SKEW LEFT BRACES AND ISOMORPHISM PROBLEMS FOR HOPF-GALOIS STRUCTURES ON GALOIS EXTENSIONS

ALAN KOCH AND PAUL J. TRUMAN

ABSTRACT. Given a finite group G, we study certain regular subgroups of the group of permutations of G, which occur in the classification theories of two types of algebraic objects: skew left braces with multiplicative group isomorphic to G and Hopf-Galois structures admitted by a Galois extension of fields with Galois group isomorphic to G. We study the questions of when two such subgroups yield isomorphic skew left braces or Hopf-Galois structures involving isomorphic Hopf algebras. In particular, we show that in some cases the isomorphism class of the Hopf algebra giving a Hopf-Galois structure is determined by the corresponding skew left brace. We investigate these questions in the context of a variety of existing constructions in the literature. As an application of our results we classify the isomorphically distinct Hopf algebras that give Hopf-Galois structures on a Galois extension of degree pq for $p > q$ prime numbers.

1. INTRODUCTION

Let G be a finite group and let $\mathrm{Perm}(G)$ denote the group of permutations of G. A subgroup $N \leq \mathrm{Perm}(G)$ is said to be *regular* if $|N| = |G|$, the action of N on G is transitive, and the stabilizer in N of every $\sigma \in G$ is trivial (any two of these conditions guarantees the third). One example of a regular subgroup of $\mathrm{Perm}(G)$ is the image of G under the left regular representation $\lambda : G \hookrightarrow \mathrm{Perm}(G)$. This map also yields an action of G on $\mathrm{Perm}(G)$ by ${}^{\sigma}\pi = \lambda(\sigma)\pi\lambda(\sigma)^{-1}$, and this paper is concerned with regular subgroups $N \leq \mathrm{Perm}(G)$ that are *stable* under this action. These subgroups are of interest because they occur in the classification theories of two types algebraic objects.

On one hand, there is a correspondence (although not a bijection) between G-stable regular subgroups of $\mathrm{Perm}(G)$ and *skew left braces* with multiplicative group isomorphic to G. Each of these yields a set theoretic solution to the Yang-Baxter equation on the underlying set G, each of which extends naturally to a solution on the vector space $K[G]$ (for a given field K). Two regular G-stable subgroups can correspond to isomorphic skew left braces, and so we obtain a partition of the set of regular G-stable subgroups of $\mathrm{Perm}(G)$. In terms of the Yang-Baxter equation, the solutions arising from isomorphic braces are equivalent up to a change of basis of $K[G]$.

On the other hand, by a theorem of Greither and Pareigis G-stable regular subgroups of $\mathrm{Perm}(G)$ correspond bijectively with *Hopf-Galois structures* admitted by

a Galois extension of fields L/K with Galois group isomorphic to G, each consisting of a K-Hopf algebra and a certain K-linear action of H on L. Applications of Hopf-Galois structures include the formulation of variants of the Galois correspondence and the study of integral module structure in extensions of local or global fields. Two distinct Hopf-Galois structures can involve isomorphic Hopf algebras (alternatively, we might view this as two distinct actions of a single Hopf algebra on L); it is possible to detect when this occurs in purely group theoretic terms, and so we obtain another partition of the set of regular G-stable subgroups of $\mathrm{Perm}(G)$.

In this paper we address the natural question of comparing the two notions of isomorphism discussed above via the corresponding partitions of the set of regular G-stable subgroups of $\mathrm{Perm}(G)$. In Section 2 we discuss the connection between skew left braces and Hopf-Galois structures in more detail, and in Section 3 we recall and reformulate existing criteria for two regular G-stable subgroup of $\mathrm{Perm}(G)$ to correspond to isomorphic skew left braces or to Hopf-Galois structures involving isomorphic Hopf algebras. We find that neither of these notions implies the other in general, but in Sections 4 - 7 we show that they have rich interactions with various existing constructions, including regular G-stable subgroups arising from *abelian maps*, as studied by Childs in [7] and generalized by the first named author in [16], and the notions of *opposite* Hopf-Galois structures and skew left braces, as studied by the authors in [20]. Finally, in Section 8 we undertake a detailed study of the case in which $|G| = pq$ with $p > q$ prime numbers. The classifications of G-stable regular subgroups, skew left braces, and Hopf-Galois structures are known in this case; by applying our techniques we identify the isomorphically distinct Hopf algebras that occur.

2. Hopf-Galois structures and Skew left braces

In this section we describe the connections between Hopf-Galois structures, G-stable regular subgroups of $\mathrm{Perm}(G)$, and skew left braces. For more detailed summaries we refer to the reader to [20, Section 2] and [24, Appendix A]

2.1. **Hopf-Galois structures.** A *Hopf-Galois structure* on a finite extension of fields L/K consists of a cocommutative K-Hopf algebra H and an action of H on L making L into an H-module algebra and such that the K-linear map $j : L \otimes H \to \mathrm{End}_K(L)$ given by $j(x \otimes h)(y) = x(h \cdot y)$ for all $h \in H$ and all $x, y \in L$ is bijective (see [6, Definition 2.7]). We say that two Hopf-Galois structures $(H, \cdot)$ and $(H', \cdot')$ on L/K are *isomorphic* if there is an isomorphism of Hopf algebras $\theta : H \to H'$ such that $\theta(h) \cdot x = h \cdot x$ for all $h \in H$ and all $x \in L$.

Greither and Pareigis [12] classify the Hopf-Galois structures admitted by a finite separable extension of fields in group theoretic terms. Specializing to the case in which L/K is a Galois extension with Galois group G, their theorem states that there is a bijection between (isomorphism classes of) Hopf-Galois structures admitted by L/K and regular G-stable subgroups of $\mathrm{Perm}(G)$. Given such a subgroup N, the Hopf algebra giving the Hopf-Galois structure corresponding to N is $H_N := L[N]^G$, where G acts on L as Galois automorphisms and on N via

$^{\sigma}\eta = \lambda(\sigma)\eta\lambda(\sigma)^{-1}$ (the assumption that N is G-stable ensures that this is indeed an action of G on N). The theorem of Greither and Pareigis also specifies the action of H_N on L, but we shall not need this information in what follows.

Example 2.1. The image of the right regular representation $\rho : G \to \text{Perm}(G)$ is a regular subgroup of $\text{Perm}(G)$, and is G-stable since we have $^{\sigma}\rho(\tau) = \rho(\tau)$ for all $\sigma, \tau \in G$. The corresponding Hopf-Galois structure is given by the Hopf algebra $K[G]$, along with its natural action on L. We call this the *classical* Hopf-Galois structure on L/K.

Example 2.2. The image of the left regular representation $\lambda : G \to \text{Perm}(G)$ is a regular subgroup of $\text{Perm}(G)$, and is G-stable since we have $^{\sigma}\lambda(\tau) = \lambda(\sigma\tau\sigma^{-1})$ for all $\sigma, \tau \in G$. If G is nonabelian then $\lambda(G) \neq \rho(G)$, and so $\lambda(G)$ corresponds to a different Hopf-Galois structure on L/K, with Hopf algebra $L[\lambda(G)]^G$. This example is considered in [12, Theorem 5.2 et seq.], and is sometimes called the *canonical nonclassical* Hopf-Galois structure on L/K.

In each of these examples the regular subgroup N is isomorphic to G. However, this need not be the case:

Example 2.3. Let L/K be a Galois extension with Galois group
$$G = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1,\ \tau\sigma\tau^{-1} = \sigma^{-1} \rangle \cong D_3.$$
For $c = 0, 1, 2$ let $N_c = \langle \lambda(\sigma), \rho(\sigma^c \tau) \rangle$. We find ([18, Lemma 1] or a routine verification) that each N_c is a distinct cyclic regular subgroup of $\text{Perm}(G)$, and is also G-stable: both generators of G act trivially on $\rho(\sigma^c \tau)$, and we have $^{\sigma}\lambda(\sigma) = \lambda(\sigma)$ and $^{\tau}\lambda(\sigma) = \lambda(\sigma^{-1})$. Thus the dihedral extension L/K admits three Hopf-Galois structures for which the corresponding regular G-stable subgroup of $\text{Perm}(G)$ is cyclic.

In Example 2.3 we have described the cyclic groups N_c using two generators, following [4] and [1]; we will continue to adopt this slightly unconventional notation in order to relate our results to the results of those papers.

If N is a regular G-stable subgroup of $\text{Perm}(G)$ then we refer to the isomorphism class of N as the *type* of the corresponding Hopf-Galois structure. For example: the previous example provides us with Hopf-Galois structures of cyclic type on a dihedral extension of degree 6.

In [3] Byott shows that the question of determining all regular G-stable subgroups of $\text{Perm}(G)$ that are isomorphic to a given group N is closely related to the question of determining all regular subgroups of the holomorph $\text{Hol}(N)$ of N, where $\text{Hol}(N) = N \rtimes \text{Aut}(N)$, that are isomorphic to G; the latter is often an easier problem since $\text{Hol}(N)$ is a smaller group that $\text{Perm}(G)$. Various authors have enumerated and described the Hopf-Galois structure admitted by a Galois extension with prescribed Galois group G; see for example [21], [4], [15]. Others have developed more general methods for creating or describing families of regular G-stable subgroups of $\text{Perm}(G)$: see for example [7], [10], [20]. We will describe some of these constructions in more detail in subsequent sections.

2.2. **Skew left braces.** A *skew left brace* is a triple $\mathfrak{B} = (B, \cdot, \circ)$ such that $(B, \cdot)$ and $(B, \circ)$ are finite groups whose operations satisfy the *brace relation*

$$x \circ (y \cdot z) = (x \circ y) \cdot x^{-1} \cdot (x \circ z) \text{ for all } x, y, z \in B, \tag{2.1}$$

where x^{-1} denotes the inverse of x in the group $(B, \cdot)$.

A consequence of the brace relation (2.1) is that $(B, \cdot)$ and $(B, \circ)$ share the same identity element, but in general the inverse of an element x in the group $(B, \circ)$ (denoted $\bar{x}$) is not equal to x^{-1}.

We call the groups $(B, \cdot)$ the *dot group*, and $(B, \circ)$ the *circle group* of the skew left brace $\mathfrak{B}$ (elsewhere in the literature these are sometimes called the *additive group* and *multiplicative group* of $\mathfrak{B}$). To ease notation, we write $x \cdot y = xy$ where there is no danger of confusion. A *homomorphism* of skew left braces is a map that respects both of the binary operations, and an *isomorphism* of skew left braces is a bijective homomorphism. For brevity, we shall henceforth refer to a skew left brace simply as a *brace*, but we note that in the historical development of the subject this term originally applied to skew left braces with abelian dot group.

Example 2.4. Let $(B, \cdot)$ be a finite group and let $x \circ y = x \cdot y$ for all $x, y \in B$. Then $\mathfrak{B} = (B, \cdot, \circ)$ is a brace, called the *trivial* brace for $(B, \cdot)$.

Example 2.5. Let $(B, \cdot)$ be a finite group and let $x \circ y = y \cdot x$ for all $x, y \in B$. Then $\mathfrak{B} = (B, \cdot, \circ)$ is a brace, called the *almost trivial* brace for $(B, \cdot)$.

In each of these examples the dot and circle groups of $\mathfrak{B}$ are isomorphic to each other. However, this need not be the case:

Example 2.6. Let $(B, \cdot)$ be a cyclic group of order 6, presented using two generators:

$$(B, \cdot) = \langle x, y \mid x^3 = y^2 = 1, \ yxy^{-1} = x \rangle,$$

and let

$$x^i y^j \circ x^k y^\ell = x^{i + (-1)^j k} y^{k + \ell}.$$

It is routine to verify that $(B, \circ)$ is a group in which x has order 3, y has order 2, and $y \circ x \circ \bar{y} = \bar{x}$, whence $(B, \circ) \cong D_3$. Moreover, $\mathfrak{B} = (B, \cdot, \circ)$ is a brace.

In [13, Proposition 1.11], Guarnieri and Vendramin show that, given groups N, G of the same order, braces $\mathfrak{B} = (B, \cdot, \circ)$ with $(B, \cdot) \cong N$ and $(B, \circ) \cong G$ correspond with *bijective 1-cocycles* $G \to N$. In [24, Appendix A] this correspondence is reformulated in terms of regular subgroups of $\mathrm{Hol}(N)$ that are isomorphic to G. Since our focus is on G-stable regular subgroups of $\mathrm{Perm}(G)$ rather than regular subgroups of $\mathrm{Hol}(N)$, we reformulate the correspondence in this framework, as follows:

Firstly, let $\mathfrak{B} = (B, \cdot, \circ)$ be a brace with $(B, \circ) \cong G$. For each $x \in B$, the map $\eta_x : B \to B$ defined by $\eta_x(y) = x \cdot y$ is a permutation of B, and since $(B, \cdot)$ is a group the set $N_{\mathfrak{B}} = \{\eta_x \mid x \in B\}$ is a regular subgroup of $\mathrm{Perm}(B)$. By using the brace relation (2.1), it can be shown that $N_{\mathfrak{B}}$ is a $(B, \circ)$-stable subgroup of $\mathrm{Perm}(B)$. Identifying $(B, \circ)$ with G, we obtain a regular G-stable subgroup of $\mathrm{Perm}(G)$.

Conversely, let N be a regular G-stable subgroup of $\mathrm{Perm}(G)$. The regularity of N implies that the map $a : N \to G$ defined by $a(\eta) = \eta[1_G]$ for all $\eta \in N$ is a bijection. Define a new binary operation on N by

$$\eta \circ \pi = a^{-1}(a(\eta)a(\pi)) \text{ for all } \eta, \pi \in N,$$

where the multiplication inside the brackets takes place in G. Then $(N, \circ)$ is a group isomorphic to G and, since N is a G-stable subgroup of $\mathrm{Perm}(G)$, the brace relation (2.1) is satisfied. Therefore $\mathfrak{B}_N = (N, \cdot, \circ)$ is a brace with $(N, \circ) \cong G$. In [11] this construction is referred to as *transport of structure*.

Alternatively, we may define a new binary operation on G by

$$\sigma \cdot \tau = a(a^{-1}(\sigma)a^{-1}(\tau)) \text{ for all } \sigma, \tau \in G,$$

where the multiplication inside the brackets takes place in N. Then $(G, \cdot)$ is a group isomorphic to N, and $(G, \cdot, \circ)$ is a brace, isomorphic to the brace $\mathfrak{B}_N$ constructed above via a^{-1}.

In Section 3 we will discuss precise criteria for two G-stable subgroups of $\mathrm{Perm}(G)$ to yield isomorphic braces.

Example 2.7. We have seen in Example 2.1 that the image of the right regular representation $\rho : G \to \mathrm{Perm}(G)$ is a regular G-stable subgroup of $\mathrm{Perm}(G)$. The corresponding bijection $a : \rho(G) \to G$ is given by $a(\rho(\sigma)) = \sigma^{-1}$, and the resulting circle operation is given by

$$\rho(\sigma) \circ \rho(\tau) = \left(\rho(\sigma)^{-1}\rho(\tau)^{-1}\right)^{-1} = \rho(\tau)\rho(\sigma).$$

Thus the subgroup $\rho(G)$ corresponds to the almost trivial brace for G (see Example 2.5).

Example 2.8. We have seen in Example 2.2 that the image of the left regular representation $\rho : G \to \mathrm{Perm}(G)$ is a regular G-stable subgroup of $\mathrm{Perm}(G)$. The corresponding bijection $a : \lambda(G) \to G$ is given by $a(\lambda(\sigma)) = \sigma$, and the resulting circle operation is simply $\lambda(\sigma) \circ \lambda(\tau) = \lambda(\sigma\tau)$. Therefore the corresponding brace is the trivial brace for G (see Example 2.4).

Example 2.9. Let $G \cong D_3$ as in Example 2.3, and consider the regular G-stable subgroup $N_0 \leq \mathrm{Perm}(G)$ constructed in that example. Let $\eta = \lambda(\sigma)$ and $\pi = \rho(\tau)$. The corresponding bijection $a : N_0 \to G$ is given by $a(\eta^i\pi^j) = \sigma^i\tau^{-j} = \sigma^i\tau^j$ (since τ has order 2). The resulting circle operation is given by

$$\begin{aligned}
\eta^i\pi^j \circ \eta^k\pi^\ell &= a^{-1}(\sigma^i\tau^j\sigma^k\tau^\ell) \\
&= a^{-1}(\sigma^i\sigma^{k(-1)^j}\tau^j\tau^\ell) \\
&= \eta^{i+k(-1)^j}\pi^{j+\ell}.
\end{aligned}$$

Therefore the corresponding brace is the brace constructed in Example 2.6. By similar calculations it can be shown that the subgroups N_1, N_2 of Example 2.3 also correspond to this brace. We shall see a more illuminating explanation of this fact in Section 4.

3. Brace equivalence and Hopf algebra isomorphisms

In our discussion of the relationship between G-stable regular subgroups N of $\mathrm{Perm}(G)$ and braces $\mathfrak{B} = (B, \cdot, \circ)$ with $(B, \cdot) \cong N$ and $(B, \circ) \cong G$ (Subsection 2.2) we noted that multiple such subgroups can correspond to the same brace. This is made precise in [13, Proposition 4.3] and [24, Appendix A] in terms of regular subgroups of $\mathrm{Hol}(N)$ that are isomorphic to G. We prefer to formulate this concept in terms of regular G-stable subgroups of $\mathrm{Perm}(G)$, since we feel this framework is more suitable for comparing it with the notion of Hopf algebra isomorphism mentioned in Section 1, and discussed in detail later in this section. Our approach is similar to [15, Proposition 2.1], but we give a self-contained proof for the convenience of the reader. We fix an identification of G with $(B, \circ)$; this identifies $\mathrm{Perm}(G)$ with $\mathrm{Perm}(B)$, $\mathrm{Aut}(G)$ with $\mathrm{Aut}(B, \circ)$, and regular G-stable subgroups of $\mathrm{Perm}(G)$ with regular $(B, \circ)$-stable subgroups of $\mathrm{Perm}(B)$.

Proposition 3.1. *Let $\mathfrak{B} = (B, \cdot, \circ)$ be a brace and let $N_{\mathfrak{B}} = \{\eta_x \mid x \in B\}$ be the corresponding regular $(B, \circ)$-stable subgroup of $\mathrm{Perm}(B)$. Then:*

(1) *a regular $(B, \circ)$-stable subgroup M of $\mathrm{Perm}(B)$ yields a brace isomorphic to $\mathfrak{B}$ if and only if $M = \varphi^{-1} N \varphi$ for some $\varphi \in \mathrm{Aut}(B, \circ)$;*

(2) *we have $\varphi^{-1} N \varphi = N$ if and only if $\varphi \in \mathrm{Aut}_{Br}(\mathfrak{B})$, the group of brace automorphisms of $\mathfrak{B}$.*

Proof.   (1) First let $\varphi \in \mathrm{Aut}(B, \circ)$, and define a new binary operation on B by

$$x \cdot_{\varphi} y = \varphi^{-1}(\varphi(x) \cdot \varphi(y)) \text{ for all } x, y \in B. \qquad (3.1)$$

Then $\mathfrak{B}_{\varphi} = (B, \cdot_{\varphi}, \circ)$ is a brace, and $\varphi : \mathfrak{B} \to \mathfrak{B}_{\varphi}$ is a brace isomorphism. The regular $(B, \circ)$-stable regular subgroup of $\mathrm{Perm}(B)$ corresponding to B_{φ} is $N_{\varphi} = \{\eta_x^{\varphi} \mid x \in B\}$, where $\eta_x^{\varphi}(y) = x \cdot_{\varphi} y$ for all $x, y \in B$. Now we have

$$\begin{aligned}
\eta_x^{\varphi}[y] &= x \cdot_{\varphi} y \\
&= \varphi^{-1}(\varphi(x) \cdot \varphi(y)) \\
&= \varphi^{-1} \eta_{\varphi(x)}[\varphi(y)] \\
&= \left(\varphi^{-1} \eta_{\varphi(x)} \varphi\right)[y],
\end{aligned}$$

and so $N_{\varphi} = \varphi^{-1} N \varphi$.

Conversely, suppose that M is a regular $(B, \circ)$-stable subgroup of $\mathrm{Perm}(B)$, let $\mathfrak{C} = (B, \star, \circ)$ be the brace corresponding to M, and suppose that $\varphi : \mathfrak{C} \to \mathfrak{B}$ is a brace isomorphism. Then $\varphi \in \mathrm{Aut}(B, \circ)$ and

$$\varphi(x \star y) = \varphi(x) \cdot \varphi(y),$$

so

$$\begin{aligned}
x \star y &= \varphi^{-1}\left(\varphi(x) \cdot \varphi(y)\right) \\
&= x \cdot_{\varphi} y,
\end{aligned}$$

where the binary operation $\cdot_{\varphi}$ is defined as in Equation (3.1). Therefore $M = \varphi^{-1} N \varphi$ for some $\varphi \in \mathrm{Aut}(B, \circ)$.

(2) First suppose that $\varphi \in \mathrm{Aut}_{Br}(\mathfrak{B})$. Then we have

$$x \cdot_\varphi y = \varphi^{-1}(\varphi(x) \cdot \varphi(y)) = x \cdot y \text{ for all } x, y \in B,$$

so $\eta_x^\varphi = \eta_x$ for all $x \in B$, and so $N_\varphi = N$.

Conversely, suppose that $N_\varphi = N$. Then for all $x \in B$ there exists $x' \in B$ such that $\eta_x^\varphi = \eta_{x'}$. That is:

$$x \cdot_\varphi y = x' \cdot y \text{ for all } y \in B.$$

Setting $y = 1_B$ we obtain $x = x'$ immediately. Therefore

$$\varphi(x) \cdot \varphi(y) = \varphi(x \cdot y) \text{ for all } x, y \in B,$$

and so $\varphi \in \mathrm{Aut}_{Br}(\mathfrak{B})$.

$\square$

As a corollary, we recover [15, Corollary 2.4]:

Corollary 3.2. *A given brace* $\mathfrak{B} = (B, \cdot, \circ)$ *yields*

$$\frac{|\mathrm{Aut}(B, \circ)|}{|\mathrm{Aut}_{Br}(\mathfrak{B})|}$$

distinct regular $(B, \circ)$*-stable subgroups of* $\mathrm{Perm}(B)$.

We now return to our original formulation, and consider regular G-stable subgroups of $\mathrm{Perm}(G)$.

Definition 3.3. We say that two regular, G-stable subgroups N, M of $\mathrm{Perm}(G)$ are *brace equivalent* if they yield isomorphic braces (i.e., braces between which there is a bijection respecting the dot and circle operations).

Brace equivalence is an equivalence relation, so we have the notion of a *brace class* of regular, G-stable subgroups, and the brace classes partition the set of regular G-stable subgroups of $\mathrm{Perm}(G)$. By Proposition 3.1, the brace class of a regular G-stable subgroup N of $\mathrm{Perm}(G)$ is $\{\varphi^{-1}N\varphi \mid \varphi \in \mathrm{Aut}(G)\}$, and this brace class has size $|\mathrm{Aut}(G)|/|\mathrm{Aut}_{Br}(\mathfrak{B})|$, where $\mathfrak{B}$ is the brace corresponding to N.

Example 3.4. Let G be a finite group, and let $N = \lambda(G)$ as in Example 2.4, thereby giving rise to the trivial brace. Any automorphism of $(\lambda(G), \circ)$ will also preserve $\cdot$, hence the brace class containing $\lambda(G)$ is precisely $\{\lambda(G)\}$.

Example 3.5. Let G be a finite group, and let $N = \rho(G)$ as in Example 2.5, thereby giving rise to the almost trivial brace. Any automorphism of $(\rho(G), \circ)$ will also preserve $\cdot$, hence the brace class containing $\rho(G)$ is precisely $\{\rho(G)\}$.

Now we turn to another natural partition of the set of G-stable regular subgroups of $\mathrm{Perm}(G)$. Recall from Subsection 2.1 that each regular G-stable subgroup N of $\mathrm{Perm}(G)$ corresponds to a Hopf-Galois structure on a Galois extension of fields L/K with Galois group G. It is possible for two distinct Hopf-Galois structures to involve isomorphic Hopf algebras (note that this is weaker than the notion of isomorphism of Hopf-Galois structures discussed in Subsection 2.1). This phenomenon has recently been studied in papers such as [17], [18], and [25], and can be formulated in purely

group theoretic terms: [9, Section 2.3] or [18, Theorem 2.2] shows that if N, M are regular G-stable subgroups of $\text{Perm}(G)$ then $H_N \cong H_M$ as Hopf algebras if and only if there is an isomorphism $\theta : N \to M$ such that $^\sigma\theta(\eta) = \theta(^\sigma\eta)$ for all $\eta \in N$ and $\sigma \in G$. In this case we say that N, M are *G-isomorphic*. Clearly G-isomorphism is an equivalence relation on the set of regular G-stable subgroups of $\text{Perm}(G)$, and so we obtain a second partition of this set.

It is also possible to detect Hopf algebra isomorphisms via regular subgroups of $\text{Hol}(N)$ that are isomorphic to G: see [18, Theorem 2.11]. However, we feel that this concept is more transparent in the $\text{Perm}(G)$ setting, and will continue to employ this point of view.

It is natural to ask whether there is a connection between brace equivalence and G-isomorphism of regular G-stable subgroups. Our first observations are that neither implies the other in general:

Example 3.6. (Brace equivalence does not imply G-isomorphism) Let L/K be a Galois extension with Galois group
$$G = \langle \sigma, \tau \mid \sigma^4 = 1, \tau^2 = \sigma^2, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle \cong Q_8.$$
It is known [25, Lemma 2.5] that L/K admits 6 Hopf-Galois structures of dihedral type. The corresponding regular subgroups of $\text{Perm}(G)$ are
$$D_{s,\lambda} = \langle \lambda(s), \lambda(t)\rho(s) \rangle \quad \text{and} \quad D_{s,\rho} = \langle \rho(s), \lambda(s)\rho(t) \rangle,$$
where in each case s, t are distinct elements of the set $\{\sigma, \tau, \sigma\tau\}$, and the choice of t does not affect the definition of the subgroups. It is also known [25, Lemma 3.5] that the subgroups described above are pairwise non G-isomorphic.

We can use Proposition 3.1 to show that the subgroups $D_{s,\rho}$ are all brace equivalent. For $\varphi \in \text{Aut}(G)$ and $g \in G$ we have
$$\begin{aligned}
\varphi^{-1}\rho(\sigma)\varphi[g] &= \varphi^{-1}[\varphi(g)\sigma^{-1}] \\
&= g\varphi(\sigma)^{-1} \\
&= \rho(\varphi(\sigma))[g],
\end{aligned}$$
so $\varphi^{-1}\rho(\sigma)\varphi = \rho(\varphi(s))$. Similarly, $\varphi^{-1}\lambda(\sigma)\rho(\tau)\varphi = \lambda(\varphi(\sigma))\rho(\varphi(\tau))$, and so $\varphi^{-1}D_{\sigma,\rho}\varphi = D_{\varphi(\sigma),\rho}$. Since there exist automorphisms of G that send σ to each of $\sigma, \tau, \sigma\tau$, Proposition 3.1 implies that the subgroups $D_{s,\rho}$ are all brace equivalent.

This example also shows that the subgroups $D_{s,\rho}$ exhaust their brace class. Similarly, the subgroups $D_{s,\lambda}$ are brace equivalent, and form a second brace class. We could prove this by the methods employed above, but we shall see a more illuminating proof in Section 7.

Example 3.7. (G-isomorphism does not imply brace equivalence) Let L/K be a Galois extension with Galois group
$$G = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \ \tau\sigma\tau^{-1} = \sigma^{-1} \rangle \cong D_4.$$
Let $\eta = \lambda(\sigma)\rho(\tau)$ and $\pi = \lambda(\tau)$, and let $N = \langle \eta, \pi \rangle \subseteq \text{Perm}(G)$. Using the fact that the elements of $\lambda(G)$ and $\rho(G)$ commute inside $\text{Perm}(G)$, we see that $N \cong G$

and that N acts regularly on G. In fact, N is G-isomorphic to $\lambda(G)$: the map $\theta : \lambda(G) \to N$ defined by

$$\theta(\lambda(\sigma)) = \eta, \quad \theta(\lambda(\tau)) = \pi$$

is a G-isomorphism. Therefore N corresponds to a Hopf-Galois structure on L/K whose Hopf algebra H_N is isomorphic to H_λ. However, we have already observed that the brace class of the regular G-stable subgroup $\lambda(G)$ contains only one element, so N cannot be brace equivalent to $\lambda(G)$.

However, if two regular G-stable subgroups are G-isomorphic then the elements of their respective brace classes can be arranged into G-isomorphic pairs:

Proposition 3.8. *Suppose that N, M are G-isomorphic regular G-stable subgroups of $\mathrm{Perm}(G)$. Then, for $\varphi \in \mathrm{Aut}(G)$, N_φ, M_φ are G-isomorphic.*

Proof. Let $\theta : N \to M$ be a G-isomorphism. Define $\theta_\varphi : N_\varphi \to M_\varphi$ by

$$\theta_\varphi(\varphi^{-1}\eta\varphi) = \varphi^{-1}\theta(\eta)\varphi.$$

Then θ_φ is an isomorphism and for $\sigma \in G$ we have

$$
\begin{aligned}
\theta_\varphi \left({}^{\sigma}\left(\varphi^{-1}\eta\varphi \right) \right) &= \theta_\varphi(\varphi^{-1}\left({}^{\varphi(\sigma)}\eta \right)\varphi) \\
&= \varphi^{-1}\theta\left({}^{\varphi(\sigma)}\eta \right)\varphi \\
&= \varphi^{-1}\,{}^{\varphi(\sigma)}\theta\left(\eta \right)\varphi \\
&= {}^{\sigma}\left(\varphi^{-1}\theta\left(\eta \right)\varphi \right) \\
&= {}^{\sigma}\theta_\varphi\left(\varphi^{-1}\eta\varphi \right).
\end{aligned}
$$

Hence N_φ, M_φ are G-isomorphic. $\qquad\square$

4. Inner automorphisms and ρ-conjugate subgroups

In this section we assume that G is nonabelian and explore the consequences of conjugating a G-stable regular subgroup N of $\mathrm{Perm}(G)$ by an inner automorphism of G.

Proposition 4.1. *Let G be a nonabelian group and let N be a regular G-stable subgroup of $\mathrm{Perm}(G)$. Let $\sigma \in G$, and let $C(\sigma)$ denote the inner automorphism of G arising from σ. Then:*

(1) *$C(\sigma)NC(\sigma)^{-1} = \rho(\sigma)N\rho(\sigma)^{-1}$, where $\rho : G \to \mathrm{Perm}(G)$ is the the right regular representation of G;*

(2) *the subgroups N and $C(\sigma)NC(\sigma)^{-1}$ are G-isomorphic.*

Proof.   (1) We may write $C(\sigma) = \rho(\sigma)\lambda(\sigma)$, and so

$$C(\sigma)NC(\sigma)^{-1} = \rho(\sigma)\lambda(\sigma)N\lambda(\sigma)^{-1}\rho(\sigma)^{-1}.$$

But N is G-stable, so $\lambda(\sigma)N\lambda(\sigma)^{-1} = N$, and so

$$C(\sigma)NC(\sigma)^{-1} = \rho(\sigma)N\rho(\sigma)^{-1},$$

as claimed.

(2) Consider the isomorphism $\theta : N \to \rho(\sigma)N\rho(\sigma)^{-1}$ defined by $\theta(\eta) = \rho(\sigma)\eta\rho(\sigma)^{-1}$ for all $\eta \in N$. Using the fact that elements of $\lambda(G)$ and $\rho(G)$ commute inside $\mathrm{Perm}(G)$ we have $\theta({}^{\tau}\eta) = {}^{\tau}\theta(\eta)$ for all $\eta \in N$ and $\tau \in G$, so θ is a G-isomorphism.

$\square$

We shall say that two regular G-stable subgroups N, M of $\mathrm{Perm}(G)$ are ρ-*conjugate* if $M = \rho(\sigma)N\rho(\sigma)^{-1}$ for some $\sigma \in G$. This concept also appears in [17, Example 2.7]. We record some immediate corollaries of Proposition 4.1:

Corollary 4.2. *If N, M are ρ-conjugate regular G-stable subgroups of $\mathrm{Perm}(G)$ then they are brace equivalent.*

Corollary 4.3. *If G has only inner automorphisms then, for regular G-stable subgroups of $\mathrm{Perm}(G)$, brace equivalence implies G-isomorphism.*

Example 4.4. Let $G \cong D_3$ as in Example 2.3, and consider the regular G-stable subgroups $N_c = \langle \lambda(\sigma), \rho(\sigma^c\tau) \rangle$ of $\mathrm{Perm}(G)$ constructed there. It is not hard to see that these subgroups are ρ-conjugate, which implies that they are brace equivalent, as stated at the end of Example 2.9 and G-isomorphic.

5. Abelian endomorphisms

An endomorphism $\psi : G \to G$ is called *abelian* if $\psi(\sigma\tau) = \psi(\tau\sigma)$ for all $\sigma, \tau \in G$, and *fixed-point-free* if $\psi(\sigma) = \sigma$ only when $\sigma = 1_G$. In [7] Childs shows that, given a Galois extension of fields L/K with nonabelian Galois group G, abelian fixed-point-free endomorphisms can be used to construct families of regular G-stable subgroups of $\mathrm{Perm}(G)$ that are isomorphic to G. In [16] the first named author generalizes this construction by removing the fixed-point-free hypothesis; a consequence of this is that resulting subgroups of $\mathrm{Perm}(G)$ are not necessarily isomorphic to G. In this section we study the braces corresponding to subgroups arising from abelian endomorphisms.

First we summarize the results of [16]. Suppose that $\psi : G \to G$ is an abelian endomorphism, and define a map $\alpha_\psi : G \to \mathrm{Perm}(G)$ by $\alpha_\psi(\sigma) = \lambda(\sigma)C(\psi(\sigma^{-1}))$ for all $\sigma \in G$, where $C(\psi(\sigma))$ denotes the inner automorphism arising from $\psi(\sigma)$. It is easy to see that α_ψ is a homomorphism, so that $N_\psi = \alpha_\psi(G)$ is a subgroup of $\mathrm{Perm}(G)$, and [16, Theorem 3.1] shows that this subgroup is regular and G-stable.

Now we study the relationships between braces corresponding to regular G-stable subgroups arising via this construction. Write $\mathrm{Ab}(G)$ for the set of abelian endomorphisms of G.

Proposition 5.1. *If $\psi \in \mathrm{Ab}(G)$ and $\varphi \in \mathrm{Aut}(G)$ then $\varphi^{-1}\psi\varphi \in \mathrm{Ab}(G)$.*

Proof. It is clear that $\varphi^{-1}\psi\varphi$ is an endomorphism of G; we need to show that it is abelian. For $\sigma, \tau \in G$ we have

$$
\begin{aligned}
\varphi^{-1}\psi\varphi(\sigma\tau) &= \varphi^{-1}\psi(\varphi(\sigma)\varphi(\tau)) \ (\varphi \text{ is an automorphism}) \\
&= \varphi^{-1}\psi(\varphi(\tau)\varphi(\sigma)) \ (\psi \text{ is abelian}) \\
&= \varphi^{-1}\psi\varphi(\tau\sigma).
\end{aligned}
$$

Therefore $\varphi^{-1}\psi\varphi$ is abelian, and hence $\varphi^{-1}\psi\varphi \in \mathrm{Ab}(G)$. $\qquad\square$

Proposition 5.2. *If $\psi \in \mathrm{Ab}(G)$ and $\varphi \in \mathrm{Aut}(G)$ then $N_{\varphi^{-1}\psi\varphi} = \varphi^{-1}N_\psi\varphi$.*

Proof. Let $\sigma \in G$. Then for all $\tau \in G$ we have

$$
\begin{aligned}
\varphi^{-1}\alpha_\psi(\sigma)\varphi[\tau] &= \varphi^{-1}\lambda(\sigma)C(\psi(\sigma^{-1}))\varphi[\tau] \\
&= \varphi^{-1}(\sigma\psi(\sigma^{-1})\varphi(\tau)\psi(\sigma)) \\
&= \varphi^{-1}(\sigma)\varphi^{-1}(\psi(\sigma^{-1}))\tau\varphi^{-1}(\psi(\sigma)) \\
&= \lambda(\varphi^{-1}(\sigma))C(\varphi^{-1}(\psi(\sigma^{-1})))[\tau] \\
&= \lambda(\varphi^{-1}(\sigma))C(\varphi^{-1}\psi\varphi(\varphi^{-1}(\sigma^{-1})))[\tau] \\
&= \alpha_{\varphi^{-1}\psi\varphi}(\varphi^{-1}(\sigma))[\tau].
\end{aligned}
$$

Therefore $\varphi^{-1}\alpha_\psi(\sigma)\varphi = \alpha_{\varphi^{-1}\psi\varphi}(\varphi^{-1}(\sigma))$ for all $\sigma \in G$, and so $\varphi^{-1}N_\psi\varphi = N_{\varphi^{-1}\psi\varphi}$.
$\qquad\square$

To ease notation, if $\psi \in \mathrm{Ab}(G)$ then we write $\mathfrak{B}_\psi$ rather than $\mathfrak{B}_{N_\psi}$ for the brace corresponding to N_ψ. However, we caution the reader that two different elements of $\mathrm{Ab}(G)$ can yield the same subgroup, so $\mathfrak{B}_\psi = \mathfrak{B}_{\psi'}$ does not imply that $\psi = \psi'$. We also note that this construction may yield a different brace from the construction in [19].

Proposition 5.3. *If $\psi \in \mathrm{Ab}(G)$ and $\varphi \in \mathrm{Aut}(G)$ then $\mathfrak{B}_\psi \cong \mathfrak{B}_{\varphi^{-1}\psi\varphi}$. Furthermore, if $\mathfrak{B}_\psi \cong \mathfrak{B}_{\psi'}$ for some $\psi' \in \mathrm{Ab}(G)$ then there exists $\varphi \in \mathrm{Aut}(G)$ such that $\psi' = \varphi^{-1}\psi\varphi$.*

Proof. By Proposition 5.2 we have $N_{\varphi^{-1}\psi\varphi} = \varphi^{-1}N_\psi\varphi$; hence $\mathfrak{B}_\psi \cong \mathfrak{B}_{\varphi^{-1}\psi\varphi}$ by Proposition 3.1. If $\mathfrak{B}_\psi \cong \mathfrak{B}_{\psi'}$ for some $\psi' \in \mathrm{Ab}(G)$ then by Proposition 3.1 $N_{\psi'} = \varphi^{-1}N_\psi\varphi$ for some $\varphi \in \mathrm{Aut}(G)$; by Proposition 5.2 we have $\varphi^{-1}N_\psi\varphi = N_{\varphi^{-1}\psi\varphi}$, and so $N_{\psi'} = N_{\varphi^{-1}\psi\varphi}$. $\qquad\square$

Proposition 5.4. *If $\psi \in \mathrm{Ab}(G)$ and N is a regular G-stable subgroup of $\mathrm{Perm}(G)$ that is brace equivalent to N_ψ then $N = \alpha_{\psi'}(G)$ for some $\psi' \in \mathrm{Ab}(G)$.*

Proof. Since N is brace equivalent to N_ψ there exists $\varphi \in \mathrm{Aut}(G)$ such that $N = \varphi^{-1}N_\psi\varphi$. Applying Proposition 5.2 we have $N = N_{\varphi^{-1}\psi\varphi}$, so $N = \alpha_{\psi'}(G)$ with $\psi' = \varphi^{-1}\psi\varphi$. $\qquad\square$

If we impose the additional assumption that ψ is fixed-point-free (as in [7]) then [16, Section 4] shows that $N_\psi \cong G$ and that there exists another fixed-point-free abelian endomorphism Ψ such that $N_\psi = \{\lambda(\sigma)\rho(\Psi(\sigma)) \mid \sigma \in G\}$; following [7] we then see that the isomorphism $\theta : \lambda(G) \to N_\psi$ defined by $\theta(\lambda(\sigma)) = \lambda(\sigma)\rho(\Psi(\sigma))$ is a G-isomorphism. Thus we have:

Corollary 5.5. *If $\psi \in \mathrm{Ab}(G)$ is fixed-point free and N is a regular G-stable subgroup of $\mathrm{Perm}(G)$ that is brace equivalent to N_ψ then N is G-isomorphic to $\lambda(G)$.*

6. λ-POINTS AND ρ-POINTS

The prototypical examples of regular G-stable subgroups of $\mathrm{Perm}(G)$ are the subgroups $\lambda(G)$ and $\rho(G)$. A general regular G-stable subgroup N may intersect nontrivially with one or both of these; in this section we show that studying these intersections can yield useful information about the brace and Hopf-Galois structure that correspond to N.

Definition 6.1. Let N a regular G-stable subgroup of $\mathrm{Perm}(G)$. The λ-*points* of N are the elements of the set $\Lambda_N = N \cap \lambda(G)$. The ρ-*points* of N are the elements of the set $P_N = N \cap \rho(G)$.

It is clear that Λ_N and P_N are both subgroups of N.

Example 6.2. Let L/K be a Galois extension with Galois group $G \cong Q_8$, as in Example 3.6, and consider the regular G-stable subgroups $D_{s,\lambda}$ and $D_{s,\rho}$ constructed there. Then the λ-points of $D_{s,\lambda}$ are $\lambda(1), \lambda(s), \lambda(s^2), \lambda(s^3)$, and the ρ-points of $D_{s,\lambda}$ are $\rho(1)$ and $\rho(s^2)$, since $s^2 \in Z(G)$. The results for $D_{s,\rho}$ are analogous.

First we study the behaviour of λ-points and ρ-points with respect to brace equivalence:

Proposition 6.3. Let N, M be regular G-stable subgroups of $\mathrm{Perm}(G)$ and suppose that N, M are brace equivalent. Then:
  (1) $\Lambda_N \cong \Lambda_M$;
  (2) $P_N \cong P_M$.

Proof. Since N, M are brace equivalent, there exists $\varphi \in \mathrm{Aut}(G)$ such that $M = \varphi^{-1} N \varphi$. To prove (1), define $\theta : \Lambda_N \to M$ by $\theta(\lambda(\sigma)) = \varphi^{-1}(\lambda(\sigma))\varphi$. Then for all $\tau \in G$ we have

$$\theta(\lambda(\sigma))[\tau] = \varphi^{-1}(\lambda(\sigma))\varphi[\tau] = \varphi^{-1}(\sigma\varphi(\tau)) = \varphi^{-1}(\sigma)\tau = \lambda(\varphi^{-1}(\sigma))[\tau].$$

Hence θ is actually a map from Λ_N to Λ_M, which is clearly an isomorphism. The proof of (2) is similar. $\qquad\square$

Proposition 6.3 provides a useful necessary condition for two regular G-stable subgroups to be brace equivalent, which we shall apply in Section 8.

In fact, the isomorphisms established in Proposition 6.3 are G-isomorphisms. More generally, ρ-points interact well with G-isomorphism:

Proposition 6.4. Let N, M be regular G-stable subgroups of $\mathrm{Perm}(G)$ and suppose that $\theta : N \to M$ is a G-isomorphism. Then $P_N = \theta(P_M)$.

Proof. We may characterize $\rho(G)$ as the centralizer of $\lambda(G)$ in $\mathrm{Perm}(G)$: thus a permutation $\eta \in \mathrm{Perm}(G)$ lies in $\rho(G)$ if and only if $^\sigma\eta = \eta$ for all $\sigma \in G$. Now let $\eta \in P_N$; then for all $\sigma \in G$ we have

$$
\begin{aligned}
^\sigma\theta(\eta) &= \theta(^\sigma\eta) \text{ since } \theta \text{ is a } G\text{-isomorphism} \\
&= \theta(\eta) \text{ since } \eta \in P_N.
\end{aligned}
$$

Hence $\theta(\eta) \in P_M$. Reversing the roles of N, M yields the result. $\qquad\square$

Proposition 6.4 provides a useful necessary condition for two regular G-stable subgroups to be G-isomorphic. However, the analogous result for λ-points is not true:

Example 6.5. Let L/K be a Galois extension with Galois group $G \cong D_4$, as in Example 3.7, and recall from that example that $N = \langle \eta, \pi \rangle$, with $\eta = \lambda(\sigma)\rho(\tau)$ and $\pi = \lambda(\tau)$, is a G-stable regular subgroup of $\mathrm{Perm}(G)$ that is G-isomorphic to $\lambda(G)$. Obviously every element of $\lambda(G)$ is a λ-point, but the λ-points of N are $\lambda(1), \lambda(\tau), \lambda(\sigma^2), \lambda(\sigma^2\tau)$.

7. Opposite braces

In Greither and Pareigis's original paper characterizing Hopf-Galois structures on separable field extensions [12] they observe that if N is a regular G-stable subgroup of $\mathrm{Perm}(G)$, then so too is $N^{opp} = \mathrm{Cent}_{\mathrm{Perm}(G)}(N)$; this construction, and the corresponding Hopf-Galois structures on a Galois extension with Galois group G, have subsequently been studied in, for example, [22], [26], and [20]. The notation N^{opp} reflects the fact that this subgroups can be naturally identified with the opposite group of N; in [20] the authors referred to the Hopf-Galois structure corresponding to N^{opp} as the *opposite* of the one corresponding to N. We showed that this construction leads naturally to the notion of the *opposite* of a brace, as follows: given a brace $\mathfrak{B} = (B, \cdot, \circ)$, we define a new binary operation on B by $x \cdot' y = y \cdot x$ for all $x, y \in B$. Then $\mathfrak{B}^{opp} := (B, \cdot', \circ)$ is a brace, called the *opposite* of the brace $\mathfrak{B}$. This concept is also developed independently by Rump [23]. If N is a regular G-stable subgroup of $\mathrm{Perm}(G)$, with corresponding brace $\mathfrak{B}_N$, then the brace corresponding to the opposite subgroup N^{opp} is then $\mathfrak{B}_{N^{opp}} = (\mathfrak{B}_N)^{opp}$. If $\mathfrak{B} = (B, \cdot, \circ)$ is a brace and N is the regular $(B, \circ)$-stable subgroup of $\mathrm{Perm}(B)$ arising from the dot operation in B then the subgroup arising from the dot operation in $\mathfrak{B}^{opp}$ is N^{opp}.

The notion of opposite extends to brace classes:

Proposition 7.1. *Let N be a regular G-stable subgroup of $\mathrm{Perm}(G)$, and let N^{opp} be the opposite subgroup to N. Then for each $\varphi \in \mathrm{Aut}(G)$ we have $\left(\varphi^{-1}N\varphi\right)^{opp} = \varphi^{-1}N^{opp}\varphi$.*

Proof. Let $\eta' \in N^{opp}$, so that $\varphi^{-1}\eta'\varphi \in \varphi^{-1}N^{opp}\varphi$. Then for all $\eta \in N$ we have

$$
\begin{aligned}
\left(\varphi^{-1}\eta'\varphi\right)\left(\varphi^{-1}\eta\varphi\right) &= \left(\varphi^{-1}\eta'\eta\varphi\right) \\
&= \left(\varphi^{-1}\eta\eta'\varphi\right) \\
&= \left(\varphi^{-1}\eta\varphi\right)\left(\varphi^{-1}\eta'\varphi\right).
\end{aligned}
$$

Hence $\varphi^{-1}N^{opp}\varphi \subseteq \left(\varphi^{-1}N\varphi\right)^{opp}$. But these groups have equal order, so in fact they are equal. $\square$

Corollary 7.2. *The brace class of N^{opp} consists precisely of the opposites of the subgroups in the brace class of N. In particular, these brace classes are of equal size.*

Example 7.3. Let L/K be a Galois extension with Galois group $G = \langle \sigma, \tau \rangle \cong Q_8$, as in Example 3.6, and consider the regular G-stable subgroups $D_{s,\lambda}$ and $D_{s,\rho}$ described in that example. We saw there that the subgroups $D_{s,\rho}$ are brace equivalent and exhaust their brace class. It is routine to verify that $D_{s,\rho}^{opp} = D_{s,\lambda}$ for each s; thus the subgroups $D_{s,\lambda}$ are brace equivalent and exhaust their brace class, as stated at the end of that example.

Corollary 7.4. *Let N, M be G-stable regular subgroups of $\mathrm{Perm}(G)$, and suppose that N, M are ρ-conjugate. Then N^{opp}, M^{opp} are ρ-conjugate.*

As pointed out in [20, Section 6], it is possible for $\mathfrak{B}_N$ and $\mathfrak{B}_{N^{opp}}$ to be isomorphic; when this occurs, the brace classes of N and N^{opp} coincide.

On the other hand, if N, M are regular G-stable subgroups of $\mathrm{Perm}(G)$ that are G-isomorphic, it does not necessarily follow that N^{opp} and M^{opp} are G-isomorphic:

Example 7.5. Let L/K be a Galois extension with Galois group $G \cong D_4$, as in Example 3.7, and recall from that example that $N = \langle \eta, \pi \rangle$, with $\eta = \lambda(\sigma)\rho(\tau)$ and $\pi = \lambda(\tau)$, is a G-stable regular subgroup of $\mathrm{Perm}(G)$ that is G-isomorphic to $\lambda(G)$. However, we have $\lambda(G)^{opp} = \rho(G)$, and no other regular G-stable subgroup of $\mathrm{Perm}(G)$ can be G-isomorphic to $\rho(G)$. Therefore N^{opp} is not G-isomorphic to $\lambda(G)^{opp}$.

8. Braces of order pq and Hopf-Galois structures of degree pq

Let p, q be prime numbers with $p > q$. In [4] Byott classifies the Hopf-Galois structures admitted by Galois extensions of fields of degree pq; building upon these results, the braces of order pq are classified in [1] and [5, Subsection 2.9].

In this section we consider in turn each of the isomorphically distinct braces $\mathfrak{B} = (B, \cdot, \circ)$ of order pq. Writing $N = (B, \cdot)$ and $G = (B, \circ)$, we recover all of the G-stable regular subgroups of $\mathrm{Perm}(G)$ that are isomorphic to N, and hence the Hopf-Galois structures of type N on a Galois extension of fields with Galois group G. We use the tools developed in the earlier sections to arrange these subgroups into G-isomorphism classes, which is equivalent to determining the Hopf algebra isomorphism classes of the Hopf algebras giving the Hopf-Galois structures. The classifications of braces in [1] and [5, Subsection 2.9] are organized by fixing a presentation of the dot group and allowing the circle group to vary. Here it is more convenient to reverse this organization; where necessary, we state maps that reconcile our descriptions with those in loc. cit.

If $p \not\equiv 1 \pmod{q}$ then N and G must both be isomorphic to C, the cyclic group of order pq; if $p \equiv 1 \pmod{q}$ then each of these groups is isomorphic to either C or to M, the metacyclic group of order pq. We describe both these groups via two generators σ, τ, using the underlying set

$$B = \{\sigma^i \tau^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\},$$

where σ has order p and τ has order q. To obtain C we impose the relation $\tau \sigma \tau^{-1} = \sigma$; to obtain M we fix an integer g whose multiplicative order modulo p is q and impose the relation $\tau \sigma \tau^{-1} = \sigma^g$. We also fix notation for the automorphisms

of these groups: we have $\mathrm{Aut}(C) = \{\varphi_t \mid \gcd(t, pq) = 1\}$, where $\varphi_t(\sigma) = \sigma^t$ and $\varphi_t(\tau) = \tau^t$, and $\mathrm{Aut}(M) = \langle \phi, \psi \rangle$, where $\phi(\sigma\tau) = \sigma^d\tau$ with d a primitive root modulo p and $\phi(\tau) = \tau$, and $\psi(\sigma) = \sigma$ and $\psi(\tau) = \sigma\tau$.

The case $\mathbf{G} \cong \mathbf{N} \cong \mathbf{C}$: Up to isomorphism, there is a unique brace $\mathfrak{B}$ with $N \cong G \cong C$, which is the trivial brace for C [1, Proposition 3.1]. The regular G-stable subgroup of $\mathrm{Perm}(G)$ obtained from the dot operation in $\mathfrak{B}$ is simply $\rho(G)$. Moreover, every automorphism of G is automatically an automorphism of $\mathfrak{B}$; hence $\rho(G)$ is the unique regular G-stable subgroup of $\mathrm{Perm}(G)$ that is isomorphic to N [4, (4.1)]. There are no G-isomorphism questions to consider in this case.

As mentioned above, if $p \not\equiv 1 \pmod{q}$ then every group of order pq is cyclic, and so this case is the only one that can occur. For the remainder of this section we assume that $p \equiv 1 \pmod{q}$.

The case $\mathbf{G} \cong \mathbf{C}$, $\mathbf{N} \cong \mathbf{M}$: There are two isomorphically distinct braces with these properties. The first is the brace A_q constructed in [1, part (iii) of the second bullet point of the main theorem]. In our notation this takes the form $\mathfrak{B} = (B, \cdot, \circ)$, where

$$\begin{aligned} \sigma^i\tau^j \cdot \sigma^k\tau^\ell &= \sigma^{i+kg^j}\tau^{j+\ell} \\ \sigma^i\tau^j \circ \sigma^k\tau^\ell &= \sigma^{i+k}\tau^{j+\ell}. \end{aligned}$$

The second brace with these properties is constructed in [1, part (ii) of the second bullet point of the main theorem]. We obtain it by taking the opposite to the brace $\mathfrak{B}$ above: we have $\mathfrak{B}^{opp} = (B, \cdot', \circ)$, where

$$\begin{aligned} \sigma^i\tau^j \cdot' \sigma^k\tau^\ell &= \sigma^{k+ig^\ell}\tau^{j+\ell} \\ \sigma^i\tau^j \circ \sigma^k\tau^\ell &= \sigma^{i+k}\tau^{j+\ell}. \end{aligned}$$

To reconcile this description with the one given in loc. cit. we apply the map $\sigma^i\tau^j \mapsto \tau^j\sigma^i$.

The regular G-stable subgroup of $\mathrm{Perm}(G)$ obtained from the dot operation in $\mathfrak{B}$ is $N = \langle \eta, \pi \rangle$, where

$$\begin{aligned} \eta(\sigma^k\tau^\ell) &= \sigma \cdot \sigma^k\tau^\ell = \sigma^{k+1}\tau^\ell \\ \pi(\sigma^k\tau^\ell) &= \tau \cdot \sigma^k\tau^\ell = \sigma^{kg}\tau^{\ell+1}. \end{aligned}$$

We determine all of the regular G-stable regular subgroups of $\mathrm{Perm}(G)$ that are brace equivalent to N. For each t coprime to pq we conjugate the generators of N by the automorphism φ_t:

$$\begin{aligned} \varphi_t^{-1}\eta\varphi_t(\sigma^k\tau^\ell) &= \sigma^{k+t^{-1}}\tau^\ell = \eta^{t^{-1}}(\sigma^k\tau^\ell) \\ \varphi_t^{-1}\pi\varphi_t(\sigma^k\tau^\ell) &= \sigma^{kg}\tau^{\ell+t^{-1}} = \pi_t(\sigma^k\tau^\ell), \end{aligned}$$

say (with $\pi = \pi_1$). The automorphism φ_t respects $\cdot$ if and only if $t \equiv 1 \pmod{q}$, and so by Proposition 3.1 the subgroups $N_t = \langle \eta, \pi_t \rangle$ are a family of $q - 1$ regular G-stable subgroups of $\mathrm{Perm}(G)$. This is the family of subgroups described in [4, Lemma 5.2, Equation (5.8)].

The regular G-stable subgroup of $\mathrm{Perm}(G)$ obtained from the dot operation in $\mathfrak{B}^{opp}$ is $N^{opp} = \langle \eta', \pi' \rangle$, where

$$\eta'(\sigma^k \tau^\ell) = \sigma \cdot' \sigma^k \tau^\ell = \sigma^{k+g^\ell} \tau^\ell$$
$$\pi'(\sigma^k \tau^\ell) = \tau \cdot' \sigma^k \tau^\ell = \sigma^k \tau^{\ell+1}.$$

We determine all of the regular G-stable regular subgroups of $\mathrm{Perm}(G)$ that are brace equivalent to N^{opp}. Proceeding as above we have

$$\varphi_t^{-1} \eta' \varphi_t(\sigma^k \tau^\ell) = \sigma^{k+t^{-1}g^{t\ell}} \tau^\ell = \eta_t'(\sigma^k \tau^\ell)$$
$$\varphi_t^{-1} \pi' \varphi_t(\sigma^k \tau^\ell) = \sigma^k \tau^{\ell+t^{-1}} = (\pi')^{t^{-1}}(\sigma^k \tau^\ell),$$

say (with $\eta' = \eta_1'$). The automorphism φ_t respects $\cdot'$ if and only if $t \equiv 1 \pmod{q}$, and so the subgroups $N_t^{opp} = \langle \eta', \pi_t' \rangle$ are a family of $q-1$ regular G-stable subgroups of $\mathrm{Perm}(G)$. This is the family of subgroups described in [4, Lemma 5.1, Equation (5.3)]. The subgroups N_t and N_t' account for all of the G-stable regular subgroups of $\mathrm{Perm}(G)$ that are isomorphic to M.

Proposition 8.1. *The subgroups N_t are mutually G-isomorphic. The subgroups N_t^{opp} are pairwise non G-isomorphic, and none are G-isomorphic to any of the subgroups N_t.*

Proof. For $1 \leq t \leq q-1$ the action of G on the subgroup N_t is given by

$$^\sigma \eta = \eta, \qquad ^\tau \eta = \eta,$$
$$^\sigma \pi_t = \eta^{1-g} \pi_t, \quad ^\tau \pi_t = \pi_t.$$

Hence the natural isomorphism $N_1 \to N_t$ defined by $\eta^i \pi_1^j \mapsto \eta_i \pi_t^j$ is a G-isomorphism, and so the subgroups N_t are mutually G-isomorphic.

On the other hand for $1 \leq t \leq q-1$ the action of G on the subgroup N_t^{opp} is given by

$$^\sigma \eta_t' = \eta_t', \quad ^\tau \eta_t' = (\eta_t')^{g^{-t}},$$
$$^\sigma \pi' = \pi', \quad ^\tau \pi' = \pi'.$$

Now if $\theta : N_{t_1}^{opp} \to N_{t_2}^{opp}$ is a G-isomorphism then $\theta(\eta_{t_1}) = \eta_{t_2}^v$ for some $v = 1, \ldots, p-1$, since η_{t_1} has order p. Taking the G action into account, we have

$$\theta(^\tau \eta_{t_1}) = \theta(\eta_{t_1}^{g^{-t_1}}) = \eta_{t_2}^{vg^{-t_1}}$$
$$\text{and} \quad ^\tau \theta(\eta_{t_1}) = {}^\tau \eta_{t_2}^v = \eta_{t_2}^{vg^{-t_2}}.$$

Since $v \not\equiv 0 \pmod{p}$, this implies that $g^{-t_1} \equiv g^{-t_2} \pmod{p}$, and since g has order q modulo p this implies that $t_1 = t_2$.

Finally note that since G is abelian the notions of λ-point and ρ-point coincide. The subgroups of the form N_t have p ρ-points, namely the elements η^i. The subgroups of the form N_t^{opp} have q ρ-points, namely the elements $(\pi')^j$. By Proposition 6.4 no subgroup of the form N_t can be G-isomorphic to a subgroup of the form N_t^{opp}. Therefore the G-isomorphisms amongst these subgroups are as in the statement of the proposition. $\square$

The case $G \cong M$, $N \cong C$: Up to isomorphism there is a unique brace with these properties, which is constructed in [1, part (ii) of the first bullet point of the main theorem]. In our notation this takes the form $\mathfrak{B} = (B, \cdot, \circ)$, where

$$\begin{aligned}
\sigma^i \tau^j \cdot \sigma^k \tau^\ell &= \sigma^{i+k} \tau^{j+\ell} \\
\sigma^i \tau^j \circ \sigma^k \tau^\ell &= \sigma^{i+kg^j} \tau^{j+\ell}.
\end{aligned}$$

The regular G-stable subgroup of $\mathrm{Perm}(G)$ obtained from the dot operation in $\mathfrak{B}$ is $N = \langle \eta, \pi \rangle$, where

$$\begin{aligned}
\eta(\sigma^k \tau^\ell) &= \sigma \cdot \sigma^k \tau^\ell = \sigma^{k+1} \tau^\ell \\
\pi(\sigma^k \tau^\ell) &= \tau \cdot \sigma^k \tau^\ell = \sigma^k \tau^{\ell+1}.
\end{aligned}$$

We determine all of the regular G-stable regular subgroups of $\mathrm{Perm}(G)$ that are brace equivalent to N. The automorphism ϕ respects $\cdot$, but the automorphism ψ does not; thus the subgroups $N_s = \psi^{-s} N \psi^s$, with $0 \le s \le p-1$, form a family of p regular G-stable subgroups of $\mathrm{Perm}(G)$ that are isomorphic to N. This is the family described in [4, Lemma 4.1, Equation (4.3)], and accounts for all of the G-stable regular subgroups of $\mathrm{Perm}(G)$ that are isomorphic to C.

Proposition 8.2. *The subgroups N_s are ρ-conjugate and mutually G-isomorphic.*

Proof. Let $C(\sigma)$ be the inner automorphism of G arising from σ. Then $C(\sigma)(\sigma) = \sigma$ and $C(\sigma)(\tau) = \sigma^{1-g}\tau$. It follows that for each $m \in \mathbb{N}$ we have $C(\sigma)^m(\tau) = \sigma^{(1-g)m}\tau$. Since $1-g$ is coprime to p, there exists $m \in \mathbb{N}$ such that $C(\sigma)^m(\tau) = \sigma\tau$, and hence ψ is an inner automorphism of G. Now Proposition 4.1 implies that the subgroups N_s are ρ-conjugate and mutually G-isomorphic. $\square$

The case $G \cong N \cong M$: There are two distinguished braces with these properties and two further families, each of size $q-2$. The distinguished braces are the trivial brace for M and the almost trivial brace for M (which is isomorphic to the opposite of the trivial brace). Assuming $q > 2$, the first family consists of the braces A_t (for $2 \le t \le q-1$) constructed in [1, part (iii) of the second bullet point of the main theorem]. (We have already seen that the brace A_q of loc. cit. has cyclic circle group.) We present these as $\mathfrak{B}_t = (B, \cdot, \circ)$ where

$$\begin{aligned}
\sigma^i \tau^j \cdot \sigma^k \tau^\ell &= \sigma^{i+kg^{jt}} \tau^{j+\ell} \\
\sigma^i \tau^j \circ \sigma^k \tau^\ell &= \sigma^{i+kg^j} \tau^{j+\ell}
\end{aligned}$$

To reconcile this presentation with that give in loc. cit. we apply the map $\sigma^i \tau^j \mapsto \sigma^i \tau^{jt^{-1}}$.

The second family consists of the braces A_t (for $2 \le t \le q-1$) constructed in [1, part (iv) of the second bullet point of the main theorem]. (We have already seen that the brace A_q of loc. cit. is isomorphic to the almost trivial brace for M.) We obtain these braces by taking the opposites to the braces $\mathfrak{B}_t$ above: we have $\mathfrak{B}_t^{opp} = (B, \cdot', \circ)$, where

$$\begin{aligned}
\sigma^i \tau^j \cdot' \sigma^k \tau^\ell &= \sigma^{k+ig^{\ell t}} \tau^{j+\ell} \\
\sigma^i \tau^j \circ \sigma^k \tau^\ell &= \sigma^{i+kg^j} \tau^{j+\ell}
\end{aligned}$$

To reconcile this presentation with that give in loc. cit. we apply the map $\sigma^i \tau^j \mapsto \sigma^i \tau^{jt}$.

We determine all of the regular G-stable regular subgroups of $\mathrm{Perm}(G)$ that yield each of these braces. We know that $\lambda(G)$ yields the trivial brace on G and that $\rho(G)$ yields the almost trivial brace on G, and that each of these in a brace class by itself.

Assuming $q > 2$, the regular G-stable subgroup of $\mathrm{Perm}(G)$ obtained from the dot operation in $\mathfrak{B}_t$ is $N_t = \langle \eta, \pi_t \rangle$, where

$$\eta(\sigma^k \tau^\ell) = \sigma \cdot \sigma^k \tau^\ell = \sigma^{k+1} \tau^\ell$$
$$\pi_t(\sigma^k \tau^\ell) = \tau \cdot \sigma^k \tau^\ell = \sigma^{kg^t} \tau^{\ell+1}.$$

Now considering automorphisms of G we see that in all cases the automorphism ϕ respects $\cdot$, but the automorphism ψ does not; we write $N_{t,u} = \psi^{-u} N_t \psi^u$ for $0 \leq u \leq p-1$. Allowing t, u to vary we obtain a family of $p(q-2)$ regular G-stable subgroups of $\mathrm{Perm}(G)$ that are isomorphic to N. We note that these subgroups have p λ-points, namely the elements η^i; it follows that these subgroups coincide with the family described in [4, Lemma 5.2, Equation (5.7)].

The G-stable regular subgroup of $\mathrm{Perm}(G)$ obtained from the dot operation in $\mathfrak{B}_t^{opp}$ is $N_t^{opp} = \langle \eta_t, \pi \rangle$, where

$$\eta_t(\sigma^k \tau^\ell) = \sigma \cdot' \sigma^k \tau^\ell = \sigma^{k+g^{\ell t}} \tau^\ell$$
$$\pi(\sigma^k \tau^\ell) = \tau \cdot' \sigma^k \tau^\ell = \sigma^k \tau^{\ell+1}.$$

As above we find that ϕ respects $\cdot'$, but ψ does not; we write $N_{t,u}^{opp} = \psi^{-u} N_t^{opp} \psi^u$ for $0 \leq u \leq p-1$, and obtain a family of $p(q-2)$ regular G-stable subgroups of $\mathrm{Perm}(G)$ that are isomorphic to N. We note that these subgroups have q ρ-points, namely the elements π^j; it follows that these subgroups coincide with the family described in [4, Lemma 5.4, Equation (5.12)]. Together with the subgroups $\rho(G)$ and $\lambda(G)$, the subgroups of the form $N_{t,u}$ and $N_{t,u}^{opp}$ account for all of the G-stable regular subgroups of $\mathrm{Perm}(G)$ that are isomorphic to N.

Proposition 8.3. *The subgroups $N_{t,u}$ are mutually G-isomorphic. The G-isomorphism classes amongst the subgroups $N_{t,u}^{opp}$ are determined by t. No subgroup of the form $N_{t,u}$ is G-isomorphic to a subgroup of the form $N_{t,u}^{opp}$.*

Proof. To establish the first claim we show that the subgroups $N_{t,u}$ arise via abelian fixed point free endomorphisms of G (see Section 5). For fixed t consider the subgroup $N_t = \langle \eta, \pi_t \rangle$ obtained from the dot operation in $\mathfrak{B}_t$. It is clear that $\eta = \lambda(\sigma)$, where λ denotes the left regular representation of G. Similarly, letting r denote the inverse of t modulo q, we have

$$\begin{aligned}
\pi_t^r(\sigma^k \tau^\ell) &= \sigma^{kg^{rt}} \tau^{\ell+r} \\
&= \sigma^{kg} \tau^{\ell+r} \\
&= \tau \sigma^k \tau^\ell \tau^{r-1} \\
&= \lambda(\tau) \rho(\tau^{1-r})(\sigma^k \tau^\ell),
\end{aligned}$$

where ρ denotes the right regular representation of G. Hence $\pi_t^r = \lambda_\circ(\tau) \rho_\circ(\tau^{1-r})$. Now consider the function $\psi : G \to G$ defined by $\psi(\sigma^k \tau^\ell) = \tau^{\ell(1-r)}$. This is

an abelian abelian fixed-point-free endomorphism (see [19]), and the corresponding regular G-stable subgroup N_ψ of $\mathrm{Perm}(G)$ is generated by $\lambda_\circ(\sigma)$ and $\lambda(\tau)\rho(\psi(\tau)) = \pi_t^r$. Thus $N_\psi = N_t$, and applying Corollary 5.5 we see that N_t is G-isomorphic to $\lambda(G)$. Since this holds for all t, the subgroups N_t are mutually G-isomorphic. Finally, applying Proposition 5.2 we see that all of the subgroups $N_{t,u}$ arise via abelian fixed point free endomorphisms, and so are mutually G-isomorphic.

Next we consider the subgroups $N_{t,u}^{opp}$. For each fixed t we have $N_{t,u}^{opp} = \psi^{-u} N_t^{opp} \psi^u$ for $0 \le u \le p - 1$, and we saw in the proof of Proposition 8.2 that ψ is an inner automorphism of G; hence by Proposition 4.1 the subgroups $N_{t,u}^{opp}$ are all ρ-conjugate and G-isomorphic. To show that there are no further G-isomorphisms within this family, it is sufficient to show that no two of the subgroups N_t^{opp} are G-isomorphic. We calculate the action of τ on η_t:

$$
\begin{aligned}
{}^\tau\eta_t(\sigma^k\tau^\ell) &= \tau\eta_t(\tau^{-1}\sigma^k\tau^\ell) \\
&= \tau\eta_t(\sigma^{kg^{-1}}\tau^{\ell-1}) \\
&= \tau(\sigma^{kg^{-1}g^{(\ell-1)t}}\tau^{\ell-1}) \\
&= \sigma^{kg^{(\ell-1)t}}\tau^\ell) \\
&= \eta_t^{g^{-t}}(\sigma^k\tau^\ell).
\end{aligned}
$$

Hence ${}^\tau\eta_t = \eta_t^{g^{-t}}$. Now if $\theta : N_{t_1}^{opp} \to N_{t_2}^{opp}$ is a G-isomorphism then $\theta(\eta_{t_1}) = \eta_{t_2}^v$ for some $v = 1, \ldots, p - 1$, since η_{t_1} has order p. Taking the G action into account, we have

$$
\theta({}^\tau\eta_{t_1}) = \theta(\eta_{t_1}^{g^{-t_1}}) = \eta_{t_2}^{vg^{-t_1}}
$$
$$
\text{and} \quad {}^\tau\theta(\eta_{t_1}) = {}^\tau\eta_{t_2}^v = \eta_{t_2}^{vg^{-t_2}}.
$$

Since $v \not\equiv 0 \pmod{p}$, this implies that $g^{-t_1} \equiv g^{-t_2} \pmod{p}$, and since g has order q modulo p this implies that $t_1 = t_2$. Therefore the G-isomorphisms amongst the subgroups $N_{t,u}^{opp}$ are as described in the statement of the proposition.

The final claim follows from Proposition 6.4 since each of the subgroups $N_{s,t}^{opp}$ has q ρ-points, whereas each of the subgroups $N_{s,t}$ has none. $\qquad\square$

Acknowledgements

References

[1] Acri, E., Bonatto, M. (2020). *Skew braces of size pq.* Communications in Algebra, 48(5), 1-10.

[2] Bachiller, D. (2016). *Counterexample to a conjecture about braces.* Journal of Algebra, 453, 160-176.

[3] Byott, N. P. (1996). *Uniqueness of Hopf-Galois structure for separable field extensions.* Communications in Algebra, 24(10), 3217-3228.

[4] Byott, N. P. (2004). *Hopf-Galois structures on Galois field extensions of degree pq.* Journal of Pure and Applied Algebra, 188(1-3), 45-57.

[5] Campedel, E., Caranti, A., and Del Corso, I. (2020) *Hopf-Galois structures on extensions of degree p^2q and skew braces of order p^2q: the cyclic Sylow p-subgroup case.* Journal of Algebra 556, 1165-1210.

[6] Childs, L. N. (2000). *Taming Wild Extensions: Hopf algebras and local Galois module theory,* American Mathematical Society.

[7] Childs, L. (2013). *Fixed-point free endomorphisms and Hopf-Galois structures.* Proceedings of the American Mathematical Society, 141(4), 1255-1265.

[8] Childs, L.N. (2018). *Skew braces and the Galois correspondence for Hopf-Galois structures.* Journal of Algebra, 511, 270-291.

[9] Crespo, T., Rio, A., Vela, M. (2015). *Non-isomorphic Hopf-Galois structures with isomorphic underlying Hopf algebras.* Journal of Algebra, 422, 270-276.

[10] Crespo, T., Rio, A., Vela, M. (2016). *Induced Hopf-Galois structures.* Journal of Algebra, 457, 312-322.

[11] Caranti, A., Stefanello, L., (2021). *From endomorphisms to bi-skew braces, regular subgroups, the Yang-Baxter equation, and Hopf-Galois structures.* Journal of Algebra, 587, 462-487

[12] Pareigis, B., Greither, C. (1987). *Hopf-Galois theory for separable field extensions.* Journal of Algebra, (1), 239-258.

[13] Guarnieri, L., Vendramin, L. (2017). *Skew braces and the Yang-Baxter equation.* Mathematics of Computation 86(307), 25192534.

[14] Nejabtai Zenouz, K. (2018). *On Hopf-Galois structures and skew braces of Order p^3.* PhD thesis, University of Exeter.

[15] Nejabtai Zenouz, K. (2019). *Skew braces and Hopf-Galois structures of Heisenberg type.* Journal of Algebra, 524, 187-225.

[16] Koch, A. (2021). *Abelian maps, bi-skew braces, and opposite pairs of Hopf-Galois structures.* Proceedings of the American Mathematical Society, Series B, 8(16), 189-203.

[17] Koch, A., Kohl, T., Truman, P. J., Underwood, R. (2017). *The structure of Hopf algebras acting on dihedral extensions.* In Southern Regional Algebra Conference (pp. 201-218). Springer, Cham.

[18] Koch, A., Kohl, T., Truman, P. J., Underwood, R. (2019). *Isomorphism problems for Hopf-Galois structures on separable field extensions.* Journal of Pure and Applied Algebra, 223(5), 2230-2245.

[19] Koch, A., Stordy, L., Truman, P. J. (2020) *Abelian fixed-point-free endomorphisms and the Yang-Baxter equation.* New York Journal of Mathematics, 26, 14731492.

[20] Koch, A., Truman, P. J. (2020). *Opposite skew left braces and applications.* Journal of Algebra, 546, 218-235.

[21] Kohl, T. (1998). *Classification of the Hopf-Galois structures on prime power radical extensions.* Journal of Algebra, 207(2), 525-546.

[22] Kohl, T. (2007). *Groups of order 4p, twisted wreath products and Hopf-Galois theory.* Journal of Algebra, 314(1), 42-74.

[23] Rump, W. (2019). *A covering theory for non-involutive set-theoretic solutions to the Yang-Baxter equation.* Journal of Algebra, 520, 136–170.

[24] Smoktunowicz, A., Vendramin, L. (2018). *On skew braces* (with an appendix by N. Byott and L. Vendramin). Journal of Combinatorial Algebra, 2(1), 47-86.

[25] Taylor, S., Truman, P. J. (2019). *The structure of Hopf algebras giving Hopf-Galois structures on Quaternionic extensions.* New York Journal of Mathematics, 25, 219-237

[26] Truman, P. J. (2018). *Commuting Hopf-Galois structures on a separable extension.* Communications in Algebra, 46(4), 1420-1427.