 0, ..., p-1, \ b = 0, 2;$$

if $a_3 \neq 1$, then G is nonabelian; in such case we have that G is exponent p^2 when $a_2(a_3 + 1) + 1 \neq 0$, and G is exponent p when $a_2(a_3 + 1) + 1 = 0$. We find regular subgroups

$$\langle \tau, \sigma\alpha_1^{a_1} \rangle, \langle \tau, \sigma\alpha_1^a\alpha_2 \rangle, \left\langle \tau, \sigma\alpha_1^a\alpha_2^b\alpha_3^{-1} \right\rangle \cong M_2, \ \left\langle \tau, \sigma^p, \sigma\alpha_1^a\alpha_2^{-1} \right\rangle \cong M_1$$

$$\text{for } a, b = 0, ..., p-1, \ a_1 = 1, ..., p-1.$$

Finally, we consider the subgroups $\left\langle \sigma\tau^d \right\rangle$ of M_2 for some $d = 0, ..., p-1$, and investigate the possibility of pairing these subgroups with a subgroup of the form $\langle \alpha_1^{a_1}\alpha_2^{a_2}\alpha_3^{a_3} \rangle$. Thus, we consider subgroups of the form

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

Note we need

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

and since we have

$$\left(\sigma\tau^d\right)^{(a_3d+a_1+1)p+1} = \sigma^{(a_3d+a_1+1)p+1}\tau^d,$$

for the pairing to be possible, we need $a_2 = 0$.

Therefore, similarly to Lemma 4.5.2, we find regular subgroups

$$\begin{aligned}
&\left\langle \sigma\tau^d, \tau\alpha_1^{-(cd+1)}\alpha_3^c \right\rangle \cong C_{p^2} \times C_p \text{ for } c, d = 0, ..., p-1,\\
&\left\langle \sigma\tau^d, \tau\alpha_1 \right\rangle, \left\langle \sigma\tau^d, \tau\alpha_1^a\alpha_3^c \right\rangle \cong M_2\\
&\text{for } a, d = 0, ..., p-1,\ c = 1, ..., p-1 \text{ with } a + cd + 1 \not\equiv 0 \bmod p.
\end{aligned}$$

In summary, we have that if $G \subseteq \mathrm{Hol}(M_2)$ is a regular subgroup with $|\Theta(G)| = p$ and $p = 3$, then G is isomorphic to either M_2, $C_{p^2} \times C_p$, M_1, or C_p^3 . In particular, there are

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

regular subgroups isomorphic to M_2,

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

isomorphic to $C_{p^2} \times C_p$, p isomorphic to M_1, and p isomorphic to C_p^3.

The corresponding non-isomorphic skew braces are

$$\langle \tau, \sigma\alpha_1 \rangle, \langle \tau, \sigma\alpha_2 \rangle, \left\langle \tau, \sigma\alpha_3^{-1} \right\rangle, \left\langle \tau, \sigma\alpha_2^a\alpha_3^{-1} \right\rangle, \langle \sigma, \tau\alpha_1 \rangle, \left\langle \sigma, \tau\alpha_1^{a-1}\alpha_3 \right\rangle \cong M_2,$$

$$\left\langle \sigma^p, \tau, \sigma\alpha_2^{-1} \right\rangle \cong M_1,\ \langle \tau, \sigma\alpha_3 \rangle, \left\langle \tau, \sigma\alpha_2^{-1}\alpha_3 \right\rangle, \left\langle \sigma, \tau\alpha_1^{-1} \right\rangle, \left\langle \sigma, \tau\alpha_1\alpha_3^{-1} \right\rangle \cong C_{p^2} \times C_p,$$

$$\langle \sigma^p, \tau, \sigma\alpha_2\alpha_3 \rangle \cong C_p^3 \text{ for } a = 1, 2;$$

therefore, we find eight M_2, four $C_{p^2} \times C_p$, one M_1, and one C_p^3-skew braces of M_2 type. □

Corollary 5.6.3. *For $p = 3$ we have*

$$\begin{aligned}
e(M_2, M_2, p) &= p^3 + p - 1,\\
e(C_{p^2} \times C_p, M_2, p) &= (p^2 - p - 1)(p-1)p,\\
e(M_1, M_2, p) &= (p^2 - 1)p,\\
e(C_p^3, M_2, p) &= (p^3 - 1)(p^2 - 1)p,
\end{aligned}$$

and $e(C_{p^3}, M_2, p) = 0$.

Furthermore, we have

$$\begin{aligned}
\widetilde{e}(M_2, M_2, p) &= 8,\\
\widetilde{e}(C_{p^2} \times C_p, M_2, p) &= 4,\\
\widetilde{e}(M_1, M_2, p) &= 1,\\
\widetilde{e}(C_p^3, M_2, p) &= 1,
\end{aligned}$$

and $\widetilde{e}(C_{p^3}, M_2, p) = 0$.

Proof. Follows from Lemma 5.6.2. □

Lemma 5.6.4. *For $p = 3$ and $|\Theta(G)| = p^2$ there are exactly $(p-1)^4 p$ regular subgroups isomorphic to M_2, $(p-1)^3 p$ isomorphic to $C_{p^2} \times C_p$, p^2 isomorphic to M_1, and p isomorphic to C_p^3 contained in* Hol(M_2).

Furthermore, there are twelve M_2, seven $C_{p^2} \times C_p$, three M_1, and one C_p^3-skew braces of M_2 type.

Proof. If $G \subseteq \mathrm{Hol}(M_2)$ with $|\Theta(G)| = p^2$ and $p = 3$, then $\Theta(G)$ 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 $G \cap M_2$ is one of

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

We shall consider all subgroups of order p in M_2 and all ways of pairing them with a subgroup of order p^2 of $\langle \alpha_1, \alpha_2, \alpha_3 \rangle$.

We start with the subgroup $\langle \sigma^p \rangle$ of M_2, and to obtain regular subgroups, following the method of Lemma 4.5.4, we consider subgroups of the form

$$G = \langle \sigma^p, u\alpha_1, v\alpha_3 \rangle, \langle \sigma^p, x\alpha_1, y\alpha_2 \alpha_3^a \rangle.$$

Note, we have

$$(u\alpha_1)^p = u^p, \ (v\alpha_3)^p = v^p, \ (y\alpha_2\alpha_3^a)^p = y^{(a+y_1+1)p}.$$

Therefore, considering the subgroups of the form

$$G = \langle \sigma^p, u\alpha_1, v\alpha_3 \rangle,$$

by calculation identical to that of Lemma 4.5.4, we find regular subgroups

$\langle \tau\alpha_1, \sigma^{-1}\tau^{v_2}\alpha_3 \rangle \cong C_{p^2} \times C_p$ for $v_2 = 0, ..., p-1$,
$\langle \tau^{u_2}\alpha_1, \sigma^{v_1}\tau^{v_2}\alpha_3 \rangle \cong M_2$ for $v_2 = 0, ..., p-1$, $u_2, v_1 = 1, ..., p-1$ with $v_1 \neq u_2 - u_1 v_2$,
$\langle u\alpha_1, v\alpha_3 \rangle \cong C_{p^2} \times C_p$ for $A = \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$ with $u_1 \neq 0$, $v_1 = u_2 + \det(A)$,
$\langle u\alpha_1, v\alpha_3 \rangle \cong M_2$ for $A = \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$ with $u_1 \neq 0$, $v_1 \neq u_2 + \det(A)$.

Next, we consider subgroups of the form

$$G = \langle \sigma^p, x\alpha_1, y\alpha_2 \alpha_3^a \rangle,$$

and for G to have size p^3, we must to set $x_1 = 0$, so for G to be regular we need

$x_2, y_1 \neq 0$. Now, the element $y\alpha_2\alpha_3^a$ has order p if $a + y_1 + 1 \equiv 0 \bmod p$ and order p^2 otherwise, also G is abelian if and only if $ax_2 - y_1 - x_2y_1 \equiv 0 \bmod p$.

Therefore, when $ax_2 = y_1 + x_2y_1$ we find regular subgroups

$$\left\langle \tau^{x_2}\alpha_1, \sigma^{y_1}\tau^{y_2}\alpha_2\alpha_3^{(1+x_2)y_1x_2^{-1}} \right\rangle \cong C_{p^2} \times C_p$$

$$\text{for } x_2, y_1 = 1, ..., p-1,\ y_2 = 0, ..., p-1 \text{ with } x_2^{-1}y_1 - y_1 + 1 \neq 0,$$

$$\left\langle \sigma^p, \tau^{-1}\alpha_1, \sigma^{-1}\tau^{y_2}\alpha_2 \right\rangle \cong C_p^3 \text{ for } y_2 = 0, ..., p-1,$$

and if $ax_2 \neq y_1 + x_2y_1$, then we have regular subgroups

$$\langle \tau^{x_2}\alpha_1, \sigma^{y_1}\tau^{y_2}\alpha_2\alpha_3^a \rangle \cong M_2 \text{ for } x_2, y_1 = 1, ..., p-1,\ a, y_2 = 0, ..., p-1,$$

$$\text{with } ax_2 \neq y_1 + x_2y_1,\ a + y_1 + 1 \neq 0,$$

$$\left\langle \sigma^p, \tau^{x_2}\alpha_1, \sigma^{y_1}\tau^{y_2}\alpha_2\alpha_3^{-y_1-1} \right\rangle \cong M_1$$

$$\text{for } x_2, y_1 = 1, ..., p-1,\ y_2 = 0, ..., p-1, \text{ with } x_2 + y_1 - x_2y_1 \neq 0.$$

Finally, we consider the subgroup $\left\langle \tau\sigma^{bp} \right\rangle$ of M_2 for $b = 0, ..., p-1$, and investigate the possibility of pairing this subgroup with the subgroups

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

It follows from (5.10) that we can consider a subgroups of the form

$$G = \left\langle \tau\sigma^{bp}, \sigma^{u_1p}\alpha_1, \sigma^{v_1}\alpha_2^{a_2}\alpha_3^{a_3} \right\rangle \text{ with } a_2a_3 + a_2v_1 + 1 = 0,\ u_1, v_1 \not\equiv 0 \bmod p.$$

Now

$$\begin{aligned}(\sigma^{pu_1}\alpha_1)\,(\sigma^{v_1}\alpha_2\alpha_3^{a_3}) &= \sigma^{u_1p}\sigma^{v_1p}\sigma^{v_1}\alpha_1\alpha_2\alpha_3^{a_3} \text{ and}\\ (\sigma^{v_1}\alpha_2\alpha_3^{a_3})\,(\sigma^{u_1p}\alpha_1) &= \sigma^{u_1p}\sigma^{v_1}\alpha_1\alpha_2\alpha_3^{a_3},\end{aligned}$$

which implies that we need $v_1 \equiv 0 \bmod p$ which is not possible if we want G to be regular. Therefore, there are no regular subgroup of this form.

In summary, we have that if $G \subseteq \text{Hol}(M_2)$ is a regular subgroup with $|\Theta(G)| = p^2$ and $p = 3$, then G is isomorphic to either M_2, $C_{p^2} \times C_p$, M_1, or C_p^3. In particular, there are

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

regular subgroup isomorphic to M_2,

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

isomorphic to $C_{p^2} \times C_p$,

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

isomorphic to M_1, and p isomorphic to C_p^3.

The corresponding non-isomorphic skew braces are

$$\left\langle \tau^{u_2}\alpha_1, \sigma^{v_1}\alpha_3 \right\rangle, \left\langle \tau^{-1}\alpha_1, \sigma\tau^{v_2}\alpha_3 \right\rangle, \left\langle \sigma\alpha_1, \sigma^{t_3}\tau^{t_4}\alpha_3 \right\rangle, \left\langle \tau^{x_2}\alpha_1, \sigma^s\alpha_2\alpha_3^a \right\rangle \cong M_2,$$

$$\left\langle \sigma^p, \tau^{x_2}\alpha_1, \sigma^s\alpha_2\alpha_3^{-s-1} \right\rangle \cong M_1, \left\langle \tau\alpha_1, \sigma^{-1}\alpha_3 \right\rangle, \left\langle \tau^{-2}\alpha_1, \sigma^2\tau\alpha_3 \right\rangle, \left\langle \sigma\alpha_1, \sigma^{u_3}\tau^{u_3}\alpha_3 \right\rangle,$$

$$\left\langle \tau^{x_2}\alpha_1, \sigma^s\alpha_2\alpha_3^{s(1+x_2)x_2^{-1}} \right\rangle \cong C_{p^2} \times C_p, \ \left\langle \sigma^p, \tau^{-1}\alpha_1, \sigma^{-1}\alpha_2 \right\rangle \cong C_p^3$$

$$\text{for } a, t_3 = 0, ..., p-1, \ u_2, v_1, t_4, x_2, u_3 = 1, ..., p-1, \ v_2 = 0, 1, \ s \in \mathbb{F}_p^\times,$$

$$\text{with } u_2 \neq -v_1, \ u_2 \neq v_1(1+u_2), \ t_3 \neq t_4, \ ax_2 \neq s(1+x_2),$$

$$a \neq -s-1, \ s(x_2^{-1}-1) \neq 2;$$

therefore there are

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

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

M_2,

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

$C_{p^2} \times C_p$,

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

M_1, and one C_p^3-skew braces of M_2 type. □

Corollary 5.6.5. *For $p = 3$ we have*

$$\begin{aligned} e(M_2, M_2, p^2) &= (p-1)^4 p, \\ e(C_{p^2} \times C_p, M_2, p^2) &= (p-1)^4 p, \\ e(M_1, M_2, p^2) &= (p^2-1)p^2, \\ e(C_p^3, M_2, p^2) &= (p^3-1)(p^2-1)p, \end{aligned}$$

and $e(C_{p^3}, M_2, p^2) = 0$.

Furthermore, we have

$$\begin{aligned} \widetilde{e}(M_2, M_2, p^2) &= 13, \\ \widetilde{e}(C_{p^2} \times C_p, M_2, p^2) &= 7, \\ \widetilde{e}(M_1, M_2, p^2) &= 3, \\ \widetilde{e}(C_p^3, M_2, p^2) &= 1, \end{aligned}$$

and $\widetilde{e}(C_{p^3}, M_2, p^2) = 0$.

Proof. Follows from Lemma 5.6.4. □

Lastly, if $G \subseteq \mathrm{Hol}(M_2)$ with $|\Theta(G)| = p^3$ and $p = 3$, then we must have $\Theta(G) = \langle \alpha_1, \alpha_2, \alpha_3 \rangle$, and so

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

For G to have size p^3 we require $u^p = w^p = 1$ and $v^{(v_1+1)p} = 1$, so we may assume

$$G = \langle \sigma^{u_1 p}\tau^{u_2}\alpha_1, \sigma^{v_1}\tau^{v_2}\alpha_2, \sigma^{w_1 p}\tau^{w_2}\alpha_2 \rangle , \text{ with } v_1(v_1+1) \equiv 0 \bmod p.$$

Note G maps isomorphically onto M_1. Now we have

$$\begin{aligned}(\sigma^{u_1 p}\tau^{u_2}\alpha_1)(\sigma^{w_1 p}\tau^{w_2}\alpha_3) &= \sigma^{u_1 p}\tau^{u_2}\sigma^{w_1 p}\tau^{w_2}\alpha_1\alpha_3 \text{ and}\\ (\sigma^{w_1 p}\tau^{w_2}\alpha_3)(\sigma^{u_1 p}\tau^{u_2}\alpha_1) &= \sigma^{w_1 p}\tau^{w_2}\sigma^{u_1 p}(\sigma^p\tau)^{u_2}\alpha_1\alpha_3,\end{aligned}$$

so we need $u_2 = 0$. We also have

$$\begin{aligned}(\sigma^{u_1 p}\alpha_1)(\sigma^{v_1}\tau^{v_2}\alpha_2) &= \sigma^{u_1 p}\sigma^{v_1 p}\sigma^{v_1}\tau^{v_2}\alpha_1\alpha_2 \text{ and}\\ (\sigma^{v_1}\tau^{v_2}\alpha_2)(\sigma^{u_1 p}\alpha_1) &= \sigma^{v_1}\tau^{v_2}\sigma^{u_1 p}\alpha_1\alpha_2,\end{aligned}$$

so we need $v_1 \equiv 0 \bmod p$, but now G cannot be regular. Therefore, there are no regular subgroups of this form.

5.7 Regular subgroups contained in $\mathrm{Hol}(D_8)$

In this section we find the regular subgroups contained in $\mathrm{Hol}(D_8)$ and the corresponding skew braces. The main result of this section is the following.

Proposition 5.7.1. *For $p = 2$ we have*

$$\begin{aligned}e(D_8, D_8) &= 6,\\ e(C_{p^2} \times C_p, D_8) &= 6,\\ e(Q_8, D_8) &= 6,\\ e(C_p^3, D_8) &= 42,\\ e(C_{p^3}, D_8) &= 2.\end{aligned}$$

Furthermore, we have

$$\begin{aligned}\widetilde{e}(D_8, D_8) &= 4,\\ \widetilde{e}(C_{p^2} \times C_p, D_8) &= 3,\\ \widetilde{e}(Q_8, D_8) &= 2,\\ \widetilde{e}(C_p^3, D_8) &= 1,\\ \widetilde{e}(C_{p^3}, D_8) &= 2.\end{aligned}$$

The proof of proposition above follows from calculations in the rest of this section. Recall, we had

$$D_8 \stackrel{\text{def}}{=} \left\langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1,\ \tau\sigma = \sigma^{-1}\tau \right\rangle.$$

We shall use the notation of Section 3.6. Recall, $\mathrm{Aut}(D_8)$ fits in the exact sequence

$$1 \longrightarrow C_2^2 \longrightarrow \mathrm{Aut}(D_8) \xrightarrow{\Psi} \mathrm{U}(\mathbb{F}_2) \longrightarrow 1$$

where

$$\mathrm{U}(\mathbb{F}_2) \stackrel{\text{def}}{=} \left\{ A \in \mathrm{GL}_2(\mathbb{F}_2) \mid A = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \right\},$$

and $\operatorname{Ker}\Psi = \langle \alpha_1, \alpha_3 \rangle \cong C_2 \times C_2$ with

$$\alpha_1 \stackrel{\text{def}}{=} \begin{pmatrix} p+1 & 0 \\ 0 & 1 \end{pmatrix},\ \alpha_3 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}.$$

Therefore, a subgroup of $\mathrm{Hol}(D_8)$ of order p^3 lies in

$$D_8 \rtimes \langle \alpha_1, \alpha_2 \rangle \cong D_8 \rtimes D_8 \text{ with } \alpha_2 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

We have

$$\begin{aligned}e(D_8, D_8, 1) &= \widetilde{e}(D_8, D_8, 1) = 1,\\ e(G, D_8, 1) &= \widetilde{e}(G, D_8, 1) = 0 \text{ if } G \neq D_8.\end{aligned}$$

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

Lemma 5.7.2. *For $p = 2$ and $|\Theta(G)| = p$ there are exactly p regular subgroups isomorphic to D_8, p^2 isomorphic to $C_{p^2} \times C_p$, one isomorphic to Q_8, p isomorphic to C_p^3, and p isomorphic to C_{p^3} contained in* $\mathrm{Hol}(D_8)$.

Furthermore, there is one D_8, two $C_{p^2} \times C_p$, one Q_8, one C_p^3, and one C_{p^3}-skew braces of D_8 type.

Proof. If $G \subseteq \mathrm{Hol}(D_8)$ with $|\Theta(G)| = p$ and $p = 2$, then we must have $\Theta(G) \subseteq \langle \alpha_1, \alpha_2 \rangle$ a subgroup of order p and $G \cap D_8$ a subgroup of order p^2. Therefore, $\Theta(G)$

is one of

$$\langle \alpha_2^p \rangle, \langle \alpha_2^a \alpha_1 \rangle \text{ for } a = 0, ..., 3,$$

and $G \cap D_8$ is one of

$$\left\langle \sigma^p, \sigma^b \tau \right\rangle, \langle \sigma \rangle \text{ for } b = 0, 1.$$

We shall consider all subgroups of order p^2 in D_8 and all ways of pairing them with a subgroup of order p of $\langle \alpha_1, \alpha_2 \rangle$.

Therefore, we can consider subgroups of the form

$$G = \left\langle \sigma^p, \sigma^b \tau, \sigma \alpha_2^{a_2} \alpha_1^{a_1} \right\rangle, \left\langle \sigma, \tau \alpha_2^{a_2} \alpha_1^{a_1} \right\rangle.$$

Let us consider $G = \left\langle \sigma^p, \sigma^b \tau, \sigma \alpha_2^{a_2} \alpha_1^{a_1} \right\rangle$. Note we have

$$\begin{aligned} \sigma \left(\alpha_2^{a_2} \alpha_1^{a_1} \cdot \left(\sigma^b \tau \right) \right) \sigma^{-1} &= \sigma \sigma^{a_1 b p} \sigma^{a_2 + b} \tau \sigma^{-1} = \sigma^{(a_1 b + 1) p} \sigma^{a_2 + b} \tau, \\ \left(\sigma \alpha_2^{a_2} \alpha_1^{a_1} \right)^p &= \sigma^{(a_1+1)p} \alpha_2^{(a_1+1) a_2 p}, \\ \left(\sigma \alpha_2^{a_2} \alpha_1^{a_1} \right) \left(\sigma^b \tau \right) &= \sigma \sigma^{a_1 b p} \sigma^{a_2 + b} \tau \alpha_2^{a_2} \alpha_1^{a_1} = \sigma^{(a_1 b + 1) p + a_2} \left(\sigma^b \tau \right) \left(\sigma \alpha_2^{a_2} \alpha_1^{a_1} \right). \end{aligned}$$

The first equation implies that we need $a_2 = 0, 2$, the second implies that G has exponent p^2 when $a_1 = 0$ and exponent p otherwise, and the third implies that G is abelian when

$$(a_1 b + 1) p + a_2 \equiv 0 \bmod p^2.$$

Therefore, using the above information, we find regular subgroups

$$\left\langle \sigma^b \tau, \sigma \alpha_2^p \right\rangle \cong C_{p^2} \times C_p, \ \left\langle \sigma^p, \sigma^b \tau, \sigma \alpha_2^{(b+1)p} \alpha_1 \right\rangle \cong C_p^3, \ \left\langle \sigma^b \tau, \sigma \alpha_2^{bp} \alpha_1 \right\rangle \cong D_8 \text{ for } b = 0, 1.$$

Note, α_2 is an automorphism which takes τ to $\sigma\tau$, so the corresponding non-isomorphic skew braces are

$$\langle \tau, \sigma \alpha_2^p \rangle \cong C_{p^2} \times C_p, \ \langle \sigma^p, \tau, \sigma \alpha_2^p \alpha_1 \rangle \cong C_p^3, \ \langle \tau, \sigma \alpha_1 \rangle \cong D_8.$$

Next, we consider $G = \langle \sigma, \tau \alpha_2^{a_2} \alpha_1^{a_1} \rangle$. Note we have

$$\begin{aligned} \tau \left(\alpha_2^{a_2} \alpha_1^{a_1} \cdot \sigma \right) \tau^{-1} &= \sigma^{(a_1+1)p+1}, \\ \left(\tau \alpha_2^{a_2} \alpha_1^{a_1} \right)^p &= \sigma^{a_2 p + a_2} \alpha_2^{(a_1+1) a_2 p}, \\ \left(\tau \alpha_2^{a_2} \alpha_1^{a_1} \right) \sigma &= \sigma^{(a_1+1)p} \sigma \left(\tau \alpha_2^{a_2} \alpha_1^{a_1} \right). \end{aligned}$$

The first equation implies that the pairing is always possible, the second determines the exponent, and the third shows that G is abelian when $a_1 = 1$.

Therefore, using the above information, we find regular subgroups

$$\langle \sigma, \tau \alpha_2^{a_2} \alpha_1 \rangle \cong C_{p^3}, \ \left\langle \sigma, \tau \alpha_2^{a_2+1} \alpha_1 \right\rangle \cong C_{p^2} \times C_p, \ \langle \sigma, \tau \alpha_2^p \rangle \cong Q_8 \text{ for } a_2 = 1, 3.$$

The corresponding non-isomorphic skew braces are

$$\langle \sigma, \tau\alpha_2\alpha_1 \rangle \cong C_{p^3},\ \langle \sigma, \tau\alpha_2^p\alpha_1 \rangle \cong C_{p^2} \times C_p,\ \langle \sigma, \tau\alpha_2^p \rangle \cong Q_8.$$

□

Corollary 5.7.3. *For $p = 2$ we have*

$$\begin{aligned} e(D_8, D_8, p) &= p, \\ e(C_{p^2} \times C_p, D_8, p) &= p^2, \\ e(Q_8, D_8, p) &= p + 1, \\ e(C_p^3, D_8, p) &= (p^3 - 1)(p + 1)p, \\ e(C_{p^3}, D_8, p) &= 1. \end{aligned}$$

Furthermore, we have

$$\begin{aligned} \widetilde{e}(D_8, D_8, p) &= 1, \\ \widetilde{e}(C_{p^2} \times C_p, D_8, p) &= 2, \\ \widetilde{e}(Q_8, D_8, p) &= 1, \\ \widetilde{e}(C_p^3, D_8, p) &= 1, \\ \widetilde{e}(C_{p^3}, D_8, p) &= 1. \end{aligned}$$

Proof. Follows from Lemma 5.7.2. □

Lemma 5.7.4. *For $p = 2$ and $|\Theta(G)| = p^2$ there are exactly $p+1$ regular subgroups isomorphic to D_8, p isomorphic to $C_{p^2} \times C_p$, one isomorphic to Q_8, and p isomorphic to C_{p^3} contained in* Hol(D_8).

Furthermore, there are two D_8, one $C_{p^2} \times C_p$, one Q_8, and one C_{p^3}-skew braces of D_8 type.

Proof. If $G \subseteq \mathrm{Hol}(D_8)$ with $|\Theta(G)| = p^2$ and $p = 2$, then we must have $\Theta(G) \subseteq \langle \alpha_1, \alpha_2 \rangle$ a subgroup of order p^2 and $G \cap D_8$ a subgroup of order p. Therefore, $\Theta(G)$ is one of

$$\left\langle \alpha_2^p, \alpha_2^b\alpha_1 \right\rangle, \langle \alpha_2 \rangle \text{ for } b = 0, 1,$$

and $G \cap D_8$ is one of

$$\left\langle \sigma^p \right\rangle, \langle \sigma^a\tau \rangle \text{ for } a = 0, ..., 3.$$

We shall consider all subgroups of order p in D_8 and all ways of pairing them with a subgroup of order p^2 of $\langle \alpha_1, \alpha_2 \rangle$.

We consider subgroups of the form

$$G = \langle u, v\alpha_2^p, w\alpha_2^{a_2}\alpha_1^{a_1} \rangle$$

for some $u = \sigma^{u_1}\tau^{u_2}, v = \sigma^{v_1}\tau^{v_2}, w = \sigma^{w_1}\tau^{w_2} \in D_8$ with $u, v, w \neq 1$ and $u^2 = 1$.

We need

$$\begin{aligned} v\left(\alpha_2^p \cdot u\right) v^{-1} &= \sigma^{u_2 p} v u v^{-1} = \sigma^{(u_2+v_2u_1-u_2v_1)p} u \in \langle u \rangle, \\ w\left(\alpha_2^{a_2}\alpha_1^{a_1} \cdot u\right) w^{-1} &= \sigma^{a_1u_1p+a_2u_2w_2p}\sigma^{a_2u_2} w u w^{-1} = \sigma^{(a_1u_1+a_2u_2w_2+w_2u_1-u_2w_1)p}\sigma^{a_2u_2} u \in \langle u \rangle, \\ (v\alpha_2^p)^p &= \sigma^{(v_2+v_1+v_2v_1)p} \in \langle u \rangle. \end{aligned}$$

Now if $u_2 = 1$, then we can assume $v_2 = w_2 = 0$, which implies, using the first equation, that we need to have $v_1 = 1$ or 3, but from the second equation, we need $v_1 = 0$ or 2 which is not possible. Hence, we must have $u = \sigma^p$. Now we have

$$\begin{aligned} v\left(\alpha_2^p \cdot \sigma^p\right) v^{-1} &= \sigma^p, \\ w\left(\alpha_2^{a_2}\alpha_1^{a_1} \cdot \sigma^p\right) w^{-1} &= \sigma^p, \\ (v\alpha_2^p)^p &= \sigma^{(v_1+v_1v_2+v_2)p}, \\ (w\alpha_2^{a_2}\alpha_1^{a_1})^p &= \sigma^{(a_1w_1+w_1+w_1w_2a_2w_2)p}\sigma^{a_2w_2}\alpha_2^{(a_1+1)a_2p}. \end{aligned} \tag{5.11}$$

We also have

$$\begin{aligned} \left(v\alpha_2^p\right)\left(w\alpha_2^{a_2}\alpha_1^{a_1}\right) &= \sigma^{w_2p} v w \alpha_2^{p+a_2}\alpha_1^{a_1}, \\ \left(w\alpha_2^{a_2}\alpha_1^{a_1}\right)\left(v\alpha_2^p\right) &= \sigma^{(a_1v_1+w_1v_1+v_2w_1+a_2v_2w_2)p}\sigma^{a_2v_2} v w \alpha_2^{p+a_2}\alpha_1^{a_1}, \end{aligned}$$

Let us consider two cases of $a_1 = 0, 1$.

If $a_1 = 0$, then we a_2 and using (5.11) we need $w_2 = 1$, so we find regular subgroups

$$\langle \sigma^{w_1}\tau\alpha_2 \rangle \cong C_{p^3} \text{ for } w_1 = 0, 1.$$

If $a_1 = 1$, then we need $a_2w_2 \equiv a_2v_2 \equiv 0 \bmod p$, and so in order for G to be regular we must set $a_2 = 0$. Thus, we consider subgroups of the form $G = \langle \sigma^p, v\alpha_2^p, w\alpha_1 \rangle$. Now G is abelian if and only if

$$w_2 + v_1 \equiv v_1w_2 + v_2w_1 \equiv 1 \bmod p.$$

Therefore, we have regular subgroups

$$\left\langle \sigma^{v_2+1}\tau\alpha_2^p, \sigma\tau^{v_2}\alpha_1 \right\rangle \cong C_{p^2} \times C_p,\ \left\langle \tau\alpha_2^p, \sigma\alpha_1 \right\rangle, \left\langle \sigma\tau^{v_2}\alpha_2^p, \tau\alpha_1 \right\rangle \cong D_8,\ \left\langle \sigma\alpha_2^p, \sigma\tau\alpha_1 \right\rangle \cong Q_8$$

$$\text{for } v_2 = 0, 1.$$

The corresponding non-isomorphic skew braces are

$$\langle \tau\alpha_2 \rangle \cong C_{p^3},\ \langle \tau\alpha_2^p, \sigma\tau\alpha_1 \rangle \cong C_{p^2} \times C_p,\ \langle \tau\alpha_2^p, \sigma\alpha_1 \rangle, \langle \sigma\alpha_2^p, \tau\alpha_1 \rangle \cong D_8,\ \langle \sigma\alpha_2^p, \sigma\tau\alpha_1 \rangle \cong Q_8.$$

□

Corollary 5.7.5. *For $p = 2$ we have*

$$\begin{aligned} e(D_8, D_8, p^2) &= p + 1, \\ e(C_{p^2} \times C_p, D_8, p^2) &= p, \\ e(Q_8, D_8, p^2) &= p + 1, \\ e(C_{p^3}, D_8, p^2) &= 1, \end{aligned}$$

and $e(G, D_8, p^2) = 0$ otherwise.

Furthermore, we have

$$\begin{aligned} \widetilde{e}(D_8, D_8, p^2) &= 2, \\ \widetilde{e}(C_{p^2} \times C_p, D_8, p^2) &= 1, \\ \widetilde{e}(Q_8, D_8, p^2) &= 1, \\ \widetilde{e}(C_{p^3}, D_8, p^2) &= 1, \end{aligned}$$

and $\widetilde{e}(G, D_8, p^2) = 0$ otherwise.

Proof. Follows from Lemma 5.7.4. □

Lemma 5.7.6. *For $p = 2$ and $|\Theta(G)| = p^3$ there are no regular subgroups contained in* Hol(D_8).

Proof. If $G \subseteq \mathrm{Hol}(D_8)$ with $|\Theta(G)| = p^3$ and $p = 2$, then we must have

$$G = \langle u\alpha_1, v\alpha_2 \rangle .$$

Note we have

$$\begin{aligned} (u\alpha_1)^p &= (\sigma^{u_1}\tau^{u_2}\alpha_1)^p = \sigma^{u_1 u_2 p} \text{ and} \\ (v\alpha_2)^p &= (\sigma^{v_1}\tau^{v_2}\alpha_2)^p = \sigma^{(v_1+v_2+v_1v_2)p}\sigma^{v_2}\alpha_2^p, \end{aligned}$$

so we need to set $v_2 = 0$ and $u_1 u_2 \equiv 0 \bmod p$, we also have

$$\begin{aligned} (u\alpha_1)\,(\sigma^{v_1}\alpha_2) &= \sigma^{v_1 p} uv\alpha_1\alpha_2 \text{ and} \\ (v\alpha_2)^{p+1}\,(\sigma^{u_1}\tau^{u_2}\alpha_1) &= \sigma^{(u_2+u_2v_1)p}\sigma^{u_2} uv\alpha_2^{p+1}\alpha_1. \end{aligned}$$

This implies that we need $u_2 = 0$, so we cannot find regular subgroups of this form. □

5.8 Regular subgroups contained in Hol(Q_8)

In this section we find the regular subgroups contained in Hol(Q_8) and the corresponding skew braces. The main result of this section is the following.

Proposition 5.8.1. *For $p = 2$ we have*

$$\begin{aligned} e(Q_8, Q_8) &= 2, \\ e(C_p^3, Q_8) &= 14, \\ e(D_8, Q_8) &= 2, \\ e(C_{p^2} \times C_p, Q_8) &= 2, \\ e(C_{p^3}, Q_8) &= 2. \end{aligned}$$

Furthermore, we have

$$\begin{aligned} \widetilde{e}(Q_8, Q_8) &= 2, \\ \widetilde{e}(C_p^3, Q_8) &= 1, \\ \widetilde{e}(D_8, Q_8) &= 2, \\ \widetilde{e}(C_{p^2} \times C_p, Q_8) &= 1, \\ \widetilde{e}(C_{p^3}, Q_8) &= 2. \end{aligned}$$

The proof of proposition above follows from calculations in the rest of this section. We shall use the notation of Section 3.6. Recall $\mathrm{Aut}(Q_8)$ fits in the exact sequence

$$1 \longrightarrow C_2^2 \longrightarrow \mathrm{Aut}(Q_8) \xrightarrow{\Psi} \mathrm{GL}_2(\mathbb{F}_2) \longrightarrow 1,$$

where $\operatorname{Ker}\Psi = \langle \alpha_1, \alpha_3 \rangle \cong C_2^2$ with

$$\alpha_1 \overset{\text{def}}{=} \begin{pmatrix} p+1 & 0 \\ 0 & 1 \end{pmatrix}, \ \alpha_3 \overset{\text{def}}{=} \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix};$$

thus a subgroup of Hol(Q_8) of order p^3 lies in one of $p+1$ conjugates of

$$Q_8 \rtimes \langle \alpha_1, \alpha_2 \rangle \cong Q_8 \rtimes D_8 \text{ with } \alpha_2 \overset{\text{def}}{=} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Now here we are not sure that the exact sequence above is a split, so the problem of finding skew braces is different from M_1. We shall determine the structure of

$\mathrm{Aut}(Q_8)$. Note, we have $\alpha_2^p = \alpha_3$, and if we let

$$\alpha_4 \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{Aut}(Q_8),$$

then we have

$$\alpha_4^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},\ \alpha_4^3 = 1,\ \alpha_4\alpha_2\alpha_4 = \alpha_2\alpha_1,$$

so $\Psi(\langle \alpha_2, \alpha_4 \rangle) = \mathrm{GL}_2(\mathbb{F}_2)$, and therefore,

$$\mathrm{Aut}(Q_8) = \langle \alpha_1, \alpha_2, \alpha_4 \rangle .$$

Therefore, we find the following formulae

$$\alpha_2\alpha_1\alpha_2^{-1} = \alpha_1\alpha_2^2,\ \alpha_4\alpha_1\alpha_4^{-1} = \alpha_2^2,\ \alpha_4\alpha_2^2\alpha_4^{-1} = \alpha_1\alpha_2^2,$$

$$\alpha_4\alpha_2\alpha_4^{-1} = \alpha_2\alpha_1\alpha_4,\ \alpha_4^{-1}\alpha_2\alpha_4 = \alpha_4\alpha_2\alpha_1,$$

which will help us in finding the non-isomorphic skew braces.

We have

$$e(Q_8, Q_8, 1) = \widetilde{e}(Q_8, Q_8, 1) = 1,$$
$$e(G, Q_8, 1) = \widetilde{e}(G, Q_8, 1) = 0 \text{ if } G \neq Q_8.$$

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

Lemma 5.8.2. *For $p = 2$ and $|\Theta(G)| = p$ there are exactly $p + 1$ regular subgroups isomorphic to D_8, $(p + 1)p$ isomorphic to $C_{p^2} \times C_p$, and $(p + 1)p$ isomorphic to C_p^3 contained in* Hol(Q_8).

Furthermore, there is one D_8, one $C_{p^2} \times C_p$, and one C_p^3-skew braces of Q_8 type.

Proof. If $G \subseteq \mathrm{Hol}(Q_8)$ with $|\Theta(G)| = p$ and $p = 2$, then we can assume, without loss of generality, that we have $\Theta(G) \subseteq \langle \alpha_1, \alpha_2 \rangle$ a subgroup of order p. We also have $G \cap Q_8$ a subgroup of order p^2. Therefore, $\Theta(G)$ is one of

$$\langle \alpha_2^p \rangle, \langle \alpha_2^a \alpha_1 \rangle \text{ for } a = 0, ..., 3,$$

and $G \cap Q_8$ is one of

$$\left\langle \sigma^b \tau \right\rangle, \langle \sigma \rangle \text{ for } b = 0, 1.$$

We shall consider all subgroups of order p^2 in Q_8 and all ways of pairing them with a subgroup of order p of $\langle \alpha_1, \alpha_2 \rangle$, and we multiply the number of regular subgroups which involve α_2^a for $a = 1$ or 3 by $p + 1$.

Therefore, we can consider subgroups of the form

$$G = \left\langle \sigma^b\tau, \sigma\alpha_2^{a_2}\alpha_1^{a_1} \right\rangle, \langle \sigma, \tau\alpha_2^{a_2}\alpha_1^{a_1} \rangle .$$

Let us consider $G = \left\langle \sigma^b\tau, \sigma\alpha_2^{a_2}\alpha_1^{a_1} \right\rangle$. Note we have

$$\begin{aligned}
\sigma\left(\alpha_2^{a_2}\alpha_1^{a_1} \cdot \left(\sigma^b\tau\right)\right)\sigma^{-1} &= \sigma\sigma^{a_1bp}\sigma^{a_2+b}\tau\sigma^{-1} = \sigma^{(a_1b+1)p}\sigma^{a_2+b}\tau, \\
(\sigma\alpha_2^{a_2}\alpha_1^{a_1})^p &= \sigma^{(a_1+1)p}\alpha_2^{(a_1+1)a_2p}, \\
(\sigma\alpha_2^{a_2}\alpha_1^{a_1})\left(\sigma^b\tau\right) &= \sigma\sigma^{a_1bp}\sigma^{a_2+b}\tau\alpha_2^{a_2}\alpha_1^{a_1} = \sigma^{(a_1b+1)p+a_2}\left(\sigma^b\tau\right)(\sigma\alpha_2^{a_2}\alpha_1^{a_1}).
\end{aligned}$$

The first equation implies that we need $a_2 = 0$ or 2, and the third equation implies that G is abelian if and only if

$$(a_1b+1)\,p + a_2 \equiv 0 \bmod p^2.$$

Therefore, we find regular subgroups

$$\left\langle \sigma^b\tau, \sigma\alpha_2^{(ab+1)p}\alpha_1^a \right\rangle \cong C_{p^2} \times C_p,\ \left\langle \sigma^b\tau, \sigma\alpha_2^{bp}\alpha_1 \right\rangle \cong D_8 \text{ for } a, b = 0, 1.$$

Next, we consider $G = \langle \sigma, \tau\alpha_2^{a_2}\alpha_1^{a_1} \rangle$. Note we have

$$\begin{aligned}
\tau\left(\alpha_2^{a_2}\alpha_1^{a_1} \cdot \sigma\right)\tau^{-1} &= \sigma^{(a_1+1)p+1}, \\
(\tau\alpha_2^{a_2}\alpha_1^{a_1})^p &= \sigma^{(a_2+1)p+a_2}\alpha_2^{(a_1+1)a_2p}, \\
(\tau\alpha_2^{a_2}\alpha_1^{a_1})\,\sigma &= \sigma^{(a_1+1)p}\sigma\left(\tau\alpha_2^{a_2}\alpha_1^{a_1}\right).
\end{aligned}$$

Now, the first equation implies that the pairing is always possible, and the third implies that G is abelian if and only if $a_1 = 1$.

Therefore we have regular subgroups

$$\langle \tau\alpha_2^{a_2}\alpha_1 \rangle \cong C_{p^3},\ \left\langle \sigma, \tau\alpha_2^{a_2+1}\alpha_1 \right\rangle \cong C_{p^2} \times C_p,\ \langle \sigma, \tau\alpha_2^p \rangle \cong D_8 \text{ for } a_2 = 1, 3.$$

Note, the automorphism represented by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & b \end{smallmatrix}\right)$ maps σ to $\sigma^b\tau$, thus any skew braces arising from regular subgroups above is conjugate to one of

$$\langle \tau\alpha_2^{a_2}\alpha_1 \rangle \cong C_{p^3},\ \left\langle \sigma, \tau\alpha_2^{a_2+1}\alpha_1 \right\rangle \cong C_{p^2} \times C_p,\ \langle \sigma, \tau\alpha_2^p \rangle \cong D_8 \text{ for } a_2 = 1, 3.$$

Therefore, the corresponding non-isomorphic skew braces are

$$\langle \tau\alpha_2\alpha_1 \rangle \cong C_{p^3},\ \langle \sigma, \tau\alpha_1 \rangle \cong C_{p^2} \times C_p,\ \langle \sigma, \tau\alpha_2^p \rangle \cong D_8.$$

□

Corollary 5.8.3. *For $p = 2$ we have*

$$\begin{aligned} e(D_8, Q_8, p) &= 1, \\ e(C_{p^2} \times C_p, Q_8, p) &= p, \\ e(C_{p^3}, Q_8, p) &= 1, \end{aligned}$$

and $e(G, Q_8, p) = 0$ otherwise.

Furthermore, we have

$$\begin{aligned} \widetilde{e}(D_8, Q_8, p) &= 1, \\ \widetilde{e}(C_{p^2} \times C_p, Q_8, p) &= 1, \\ \widetilde{e}(C_{p^3}, Q_8, p) &= 1, \end{aligned}$$

and $\widetilde{e}(G, Q_8, p) = 0$ otherwise.

Proof. Follows from Lemma 5.8.2. □

Lemma 5.8.4. *For $p = 2$ and $|\Theta(G)| = p^2$ there is exactly one regular subgroup isomorphic to Q_8, p isomorphic to C_p^3, $p+1$ isomorphic to D_8, and $(p+1)p$ isomorphic to C_{p^3} contained in* Hol(Q_8).

Furthermore, there is one Q_8, one D_8, one C_p^3, and one C_{p^3}-skew brace of Q_8 type.

Proof. If $G \subseteq \mathrm{Hol}(Q_8)$ with $|\Theta(G)| = p^2$ and $p = 2$, then we must have $\Theta(G) \subseteq \langle \alpha_1, \alpha_2 \rangle$ a subgroup of order p^2 and $G \cap Q_8$ a subgroup of order p. Therefore, $\Theta(G)$ is one of

$$\left\langle \alpha_2^p, \alpha_2^b \alpha_1 \right\rangle, \langle \alpha_2 \rangle \text{ for } b = 0, 1,$$

and $G \cap Q_8$ is $\langle \sigma^p \rangle$.

Therefore, we consider subgroups of the form

$$G = \langle \sigma^p, v\alpha_2^p, w\alpha_2^{a_2}\alpha_1^{a_1} \rangle \text{ for some } v = \sigma^{v_1}\sigma^{v_2}, w = \sigma^{w_1}\sigma^{w_2} \neq 1,\ v_2, w_2 = 0, 1.$$

Now we have

$$\begin{aligned} (v\alpha_2^p)^p &= \sigma^{(v_2+1)v_1 p}, \\ (w\alpha_2^{a_2}\alpha_1^{a_1})^p &= \sigma^{(a_2w_2 + a_1w_1 + w_1 + w_2 + w_1w_2)p}\sigma^{a_2w_2}\alpha_2^{(a_1+1)a_2 p}. \end{aligned}$$

We also have

$$\begin{aligned} (v\alpha_2^p)\,(w\alpha_2^{a_2}\alpha_1^{a_1}) &= \sigma^{w_2 p} vw \alpha_2^{p+a_2}\alpha_1^{a_1} \text{ and,} \\ (w\alpha_2^{a_2}\alpha_1^{a_1})\,(v\alpha_2^p) &= \sigma^{(a_1v_1 + v_1w_2 + v_2w_1 + a_2v_2w_2)p}\sigma^{a_2v_2} vw \alpha_2^{p+a_2}\alpha_1^{a_1}, \end{aligned}$$

Now we consider two cases for $a_1 = 0$ or 1. If $a_1 = 0$, then we need $a_2 = w_2 = 1$, and we find regular subgroups

$$\langle \sigma^{w_1} \tau \alpha_2 \rangle \cong C_{p^3} \text{ for } w_1 = 0, 1.$$

If $a_1 = 1$, then we need $a_2 = 0$, and so we consider $G = \langle \sigma^p, v\alpha_2^p, w\alpha_1 \rangle$ where we need $v_1 w_2 + v_2 w_1 \equiv 1 \bmod p$. Now the group G is abelian if and only if

$$v_1 + w_2 \equiv v_1 w_2 + v_2 w_1 \equiv 1 \bmod p.$$

Therefore, we have regular subgroups

$$\left\langle \sigma^p, \sigma^{v_1+1} \tau \alpha_2^p, \sigma \tau^{v_1} \alpha_1 \right\rangle \cong C_p^3, \ \langle \tau \alpha_2^p, \sigma \alpha_1 \rangle, \left\langle \sigma \tau^{v_1} \alpha_2^p, \sigma^{v_1+1} \tau \alpha_1 \right\rangle \cong D_8, \ \langle \tau \alpha_2^p, \sigma \alpha_1 \rangle \cong Q_8,$$

$$\text{for } v_1 = 0, 1.$$

The corresponding non-isomorphic skew braces are

$$\langle \sigma \tau \alpha_2 \rangle \cong C_{p^3}, \ \langle \sigma^p, \sigma \tau \alpha_2^p, \sigma \alpha_1 \rangle \cong C_p^3, \ \langle \tau \alpha_2^p, \sigma \alpha_1 \rangle \cong D_8, \ \langle \tau \alpha_2^p, \sigma \alpha_1 \rangle \cong Q_8.$$

□

Corollary 5.8.5. *For $p = 2$ we have*

$$\begin{aligned} e(Q_8, Q_8, p^2) &= 1, \\ e(C_p^3, Q_8, p^2) &= (p^3 - 1)p, \\ e(D_8, Q_8, p^2) &= 1, \\ e(C_{p^3}, Q_8, p^2) &= 1, \end{aligned}$$

and $e(C_{p^2} \times C_p, Q_8, p^2) = 0$.

Furthermore, we have

$$\begin{aligned} \widetilde{e}(Q_8, Q_8, p^2) &= 1, \\ \widetilde{e}(C_p^3, Q_8, p^2) &= 1, \\ \widetilde{e}(D_8, Q_8, p^2) &= 1, \\ \widetilde{e}(C_{p^3}, Q_8, p^2) &= 1, \end{aligned}$$

and $\widetilde{e}(C_{p^2} \times C_p, Q_8, p^2) = 0$.

Proof. Follows from Lemma 5.8.4. □

Finally, if $G \subseteq \text{Hol}(Q_8)$ with $|\Theta(G)| = p^3$ and $p = 2$, then we must have

$$G = \langle \sigma^{u_2} \tau^{u_1} \alpha_1, \sigma^{v_2} \tau^{v_1} \alpha_2 \rangle \text{ with } u_1, v_1 = 0, 1.$$

Note we have

$$(\sigma^{u_1}\tau^{u_2}\alpha_1)^p = \sigma^{(u_1+1)u_2 p},$$
$$(\sigma^{v_1}\tau^{v_2}\alpha_2)^p = \sigma^{(v_2+1)v_1 p}\sigma^{v_2}\alpha_2^p$$

for G to have size p^3 and be regular we need to set $v_2 \equiv 0 \bmod p$ and $(u_1+1)\,u_2 \equiv 0 \bmod p$. Now we also have

$$(\sigma^{u_1}\tau^{u_2}\alpha_1)(\sigma^{v_1}\alpha_2) = \sigma^{(v_1+u_2 v_1)p}\sigma^{u_1+v_1}\tau^{u_2}\alpha_1\alpha_2 \text{ and}$$
$$(\sigma^{v_1}\alpha_2)^{p+1}(\sigma^{u_1}\tau^{u_2}\alpha_1) = \sigma^{v_1 p}\sigma^{u_2}\sigma^{v_1+u_1}\tau^{u_2}\alpha_2^{p+1}\alpha_1,$$

but this implies that we need $u_2 = 0$, so there is no regular subgroup of this form.

This will end our investigation into the classification of Hopf-Galois structures and skew braces of order p^3.

> Me thinks I am like a man, who having struck on many shoals, and having narrowly escaped shipwreck in passing a small frith, has yet the temerity to put out to sea in the same leaky weather-beaten vessel, and even carries his ambition so far to think of compassing the globe under these disadvantageous circumstances. My memory of past errors and perplexities, makes me diffident for the future. The wretched condition, weakness and disorder of the faculties, I must employ in my enquires, increase my apprehensions. And the impossibility of amending or correcting these faculties, reduces me almost to despair, and makes me resolve to perish on the barren rock, on which I am at present, rather than venture myself upon that boundless ocean, which runs into immensity...
>
> *A Treatise of Human Nature*
> *David Hume*

Bibliography

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

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

[BCJ16] David Bachiller, Ferran Cedó, and Eric Jespers. Solutions of the Yang-Baxter equation associated with a left brace. *J. Algebra*, 463:80–102, 2016.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

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

[Byo04a] Nigel P. Byott. Hopf-Galois structures on field extensions with simple Galois groups. *Bull. London Math. Soc.*, 36(1):23–29, 2004.

[Byo04b] Nigel P. Byott. Hopf-Galois structures on Galois field extensions of degree pq. *J. Pure Appl. Algebra*, 188(1-3):45–57, 2004.

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

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

[Chi00] Lindsay N. Childs. *Taming wild extensions: Hopf algebras and local Galois module theory*, volume 80 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2000.

[CJO14] Ferran Cedó, Eric Jespers, and Jan Okniński. Braces and the Yang-Baxter equation. *Comm. Math. Phys.*, 327(1):101–116, 2014.

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

[Dri92] V. G. Drinfel'd. On some unsolved problems in quantum group theory. In *Quantum groups (Leningrad, 1990)*, volume 1510 of *Lecture Notes in Math.*, pages 1–8. Springer, Berlin, 1992.

[GP87] Cornelius Greither and Bodo Pareigis. Hopf-Galois theory for separable field extensions. *J. Algebra*, 106(1):239–258, 1987.

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

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

[Rib89] Paulo Ribenboim. *The book of prime number records*. Springer-Verlag, New York, second edition, 1989.

[Rob96] Derek J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.

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

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

[SV17] A. Smoktunowicz and L. Vendramin. On skew braces (with an appendix by N. Byott and L. Vendramin). *Journal of combinatorial algebra - to appear*, 2017.