ON BI-SKEW BRACES AND BRACE BLOCKS

L. STEFANELLO AND S. TRAPPENIERS

ABSTRACT. L. N. Childs defined a bi-skew brace to be a skew brace such that if we swap the role of the two operations, then we find again a skew brace.

In this paper, we give a systematic analysis of bi-skew braces. We study nilpotency and solubility, and connections between bi-skew braces and set-theoretic solutions of the Yang–Baxter equation. Further, we deal with Byott's conjecture in the case of bi-skew braces, and we use bi-skew braces as a tool to solve a classification problem proposed by L. Vendramin.

In the final part, we investigate brace blocks, defined by A. Koch to be families of group operations on a given set such that any two of them yield a bi-skew brace. We provide a characterisation of brace blocks, illustrate how all known constructions in literature follow in a natural way from our characterisation, and give several new examples.

1. INTRODUCTION

After the definition of skew braces in [GV17], built on the pioneering work of [Rum07a], a considerable part of literature has been devoted to the study of the main properties of these objects and their relations with other topics, such as Jacobson radical rings, regular subgroups of the holomorph, the Yang–Baxter equation, and Hopf–Galois structures [Bac18, Ced18, SV18, BCJO19]. In particular, these relations motivated even more the study of the involved topics, and allowed various problems to be translated in different settings. For example, one deep problem regarding the properties of the underlying groups of a skew brace was initially formulated by N. P. Byott as a statement on regular subgroups of the holomorph of a soluble group [Byo15], and it is now known as Byott's conjecture.

In [Chi19], L. N. Childs defined a bi-skew brace to be a skew brace $(A, \cdot, \circ)$ such that also $(A, \circ, \cdot)$ is a skew brace. His main focus was the relation with Hopf–Galois theory; a bi-skew brace $(A, \cdot, \circ)$ with A finite provides not only a Hopf–Galois structure of type $(A, \cdot)$ on every Galois extension with Galois group $(A, \circ)$, but also a Hopf–Galois structure of type $(A, \circ)$ on every Galois extension with Galois group $(A, \cdot)$; see [Chi00] for a general treatment of Hopf–Galois theory, and the appendix of [SV18], [CGK$^+$21, Chapter 2], and [ST22] for the relation between skew braces and Hopf–Galois structures.

A. Caranti studied different characterisations of bi-skew braces and gave various constructions in [Car20]. These characterisations were formulated both using gamma functions and from the point of view of regular subgroups of the holomorph.

Bi-skew braces were further studied by A. Koch in [Koc21], where a construction for bi-skew braces is given starting from group endomorphisms with abelian image. An iterative version of this construction was then obtained in [Koc22], where also the notion of a brace block is given. This is a family of group operations on a fixed set such that any two operations form a skew brace. In particular, every bi-skew brace yields a brace block with two operations. The constructions by Koch and a construction of Caranti [Car18] were subsequently generalised by Caranti and the first author in [CS21, CS22]. In the recent manuscript [BNY22b], an iterative construction is given to obtain a brace block from a given bi-skew brace satisfying a certain property. A common factor in these works is the study of the questions, "How can we better understand bi-skew braces or brace blocks? What are new, effective ways to construct them?" The same idea lives on throughout this paper. In particular, a better understanding of bi-skew braces and brace blocks leads to new ways of constructing them and explains known constructions and their conditions in a natural way.

The paper is organised as follows.

In section 2 we recall the preliminaries that are used throughout the paper.

In section 3 we state several structural results of bi-skew braces. We relate structural properties of a bi-skew brace to those of its associated skew brace with swapped operations and also to properties of a suitable group associated with the skew brace. Moreover, we give an affirmative answer to Byott's conjecture in the case of bi-skew braces, employing an approach that also works for several other classes of skew braces. At last, we state a characterisation of a recently defined class of skew braces [BNY22a], called γ-homomorphic skew braces, which bears a strong resemblance to a characterisation of bi-skew braces by Caranti. This resemblance is further emphasised when we discuss two slightly different constructions. One yields a new construction of γ-homomorphic skew braces and the other is a new way to obtain examples of bi-skew braces described by Childs.

Section 4 contains two classification results. We first prove an upper bound on the right nilpotency class of braces with multiplicative group isomorphic to $\mathbb{Z}^n$. In particular, we recover the known result that such a brace is trivial if $n = 1$ and the new result that it is a bi-skew brace if $n = 2$. Secondly, we use bi-skew braces to prove an open problem posed by L. Vendramin concerning the classification of skew braces with a multiplicative group isomorphic to $\mathbb{Z}$.

Section 5 starts with a short summary concerning the connection between skew braces and set-theoretic solutions of the Yang–Baxter equation. We then give new results which show that the property of being a bi-skew brace can still be recognised when we look at the associated set-theoretic solution of the Yang–Baxter equation. On the other hand, we show with a counterexample that the associated solutions to both skew brace structures of a bi-skew brace can not be related in a direct way. We also study when the structure group of a solution is a bi-skew brace.

In section 6 we investigate brace blocks. We start with a general characterisation of brace blocks on a given group. It is only when we add an extra condition that we obtain a more manageable characterisation from which we can construct new brace blocks. Nonetheless, we illustrate that this more restrictive characterisation still covers all known constructions of brace blocks in literature. This also allows to work with abelian groups, a case where most known constructions only yield trivial

examples. We further give two new concrete constructions of brace blocks using rings and semidirect products.

2. Preliminaries

We begin with the definition of a skew left brace.

Definition 2.1. A *skew left brace* $A = (A, \cdot, \circ)$ is a set A together with group structures $(A, \cdot)$ and $(A, \circ)$ such that for all $a, b, c \in A$,

$$a \circ (b \cdot c) = (a \circ b) \cdot a^{-1} \cdot (a \circ c).$$

Here a^{-1} denotes the inverse of a in $(A, \cdot)$.

Remark 2.2. From this definition it is already clear that in this work sets might be endowed with more than one group structure. When there is possible confusion, we specify the group structure when well-known notations concerning groups are used. For example, the centre of $(A, \cdot)$ is denoted by $Z(A, \cdot)$, and the automorphism group of $(A, \circ)$ is denoted by $\text{Aut}(A, \circ)$.

In a natural way, also *right* and *two-sided skew braces* can be defined. However, for simplicity, we talk about *skew braces* when actually meaning skew left braces. A skew brace $(A, \cdot, \circ)$ is called a *brace* if $(A, \cdot)$ is an abelian group. Given a skew brace $(A, \cdot, \circ)$, we call $(A, \cdot)$ the *additive group*; this somewhat ambiguous notation follows from the fact that for braces this group was originally denoted by $(A, +)$ and this notation is still common for skew braces. The group $(A, \circ)$ is called the *multiplicative group*. By $\overline{a}$ we denote the inverse of an element $a \in A$ with respect to the multiplicative group. For $n \in \mathbb{Z}$ and $a \in A$, we use a^n for the n-th power of a in $(A, \cdot)$ and $a^{\circ n}$ for the n-th power in $(A, \circ)$. It is easily proved that the neutral elements of the additive and multiplicative group coincide; this common neutral element is denoted by 1. Given two skew braces A and B, a map $f \colon A \to B$ is a *homomorphism of skew braces* if both $f(a \cdot b) = f(a) \cdot f(b)$ and $f(a \circ b) = f(a) \circ f(b)$ hold for all $a, b \in A$. *Isomorphisms* and *automorphisms* are defined accordingly, and the group of automorphisms of a skew brace $(A, \cdot, \circ)$ is denoted by $\text{Aut}(A, \cdot, \circ)$.

One way to construct skew braces is to start from any group $(G, \circ)$ and define $a \cdot b = a \circ b$ for all $a, b \in G$. This is called the *trivial skew brace* on $(G, \circ)$, for which we use the notation $\text{Triv}(G, \circ)$. If we instead define $a \cdot b = b \circ a$, then we obtain the *almost trivial skew brace* on $(G, \circ)$, denoted by $\text{opTriv}(G, \circ)$. When the group operation on G is clear, also $\text{Triv}(G)$ and $\text{opTriv}(G)$ are used.

With each element a of a skew brace $(A, \cdot, \circ)$ we associate the bijective map

$$\gamma(a) \colon A \to A, \quad b \mapsto {}^{\gamma(a)}b = a^{-1} \cdot (a \circ b),$$

which we write as a left exponent. Note that this map is also denoted by λ_a in literature. By [GV17, Proposition 1.9], this gives a well-defined group homomorphism $\gamma \colon (A, \circ) \to \text{Aut}(A, \cdot)$. Note that $(A, \circ)$ is fully determined by $(A, \cdot)$ and the function γ, as

$$(2.1) \qquad\qquad a \circ b = a \cdot {}^{\gamma(a)}b.$$

It follows that any group $(A, \cdot)$ and map $\gamma \colon A \to \text{Aut}(A, \cdot)$ such that for all $a, b \in A$,

$$(2.2) \qquad\qquad \gamma(a \cdot {}^{\gamma(a)}b) = \gamma(a)\gamma(b),$$

determine a skew brace $(A, \cdot, \circ)$, where $(A, \circ)$ is given by (2.1). Any map γ satisfying (2.2) is called a *gamma function* on $(A, \cdot)$.

Definition 2.3. Let A be a skew brace.

    (1) A *left ideal* of A is a subgroup I of $(A, \cdot)$ such that $\gamma^{(a)}I \subseteq I$ for all $a \in A$.

    (2) An *ideal* of A is a left ideal I which is moreover normal in $(A, \cdot)$ and $(A, \circ)$.

From (2.1) we immediately see that (left) ideals of a skew brace A are also subgroups of $(A, \circ)$, so in particular they are subskew braces of A. Ideals are precisely the appropriate substructures needed to define the quotient of a skew brace by this substructure. Indeed, given an ideal I of A, we have $a \cdot I = I \cdot a = a \circ I = I \circ a$ for all $a \in A$. We can thus construct the *quotient skew brace* A/I in the natural way. An example of an ideal is the *socle* of a skew brace A, defined as $\mathrm{Soc}(A) = \ker(\gamma) \cap Z(A, \cdot)$. Another example is given by the kernel of any skew brace homomorphism.

For $a, b \in A$, we define $a * b = \gamma^{(a)}b \cdot b^{-1} = a^{-1} \cdot (a \circ b) \cdot b^{-1}$. One way to think about this new operation is as a commutator which measures how close $\gamma^{(a)}b$ is to b. Equivalently, $a * b$ can be seen as a measure in difference between $a \cdot b$ and $a \circ b$. Indeed, it is clear that these coincide if and only if $a * b = 1$. Yet another way to see this operation becomes apparent when we look at the correspondence between two-sided braces and Jacobson radical rings, where $*$ yields precisely the ring operation of the associated Jacobson radical ring [Rum07a]. For subsets $X, Y \subseteq A$ we define $X * Y$ as the subgroup of $(A, \cdot)$ generated by

$$\{x * y \mid x \in X \text{ and } y \in Y\}.$$

Taking $X = Y = A$ we obtain $A^2 = A * A$, which is an ideal of A with the property that A/A^2 is a trivial skew brace.

We can associate with every skew brace $(A, \cdot, \circ)$ its *opposite skew brace* $A_{\mathrm{op}} = (A, \cdot_{\mathrm{op}}, \circ)$ where $a \cdot_{\mathrm{op}} b = b \cdot a$. This construction was first considered by A. Koch and P. J. Truman [KT20]. It is now clear where the notation of the almost trivial skew brace on a given group $(A, \circ)$ comes from, as $\mathrm{opTriv}(A, \circ) = \mathrm{Triv}(A, \circ)_{\mathrm{op}}$. In general, we use "op" to denote that we consider a known construction in the opposite skew brace. For example, γ_{op}, respectively $*_{\mathrm{op}}$, is the gamma function, respectively $*$-operation, associated with A_{op}. Concretely, for all $a, b \in A$,

$$\gamma_{\mathrm{op}}(a)b = (a \circ b) \cdot a^{-1},$$

$$a *_{\mathrm{op}} b = \gamma_{\mathrm{op}}(a)b \cdot_{\mathrm{op}} b^{-1} = b^{-1} \cdot (a \circ b) \cdot a^{-1}.$$

Note that $A = A_{\mathrm{op}}$ if and only if A is a brace. It is still possible that $A \cong A_{\mathrm{op}}$ when $A \neq A_{\mathrm{op}}$, although this is generally not the case. The internal structures of A and A_{op} are strongly related however, as the following result, whose proof is immediate, shows.

Proposition 2.4. *Let A be a skew brace. Then the ideals of A and A_{op} coincide.*

As a concrete application of Proposition 2.4 we observe that $A_{\mathrm{op}}^2 = A *_{\mathrm{op}} A$ is an ideal of A.

Definition 2.5. A skew brace $(A, \cdot, \circ)$ is a *bi-skew brace* if also $(A, \circ, \cdot)$ is a skew brace.

Given a bi-skew brace $A = (A, \cdot, \circ)$ we use the notation $A_{\leftrightarrow} = (A, \circ, \cdot)$. The gamma function $\gamma_{\leftrightarrow}$ associated with $A_{\leftrightarrow}$ is given by $\gamma_{\leftrightarrow}(a) = \gamma(a)^{-1}$ and its $*$-operation is denoted by $*_{\leftrightarrow}$. The following characterisation of bi-skew braces using the gamma function is a slight reformulation of [Car20, Theorem 3.1].

Theorem 2.6. *Let A be a skew brace. Then the following are equivalent:*

(1) *A is a bi-skew brace.*
(2) *$\gamma : (A, \cdot) \to \mathrm{Aut}(A, \cdot)$ is a group antihomomorphism.*
(3) *A_{op}^2 is contained in $\ker(\gamma)$.*

Remark 2.7. We remark that another equivalent condition to the ones in Theorem 2.6 is that $A_{\mathrm{op}}^2 * A = \{1\}$. Indeed, this follows from the fact that $a * b = 1$ if and only if $\gamma^{(a)}b = b$. Also note that in particular A_{op}^2 is a trivial skew brace in this case.

We recall the following notion, introduced as λ-homomorphic skew braces by V. G. Bardakov, M. V. Neshchadim, and M. K. Yadav [BNY22a].

Definition 2.8. A skew brace A is γ-*homomorphic* if $\gamma \colon (A, \cdot) \to \mathrm{Aut}(A, \cdot)$ is a group homomorphism.

From Theorem 2.6 we recover the following result; see [Car20, Lemma 3.7].

Lemma 2.9. *Let A be a skew brace. Then any two of the following statements imply the third:*

- *A is γ-homomorphic.*
- *A is a bi-skew brace.*
- *$\gamma(A)$ is abelian.*

To conclude this section, we move our attention to solubility and nilpotency properties of skew braces. Define inductively $A^{(1)} = A^1 = A^{[1]} = A_1 = A$, and

$$A^{(n)} = A^{(n-1)} * A,$$
$$A^n = A * A^{n-1},$$
$$A^{[n]} = \left\langle \bigcup_{i=1}^{n-1} A^{[i]} * A^{[n-i]} \right\rangle,$$
$$A_n = A_{n-1} * A_{n-1}$$

for all $n \geq 2$, where on the third line we mean the subgroup generated in $(A, \cdot)$. Here $A^{(n)}$ is an ideal of A, A^n and $A^{[n]}$ are left ideals of A, and A_n is a subskew brace of A; see [CSV19, KSV21].

Definition 2.10. A skew brace A is

- *right nilpotent* if there exists $n \geq 1$ such that $A^{(n)} = \{1\}$; if n is minimal with this property, then we call $n-1$ the *right nilpotency class* of A.
- *left nilpotent* if there exists $n \geq 1$ such that $A^n = \{1\}$; if n is minimal with this property, then we call $n-1$ the *left nilpotency class* of A.
- *strongly nilpotent* if there exists $n \geq 1$ such that $A^{[n]} = \{1\}$; if n is minimal with this property, then we call $n-1$ the *strong nilpotency class* of A.
- *soluble* if there exists $n \geq 1$ such that $A_n = \{1\}$; if n is minimal with this property, then we call $n-1$ the *solubility class* of A.

For two-sided braces, the above notions all coincide with nilpotency of the associated Jacobson radical ring. Note that when the skew brace is almost trivial, then $a * b$ is the commutator of a^{-1} and b, so the above notions coincide with their group theoretical counterparts. We have the following connection between left, right and strongly nilpotent skew braces, proved in [Smo18, Theorem 12] for braces and generalised in [CSV19, Theorem 2.30] to skew braces.

Theorem 2.11. *Let A be a skew brace. Then the following are equivalent:*

1. *A is left and right nilpotent.*
2. *A is strongly nilpotent.*

We conclude with the following result, which was stated in [BCJO19, Proposition 2.4] for braces but can easily be generalised to skew braces.

Lemma 2.12. *Let A be a skew brace and let I be an ideal. Then A is a soluble skew brace if and only if A/I and I are soluble skew braces.*

3. Structural results for bi-skew braces

In this section, we deal with results on nilpotency and solubility of bi-skew braces. We start by relating the structure of a bi-skew brace A with that of $A_{\leftrightarrow}$.

Lemma 3.1. *Let A be a bi-skew brace. Then the (left) ideals of A and $A_{\leftrightarrow}$ coincide.*

Proof. Let I be a subskew brace of A. As $\gamma_{\leftrightarrow}(a) = \gamma(a)^{-1} = \gamma(\overline{a})$, we have that I is mapped to itself by $\gamma(a)$ for all $a \in A$ if and only if I is mapped to itself by $\gamma_{\leftrightarrow}(a)$ for all $a \in A$. $\square$

Lemma 3.2. *Let A be a bi-skew brace, and let I be a left ideal of A. Then $A * I = A *_{\leftrightarrow} I$. If furthermore I is an ideal, then $I * A = I *_{\leftrightarrow} A$.*

Proof. Suppose that I is a left ideal of A. Take $a \in A$ and $b \in I$. We have

$$a * b = {}^{\gamma(a)}b \cdot b^{-1} = ({}^{\gamma(a)}b \circ \overline{b} \circ b) \cdot b^{-1}$$
$$= ({}^{\gamma(a)}b \circ \overline{b}) \cdot {}^{\gamma({}^{\gamma(a)}b \circ \overline{b})}b \cdot b^{-1}$$
$$(3.1) \qquad = (\overline{a} *_{\leftrightarrow} b) \cdot ((\overline{a} *_{\leftrightarrow} b) * b).$$

Hence $\overline{a} *_{\leftrightarrow} b = (a * b) \cdot ((\overline{a} *_{\leftrightarrow} b) * b)^{-1} \in A * I$, and thus $A *_{\leftrightarrow} I \subseteq A * I$. By a symmetric argument and Lemma 3.1, we also obtain $A * I \subseteq A *_{\leftrightarrow} I$.

Suppose now that I is an ideal. By (3.1) with $a \in I$ and $b \in A$ and Lemma 3.1, we get that $I *_{\leftrightarrow} A \subseteq I * A$. Therefore the result follows by a symmetric argument. $\square$

As a consequence, we derive the following propositions.

Proposition 3.3. *Let A be a bi-skew brace. Then A is soluble of class n if and only if $A_{\leftrightarrow}$ is soluble of class n.*

Proposition 3.4. *Let A be a bi-skew brace. Then A is left, respectively right, nilpotent of class n if and only if $A_{\leftrightarrow}$ is left, respectively right, nilpotent of class n.*

We show now that we can check whether a bi-skew brace is right nilpotent or soluble just looking at a suitable group. A prominent role is played by Theorem 2.6 and Remark 2.7. Also the following lemma is used throughout the rest of this section.

Lemma 3.5. *Let A be a bi-skew brace. Then $\ker(\gamma)$ is an ideal of A.*

Proof. It suffices to note that $\gamma \colon A \to \mathrm{opTriv}(\mathrm{Aut}(A, \cdot))$ is well-defined skew brace homomorphism. $\square$

Theorem 3.6. *Let $A \neq \{1\}$ be a bi-skew brace. Then A is right nilpotent of class $n + 1$ if and only if $\gamma(A)$ is a nilpotent group of class n.*

Proof. As A is a bi-skew brace, $\ker(\gamma)$ is an ideal, trivial as a skew brace. Because $A \neq \{1\}$, it is clear that A is right nilpotent of class $n+1$ if and only if $A/\ker(\gamma)$ is right nilpotent of class n.

As $A_{\mathrm{op}}^2 \subseteq \ker(\gamma)$, we know that $A/\ker(\gamma)$ is an almost trivial skew brace. In particular, $A/\ker(\gamma)$ is right nilpotent of class n if and only if the group $(A/\ker(\gamma), \circ)$ is nilpotent of class n, and $(A/\ker(\gamma), \circ)$ is clearly isomorphic to $\gamma(A)$. $\qquad\square$

Corollary 3.7. *Let A be a bi-skew brace such that $(A, \cdot)$ or $(A, \circ)$ are nilpotent. Then A is right nilpotent.*

Proof. It suffices to note that $\gamma(A)$ is a quotient of both $(A, \cdot)$ and $(A, \circ)$, and then to apply Theorem 3.6. $\qquad\square$

Corollary 3.8. *Let A be a bi-skew brace. Then A is left nilpotent if and only if A is strongly nilpotent.*

Proof. By Theorem 2.11, it suffices to show that in this case left nilpotency implies right nilpotency. If A is left nilpotent, then so is the skew brace $A/\ker(\gamma)$. But as $A/\ker(\gamma)$ is almost trivial, we find that this is equivalent to the group $(A/\ker(\gamma), \circ) \cong \gamma(A)$ being nilpotent. The result then follows from Theorem 3.6. $\qquad\square$

Proposition 3.9. *Let A be a bi-skew brace. Then A is a soluble skew brace if and only if $\gamma(A)$ is a soluble group.*

Proof. As A is a bi-skew brace, $\ker(\gamma)$ is an ideal, trivial as a skew brace. Therefore A is soluble if and only if $A/\ker(\gamma)$ is soluble, by Lemma 2.12.

Now as $A_{\mathrm{op}}^2 \subseteq \ker(\gamma)$, we know that $A/\ker(\gamma)$ is an almost trivial skew brace. In particular, $A/\ker(\gamma)$ is soluble if and only if the group $(A/\ker(\gamma), \circ)$ is soluble, and $(A/\ker(\gamma), \circ)$ is clearly isomorphic to $\gamma(A)$. $\qquad\square$

We conclude this section by proving Byott's conjecture in the case of bi-skew braces.

Conjecture 3.10 (Byott's Conjecture)**.** *Let A be a finite skew brace. If $(A, \cdot)$ is soluble, then $(A, \circ)$ is soluble.*

Theorem 3.11. *Let A be a bi-skew brace. Then $(A, \cdot)$ is soluble if and only if $(A, \circ)$ is soluble. Moreover, in this case also A is soluble as a skew brace.*

Proof. Assume that $(A, \cdot)$ is soluble. As A/A_{op}^2 is an almost trivial skew brace, $(A/A_{\mathrm{op}}^2, \cdot) \cong (A/A_{\mathrm{op}}^2, \circ)$, and in particular it follows from the assumption that both are soluble. Since A_{op}^2 is a trivial skew brace, clearly $(A_{\mathrm{op}}^2, \cdot) \cong (A_{\mathrm{op}}^2, \circ)$. In particular, it once again follows from the assumption that both groups are soluble. We conclude that $(A/A_{\mathrm{op}}^2, \circ)$ and $(A_{\mathrm{op}}^2, \circ)$ are soluble, so $(A, \circ)$ is also soluble.

The exact same argument proves the other implication.

To prove that in this case A is also soluble as a skew brace, it suffices to note that $\gamma(A)$ is a soluble group as it is a quotient of $(A, \circ)$. The solubility of A then follows by Proposition 3.9. $\qquad\square$

Remark 3.12. The same idea can be used to prove Byott's conjecture for skew braces with a composition series where the factors are trivial or almost trivial skew braces, so in particular for soluble skew braces. This means that Byott's conjecture holds for several classes of skew braces studied in recent years, but as there exist

finite simple skew braces which are neither trivial nor almost trivial [BCJO19], this does not provide a general way to prove the conjecture.

3.1. **Bi-skew braces and γ-homomorphic skew braces.** Recall from Theorem 2.6 that the gamma function of a bi-skew brace is an antihomomorphism with respect to the additive group. It is therefore to be expected that there is a connection with γ-homomorphic skew braces. Indeed, as we noted before these two notions coincide when $\gamma(A)$ is abelian. In the remainder of this section we further discuss some similarities.

We start with a theorem for γ-homomorphic skew braces similar to Theorem 2.6 and Remark 2.7.

Theorem 3.13. *Let A be a skew brace. Then the following are equivalent:*

(1) *A is γ-homomorphic.*
(2) *A^2 is contained in $\ker(\gamma)$.*
(3) *A is right nilpotent of class at most 2.*

Proof. Assume that A is γ-homomorphic. Then for all $a, b \in A$,

$$\gamma(a * b) = \gamma(a)^{-1}\gamma(a)\gamma(b)\gamma(b)^{-1} = 1.$$

It follows that $A^2 \subseteq \ker(\gamma)$. Conversely, assume that $\ker(\gamma)$ contains A^2. As A/A^2 is a trivial skew brace it follows for all $a, b \in A$ that $(a \cdot b) \circ A^2 = (a \circ b) \circ A^2$. The assumption then implies

$$\gamma(a \cdot b) = \gamma(a \circ b) = \gamma(a)\gamma(b).$$

The equivalence of the second and third condition is clear. $\qquad\square$

Recall that a skew brace A is *metatrivial* if it is soluble of class at most 2, which by definition means that A^2 is a trivial skew brace. As a consequence of Theorem 3.13, we find a short proof of [BNY22a, Theorem 2.12], as follows.

Corollary 3.14. *Every γ-homomorphic skew brace is metatrivial.*

Proof. Let A be a γ-homomorphic skew brace. Then by Theorem 3.13, $A^{(3)} = \{1\}$, and this clearly implies that $A^2 * A^2 \subseteq A^2 * A = \{1\}$. $\qquad\square$

Note that the converse does not hold.

Example 3.15. Let $A = \mathrm{opTriv}(\mathbb{S}_3)$, with $\mathbb{S}_3$ the symmetric group on 3 elements. Then A is metatrivial because $\mathbb{S}_3$ is metabelian. As $\mathbb{S}_3$ is not nilpotent, it follows that A is not right nilpotent and in particular not γ-homomorphic.

Example 3.16. Recall that if A is a Jacobson radical ring, then A yields a two-sided brace [Rum07a]. By Theorem 2.6 (or equivalently, Theorem 3.13), we find that the corresponding brace is a bi-skew brace (or equivalently a γ-homomorphic skew brace) if and only if $A^{(3)} = A^3 = \{1\}$, as already shown in [Chi19, Proposition 4.1] when A is finite or nilpotent.

We conclude the section by showing that one can use the semidirect product of skew braces to obtain two slightly different constructions, one yielding γ-homomorphic skew braces and one yielding bi-skew braces. For bi-skew braces it turns out that we find a different construction for examples which were already described by Childs.

We recall first the semidirect product of skew braces, as developed in [SV18, Corollary 2.36]. If A and B are skew braces, an *action* of A on B is a group homomorphism $\alpha \colon (A, \circ) \to \mathrm{Aut}(B, \cdot, \circ)$. If we have such an α, whose action is written as a left exponent, then the set $A \times B$, with operations

$$(a, b) \cdot (a', b') = (a \cdot a', b \cdot b'),$$
$$(a, b) \circ (a', b') = (a \circ a', b \circ {}^{\alpha(a)}(b')),$$

is a skew brace, which we denote by $A \ltimes B$.

Example 3.17. Let G and H be groups, and let G act by automorphisms on H, with the action denoted by α. This induces an action of the trivial skew brace $A = \mathrm{Triv}(G)$ on the trivial skew brace $B = \mathrm{Triv}(H)$. By the semidirect product construction, we find a skew brace $A \ltimes B$. Explicitly,

$$(g, h) \cdot (g', h') = (gg', hh'),$$
$$(g, h) \circ (g', h') = (gg', h^{\alpha(g)}(h')).$$

We have recovered in this way [GV17, Example 1.4]. Note that here the gamma function is $\gamma(g, h) = (\mathrm{id}, \alpha(g))$. In particular, $A \ltimes B$ is a γ-homomorphic skew brace, and it is a bi-skew brace if and only if $[G, G] \subseteq \ker(\alpha)$, as an immediate computation shows.

Example 3.18. Let G and H be groups, and let G act by automorphisms on H, with the action denoted by α. This induces an action of the almost trivial skew brace $A = \mathrm{opTriv}(G)$ on the trivial skew brace $B = \mathrm{Triv}(H)$. By the semidirect product construction, we find a skew brace $A \ltimes B$. Explicitly,

$$(g, h) \cdot (g', h') = (g'g, hh'),$$
$$(g, h) \circ (g', h') = (gg', h^{\alpha(g)}(h')).$$

The skew brace $A \ltimes B$ has gamma function $\gamma(g, h) = (\phi(g), \alpha(g))$, where $\phi(g)$ denotes conjugation by g. This immediately implies that $A \ltimes B$ is a bi-skew brace, already obtained in [Chi19, Proposition 7.1] from the semidirect product of the groups G and H. Moreover it is γ-homomorphic if and only if $[G, G] \subseteq \ker(\alpha) \cap Z(G)$. Note that when G is abelian, this construction coincides with the one in Example 3.17.

4. Some classification results

We begin this section by showing that all the braces with multiplicative group isomorphic to $\mathbb{Z}^2$ are in fact bi-skew braces. We need the following result.

Theorem 4.1. *Let $(A, \cdot, \circ)$ be a two-sided brace such that $(A, \circ)$ is finitely generated abelian of rank n. Then $(A, \cdot)$ is finitely generated abelian of rank n.*

Proof. By [Wat68, Theorem 3], if $(A, \circ)$ is finitely generated abelian, then $(A, \cdot)$ is finitely generated. By [AD95, Theorem B], the ranks of $(A, \circ)$ and $(A, \cdot)$ coincide. □

Proposition 4.2. *Let A be a brace with multiplicative group isomorphic to $\mathbb{Z}^n$. Then A is right nilpotent of class at most n.*

Proof. By Theorem 4.1, $(A, \cdot)$ is finitely generated of rank n. Let T be the (necessarily finite) torsion subgroup of $(A, \cdot)$. As T is a characteristic subgroup of $(A, \cdot)$, it is a left ideal of A, so also a finite subgroup of $(A, \circ)$, and thus T is trivial. It follows that $(A, \cdot) \cong \mathbb{Z}^n$.

Now for a prime p, let $I_p \cong (p\mathbb{Z})^n$ be the characteristic subgroup of $(A, \cdot)$ generated by all p-powers of elements. Then A/I_p has order p^n, and therefore it is left nilpotent of class at most n by [Rum07a, Corollary of Proposition 8]. As A/I_p is a two-sided brace it is also right nilpotent of class at most n, or equivalently, $A^{(n+1)} \subseteq I_p$. We conclude that

$$A^{(n+1)} \subseteq \bigcap_{p \text{ prime}} I_p = \{1\}. \qquad \qquad \square$$

We immediately recover [CSV19, Theorem 5.5], and we find the result we have claimed.

Corollary 4.3. *Let A be a brace with multiplicative group isomorphic to $\mathbb{Z}$. Then A is a trivial skew brace.*

Corollary 4.4. *Let A be a brace with multiplicative group isomorphic to $\mathbb{Z}^2$. Then A is a bi-skew brace.*

Proof. It follows from Proposition 4.2 that A is right nilpotent of degree at most 2. The statement then follows from Theorem 2.6 and the fact that $A_{\mathrm{op}} = A$. $\square$

Motivated by Corollary 4.3, we now want to classify all the skew braces with multiplicative group isomorphic to $\mathbb{Z}$, as asked in [Ven19, Problem 2.27]. Let $(A, \cdot)$ be an infinite cyclic group, with generator x. We can define the following operation on A:

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

Then, as shown in the proof of [Rum07b, Proposition 6], the operation $\circ$ is the unique one such that $(A, \cdot, \circ)$ is a nontrivial brace, and $(A, \circ)$ is isomorphic to the infinite dihedral group

$$\langle x, y \mid y^2 = 1, yxy = x^{-1} \rangle \cong C_2 \ltimes \mathbb{Z}.$$

We can easily see that $(A, \cdot, \circ)$ is a bi-skew brace. Moreover, there are just two group automorphisms of $(A, \circ)$, namely the identity and the inversion, and it is easily verified that both are also automorphisms of the skew brace $(A, \cdot, \circ)$ and therefore also of $(A, \circ, \cdot)$.

We claim that $(A, \circ, \cdot)$ is not isomorphic to its opposite skew brace. They are clearly not equal, as $(A, \circ)$ is not abelian. Therefore, the only candidate for an isomorphism is given by the inversion automorphism of $(A, \cdot)$ which also induces an automorphism of $(A, \circ)$. If this yields an isomorphism of skew braces, then it would be both an automorphism and antiautomorphism of $(A, \circ)$ which implies that $(A, \circ)$ is abelian. As $(A, \circ)$ is isomorphic to the infinite dihedral group, this is a contradiction.

In the remainder of this section we prove that the two skew braces with infinite cyclic multiplicative group above are in fact the only nontrivial ones.

Lemma 4.5. *Let B be a skew brace with an abelian multiplicative group. Then for all $X, Y \subseteq B$, the equality $X * Y = Y *_{\mathrm{op}} X$ holds.*

Proof. It suffices to note that for all $a, b \in B$,

$$a * b = a^{-1} \cdot (a \circ b) \cdot b^{-1} = a^{-1} \cdot (b \circ a) \cdot b^{-1} = b *_{\mathrm{op}} a. \qquad \square$$

Theorem 4.6. *Let $(A, \circ) = \{x^{\circ i} \mid i \in \mathbb{Z}\}$ be an infinite cyclic group. If $A = (A, \cdot, \circ)$ is a skew brace, then the additive operation is given by one of the following equalities:*

$$(4.1) \qquad\qquad\qquad\qquad x^{\circ i} \cdot x^{\circ j} = x^{\circ(i+j)},$$

$$(4.2) \qquad\qquad\qquad\qquad x^{\circ i} \cdot x^{\circ j} = x^{\circ(i+(-1)^i j)},$$

$$(4.3) \qquad\qquad\qquad\qquad x^{\circ i} \cdot x^{\circ j} = x^{\circ(j+(-1)^j i)}.$$

Proof. If $(A, \cdot)$ is abelian, then $\cdot$ is given by (4.1) by Corollary 4.3.

From now on, we assume that $(A, \cdot)$ is not abelian. As A is two-sided, it follows from [Nas19, Lemma 4.5] that $(A^2, \cdot)$ is abelian. In particular, $A^2 \neq A$. Moreover, note that $A^2 \neq 1$, otherwise A would be trivial, so $(A, \cdot)$ would be abelian. We deduce that there exists $n \geq 2$ such that $A^2 = \{x^{\circ nk} \mid k \in \mathbb{Z}\}$.

As A^2 is a brace with multiplicative group isomorphic to $\mathbb{Z}$, it follows from Corollary 4.3 that A^2 is a trivial skew brace. Because $(A/A^2, \circ) \cong C_n$, we find that $A/A^2 \cong \mathrm{Triv}(C_n)$.

As x generates $(A, \circ)$, its equivalence class in A/A^2 generates $(A/A^2, \circ)$, and therefore also $(A/A^2, \cdot)$. If we take $a \in A^2$ to be a generator of $(A^2, \cdot)$, then $(A, \cdot)$ is generated by a and x. Denote by ψ the inner automorphism on $(A^2, \cdot)$ induced by x in $(A, \cdot)$. As $(A, \cdot)$ is not abelian, ψ is not trivial, so necessarily ψ is the inversion automorphism.

Likewise, $\gamma(x)$ restricts to an automorphism of $(A^2, \cdot)$, which is either the identity or equals ψ.

(1) If $\gamma(x)$ is the identity on A^2, then using Lemma 4.5 we find $A^2 *_{\mathrm{op}} A = A * A^2 = \{1\}$, so A_{op} is a bi-skew brace. This means that $(A, \circ, \cdot_{\mathrm{op}})$ is a nontrivial skew brace on $(A, \circ)$, so necessarily $\cdot$ is given by (4.3).

(2) If $\gamma(x)$ restricts to the inversion automorphism on $(A^2, \cdot)$, and therefore is equal to ψ on A^2, then $\gamma_{\mathrm{op}}(x)$ equals $\psi^2 = \mathrm{id}$ on A^2. Using Lemma 4.5 we find $A^2_{\mathrm{op}} * A = A *_{\mathrm{op}} A^2 = \{1\}$. So $(A, \circ, \cdot)$ is a non-trivial skew brace on $(A, \circ)$, which implies that $\cdot$ is given by (4.2). $\qquad \square$

5. Bi-skew braces and solutions of the Yang–Baxter equation

The interest in set-theoretic solutions of the Yang–Baxter equation, as a simplification of its linear solutions, goes back to V. G. Drinfel'd [Dri92]. Compared to the linear version, set-theoretic solutions are easier to study and classify. Nonetheless, set-theoretic solutions can be linearised and are also omnipresent in the study of link and knot invariants [NV06]. In this section we investigate connections between bi-skew braces and associated set-theoretic solutions of the Yang–Baxter equation. Before doing so, we give a short summary of all the necessary notions involved.

A *set-theoretic solution of the Yang–Baxter equation* is a pair (X, r) with X a nonempty set and $r \colon X^2 \to X^2$ a bijective map satisfying the braid equation

$$r_1 r_2 r_1 = r_2 r_1 r_2,$$

where $r_1 = r \times \mathrm{id}_X$ and $r_2 = \mathrm{id}_X \times r$. On every nonempty set X, the map $(x, y) \mapsto (y, x)$ satisfies the braid equation; this solution is said to be *trivial*. We say that a solution is *nondegenerate* if the maps $\sigma_x, \tau_x \colon X \to X$ defined by

$r(x, y) = (\sigma_x(y), \tau_y(x))$ are bijective. In the rest of this section, we will shortly refer to a nondegenerate set-theoretic solution of the Yang–Baxter equation as a *solution*. Furthermore, we say that a solution is *involutive* if $r^2 = \mathrm{id}$. Given a solution (X, r), it is easily checked that also (X, r^{-1}) is a solution. We define $\hat{\sigma}, \hat{\tau} \colon X \to X$ by $r^{-1}(x, y) = (\hat{\sigma}_x(y), \hat{\tau}_y(x))$.

Given two solutions (X, r) and (Y, s), we say that a map $f \colon X \to Y$ is a *homomorphism of solutions* if $(f \times f)r = s(f \times f)$. One can prove that in this case the image of f is a subsolution of (Y, s), meaning that s restricts to $f(X) \times f(X)$. A bijective homomorphism of solutions is called an *isomorphism of solutions*.

Given a skew brace A, define

$$r_A \colon A^2 \to A^2, \quad (a, b) \mapsto ({}^{\gamma(a)}b, \overline{{}^{\gamma(a)}b} \circ a \circ b).$$

Then the pair (A, r_A) is a solution [LYZ00, GV17] and $(A_{\mathrm{op}}, r_{A_{\mathrm{op}}})$ is its inverse solution [KT20]. This construction is functorial: a skew brace homomorphism $f \colon A \to B$ induces a homomorphism of solutions $f \colon (A, r_A) \to (B, r_B)$.

Following [ESS99] we define the *structure group* of a solution (X, r) as

$$G(X, r) = \langle X \mid x \circ y = \sigma_x(y) \circ \tau_y(x) \text{ for all } x, y \in X \rangle.$$

For each solution (X, r), one can also define its *derived structure group* as

$$A(X, r) = \langle X \mid x \cdot y = y \cdot \sigma_y \hat{\sigma}_y(x) \rangle.$$

It is possible to construct a bijection between $A(X, r)$ and $G(X, r)$ such that, transferring the group structure of $A(X, r)$ to $G(X, r)$, one obtains a skew brace $(G(X, r), \cdot, \circ)$. This is a brace if and only if (X, r) is involutive; see [Sol00, LV19]. Under this bijection, the generator of $A(X, r)$ corresponding to some element $x \in X$ is mapped to the generator of $G(X, r)$ corresponding to x. We define $\iota \colon X \to G(X, r)$ as the canonical map sending each element to its corresponding generator. We therefore find that $\iota(X) \subseteq (G(X, r), \cdot, \circ)$ generates both the additive and multiplicative group. Moreover, the skew brace $(G(X, r), \cdot, \circ)$ satisfies the property that ι is a homomorphism of solutions $\iota \colon (X, r) \to (G(X, r), r_{G(X,r)})$. In particular, this means that for all $x, y \in X$ the equality $\iota(\sigma_x(y)) = {}^{\gamma(\iota(x))}(\iota(y))$ holds in $G(X, r)$. Similarly, it follows that $\iota(\hat{\sigma}_x(y)) = {}^{\gamma_{\mathrm{op}}(\iota(x))}(\iota(y))$ holds in $G(X, r)$. A solution is *injective* if ι is an injective map. An involutive solution is always injective. To any solution (X, r) one can associate its *injectivization* $\mathrm{Inj}(X, r)$, which is the image of the homomorphism $\iota \colon (X, r) \to (G(X, r), r_{G(X,r)})$. It is clear that $G(\mathrm{Inj}(X, r))$ and $G(X, r)$ are isomorphic as skew braces and therefore $\mathrm{Inj}(X, r)$ is indeed an injective solution.

Following [Bac18, CJK$^+$23], we can associate to any solution (X, r) another group called the *permutation group*, defined as

$$\mathcal{G}(X, r) = \langle (\sigma_x, \tau_x^{-1}) \mid x \in X \rangle \subseteq \mathrm{Perm}(X) \times \mathrm{Perm}(X).$$

There exists a unique surjective group homomorphism $\pi \colon G(X, r) \to \mathcal{G}(X, r)$ satisfying $\pi(x) = (\sigma_x, \tau_x^{-1})$. It can be shown that the kernel of this map π is an ideal of $(G(X, r), \cdot, \circ)$, hence there is a natural skew brace structure induced on $\mathcal{G}(X, r)$ such that π is a skew brace homomorphism. If (X, r) is injective, then $\ker(\pi) = \mathrm{Soc}(G(X, r))$. In particular, note that for any involutive (hence injective) solution (X, r), we find that $\ker(\pi) = \ker(\gamma)$. As the construction of the solution associated to a skew brace is functorial, we find a homomorphism of solutions

$\pi\iota\colon (X, r) \to (\mathcal{G}(X, r), r_{\mathcal{G}(X,r)})$. The image of this homomorphism is called the *retract* of (X, r), denoted by $\mathrm{Ret}(X, r)$. It can be verified that $\mathrm{Ret}(X, r)$ can also be obtained as the induced solution on the equivalence classes of the equivalence relation given by

$$x \sim y \iff \sigma_x = \sigma_y \text{ and } \tau_x = \tau_y,$$

which is its original definition in literature.

We now move on to our first result.

Proposition 5.1. *Let A be a skew brace. Then A is a bi-skew brace if and only if for all $a, b \in A$,*

$$\tag{5.1} \gamma(^{\gamma_{\mathrm{op}}(a)}b) = \gamma(b).$$

Proof. If A is a bi-skew brace, then the assertion follows from Theorem 2.6.

For the other implication, suppose that (5.1) holds. For all $a, b \in A$, we have

$$\begin{aligned}
\gamma(a \cdot b) &= \gamma(^{\gamma_{\mathrm{op}}(b)\gamma_{\mathrm{op}}(\overline{b})}a \cdot b) \\
&= \gamma(b \circ {}^{\gamma_{\mathrm{op}}(\overline{b})}a) \\
&= \gamma(b)\gamma(^{\gamma_{\mathrm{op}}(\overline{b})}a) \\
&= \gamma(b)\gamma(a).
\end{aligned}$$

Hence, again, by Theorem 2.6, A is a bi-skew brace. □

The following is a straightforward corollary.

Proposition 5.2. *Let A be a skew brace. Then A is a bi-skew brace if and only if its associated solution (A, r_A) satisfies, for all $x, y \in A$,*

$$\sigma_{\hat{\sigma}_x(y)} = \sigma_y.$$

As a result, the information whether A is a bi-skew brace is not lost when one only considers its associated solution. Next, it is natural to ask whether, if we know that A is a bi-skew brace, it is possible to recover the associated solution of $A_{\leftrightarrow}$ from the associated solution of A. The following example shows that this is in general not possible, as we construct nonisomorphic bi-skew braces A and B such that the associated solutions are isomorphic, but the solutions associated to $A_{\leftrightarrow}$ and $B_{\leftrightarrow}$ are not isomorphic.

Example 5.3. Let $(G, \cdot) = C_2 \times C_8$, with $C_2 = \langle x \rangle$, and let $\psi_1\colon C_2 \to \mathrm{Aut}(G)$ be the group homomorphism mapping x to the inversion automorphism of G. By the semidirect product construction (see section 3), we find a bi-skew brace A on the set $C_2 \times G$, whose associated solutions can easily be computed as follows:

$$\begin{aligned}
r_A((x^i, g), (x^j, h)) &= ((x^j, {}^{\psi_1(x)^i}h), (x^i, {}^{\psi_1(x)^j}g)), \\
r_{A_{\leftrightarrow}}((x^i, g), (x^j, h)) &= ((x^j, {}^{\psi_1(x)^i}h), (x^i, g \cdot h \cdot {}^{\psi_1(x)^i}(h^{-1}))).
\end{aligned}$$

In particular, $\tau_{\leftrightarrow,(x^j,h)}(1, g) = (1, g)$ and $\tau_{\leftrightarrow,(x^j,h)}(x, g) = (x, g \cdot h^2)$. Here $\tau_{\leftrightarrow}$ is the usual map associated with the solution $(A, r_{A_{\leftrightarrow}})$. Note that if $h \in G$ is an element of order 8, then $\tau_{\leftrightarrow,(x^j,h)}$ has order 4.

Now take $(H, \cdot) = C_2^4$, and let $\psi_2\colon C_2 \to \mathrm{Aut}(H)$, where still $C_2 = \langle x \rangle$, be the map which sends x to the automorphism interchanging the first two and the last

two coordinates of H. In the same way as before we can then obtain a bi-skew brace B, and two associated solutions:

$$r_B((x^i, g), (x^j, h)) = ((x^j, \psi_2(x)^i h), (x^i, \psi_2(x)^j g)),$$

$$r_{B_\leftrightarrow}((x^i, g), (x^j, h)) = ((x^j, \psi_2(x)^i h), (x^i, g \cdot h \cdot \psi_2(x)^i h)).$$

In this case once again, we find that $\tau_{\leftrightarrow,(x^j,h)}(1, g) = (1, g)$ and $\tau_{\leftrightarrow,(x^j,h)}(x, g) = (x, g \cdot h \cdot \psi_2(x)^i h)$. One easily checks that all τ-maps associated to $r_{B_\leftrightarrow}$ have either order one or two. Therefore, $r_{A_\leftrightarrow}$ can not be isomorphic to $r_{B_\leftrightarrow}$.

The cycle structures of $\psi_1(x)$ and $\psi_2(x)$ are the same; they are both of order two and fix four points. Therefore, there exists a bijection $\theta \colon G \to H$ such that $\theta \psi_1(x) = \psi_2(x)\theta$, and in particular the bijection

$$C_2 \times G \to C_2 \times H, \quad (x^i, g) \mapsto (x^i, \theta(g))$$

gives an isomorphism between the solutions r_A and r_B.

We now deal with the opposite situation, where we start with a given solution and ask whether the skew brace on the structure group is a bi-skew brace.

Theorem 5.4. *Let (X, r) be an injective solution. Then $G(X, r)$ is a bi-skew brace if and only if $\sigma_{\hat{\sigma}_x(y)} = \sigma_y$ for all $x, y \in X$.*

Proof. The implication from left to right is a consequence of Proposition 5.2 and the fact that (X, r) is injective.

Now assume that for all $x, y \in X$, we have that $\sigma_{\hat{\sigma}_x(y)} = \sigma_y$. This means that $\gamma(\gamma_{\mathrm{op}}(x)y) = \gamma(y)$ where x, y are now considered as the generators of $G(X, r)$ and γ, respectively γ_{op}, is the gamma function associated to $G(X, r)$, respectively $G(X, r)_{\mathrm{op}}$. In particular, as X generates the multiplicative group $(G(X, r), \circ)$, it follows that $\gamma(\gamma_{\mathrm{op}}(g)y) = \gamma(y)$ for all $g \in G(X, r)$.

For a word $w = x_1^{\epsilon_1} \cdot \ldots \cdot x_n^{\epsilon_n}$ with $x_i \in X$ and $\epsilon_i \in \{-1, 1\}$, we will prove that

$$\gamma(w) = \gamma(x_n)^{\epsilon_n} \ldots \gamma(x_1)^{\epsilon_1}.$$

As $(G(X, r), \cdot)$ is generated by X, this then proves that

$$\gamma \colon (G(X, r), \cdot) \to \mathrm{Aut}(G(X, r), \cdot)$$

is a group antihomomorphism, and therefore $G(X, r)$ is a bi-skew brace. We will prove this claim by induction on n. For $n = 1$ and $\epsilon_1 = 1$ the statement is trivial. To also cover the case where $n = 1$ and $\epsilon_1 = -1$, we have to prove that $\gamma(x^{-1}) = \gamma(x)^{-1}$ for all $x \in X$. For this, we note that there is the equality $\gamma_{\mathrm{op}}(a)(\overline{a}) = (a \circ \overline{a}) \cdot a^{-1} = a^{-1}$, or equivalently, $\overline{\gamma_{\mathrm{op}}(a)^{-1}(a^{-1})} = a$, so substituting a by x^{-1} we find $\overline{\gamma_{\mathrm{op}}(x^{-1})^{-1}(x)} = x^{-1}$, thus

$$\gamma(x^{-1}) = \gamma\left(\overline{\gamma_{\mathrm{op}}(x^{-1})^{-1}(x)}\right) = \gamma\left(\gamma_{\mathrm{op}}(x^{-1})^{-1}(x)\right)^{-1} = \gamma(x)^{-1}.$$

Now assume that the statement holds for words of length $n - 1$, and let $w = x_1^{\epsilon_1} \cdot \ldots \cdot x_n^{\epsilon_n}$ be a word of length n. If we write $v = x_2^{\epsilon_2} \cdot \ldots \cdot x_n^{\epsilon_n}$, then

$$\begin{aligned}
\gamma(w) &= \gamma(v \circ \gamma_{\mathrm{op}}(v)(x_1^{\epsilon_1})) \\
&= \gamma(v)\gamma(\gamma_{\mathrm{op}}(v)(x_1^{\epsilon_1})) \\
&= \gamma(x_n)^{\epsilon_n} \ldots \gamma(x_2)^{\epsilon_2} \gamma(\gamma_{\mathrm{op}}(v)(x_1))^{\epsilon_1} \\
&= \gamma(x_n)^{\epsilon_n} \ldots \gamma(x_2)^{\epsilon_2} \gamma(x_1)^{\epsilon_1}. \qquad \square
\end{aligned}$$

Corollary 5.5. *Let (X, r) be a solution such that for all $x, y \in X$,*

$$\sigma_{\hat{\sigma}_x(y)} = \sigma_y.$$

Then $G(X, r)$ is a bi-skew brace.

Proof. As $\mathrm{Inj}(X, r)$ is a homomorphic image of (X, r), it follows that $\mathrm{Inj}(X, r)$ still has the property that $\sigma_{\hat{\sigma}_x(y)} = \sigma_y$ for all $x, y \in \mathrm{Inj}(X, r)$. Because $G(X, r)$ and $G(\mathrm{Inj}(X, r))$ are isomorphic skew braces, the result follows from Proposition 5.4. $\square$

As an application, we find a nice description for involutive solutions such that the skew brace on the structure group is a bi-skew brace.

Proposition 5.6. *Let (X, r) be an involutive solution. Then the following statements are equivalent:*
   (1) *$G(X, r)$ is a bi-skew brace.*
   (2) *$\mathcal{G}(X, r)$ is a trivial brace.*
   (3) *$\mathrm{Ret}(X, r)$ is a trivial solution.*

Proof. As (X, r) is involutive, $\mathcal{G}(X, r) \cong G(X, r)/\ker(\gamma)$, where γ is the gamma function of $G(X, r)$. It follows that $G(X, r)^{(3)} = \{1\}$ if and only if $\mathcal{G}(X, r)^{(2)} = \{1\}$. This proves the equivalence of the first two properties.

Assume that $\mathcal{G}(X, r)$ is a trivial brace, so its associated solution is a trivial solution. Because $\mathrm{Ret}(X, r)$ is equal to the image of the canonical map $\pi\iota \colon (X, r) \to (\mathcal{G}(X, r), r_{\mathcal{G}(X,r)})$, we find that $\mathrm{Ret}(X, r)$ is also trivial.

At last, assume that $\mathrm{Ret}(X, r)$ is a trivial solution. Once again using the fact that $\mathrm{Ret}(X, r)$ embeds into $(\mathcal{G}(X, r), r_{\mathcal{G}(X,r)})$, we know that $^{\gamma(x)}y = y$ in $\mathcal{G}(X, r)$ for all $x, y \in \mathrm{Ret}(X, r) \subseteq \mathcal{G}(X, r)$. As $\mathrm{Ret}(X, r)$ generates both the additive and multiplicative group of $\mathcal{G}(X, r)$, it follows that $^{\gamma(g)}h = h$ for all $g, h \in \mathcal{G}(X, r)$. This means that $\mathcal{G}(X, r)$ is a trivial skew brace. $\square$

Remark 5.7. If (X, r) is an involutive solution such that $\mathrm{Ret}(X, r)$ is trivial, then clearly $\mathrm{Ret}(\mathrm{Ret}(X, r))$ is the trivial solution on a singleton. Solutions with this property are said to be of *multipermutation level 2*. Involutive multipermutation solutions of level 2 were classified in [JPZD20] and in particular, [JPZD20, Theorem 7.8] gives an explicit construction of all involutive solutions with a trivial retract.

6. A CHARACTERISATION OF BRACE BLOCKS, AN EXPLICIT CONSTRUCTION, AND SOME EXAMPLES

Recall the definition of a brace block.

Definition 6.1. Let A be a set. A *brace block*, denoted by $((A, \circ_i) \mid i \in I)$, consists of a family of group operations $(\circ_i \mid i \in I)$ on A such that $(A, \circ_i, \circ_j)$ is a bi-skew brace for all $i, j \in I$.

In order to give a characterisation of brace blocks, we begin with a result on transitivity of bi-skew braces.

Theorem 6.2. *Let $(A, \cdot, \circ_1)$ and $(A, \cdot, \circ_2)$ be bi-skew braces with gamma functions γ_1 and γ_2, respectively. Then $(A, \circ_1, \circ_2)$ is a bi-skew brace if and only if the following conditions hold: for all $a, b \in A$ and $i, j \in \{1, 2\}$ with $i \neq j$,*

$$\gamma_i(a)\gamma_j(b)\gamma_i(a)^{-1} = \gamma_j(^{\gamma_i(a)}b).$$

Proof. By symmetry, we can just look at when $(A, \circ_1, \circ_2)$ is a skew brace. As

$$a \circ_2 b = a \cdot {}^{\gamma_2(a)}b = a \circ_1 {}^{\gamma_1(a)^{-1}\gamma_2(a)}b,$$

we need to find under which conditions $\gamma(a) = \gamma_1(a)^{-1}\gamma_2(a)$ is a gamma function on $(A, \circ_1)$.

The first condition to check is whether for all $a \in A$, we have $\gamma(a) \in \mathrm{Aut}(A, \circ_1)$, or equivalently, $\gamma_2(a) \in \mathrm{Aut}(A, \circ_1)$. Here we have

$$^{\gamma_2(a)}(b \circ_1 c) = {}^{\gamma_2(a)}(b \cdot {}^{\gamma_1(b)}c) = {}^{\gamma_2(a)}b \cdot {}^{\gamma_2(a)\gamma_1(b)}c$$

and

$$^{\gamma_2(a)}b \circ_1 {}^{\gamma_2(a)}c = {}^{\gamma_2(a)}b \cdot {}^{\gamma_1({}^{\gamma_2(a)}b)\gamma_2(a)}c.$$

We find that $\gamma(a) \in \mathrm{Aut}(A, \circ_1)$ if and only if for all $a, b \in A$,

$$(6.1) \qquad \gamma_2(a)\gamma_1(b)\gamma_2(a)^{-1} = \gamma_1({}^{\gamma_2(a)}b).$$

Now suppose that (6.1) holds. We claim that it is already enough to deduce that $\gamma\colon (A, \circ_2) \to \mathrm{Aut}(A, \circ_1)$ is a group homomorphism. For all $a, b \in A$,

$$\begin{aligned}
\gamma(a \circ_2 b) &= \gamma_1(a \cdot {}^{\gamma_2(a)}b)^{-1}\gamma_2(a \circ_2 b) \\
&= \gamma_1(a)^{-1}\gamma_1({}^{\gamma_2(a)}b)^{-1}\gamma_2(a)\gamma_2(b) \\
&= \gamma_1(a)^{-1}\gamma_2(a)\gamma_1(b)^{-1}\gamma_2(a)^{-1}\gamma_2(a)\gamma_2(b) \\
&= \gamma_1(a)^{-1}\gamma_2(a)\gamma_1(b)^{-1}\gamma_2(b) = \gamma(a)\gamma(b). \qquad \square
\end{aligned}$$

Definition 6.3. Let $(A, \cdot)$ be a group. A *brace block on* $(A, \cdot)$ is a brace block $((A, \circ_i) \mid i \in I)$ such that $(A, \circ_k) = (A, \cdot)$ for some $k \in I$.

We deduce the following characterisation for brace blocks on a given group.

Theorem 6.4. *Let $(A, \cdot)$ be a group. Then the following data are equivalent:*

(1) *A brace block on $(A, \cdot)$.*
(2) *A family of maps $(\gamma_i \mid i \in I)$ such that the following conditions hold:*
   - $\gamma_i\colon (A, \cdot) \to \mathrm{Aut}(A, \cdot)$ *is a group antihomomorphism for all $i \in I$.*
   - *There exists $k \in I$ such that $\gamma_k(a) = \mathrm{id}$ for all $a \in A$.*
   - *For all $i, j \in I$ and $a, b \in A$,*

$$\gamma_i(a)\gamma_j(b)\gamma_i(a)^{-1} = \gamma_j({}^{\gamma_i(a)}b).$$

Proof. For all $i \in I$, we find that $(A, \cdot, \circ_i)$ is a bi-skew brace because γ_i is a group antihomomorphism and the last condition for $i = j$ implies that

$$\gamma_i(a \cdot {}^{\gamma_i(a)}b) = \gamma_i(a)\gamma_i(b).$$

Now apply Theorem 6.2. $\qquad \square$

Remark 6.5. A similar condition was found in a particular case in [Spa22, Theorem 4.30], where the problem of finding mutually normalising regular subgroups in the holomorph of a cyclic group of prime order was dealt with. This problem is equivalent to looking for brace blocks; see [CS22, section 7] for more details.

We use this characterisation to propose an intermediate construction of brace blocks, which already can provide several examples.

Theorem 6.6. *Let $(A, \cdot)$ be a group, let M be an abelian subgroup of $\mathrm{Aut}(A, \cdot)$, and let $\mathcal{S}$ be the set of group homomorphisms $\gamma \colon A \to M$ such that $\gamma(\psi(a)) = \gamma(a)$ for all $a \in A$ and $\psi \in M$. Then $((A, \circ_\gamma) \mid \gamma \in \mathcal{S})$ is a brace block, where*

$$a \circ_\gamma b = a \cdot {}^{\gamma(a)}b.$$

Moreover, $(A, \circ_{\gamma_1}, \circ_{\gamma_2})$ is γ-homomorphic for all $\gamma_1, \gamma_2 \in \mathcal{S}$.

Proof. The first part is immediate from Theorem 6.4. To conclude the second part, recall that the gamma function $\gamma_{1,2}$ of $(A, \circ_{\gamma_1}, \circ_{\gamma_2})$ is given by $\gamma_{1,2}(a) = \gamma_1(a)^{-1}\gamma_2(a)$. As $\gamma_{1,2}(A) \subseteq M$, so in particular it is abelian, we find that $(A, \circ_{\gamma_1}, \circ_{\gamma_2})$ is γ-homomorphic by Lemma 2.9. $\qquad\square$

Example 6.7. Let R be a ring with unity (not necessarily commutative), and for all $x \in R$, define the following map:

$$\gamma_x \colon R^2 \to \mathrm{Aut}(R^2, +), \quad \begin{pmatrix} r \\ s \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ xr & 1 \end{pmatrix}.$$

We note the following facts:

- For all $x \in R$,

$$\gamma_x(R^2) \subseteq M = \left\{ \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \mid y \in R \right\},$$

  and M is clearly abelian.
- For all $x \in R$, we have that γ_x is a group homomorphism.
- For all $x \in R$, $a \in R^2$, and $\psi \in M$, we have $\gamma_x(\psi(a)) = \gamma_x(a)$.

We conclude that $((R^2, \circ_x) \mid x \in R^2)$ is a brace block, where

$$\begin{pmatrix} r \\ s \end{pmatrix} \circ_x \begin{pmatrix} r' \\ s' \end{pmatrix} = \begin{pmatrix} r + r' \\ s + s' + xrr' \end{pmatrix}.$$

Moreover, all the operations are distinct, because for all $x \in R$,

$$\gamma_x \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}.$$

Assume that R is commutative and that for all $r \in R$ there exists a unique $r' \in R$ such that $2r' = r^2 - r$ (by abuse of notation, we say $r' = \frac{r^2 - r}{2}$), which is for example the case if R is $\mathbb{Z}$ or an algebra over a field of characteristic different from 2. It is straightforward to verify that we have a group isomorphism

$$\theta \colon (R^2, +) \to (R^2, \circ_{\gamma_x}), \quad \begin{pmatrix} r \\ s \end{pmatrix} \mapsto \begin{pmatrix} r \\ s + \frac{x(r^2 - r)}{2} \end{pmatrix}.$$

Example 6.8. If in the previous example we take $R = \mathbb{Z}$, we find that if $x \neq \pm y$ then $(\mathbb{Z}^2, +, \circ_{\gamma_x}) \not\cong (\mathbb{Z}^2, +, \circ_{\gamma_y})$. Indeed,

$$\begin{pmatrix} r \\ s \end{pmatrix} * \begin{pmatrix} r' \\ s' \end{pmatrix} = \begin{pmatrix} 0 \\ xrr' \end{pmatrix}$$

and therefore $(\mathbb{Z}^2, +, \circ_{\gamma_x})/(\mathbb{Z}^2, +, \circ_{\gamma_x})^2 \cong \mathrm{Triv}(\mathbb{Z} \times C_{|x|})$. This nicely contrasts the case of additive group $\mathbb{Z}$, where only 2 distinct group operations $\circ$ giving a skew brace $(\mathbb{Z}, +, \circ)$ are possible, as we have recalled in section 4.

One can show that the skew braces $(\mathbb{Z}^2, +, \circ_{\gamma_x})$ are isomorphic to the λ-cyclic skew braces with infinite cyclic image constructed in [BNY22a, Section 4].

Example 6.9. Let us reconsider Example 6.7 with R a field of characteristic not 2. As explained above, we obtain a brace block $((R^2, \circ_{\gamma_x}) \mid x \in R)$, where $(R^2, +) \cong (R^2, \circ_{\gamma_x})$ for all $x \in R$. We claim that in this case all bi-skew brace of the form $(R^2, \circ_x, \circ_y)$, where $x, y \in R$ and $x \neq y$, are isomorphic. For this, it suffices to check that an isomorphism of skew braces is given by

$$\theta \colon (R^2, +, \circ_{\gamma_1}) \to (R^2, \circ_{\gamma_x}, \circ_{\gamma_y}), \quad \begin{pmatrix} r \\ s \end{pmatrix} \mapsto \begin{pmatrix} r \\ (y-x)s + \frac{x(r^2-r)}{2} \end{pmatrix}.$$

Let now G and H be groups. We have seen in section 3 that semidirect products of the form $\mathrm{Triv}(G) \ltimes \mathrm{Triv}(H)$, respectively $\mathrm{opTriv}(G) \ltimes \mathrm{Triv}(H)$, are an easy way to construct γ-homomorphic skew braces, respectively bi-skew braces. It is therefore natural to try to generalise this construction in order to obtain brace blocks.

For a group homomorphism $\alpha \colon G \to \mathrm{Aut}(H)$, we write $\circ_\alpha$ for the group operation on $G \times H$ given by the semidirect product of G and H.

Proposition 6.10. *Let G and H be groups, let M be an abelian subgroup of $\mathrm{Aut}(H)$, and let $\mathcal{S}$ be the set of group homomorphisms $\alpha \colon G \to M$. Then $((G \times H, \circ_\alpha) \mid \alpha \in \mathcal{S})$ is a brace block.*

Proof. For all $\alpha \in \mathcal{S}$, let γ_α be the gamma function associated with $(G \times H, \cdot, \circ_\alpha)$:

$$\gamma_\alpha \colon G \times H \to \mathrm{Aut}(G) \times \mathrm{Aut}(H) \subseteq \mathrm{Aut}(G \times H), \quad (g, h) \mapsto (\mathrm{id}, \alpha_g).$$

These images are all contained in the abelian subgroup $\{\mathrm{id}\} \times M$ of $\mathrm{Aut}(G \times H)$. In order to apply Theorem 6.6, it suffices to check that $\gamma_\alpha(\psi(g, h)) = \gamma_\alpha(g, h)$ for all $\alpha \in \mathcal{S}$, $\psi = (\mathrm{id}, \psi') \in \{\mathrm{id}\} \times M$, and $(g, h) \in G \times H$. We find

$$\gamma_\alpha(\psi(g, h)) = \gamma_\alpha(g, \psi'(h)) = (\mathrm{id}, \alpha_g) = \gamma_\alpha(g, h). \qquad \square$$

Example 6.11. For all $n \in \mathbb{N}$, define

$$\alpha_n \colon \mathbb{Z} \to \mathrm{GL}_2(\mathbb{Z}), \quad x \mapsto \begin{pmatrix} 1 & 0 \\ nx & 1 \end{pmatrix},$$

which is a well-defined group homomorphism. As

$$B = \left\{ \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \mid x \in \mathbb{Z} \right\}$$

is clearly an abelian subgroup of $\mathrm{GL}_2(\mathbb{Z})$, from Proposition 6.10 we obtain a brace block $((\mathbb{Z} \times \mathbb{Z}^2, \circ_n) \mid n \in \mathbb{N})$. More precisely,

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \circ_n \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} x + x' \\ y + y' \\ z + z' + nxy' \end{pmatrix}$$

In particular, if $n \neq m$, then $(\mathbb{Z} \times \mathbb{Z}^2, \circ_{\alpha_n})$ and $(\mathbb{Z} \times \mathbb{Z}^2, \circ_{\alpha_m})$ are nonisomorphic, as the abelianisation of $(\mathbb{Z} \times \mathbb{Z}^2, \circ_{\alpha_n})$ is isomorphic to $\mathbb{Z}^2 \times C_n$. We have thus obtained a brace block with countably many nonisomorphic groups.

Example 6.12. Let $(A, \cdot)$ be a group, and let B be a subgroup of A. Assume that the group of inner automorphisms of $(A, \cdot)$ induced by B, which we denote by $H(B)$, is abelian. It is easy to check that this is equivalent to $[B, B] \subseteq Z(A)$.

A straightforward verification shows that $\gamma(\psi(a)) = \gamma(a)$ for all group homomorphisms $\gamma \colon A \to H(B)$, $\psi \in H(B)$, and $a \in A$. This means that if we denote

by $\mathcal{S}$ the set of group homomorphisms from A to $H(B)$, we obtain a brace block $((A, \circ_\gamma) \mid \gamma \in \mathcal{S})$ with

$$a \circ_\gamma b = a \cdot {}^{\gamma(a)}b.$$

Note that the groups homomorphisms $A \to H(B)$ correspond precisely to the group homomorphisms $A \to B/(B \cap Z(A))$, because $H(B) \cong B/(B \cap Z(A))$. For example, every group homomorphism $\psi \colon A \to B$ yields a group homomorphism $A \to B/(B \cap Z(A))$, which we can use for our construction. Moreover, we have $\psi[A, A] \subseteq [B, B] \subseteq Z(A)$, so we find precisely the condition described in [CS21, Theorem 1.2]. In particular, when B is abelian, we recover [Koc21, Koc22]. Indeed, all the bi-skew braces found in these works are associated with gamma functions which act by conjugation and have a common abelian codomain; see also Remark 6.15. For a concrete application of this construction in Hopf–Galois theory, see [ST22, Theorem 4.9].

Example 6.13. We show now how the main construction of [CS22] follows from Theorem 6.6. Let $(A, \cdot)$ be a group, let B be a subgroup of $(A, \cdot)$ such that $[B, B]$ is contained in $Z(A)$ (so that $H(B)$, defined as before, is abelian), and let K be a subgroup of B contained in $Z(A)$. (Note that we do not require that B/K is abelian.) Define

$$\mathcal{A} = \{\psi \colon A/K \to B/K \text{ group homomorphism}\},$$

$$\mathcal{B} = \{\alpha \colon A \times A \to K \mid \alpha \text{ is bilinear and } \alpha(A, K) = \alpha(K, A) = \{1\}\}.$$

For all $\psi \in \mathcal{A}$ and $\alpha \in \mathcal{B}$, define

$$a \circ_{\psi, \alpha} b = a \cdot \psi(a) \cdot b \cdot \psi(a)^{-1} \cdot \alpha(a, b),$$

where with a little abuse of notation we write $\psi(a)$ for any element in the coset $\psi(aK)$. In [CS22] it is shown that this construction is well-defined, and that moreover $((A, \circ_{\psi, \alpha}) \mid (\psi, \alpha) \in \mathcal{A} \times \mathcal{B})$ is a brace block. We can write

$$a \circ_{\psi, \alpha} b = a \cdot {}^{\gamma_1(a)\gamma_2(a)}b,$$

where $\gamma_1(a)$ denotes conjugation by $\psi(a)$ and $\gamma_2(a) \colon b \mapsto b \cdot \alpha(a, b)$. Consider now the following subgroup of the central automorphisms of $(A, \cdot)$:

$$L = \{\delta \in \operatorname{Aut}(A, \cdot) \mid \delta(b) \cdot b^{-1} \in K \text{ and } \delta(k) = k \text{ for all } b \in A \text{ and } k \in K\}.$$

The group L is abelian and it centralises the subgroup of inner automorphisms of $\operatorname{Aut}(A, \cdot)$, so that $M = H(B)L$ is abelian. Now define $\mathcal{S}$ as in Theorem 6.6, with respect to M. It is just a matter of computation to show that the group homomorphism $a \mapsto \gamma_1(a)\gamma_2(a)$ is an element of $\mathcal{S}$, so we apply Theorem 6.6 to derive our claim.

Note that in fact there is no need for the codomain of the maps in $\mathcal{A}$ to be B/K. We could just consider group homomorphisms from A/K to $B/(B \cap Z(A))$ and find that the construction still works. This means that we do not require any relation between K and B; in this way we find a further generalisation of the original construction.

We now use Theorem 6.6 to obtain an iterative construction of brace blocks.

Corollary 6.14. *Let $(A, \cdot, \circ)$ be a γ-homomorphic bi-skew brace, and for all $n \in \mathbb{Z}$ and $a \in A$, let $\gamma_n(a) = \gamma(a^n) = \gamma(a)^n$. Then $((A, \circ_n) \mid n \in \mathbb{Z})$ is a brace block, where*

$$a \circ_n b = a \cdot {}^{\gamma_n(a)}b.$$

Proof. Apply Theorem 6.6 with $M = \gamma(A)$, which is abelian by Lemma 2.9. $\square$

Remark 6.15. This construction presents some similarities with Koch's construction [Koc22] (or more precisely, the variation presented in [CS22, Example 5.2]), but the operations we find are different. Indeed, let $(A, \cdot)$ be a group, and let ψ be an abelian endomorphism. Then $(A, \cdot, \circ)$ is a γ-homomorphic bi-skew brace, where $\gamma(a)$ is conjugation by $\psi(a)$. Both constructions yield a brace block $((A, \circ_n) \mid n \in \mathbb{Z})$, where

$$a \circ_n b = a \cdot \psi_n(a) \cdot b \cdot \psi_n(a)^{-1}.$$

In Koch's case, $\psi_n(a) = \prod_{i=1}^{n} \psi^i \left(a^{\binom{n}{i}} \right)$, while in our case, $\psi_n(a) = \psi(a^n)$.

Remark 6.16. Corollary 6.14, which is a natural application of Theorem 6.6, also recently appeared in [BNY22b, Theorem 4.12], where the approach followed is significantly different.

Example 6.17. Let

$$\gamma \colon \mathbb{Z}^2 \to \mathrm{GL}_2(\mathbb{Z}), \quad \begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}.$$

This clearly is a gamma function which provides a γ-homomorphic bi-skew brace, and applying Corollary 6.14 to γ, we find precisely the γ_n, $n \in \mathbb{N}$, as in Example 6.8. In particular, our iterative construction yields a brace block containing countably many nonisomorphic skew braces.

It is natural to ask whether a similar construction as Corollary 6.14 is still possible when we are not necessarily starting from a γ-homomorphic bi-skew brace. The following proposition shows that this is indeed the case.

Proposition 6.18. *Let A be a skew brace, and let ψ a group endomorphism of $(A, \cdot)$ such that for all $a, b \in A$, the equation*

$$\psi(^{\gamma(\psi(a))}b) = {}^{\gamma(\psi(a))}(\psi(b))$$

holds. Then $(A, \cdot, \circ_\psi)$ is skew brace, where

$$a \circ_\psi b = a \cdot {}^{\gamma(\psi(a))}b.$$

Proof. It suffices to prove that the map $A \mapsto \mathrm{Aut}(A, \cdot)$ given by $a \mapsto \gamma(\psi(a))$ is a gamma function on $(A, \cdot)$. For all $a, b \in A$, we find that

$$\gamma(\psi(a \cdot {}^{\gamma(\psi(a))}b)) = \gamma(\psi(a) \cdot {}^{\gamma(\psi(a))}\psi(b)) = \gamma(\psi(a) \circ \psi(b)) = \gamma(\psi(a))\gamma(\psi(b)). \quad \square$$

The relation with Corollary 6.14 is especially clear when we look at the following straightforward corollary, which in particular applies to Jacobson radical rings.

Corollary 6.19. *Let $(A, \cdot, \circ)$ be a (two-sided) brace. Then $(A, \cdot, \circ_n)$ is a (two-sided) brace for all $n \in \mathbb{Z}$, where*

$$a \circ_n b = a \cdot {}^{\gamma(a^n)}b.$$

Proof. The fact that $(A, \cdot, \circ_n)$ is a brace follows by applying Proposition 6.18, with $\psi \colon a \to a^n$. A straightforward calculation shows that if $(A, \cdot, \circ)$ is two-sided, then also $(A, \cdot, \circ_n)$ is two-sided. $\square$

Acknowledgment

References

[AD95] Bernhard Amberg and Oliver Dickenschied, *On the adjoint group of a radical ring*, Canad. Math. Bull. **38** (1995), no. 3, 262–270. MR 1347297

[Bac18] David Bachiller, *Solutions of the Yang–Baxter equation associated to skew left braces, with applications to racks*, J. Knot Theory Ramifications **27** (2018), no. 8, 1850055, 36. MR 3835326

[BCJO19] D. Bachiller, F. Cedó, E. Jespers, and J. Okniński, *Asymmetric product of left braces and simplicity; new solutions of the Yang–Baxter equation*, Commun. Contemp. Math. **21** (2019), no. 8, 1850042, 30. MR 4020748

[BNY22a] Valeriy G. Bardakov, Mikhail V. Neshchadim, and Manoj K. Yadav, *On λ-homomorphic skew braces*, J. Pure Appl. Algebra **226** (2022), no. 6, Paper No. 106961, 37. MR 4346001

[BNY22b] _____, *Symmetric skew braces and brace systems*, arXiv:2204.12247, 2022.

[Byo15] Nigel P. Byott, *Solubility criteria for Hopf-Galois structures*, New York J. Math. **21** (2015), 883–903. MR 3425626

[Car18] A. Caranti, *Multiple holomorphs of finite p-groups of class two*, J. Algebra **516** (2018), 352–372. MR 3863482

[Car20] _____, *Bi-skew braces and regular subgroups of the holomorph*, J. Algebra **562** (2020), 647–665. MR 4130907

[Ced18] Ferran Cedó, *Left braces: solutions of the Yang-Baxter equation*, Adv. Group Theory Appl. **5** (2018), 33–90. MR 3824447

[CGK+21] Lindsay N. Childs, Cornelius Greither, Kevin P. Keating, Alan Koch, Timothy Kohl, Paul J. Truman, and Robert G. Underwood, *Hopf algebras and Galois module theory*, Mathematical Surveys and Monographs, vol. 260, American Mathematical Society, Providence, RI, [2021] ©2021. MR 4390798

[Chi00] Lindsay N. Childs, *Taming wild extensions: Hopf algebras and local Galois module theory*, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, Providence, RI, 2000. MR 1767499

[Chi19] _____, *Bi-skew braces and Hopf Galois structures*, New York J. Math. **25** (2019), 574–588. MR 3982254

[CJK+23] F. Cedó, E. Jespers, Ł. Kubat, A. Van Antwerpen, and C. Verwimp, *On various types of nilpotency of the structure monoid and group of a set-theoretic solution of the Yang–Baxter equation*, J. Pure Appl. Algebra **227** (2023), no. 2, Paper No. 107194, 38. MR 4457900

[CS21] A. Caranti and L. Stefanello, *From endomorphisms to bi-skew braces, regular subgroups, the Yang–Baxter equation, and Hopf–Galois structures*, J. Algebra **587** (2021), 462–487. MR 4304796

[CS22] _____, *Brace blocks from bilinear maps and liftings of endomorphisms*, J. Algebra **610** (2022), 831–851. MR 4473766

[CSV19] Ferran Cedó, Agata Smoktunowicz, and Leandro Vendramin, *Skew left braces of nilpotent type*, Proc. Lond. Math. Soc. (3) **118** (2019), no. 6, 1367–1392. MR 3957824

[Dri92] V. G. Drinfel'd, *On some unsolved problems in quantum group theory*, Quantum groups (Leningrad, 1990), Lecture Notes in Math., vol. 1510, Springer, Berlin, 1992, pp. 1–8. MR 1183474

[ESS99] Pavel Etingof, Travis Schedler, and Alexandre Soloviev, *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Math. J. **100** (1999), no. 2, 169–209. MR 1722951

[GV17] L. Guarnieri and L. Vendramin, *Skew braces and the Yang–Baxter equation*, Math. Comp. **86** (2017), no. 307, 2519–2534. MR 3647970

[JPZD20]   Přemysl Jedlička, Agata Pilitowska, and Anna Zamojska-Dzienio, *The construction of multipermutation solutions of the Yang-Baxter equation of level 2*, J. Combin. Theory Ser. A **176** (2020), 105295, 35. MR 4123749

[Koc21]   Alan Koch, *Abelian maps, bi-skew braces, and opposite pairs of Hopf-Galois structures*, Proc. Amer. Math. Soc. Ser. B **8** (2021), 189–203. MR 4273165

[Koc22]   ⎯⎯⎯, *Abelian maps, brace blocks, and solutions to the Yang-Baxter equation*, J. Pure Appl. Algebra **226** (2022), no. 9, Paper No. 107047. MR 4381676

[KSV21]   Alexander Konovalov, Agata Smoktunowicz, and Leandro Vendramin, *On skew braces and their ideals*, Exp. Math. **30** (2021), no. 1, 95–104. MR 4223285

[KT20]   Alan Koch and Paul J. Truman, *Opposite skew left braces and applications*, J. Algebra **546** (2020), 218–235. MR 4033084

[LV19]   Victoria Lebed and Leandro Vendramin, *On structure groups of set-theoretic solutions to the Yang–Baxter equation*, Proc. Edinb. Math. Soc. (2) **62** (2019), no. 3, 683–717. MR 3974961

[LYZ00]   Jiang-Hua Lu, Min Yan, and Yong-Chang Zhu, *On the set-theoretical Yang-Baxter equation*, Duke Math. J. **104** (2000), no. 1, 1–18. MR 1769723

[Nas19]   Timur Nasybullov, *Connections between properties of the additive and the multiplicative groups of a two-sided skew brace*, J. Algebra **540** (2019), 156–167. MR 4003478

[NV06]   Sam Nelson and John Vo, *Matrices and finite biquandles*, Homology Homotopy Appl. **8** (2006), no. 2, 51–73. MR 2246021

[Rum07a]   Wolfgang Rump, *Braces, radical rings, and the quantum Yang–Baxter equation*, J. Algebra **307** (2007), no. 1, 153–170. MR 2278047

[Rum07b]   ⎯⎯⎯, *Classification of cyclic braces*, J. Pure Appl. Algebra **209** (2007), no. 3, 671–685. MR 2298848

[Smo18]   Agata Smoktunowicz, *On Engel groups, nilpotent groups, rings, braces and the Yang-Baxter equation*, Trans. Amer. Math. Soc. **370** (2018), no. 9, 6535–6564. MR 3814340

[Sol00]   Alexander Soloviev, *Non-unitary set-theoretical solutions to the quantum Yang-Baxter equation*, Math. Res. Lett. **7** (2000), no. 5-6, 577–596. MR 1809284

[Spa22]   Filippo Spaggiari, *The mutually normalizing regular subgroups of the holomorph of a cyclic group of prime power order*, Communications in Algebra (2022), 1–31.

[ST22]   L. Stefanello and S. Trappeniers, *On the connection between Hopf–Galois structures and skew braces*, arXiv:2206.07610, 2022.

[SV18]   Agata Smoktunowicz and Leandro Vendramin, *On skew braces (with an appendix by N. Byott and L. Vendramin)*, J. Comb. Algebra **2** (2018), no. 1, 47–86. MR 3763907

[Ven19]   Leandro Vendramin, *Problems on skew left braces*, Adv. Group Theory Appl. **7** (2019), 15–37. MR 3974481

[Wat68]   J. F. Watters, *On the adjoint group of a radical ring*, J. London Math. Soc. **43** (1968), 725–729. MR 229677

Department of Mathematics, Università di Pisa, Largo Bruno Pontecorvo 5, 56127 Pisa, Italy

Email address: `lorenzo.stefanello@phd.unipi.it`

URL: `https://people.dm.unipi.it/stefanello/`

Department of Mathematics and Data Science, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium

Email address: `senne.trappeniers@vub.be`