This is a ``preproof'' accepted article for *Canadian Mathematical Bulletin*
This version may be subject to change during the production process.
DOI: 10.4153/S0008439525000098

Constructing skew left braces whose additive group has trivial centre

A. Ballester-Bolinches* R. Esteban-Romero*
P. Jiménez-Seral† V. Pérez-Calabuig*

Abstract

A complete description of all possible multiplicative groups of finite skew left braces whose additive group has trivial centre is given. As a consequence, some earlier results of Tsang can be improved and an answer to an open question set by Tsang at Ischia Group Theory 2024 Conference is provided.

Keywords: skew left brace, trifactorised group, trivial centre

Mathematics Subject Classification (2020): 16T25, 81R50, 20C35, 20C99, 20D40.

1 Introduction

Skew brace structure plays a key role in the combinatorial theory of Yang-Baxter equation. Skew left braces, introduced in [9], can be regarded as extensions of Jacobson radical rings and show connections with several areas of mathematics such as triply factorised groups and Hopf-Galois structures (see [1, 4, 5])

Skew left braces classify solutions of the Yang-Baxter equation (see [9]). This connection to the Yang-Baxter equation motivates the search for constructions of skew braces and classification results.

Recall that a *skew left brace* is a set endowed with two group structures $(B, +)$, not necessarily abelian, and $(B, \cdot)$ which are linked by the distributive-like law $a(b + c) = ab - a + ac$ for a, b, $c \in B$.

*Departament de Matemàtiques, Universitat de València, Dr. Moliner, 50, 46100 Burjassot, València, Spain; Adolfo.Ballester@uv.es, Ramon.Esteban@uv.es, Vicent.Perez-Calabuig@uv.es; ORCID 0000-0002-2051-9075, 0000-0002-2321-8139, 0000-0003-4101-8656

†Departamento de Matemáticas, Universidad de Zaragoza, Pedro Cerbuna, 12, 50009 Zaragoza, Spain; paz@unizar.es; ORCID 0000-0003-4809-1784

In the sequel, the word *brace* refers to a skew left brace.

Given a brace B, there is an action of the multiplicative group on the additive group by means of the so-called *lambda map*:

$$\lambda\colon a \in (B,\cdot) \longmapsto \lambda_a \in \operatorname{Aut}(B,+), \quad \lambda_a(b) = -a + ab, \text{ for all } a, b \in B.$$

Braces can be described in terms of regular subgroups of the holomorph of the additive group. Recall that the holomorph of a group G is the semidirect product $\operatorname{Hol}(G) = [G] \operatorname{Aut}(G)$. Let B be a brace and set $K = (B,+)$. Then $H = \{(a, \lambda_a) \mid a \in B\}$ is a regular subgroup of the holomorph $\operatorname{Hol}(K)$ isomorphic to $(B,\cdot)$ (see [9, Theorem 4.2]). If we consider the subgroup $S = KH \leq \operatorname{Hol}(K)$, then

$$S = KH = KE = HE,$$

where $E = \{(0, \lambda_b) \mid b \in B\}$ and $\mathrm{C}_E(K) = K \cap E = H \cap E = 1$. We call $\mathsf{S}(B) = (S, K, H, E)$ the *small trifactorised group* associated with B.

In [11], Tsang showed it is possible to construct finite braces by just looking at the automorphism group of the additive group instead of looking at the whole holomorph. This is a significant improvement both from an algebraic and computational approach.

Theorem 1 (see [11, Corollary 2.2]). *If the finite group G is the multiplicative group of a brace with additive group K, then there exist two subgroups X and Y of $\operatorname{Aut}(K)$ that are quotients of G satisfying*

$$XY = X\operatorname{Inn}(K) = Y\operatorname{Inn}(K).$$

She looks for a sort of converse of the above theorem in the case of finite braces with an additive group of trivial centre, and proved the following:

Theorem 2 (see [11, Proposition 2.7]). *Suppose that the centre of a finite group $(K,+)$ is trivial and let P be a subgroup of $\operatorname{Aut}(K)$ containing $\operatorname{Inn}(K)$. If $P = XY$ is a factorisation by two subgroups X and Y such that $X \cap Y = 1$, $X\operatorname{Inn}(K) = Y\operatorname{Inn}(K) = P$ and X splits over $X \cap \operatorname{Inn}(K)$, then there exists a brace B whose additive group is isomorphic to $(K,+)$ and whose multiplicative group is isomorphic to a semidirect product $[X \cap \operatorname{Inn}(K)]Y$ for a suitable choice of the action $\alpha\colon Y \longrightarrow \operatorname{Aut}(X \cap \operatorname{Inn}(K))$.*

The above two theorems are the key to prove the main results of [11,12].

In [13], Tsang posed the following question:

Question 3. Is it possible to extend Theorem 2 by dropping the assumption that X splits over $X \cap \operatorname{Inn}(K)$?

The aim of this paper is to give a complete characterisation of the multiplicative groups of a brace with additive group of trivial centre. As a consequence, we present an improved version of Theorem 2 (on which the main result of [11] heavily depends), and we give an affirmative answer to Question 3.

Theorem A. *Let K be a finite group with trivial centre. For every brace B with additive group $K = (B, +)$ and multiplicative group $C = (B, \cdot)$, there exist subgroups X and Y of $\mathrm{Aut}(K)$ satisfying the following properties:*

(a) $XY = X\mathrm{Inn}(K) = Y\mathrm{Inn}(K)$,

(b) there are two subgroups N and M of $\mathrm{Inn}(K)$ such that $N \trianglelefteq X$ and $M \trianglelefteq Y$,

(c) there exists an isomorphism $\gamma\colon Y/M \longrightarrow X/N$ such that

$$\mathrm{Inn}(K) = \{xy^{-1} \mid x \in X,\, y \in Y,\, \gamma(yM) = xN\},$$

(d) $|K| = |X||M| = |Y||N|$.

In this case,

(e) C has two normal subgroups T and V with $T \cap V = 1$, $X \cong C/T$ and $Y \cong C/V$, that is, C is a subdirect product of X and Y.

Conversely, for every pair X, Y of subgroups of $\mathrm{Aut}(K)$ satisfying conditions (a)–(d), there exists a brace B with $K = (B, +)$ and $C = (B, \cdot)$ satisfying (e).

Corollary 4. *Let K be a finite group with trivial centre. Suppose that there exist subgroups X, Y of $\mathrm{Aut}(K)$ such that $X \cap Y = 1$ and $XY = X\mathrm{Inn}(K) = Y\mathrm{Inn}(K)$. Then there exists a brace with additive group K and a multiplicative group that is isomorphic to a subdirect product of X and Y.*

Proof. Assume that $X \cap Y = 1$. Consider $N = X \cap \mathrm{Inn}(K)$, $M = Y \cap \mathrm{Inn}(K)$. Then $|X||M| = |K|$ as $|X||Y| = |\mathrm{Inn}(K)||Y|/|Y \cap \mathrm{Inn}(K)|$. Analogously, $|Y||N| = |K|$. Moreover, since

$$Y/M \cong Y\mathrm{Inn}(K)/\mathrm{Inn}(K) = X\mathrm{Inn}(K)/\mathrm{Inn}(K) \cong X/N,$$

we have an isomorphism $\gamma\colon Y/M \longrightarrow X/N$ given by $\gamma(bM) = aN$, where $b \in Y$, $a \in X$ such that $ab^{-1} \in \mathrm{Inn}(K)$. Since $X \cap Y = 1$, for each $k \in K$, conjugation by k can be expressed as ab^{-1}, for a unique $a \in X$ and $b \in Y$. Then, the groups X and Y satisfy Statements (a)–(d) of Theorem A, and therefore, there exists a brace whose additive group is K and whose multiplicative group is isomorphic to a subdirect product of X and Y. $\square$

https://doi.org/10.4153/S0008439525000098 Published online by Cambridge University Press

Corollary 4 also allows to give a considerably shorter proof of the main results of [11, 12] about the almost simple groups K that can appear as additive groups of braces with soluble multiplicative group. By Corollary 4, it is enough to find two subgroups X and Y of $\mathrm{Aut}(K)$ such that $X \cap Y = 1$ and $XY = X\mathrm{Inn}(K) = Y\mathrm{Inn}(K)$. Therefore, Codes 2, 3, and 4 in the proof of [11, Theorem 1.3] can be avoided, as well as checking in every case that the subgroup X splits over $X \cap \mathrm{Inn}(K)$.

In Section 3 we present a worked example of a construction of a brace with additive group $K = \mathrm{PSL}_2(25)$ by means of subgroups X and Y of $\mathrm{Aut}(K)$ satisfying all conditions of Theorem A but $X \cap Y \neq 1$.

2 Proof of Theorem A

Proof of Theorem A. Suppose that B is a brace with additive group K and lambda map λ. Let $H = \{(b, \lambda_b) \mid b \in B\}$ be the regular subgroup of $\mathrm{Hol}(K)$ appearing in the small trifactorised group $\mathsf{S}(B) = (S, K, H, E)$ associated with B. Recall that H is isomorphic to the multiplicative group $(C, \cdot)$ of B, $E = \{(0, \lambda_b) \mid b \in B\} \leq \mathrm{Hol}(K)$, and $S = KH = KE = HE$ with $K \cap E = H \cap E = 1$.

Observe that S acts on K by means of the homomorphism $\pi\colon (b, \omega) \in S \mapsto \omega \in \mathrm{Aut}(K)$. On the other hand, S also acts on K by conjugation. In fact, this action naturally induces a homomorphism $\alpha\colon S \to \mathrm{Aut}(K)$. In particular, for every $b \in B$ and every $k \in K$, $(0, \lambda_b)(k, 1)(0, \lambda_b)^{-1} = (\lambda_b(k), 1)$, that is, $\alpha(0, \lambda_b) = \lambda_b = \pi(0, \lambda_b)$. Thus, $\alpha(E) = \pi(E) = \pi(H)$.

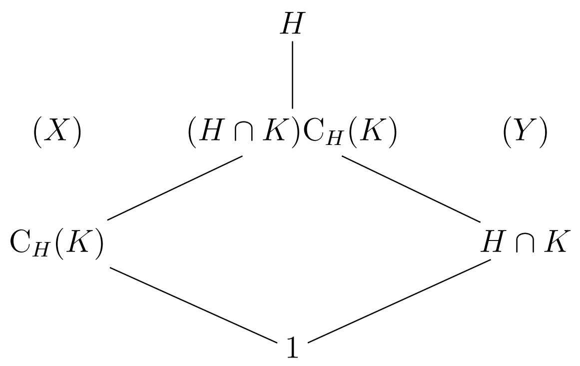

Figure 1: Structure of the multiplicative group in Theorem A

The restrictions of π and α to H induce two actions of H on K, with respective kernels $\mathrm{Ker}\,\pi|_H = K \cap H \trianglelefteq H$ and $\mathrm{Ker}\,\alpha|_H = \mathrm{C}_H(K) \trianglelefteq H$.

https://doi.org/10.4153/S0008439525000098 Published online by Cambridge University Press

Moreover, it holds that

$$\begin{aligned}\operatorname{Ker}\pi|_H \cap \operatorname{Ker}\alpha|_H &= K \cap H \cap \mathrm{C}_H(K) = K \cap H \cap \mathrm{C}_S(K) \\ &= H \cap \mathrm{C}_K(K) = H \cap \mathrm{Z}(K) = 1 \quad \text{(see Figure 1)}.\end{aligned}$$

Let $X := \alpha(H)$ and $Y := \pi(H) = \alpha(E) = \{\lambda_b \mid b \in B\}$ such that $X \cong H/\mathrm{C}_H(K)$ and $Y \cong H/(K \cap H)$. Since $\alpha(K) = \mathrm{Inn}(K)$, we have that

$$\begin{aligned}\alpha(S) &= \alpha(HE) = \alpha(KH) = \alpha(KE) \\ &= \alpha(H)\alpha(E) = \alpha(K)\alpha(H) = \alpha(K)\alpha(E) \\ &= XY = (\mathrm{Inn}(K))X = (\mathrm{Inn}(K))Y.\end{aligned}$$

Take $R := (H \cap K)\mathrm{C}_H(K) \trianglelefteq H$. Then, $N := \alpha(R) \trianglelefteq \alpha(H) = X$ and $M := \pi(R) \trianglelefteq \pi(H) = Y$. It follows that $N = \alpha(H \cap K) \leq \alpha(K) = \mathrm{Inn}(K)$. On the other hand, $M = \pi(\mathrm{C}_H(K))$ and if $(b, \lambda_b) \in \mathrm{C}_H(K)$, then for every $k \in K$,

$$(b, \lambda_b)(k, 1)(b, \lambda_b)^{-1} = (b + \lambda_b(k) - b, 1) = (k, 1),$$

that is, λ_b coincides with the inner automorphism of K induced by $-b$. Thus, $M \leq \mathrm{Inn}(K)$. Moreover, we see that

$$\begin{aligned}Y/M &\cong (H/\operatorname{Ker}\pi|_H)/(R/\operatorname{Ker}\pi|_H) \cong H/R \\ &\cong (H/\operatorname{Ker}\alpha|_H)/(R/\operatorname{Ker}\alpha|_H) \cong X/N;\end{aligned}$$

here the isomorphism $\gamma\colon Y/M \longrightarrow X/N$ is given by $\gamma(\lambda_b M) = \alpha_b\lambda_b N$, where α_b is the inner automorphism of K induced by b. Given $a \in \gamma(\lambda_b M)$, we have that $a\lambda_b^{-1} \in \alpha_b N \subseteq \mathrm{Inn}(K)$. Furthermore, given $x \in \mathrm{Inn}(K)$, we have that $x = \alpha_b$ for some $b \in B$ and so $\gamma(\lambda_b M) = \alpha_b\lambda_b N = x\lambda_b N$ with $(\alpha_b\lambda_b)\lambda_b^{-1} = x$.

Since $\operatorname{Ker}\pi|_H \cap \operatorname{Ker}\alpha|_H = (H \cap K) \cap \mathrm{C}_H(K) = 1$, we have that $|R| = |H \cap K||\mathrm{C}_H(K)|$ and $|M| = |R/(H \cap K)| = |\mathrm{C}_H(K)|$, $|N| = |R/\mathrm{C}_H(K)| = |H \cap K|$. As $|X| = |K|/|\mathrm{C}_H(K)|$ and $|Y| = |K|/|H \cap K|$, the claim about the order follows.

Item (e) follows by the fact that H is isomorphic to the multiplicative group $(C, \cdot)$ of B, so that T and V are respectively isomorphic to $\operatorname{Ker}\alpha|_H$ and $\operatorname{Ker}\pi|_H$.

Now, suppose that $\mathrm{Aut}(K)$ possesses subgroups X and Y satisfying conditions (a)–(d). Let

$$W = \{(x, y) \mid x \in X,\, y \in Y,\, \gamma(yM) = xN\}$$

be a subdirect product of X and Y with amalgamated factor group $Y/M \cong X/N$ (see [7, Chapter A, Definition 19.2]). By [7, Chapter A, Proposition 19.1], and the hypothesis, we have that $|W| = |K|$. Since $\mathrm{Z}(K)$ is trivial,

https://doi.org/10.4153/S0008439525000098 Published online by Cambridge University Press

the map $\zeta\colon K \longrightarrow \mathrm{Inn}(K)$, where $\zeta(k)$ is the inner automorphism of K induced by k, is an isomorphism. By hypothesis, the map $W \longrightarrow \mathrm{Inn}(K)$ given by $(x,y) \longmapsto xy^{-1}$ is surjective. Since $|W| = |\mathrm{Inn}(K)| = |K|$, it is a bijection. We can consider $H = \{(b,y) \mid (x,y) \in W,\, \zeta(b) = xy^{-1}\} \subseteq \mathrm{Hol}(K)$. Given (b,y), $(b_1,y_1) \in H$, we have that $(b,y)(b_1,y_1) = (b + y(b_1), yy_1)$, $\zeta(b) = xy^{-1}$, and $\zeta(b_1) = x_1y_1^{-1}$ with (x,y), $(x_1,y_1) \in B$. Then

$$\zeta(b+y(b_1)) = \zeta(b)\zeta(y(b_1)) = \zeta(b)y\zeta(b_1)y^{-1} = xy^{-1}yx_1y_1^{-1}y^{-1} = (xx_1)(yy_1)^{-1}$$

with $(xx_1, yy_1) = (x,y)(x_1,y_1) \in W$. Furthermore, if $(b,y) \in H$, with $\zeta(b) = xy^{-1}$, we have that $(b,y)^{-1} = (y^{-1}(-b), y^{-1})$ and

$$\zeta(y^{-1}(-b)) = y^{-1}\zeta(-b)y = y^{-1}\zeta(b)^{-1}y = y^{-1}yx^{-1}y = x^{-1}(y^{-1})^{-1}$$

with $(x^{-1}, y^{-1}) = (x,y)^{-1} \in W$. We conclude that H is a subgroup of $\mathrm{Hol}(K)$. As the projection onto its first component is surjective, it turns out that it H is a regular subgroup of $\mathrm{Hol}(K)$ by [2, Proposition 2.5] and so it is isomorphic to the multiplicative group of a brace with additive group K (see [9, Theorem 4.2]).

We finish the proof by showing that the map $\phi\colon H \to W$ given by $(b,y) \longmapsto (\zeta(b)y, y)$, where $\zeta(b) = xy^{-1}$ and $(x,y) \in W$, is an isomorphism. Indeed, if $\zeta(b) = xy^{-1}$, $\zeta(b_1) = x_1y_1^{-1}$, where (x,y), $(x_1,y_1) \in W$, we have that

$$\begin{aligned}
\phi(b,y)\phi(b_1,y_1) &= (\zeta(b)y, y)(\zeta(b_1)y_1, y_1) = (x,y)(x_1,y_1) = (xx_1, yy_1),\\
\phi((b,y)(b_1,y_1)) &= \phi(b + y(b_1), yy_1) = (\zeta(b + y(b_1))yy_1, yy_1)\\
&= (\zeta(b)y\zeta(b_1)y^{-1}yy_1, yy_1) = (xy^{-1}yx_1y_1^{-1}y_1, yy_1)\\
&= (xx_1, yy_1).
\end{aligned}$$

We conclude that ϕ is a group homomorphism. Assume that $\phi(b,y) = (\zeta(b)y, y) = (1,1)$, with $\zeta(b) = xy^{-1}$ and $(x,y) \in W$, then $y = 1$ and so $\zeta(b) = x = 1$, which implies that $b = 0$. Consequently, ϕ is injective. As W and H are finite and have the same order, we obtain that ϕ is an isomorphism. Since C is isomorphic to H we have just proved that (e) holds for C. □

3 A worked example

In general, we do not have that $X \cap Y = 1$. Let us consider $K = \mathrm{PSL}_2(25)$. Its automorphism group $A = \mathrm{Aut}(K)$ is generated by $\mathrm{Inn}(K)$, the diagonal

https://doi.org/10.4153/S0008439525000098 Published online by Cambridge University Press

automorphism d induced by the conjugation by the matrix

$$\mathsf{D} = \begin{bmatrix} \zeta & 0 \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}_2(25),$$

where ζ is a primitive 24th-root of unity of GF(25), and the field automorphism f. The group A possesses a subgroup X generated by the inner automorphisms c_1, c_2, and c_3 induced by the matrices

$$\mathsf{C}_1 = \begin{bmatrix} \zeta^4 & 0 \\ 0 & \zeta^{20} \end{bmatrix}, \qquad \mathsf{C}_2 = \begin{bmatrix} 1 & 0 \\ \zeta & 1 \end{bmatrix}, \qquad \mathsf{C}_3 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},$$

respectively, and df. We have that c_1 has order 3, $\langle c_2, c_3\rangle$ is an elementary abelian group of order 25, c_1 normalises $\langle c_2, c_3\rangle$, $(df)c_1(df)^{-1} = c_1^{-1}$, df has order 8, and df normalises $\langle c_2, c_3\rangle$. Then the group $\langle df, c_1, c_2, c_3\rangle$ has order 600.

Let u_1 and u_2 be the inner automorphisms induced by the conjugation by

$$\mathsf{U}_1 = \begin{bmatrix} \zeta^3 & \zeta^{16} \\ \zeta^{13} & \zeta^{11} \end{bmatrix}, \qquad \mathsf{U}_2 = \begin{bmatrix} \zeta^5 & \zeta^5 \\ \zeta^9 & \zeta^{22} \end{bmatrix}.$$

Let $Y = \langle u_1, dfu_2\rangle$. We have that u_1 has order 13. Let

$$\mathsf{R} = \begin{bmatrix} \zeta & 0 \\ 0 & \zeta \end{bmatrix} \in \mathrm{Z}(\mathrm{GL}_2(25)), \qquad \mathsf{T} = \begin{bmatrix} 3 & 0 \\ 4 & 2 \end{bmatrix}$$

and let t be the automorphism induced by conjugation by T. Then $(dfu_2)^2 = dfu_2dfu_2 = d^fu_2d^5u_2$ is the automorphism induced by conjugation by

$$\mathsf{D}\mathsf{U}_2^{(5)}\mathsf{D}^5\mathsf{U}_2 = \mathsf{R}^{15}\mathsf{T}, \tag{1}$$

where $\mathsf{U}_2^{(5)}$ denotes the matrix whose entries are obtained from the entries of U_2 by applying the Frobenius field automorphism, that is, $(dfu_2)^2 = t$. As $(\mathsf{R}^{15}\mathsf{T})^2 = \mathsf{R}^3$, we conclude that dfu_2 has order 4. We can also check that $(dfu_2)u_1(dfu_2)^{-1} = u_1^8$. It follows that Y has order 52.

By [6], X and Y are maximal subgroups of the almost simple group $\mathrm{Inn}(K)\langle df\rangle$. Observe that $(df)^4c_3^2 = (dfdf)^2c_3^2 = (dd^5)^2c_3^2 = d^{12}c_3^2$ is induced by $\mathsf{D}^{12}\mathsf{C}_3^2 = \mathsf{R}^{18}\mathsf{T}$, consequently, $(df)^4c_3^2 = t$. This, together with Equation (1), shows that $t \in X \cap Y$. We note that $\mathrm{Inn}(K)X = \mathrm{Inn}(K)Y = \mathrm{Inn}(K)\langle df\rangle$. Moreover, $|X \cap Y|$ divides $\gcd(|X|, |Y|) = 4$. If $|X \cap Y| = 4$, then $X \cap Y$ is contained in $X \cap \mathrm{Inn}(K)$, but it is not contained in $Y \cap \mathrm{Inn}(K)$. This shows that $|X \cap Y| \leq 2$. Hence $|X \cap Y| = 2$. As $XY \subseteq \mathrm{Inn}(K)\langle df\rangle$,

$$15\,600 = |\mathrm{Inn}(K)\langle df\rangle| \geq |XY| = \frac{|X||Y|}{|X \cap Y|} = 15\,600 \cdot \frac{2}{|X \cap Y|} = 15\,600,$$

and so $XY = \mathrm{Inn}(K)\langle df\rangle$.

Let $N = \langle c_1, c_2, c_3, (df)^2\rangle \trianglelefteq X$, $M = \langle u_1\rangle \trianglelefteq Y$. Then $|N| = 150$, $|M| = 13$, $N \leq X \cap \mathrm{Inn}(K)$, $M \leq Y \cap \mathrm{Inn}(K)$, $Y/M \cong X/N \cong C_4$, and $|K| = |X||M| = |Y||N|$. The isomorphism between Y/M and X/N is given by $\gamma((dfu_2)^r M) = (df)^r N$ for $0 \leq r < 4$, and, since $d^6 \in \mathrm{Inn}(K)$, it is clear that

$$
\begin{aligned}
(df)(dfu_2)^{-1} &= c_0 u_0^{-1} \in \mathrm{Inn}(K),\\
(df)^2(dfu_2)^{-2} &= d^6 t^{-1} \in \mathrm{Inn}(K),\\
(df)^3(dfu_2)^{-3} &= (df)(d^6 t^{-1} u_2^{-1})(df)^{-1} \in \mathrm{Inn}(K).
\end{aligned}
$$

Let $z \in XY \cap \mathrm{Inn}(K)$. Recall that $X \cap Y = \langle t\rangle$. Then there exist $x \in X$, $y \in Y$ with $z = xy^{-1} = (xt)(yt)^{-1}$. We observe that $t = (df)^4 c_3^2 \in N$, but $t \notin M$ by order considerations. Given $x \in X$, $y \in Y$, there exist r, $s \in \{0, 1, 2, 3\}$ such that $xN = (df)^r N$ and $yM = (dfc_3)^s M$. We also observe that $x \in \mathrm{Inn}(K)$ if, and only if, $y \in \mathrm{Inn}(K)$. To prove that we can choose $x \in X$, $y \in Y$ such that $z = xy^{-1}$ and $\gamma(yM) = xN$, it is enough to prove that for such a choice we have that $z = xy^{-1}$ and $r = s$. Note that if $x \in N$, then $r = 0$; if $x \in \mathrm{Inn}(K) \setminus N$, then $r = 2$; and if $x \notin \mathrm{Inn}(K)$, then $r \in \{1, 3\}$. Analogously, if $y \in M$, then $s = 0$; if $y \in \mathrm{Inn}(K) \setminus M$, then $s = 2$; and if $y \notin \mathrm{Inn}(K)$, then $s \in \{1, 3\}$. We also have that $tM = (dfu_2)^2 M$ and that $tN = N$, as $t \in \mathrm{Inn}(K)$, $t \in N$, but $t \notin M$. If $x \in N$ and $y \in M$, we can choose $r = s = 0$ and $\gamma(yM) = xN$. Suppose that $x \in N$ and $y \notin M$. Then $y \in \mathrm{Inn}(K)$ and so, $xN = N$ and $yM = (dfu_2)^2 M$. Consequently, $xtN = N$, $ytN = N$, and $\gamma(ytN) = xtN$. Suppose that $x \notin N$ and $y \in M$. We have that $x \in \mathrm{Inn}(K)$ and so, $xN = (df)^2 N$ and $yM = M$. It follows that $xtN = (df)^2 N$ and $ytM = (dfu_2)^2 M$, that is, $\gamma(ytM) = xtN$. Suppose that x, $y \in \mathrm{Inn}(K)$, $x \notin N$, and $y \notin M$. Then $xN = (df)^2 N$, $yM = (dfu_2)^2 M$, and $\gamma(yM) = xN$. Finally, suppose that x and $y \notin M$. Then $xN = (df)^r N$ and $yM = (dfu_2)^s M$, with r, $s \in \{1, 3\}$. If $r = s$, then $\gamma(yM) = xN$. If $r \neq s$, then $xtN = (df)^r N$ and $ytM = (dfu_2)^{s+2} M$, with $r \equiv s + 2 \pmod 4$. Thus $\gamma(ytM) = xtN$.

It follows that X, Y satisfy all conditions of Theorem A. We can also check with GAP [8] all this information about these subgroups.

Aknowledgements

We would like to thank the referee for his thoughtful comments toward improving our article.

https://doi.org/10.4153/S0008439525000098 Published online by Cambridge University Press

References

[1] A. Ballester-Bolinches and R. Esteban-Romero. Triply factorised groups and the structure of skew left braces. *Commun. Math. Stat.*, 10:353–370, 2022.

[2] A. Ballester-Bolinches, R. Esteban-Romero, and V. Pérez-Calabuig. Enumeration of left braces with additive group $C_4 \times C_4 \times C_4$. *Math. Comp.*, 93(346):911–919, March 2024.

[3] V. G. Bardakov, M. V. Neshchadim, and M. K. Yadav. Computing skew left braces of small orders. *Int. J. Algebra Comput.*, 30(4):839–851, 2020.

[4] A. Caranti, and L. Stefanello. From endomorphisms to bi-skew braces, regular subgroups, the Yang-Baxter equation, and Hopf-Galois structures. *J. Algebra*, 587:462–487, 2021.

[5] L. N. Childs. Skew braces and the Galois correspondence for Hopf Galois structures. *J. Algebra*, 511:270–291, 2018.

[6] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of Finite Groups.* Oxford Univ. Press, London, 1985.

[7] K. Doerk and T. Hawkes. *Finite soluble groups*, volume 4 of *De Gruyter Expositions in Mathematics.* Walter de Gruyter & Co., Berlin, 1992.

[8] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.14.0*, 2024. `http://www.gap-system.org`.

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

[10] W. Rump. Braces, radical rings, and the quantum Yang-Baxter equation. *J. Algebra*, 307:153–170, 2007.

[11] C. (S. Y.) Tsang. Non-abelian simple groups which occur as the type of a Hopf-Galois structure on a solvable extension. *Bull. London Math. Soc.*, 55(5):2324–2340, 2023.

[12] C. (S. Y.) Tsang. Finite almost simple groups whose holomorph contains a solvable regular subgroup. *Adv. Group Theory Appl.*, in press.

[13] C. (S. Y.) Tsang. Factorizations of groups and skew braces. In *Ischia Group Theory 2024 Conference*, Ischia, Italy, April 12th 2024.

https://doi.org/10.4153/S0008439525000098 Published online by Cambridge University Press