# FACTORIZATIONS OF SKEW BRACES

E. JESPERS, Ł. KUBAT, A. VAN ANTWERPEN, L. VENDRAMIN

ABSTRACT. We introduce strong left ideals of skew braces and prove that they produce non-trivial decomposition of set-theoretic solutions of the Yang–Baxter equation. We study factorization of skew left braces through strong left ideals and we prove analogs of Itô's theorem in the context of skew left braces. As a corollary, we obtain applications to the retractability problem of involutive non-degenerate solutions of the Yang–Baxter equation. Finally, we classify skew braces that contain no non-trivial proper ideals.

## INTRODUCTION

An important family of finite set-theoretic solutions of the Yang–Baxter equation is that of involutive non-degenerate multipermutation solutions. Such solutions first appeared in the work [13] of Etingof, Schedler, and Soloviev as generalizations of Lyubachenko's permutation solutions. Now, these solutions appear in many different contexts: it is known, for example, that a finite involutive non-degenerate solution is multipermutation if and only if its structure group is left orderable [4,12,19]. The structure group of a finite solution has a particularly important finite quotient known as the permutation group of the solution. It is natural to ask which group-theoretical properties of permutation groups detect multipermutation solutions. There are strong results in this directions [7,14,15,22,23,25]. However, to understand multipermutation solutions it is not enough to know the group structure of their permutation groups. One really needs to understand deeply the permutation group of a solution, meaning that one needs to understand this as a brace. Braces (and more generally skew braces) are generalizations of radical rings that turn out to provide the right algebraic framework to study set-theoretic solutions of the Yang–Baxter equation [16,23]. Skew braces are intensively studied, as they are known to have connections to several different topics [2,8,11,24,26]. The structure group and the permutation group of a solution are examples of skew braces. So these groups are not merely groups: there is some deep ring-theoretic information hidden behind these groups associated with set-theoretic solutions.

In this work, we study involutive non-degenerate (multipermutation) solutions by means of the skew brace structure of their permutation groups and via factorizations of this skew brace. Our first main result is a sort of analog of Itô's celebrated theorem on metabelian groups, but now in the context of skew braces. As an application, we understand better involutive non-degenerate (multipermutation) solutions. We also show that in some sense our Itô's theorem cannot be improved naively, meaning that we cannot expect a result similar to that of Kegel–Wielandt on products of nilpotent groups being solvable. It is interesting to remark that recently Sysak asked about extending the results of factorization of groups to skew braces. We know precisely which is the setting in which the results of factorization can be studied in the skew brace situation. This is why we introduce strong left

ideals. We show that these strong left ideals are related to non-trivial decomposability of solutions. Decomposable solutions also were introduced by Etingof, Schedler, and Soloviev in [13], the same paper where multipermutation solutions were first considered. With concrete examples, we show that our method for studying multipermutation solutions gives deeper insights. Indeed, there are solutions where group theory is not enough to detect multipermutability and where this property can be easily recognized by means of the brace factorization.

As another application of skew brace factorization we obtain several results on the structure of skew left braces. In the final main result we consider characteristic ideals of skew left braces and we characterise skew left braces that are characteristically simple. They turn out to be factorizable into copies of a simple skew left subbrace.

The paper is organized as follows. In Section 1 we review some basics on skew left braces and we introduce strong left ideals. In Proposition 1.5 we show that strong left ideals yield non-trivial decomposable solutions of the Yang–Baxter equation. In Section 2 we introduce factorizations of skew left braces and prove our main results in Theorems 2.5 and 2.9. These results can be seen as analogs of well-known theorems of Itô. In Corollary 2.12 we apply these results to set-theoretic involutive non-degenerate solutions of the Yang–Baxter equation. In Section 3 we introduce characteristic ideals of skew braces and we classify finite skew left braces that do not contain non-trivial characteristic ideals.

## 1. Skew braces and strong left ideals

A *skew left brace* is a triple $(A, +, \circ)$, where $(A, +)$ and $(A, \circ)$ are groups and, for all $a, b, c \in A$, the following compatibility condition holds

$$a \circ (b + c) = a \circ b - a + a \circ c.$$

The group $(A, +)$ is called the *additive group* of $A$ and $(A, \circ)$ is called the *multiplicative group* of $A$. For $a \in A$ we denote by $a'$ the inverse of $a$ with respect to the circle operation $\circ$. By convention, left braces will be those skew left braces with abelian additive group. A skew left brace $A$ is said to be *trivial* if both operations $+$ and $\circ$ coincide, i.e., if $a + b = a \circ b$ for all $a, b \in A$. If $A$ is a skew left brace, then the map $\lambda \colon (A, \circ) \to \mathrm{Aut}(A, +)$, $a \mapsto \lambda_a$, where $\lambda_a(b) = -a + a \circ b$, is a group homomorphism. It follows that

$$a \circ b = a + \lambda_a(b), \quad a + b = a \circ \lambda_a^{-1}(b), \quad \lambda_a(a') = -a \qquad (1.1)$$

for all $a, b \in A$.

For elements $a$ and $b$ of a skew left brace $A$ we put

$$a * b = \lambda_a(b) - b = -a + a \circ b - b.$$

The operation $*$ measures the "difference" between the additive and multiplicative operations. In particular, if for all $a, b \in A$ we have $a * b = 0$, then both operations are the same, i.e., the skew left brace simply reduces to a group; and thus for braces this is an abelian group.

**Lemma 1.1.** *Let $A$ be a skew left brace. For any $x, y, z \in A$ the following statements hold:*

(1) $x * (y + z) = x * y + y + x * z - y,$
(2) $(x \circ y) * z = x * (y * z) + y * z + x * z.$

*Proof.* As $\lambda_x \colon (A,+) \to (A,+)$ is a group homomorphism, it follows that

$$\begin{aligned} x * (y + z) &= \lambda_x(y+z) - z - y \\ &= \lambda_x(y) + \lambda_x(z) - z - y \\ &= x * y + y + x * z - y. \end{aligned}$$

Since $\lambda \colon (A,\circ) \to \operatorname{Aut}(A,+)$ is a group homomorphism,

$$\begin{aligned} (x \circ y) * z &= \lambda_{x \circ y}(z) - z \\ &= \lambda_x(\lambda_y(z)) - z \\ &= \lambda_x(y * z) + \lambda_x(z) - z \\ &= x * (y * z) + y * z + x * z. \qquad \square \end{aligned}$$

Note that if we replace both $+$ and $\circ$ by a single operation, and $*$ by the ordinary commutator corresponding to this new operation, then in the previous lemma we obtain well-known commutator formulas from group theory. Thus, intuitively, one can understand this operation as an analog of the group-theoretical commutator. In this spirit, a trivial skew left brace corresponds with an "abelian structure". As we will show later, this inspires a counterpart to the Itô theorem on metabelian groups in the context of skew left braces. However, this analogy fails for other properties defined by commutators (e.g., nilpotency, solvablility, ... ).

**Remark 1.2.** Using the formulas of (1.1) we obtain that

$$\begin{aligned} a \circ b \circ a' &= a + \lambda_a(b \circ a') \\ &= a + \lambda_a(b + b * a' + a') \\ &= a + \lambda_a(b + b * a') - a \end{aligned}$$

for all $a, b \in A$.

A *left ideal* of a skew left brace $A$ is a subgroup $I$ of $(A,+)$ such that $\lambda_a(I) \subseteq I$ for all $a \in A$, which is equivalent to $a * b \in I$ for all $a \in A$ and $b \in I$. It follows that a left ideal is a skew left subbrace and, in particular, $(I,\circ)$ is a subgroup of $(A,\circ)$. Moreover, if $(I,\circ)$ is normal in $(A,\circ)$ and $(I,+)$ is normal in $(A,+)$ then one says that $I$ is an *ideal* of $A$. It is known that ideals of skew braces correspond bijectively to kernels of skew brace homomorphisms. The socle $\operatorname{Soc}(A)$ of a skew left brace $A$ is defined as

$$\operatorname{Soc}(A) = \operatorname{Ker}\lambda \cap \operatorname{Z}(A,+)$$

and it is an ideal of $A$.

**Definition 1.3.** Let $(A,+,\circ)$ be a skew left brace. A left ideal $I$ is called a *strong left ideal* if $(I,+)$ is a normal subgroup of $(A,+)$.

**Example 1.4.** A characteristic subgroup of the additive group of a skew left brace is a strong left ideal. Furthermore, ideals are strong left ideals.

Braces were introduced by Rump in [23] as an algebraic tool to study involutive non-degenerate set-theoretic solutions of the Yang–Baxter equation. A *set-theoretic solution* of the Yang–Baxter equation is a pair $(X,r)$, where $X$ is a set and $r \colon X \times X \to X \times X$ is a bijective map such that

$$(r \times \operatorname{id})(\operatorname{id} \times r)(r \times \operatorname{id}) = (\operatorname{id} \times r)(r \times \operatorname{id})(\operatorname{id} \times r).$$

If we write $r(x,y) = (\sigma_x(y), \tau_y(x))$, then $(X,r)$ is said to be *non-degenerate* if all maps $\sigma_x, \tau_x \colon X \to X$ are bijective.

A set-theoretic solution $(X,r)$ is called *decomposable* if there exists a non-trivial partition $X = Y \cup Z$ such that $(Y, r|_{Y \times Y})$ and $(Z, r|_{Z \times Z})$ are set-theoretic solutions and $r(Y \times Z) = Z \times Y$ and $r(Z \times Y) = Y \times Z$.

Skew left braces produce non-degenerate solutions of the Yang–Baxter equation: if $A$ is a skew left brace, then the pair $(A, r_A)$, where

$$r_A \colon A \times A \to A \times A, \quad r_A(a, b) = (\lambda_a(b), \lambda_a(b)' \circ a \circ b),$$

is a non-degenerate solution of the Yang–Baxter equation. Moreover, $(A, r_A)$ is involutive (i.e., $r_A^2 = \mathrm{id}$) if and only if the group $(A, +)$ is abelian.

The set-theoretic solution $(A, r_A)$ associated to a non-zero skew left brace $A$ is always decomposable as $A = \{0\} \cup A \setminus \{0\}$. We show that strong left ideals of $A$ provide more decompositions of $(A, r_A)$.

**Proposition 1.5.** *Let $A$ be a skew left brace. If there exists a proper strong left ideal $I$, then $(A, r_A)$ is decomposable as $A = I \cup A \setminus I$.*

*Proof.* Let $I$ be a proper strong left ideal. As $I$ is a left ideal, it holds, for any $x \in A$, that $\lambda_x(I) = I$. Moreover, $\lambda_x(A \setminus I) = A \setminus I$. Let $x \in A$ and $a \in I$. Let $\rho_x(a) = \lambda_a(x)' \circ a \circ x$. Then

$$\rho_x(a) = \lambda_a(x)' \circ a \circ x = (a' \circ \lambda_{a'}^{-1}(x))' \circ x = (a' + x)' \circ x.$$

As $I$ is normal in $(A, +)$ this is equal to $(x + b)' \circ x$ for some $b \in I$. As $I$ is a left ideal, there exists $c \in I$ such that the previous is equal to

$$(x \circ c)' \circ x = c' \circ x' \circ x = c' \in I.$$

Hence $\rho_x(I) = I$. By [2, Lemma 2.4], $\rho_x(A \setminus I) = A \setminus I$ and hence the claim follows. $\qquad\square$

## 2. Skew left braces admitting a factorization

In this section we study skew left braces $A$ such that $A = B + C$ for left ideals $B$ and $C$. Observe that in this case it follows from (1.1) that

$$A = B + C = C + B = B \circ C = C \circ B.$$

**Definition 2.1.** Let $A$ be a skew left brace and let $B$ and $C$ be left ideals of $A$. We say that $A$ admits a *factorization* through $B$ and $C$ if $A = B + C$.

We will study the case where $B$ and $C$ are trivial skew left braces. For that purpose, we shall need the following lemma.

**Lemma 2.2.** *Let $A$ be a skew left brace such that $A = B + C$, where $B$ and $C$ are left ideals. If $B$ and $C$ are trivial as skew left braces then, for any $b, \beta \in B$ and $c, \gamma \in C$ and $a \in A$, the following statements hold:*

(1) $\lambda_{\beta \circ \gamma} = \lambda_{\gamma \circ \beta}$,
(2) $(c + b) \circ \beta - \beta = c + b + c * \beta$,
(3) $b \circ c \circ b' \circ c' = b \circ c - c \circ b = b + \lambda_b(c) - \lambda_c(b) - c \in \operatorname{Ker} \lambda$.

*Proof.* To prove (1) put $c_1 = \lambda_\beta(c) \in C$ and $b_1 = \lambda_\gamma(b) \in B$. Then, as $B$ and $C$ are trivial skew left braces,

$$\lambda_\beta(b + c) = \lambda_\beta(b) + \lambda_\beta(c) = b + c_1,$$
$$\lambda_\gamma(b + c) = \lambda_\gamma(b) + \lambda_\gamma(c) = b_1 + c.$$

Hence,

$$\lambda_{\beta \circ \gamma}(b + c) = b_1 + c_1 = \lambda_{\gamma \circ \beta}(b + c).$$

Let us prove (2). As $B$ is a trivial skew left brace, it follows from (1.1) that

$$
\begin{aligned}
(c + b) \circ \beta - \beta &= (c \circ \lambda_{c'}(b)) \circ \beta - \beta \\
&= c \circ (\lambda_{c'}(b) \circ \beta) - \beta \\
&= c \circ (\lambda_{c'}(b) + \beta) - \beta \\
&= c \circ \lambda_{c'}(b) - c + c \circ \beta - \beta \\
&= c + b + c * \beta.
\end{aligned}
$$

Part (3) follows from the following computation

$$
\begin{aligned}
b \circ c \circ b' \circ c' &= (b \circ c) + \lambda_{b \circ c}(b' + \lambda_{b'}(c')) \\
&= b + \lambda_b(c) + \lambda_{b \circ c}(b') + \lambda_{b \circ c \circ b'}(c') \\
&= b + \lambda_b(c) + \lambda_c(b') + \lambda_{b \circ b'}(c') \\
&= b + \lambda_b(c) + \lambda_c(-b) - c \\
&= b \circ c - c \circ b.
\end{aligned}
$$

Moreover, by (1) it follows that $b \circ c \circ b' \circ c' \in \operatorname{Ker} \lambda$.                $\square$

If $X$ and $Y$ are non-empty subsets of a skew left brace $A$, we define $X * Y$ as the additive subgroup of $A$ generated by all elements of the form $x * y$, where $x \in X$ and $y \in Y$. One defines $A^{(1)} = A$ and $A^{(n)} = A^{(n-1)} * A$ for $n \geqslant 2$. Then

$$
A^{(1)} \supseteq A^{(2)} \supseteq A^{(3)} \supseteq \cdots
$$

is a chain of ideals of $A$ known as the *right series* of $A$, see [10, Proposition 2.1]. Following Rump [23], the skew left brace $A$ is said to be *right nilpotent* of class $m$ if $A^{(m)} = 0$ and $A^{(m-1)} \neq 0$.

**Definition 2.3.** A skew left brace $A$ is said to be *meta-trivial* if $A^{(2)}$ is a trivial skew left brace. Equivalently, there exists an ideal $I$ of $A$ such that $I$ and $A/I$ are trivial as skew left braces.

A left ideal $I$ of a skew left brace $A$ is said to be *meta-trivial* if $I$ is meta-trivial as a skew left brace.

**Lemma 2.4.** *Let $A$ be a skew left brace such that $A = B + C$ is a factorization through left ideals $B$ and $C$. If $B$ and $C$ are trivial skew left braces, then:*

(1) $B * C$ *and* $C * B$ *are strong left ideals of $A$,*
(2) $B * C$ *and* $C * B$ *are trivial skew left braces, and*
(3) $A^{(2)} = C * B + B * C = B * C + C * B$.

*Proof.* Since $C$ is a left ideal, it follows that $B * C \subseteq C$. Let $b, \beta \in B$ and $c, \gamma \in C$. As $C$ is trivial, it follows that

$$
\begin{aligned}
\lambda_{b \circ c}(\beta * \gamma) &= \lambda_b(\beta * \gamma) \\
&= \lambda_b \lambda_\beta(\gamma) - \lambda_b(\gamma) \\
&= \lambda_{b \circ \beta \circ b'} \lambda_b(\gamma) - \lambda_b(\gamma) \\
&= (b \circ \beta \circ b') * \lambda_b(\gamma) \in B * C.
\end{aligned}
$$

Hence $B * C$ is a left ideal and trivial as a skew left brace.

Let $a \in A$, $b \in B$ and $c \in C$. Write $a = b_1 + c_1$, with $b_1 \in B$ and $c_1 \in C$. Then, by Lemma 1.1,

$$
\begin{aligned}
a + (b * c) - a &= a + \lambda_b(c) - c - a \\
&= -(b * a) + b * (a + c) \\
&= -(b * (b_1 + c_1)) + b * (b_1 + c_1 + c).
\end{aligned}
\tag{2.1}
$$

Now, as $B + C = C + B$, it follows that for any $\beta \in B$ and $\gamma \in C$, there exist $\beta_1 \in B$ and $\gamma_1 \in C$ such that $\beta + \gamma = \gamma_1 + \beta_1$. Hence, for any $b \in B$ it holds, by Lemma 1.1, that

$$b * (\beta + \gamma) = b * (\gamma_1 + \beta_1) = b * \gamma_1 + \gamma_1 + b * \beta_1 - \gamma_1 = b * \gamma_1,$$

as $B$ is trivial. Applying this on (2.1) it follows that $B * C$ is a normal subgroup of $(A, +)$. This proves (1) and (2) for $B * C$. The proof for $C * B$ is similar.

Now we show that $A^{(2)} \subseteq C * B + B * C$. Let $b, b_1 \in B$ and $c, c_1 \in C$. Then, by Lemma 1.1,

$$
\begin{aligned}
(b \circ c) * (b_1 + c_1) &= (b \circ c) * b_1 + b_1 + (b \circ c) * c_1 - b_1 \\
&= \lambda_{b \circ c}(b_1) - b_1 + b_1 + b * (c * c_1) + c * c_1 + b * c_1 - b_1 \\
&= \lambda_c(b_1) - b_1 + b_1 + b * c_1 - b_1 \\
&= c * b_1 + b_1 + b * c_1 - b_1 \in C * B + B * C.
\end{aligned}
$$

Clearly $C * B + B * C \subseteq A^{(2)}$ and thus $A^{(2)} = C * B + B * C = B * C + C * B$. □

The possible approach to skew left brace factorization is through strong left ideals. In this setting we prove an analog of Itô's theorem [18] for skew left braces.

**Theorem 2.5.** *Let $A$ be a skew left brace. If $A = B + C$ is a factorization through strong left ideals $B$ and $C$ that are trivial as skew left braces, then $A$ is right nilpotent of class at most three. In particular, $A$ is meta-trivial.*

*Proof.* By Lemma 2.4, $B * C$ and $C * B$ are strong left ideals of $A$, and both are trivial as skew left braces. Furthermore,

$$A^{(2)} = B * C + C * B = (B * C) \circ (C * B).$$

It rests to show that $A^{(2)}$ acts trivially on $A$. We first show that $B * C$ acts trivially on $A$. For that purpose, let $b \in B$, $c \in C$ and $a \in A$. Write $a = \beta + \gamma$, where $\beta \in B$ and $\gamma \in C$. Then, again by Lemma 1.1,

$$(b * c) * (\beta + \gamma) = (b * c) * \beta + \beta + (b * c) * \gamma - \beta = (b * c) * \beta,$$

as $C$ is a trivial skew left brace. By Lemma 2.2(3),

$$(b \circ c - c \circ b) + \beta = (b \circ c - c \circ b) \circ \beta = (b + \lambda_b(c) - \lambda_c(b) - c) \circ \beta.$$

Since $(B, +)$ is a normal subgroup of $(A, +)$,

$$b \circ c - c \circ b = b + \lambda_b(c) - \lambda_c(b) - c = \lambda_b(c) - c + b_1$$

for some $b_1 \in B$. By Lemma 2.2(2),

$$
\begin{aligned}
(b \circ c - c \circ b) + \beta &= (\lambda_b(c) - c + b_1) \circ \beta \\
&= \lambda_b(c) - c + b_1 + (b * c) * \beta + \beta
\end{aligned}
$$

and therefore $(b * c) * \beta = 0$. Thus $B * C$ acts trivially on $A$. As $(C, +)$ also is a normal subgroup of $(A, +)$, it follows by symmetry that $C * B$ acts trivially on $A$. Hence $A^{(2)}$ acts trivially on $A$. □

**Corollary 2.6.** *Let $A$ be a skew left brace. Assume that $A = B + C$, where $B$ and $C$ are (not necessarily strong) left ideals, which are trivial as skew left braces. Then $A$ has a meta-trivial ideal $I$ such that $A/I$ is a trivial skew left brace.*

*Proof.* By Lemma 2.4, the ideal $A^{(2)}$ has a factorization through the strong left ideals $B * C$ and $C * B$, which are trivial skew left braces. Hence, by Theorem 2.5, $A^{(2)}$ is meta-trivial. Thus the claim follows. □

The assumptions of Theorem 2.5 cannot be relaxed. For the examples stated below we use GAP and the database of small skew left braces of [16], see [21, §2.1] for notation.

**Example 2.7.** The skew left brace $S(36, 271)$ has additive group isomorphic to $C_3 \times A_4$ and multiplicative group isomorphic to $C_6 \times S_3$ and can be factorized in left ideals $X$ and $Y$, which are trivial as skew left braces, where $|X| = 4$ and $|Y| = 9$. In this example, $X$ is a strong left ideal, but $Y$ is not. This skew left brace is not meta-trivial or left nilpotent. However, it is right nilpotent of class four.

The condition in the statement of Theorem 2.5 that both left ideals have to be normal in $(A, +)$ cannot be replaced by normality in $(A, \circ)$:

**Example 2.8.** The group $(G, +) = S_4$ can be exactly factorized by the subgroups $X = \langle (243) \rangle$ and $Y = \langle (34), (13)(24), (14)(23) \rangle$. The operation

$$(x + y) \circ (x_1 + y_1) = (x + x_1) + (y_1 + y)$$

turns $G$ into a skew left brace such that $G^{(2)}$ is not a trivial skew left brace. In this example, $Y$ is a left ideal and $X$ and $Y$ are normal in $(G, \circ)$.

**Theorem 2.9.** *Let $A$ be a non-zero skew left brace that has a factorization $A = B + C$ through left ideals $B$ and $C$, where both are trivial as skew left braces. If $B$ is a strong left ideal of $A$, then $B$ or $C$ contains a non-zero ideal $I$ of $A$ that acts trivially on $A$.*

*Proof.* By Lemma 2.4, it holds that $B * C$ and $C * B$ are trivial skew left braces, strong left ideals of $A$ and $A^{(2)} = B * C + C * B$. Using the same calculation as in Theorem 2.5, it follows that $B * C$ acts trivially on $A$. We show that $(B * C, \circ)$ is a normal subgroup of $(A, \circ)$. Let $b, \beta \in B$ and $c, \gamma \in C$. By Lemma 2.2, it holds that

$$c \circ b \circ (\beta * \gamma) \circ b' \circ c' = c \circ (b + \lambda_b(\beta * \gamma + \beta * b') - b) \circ c'$$
$$= c \circ (b + \lambda_b(\beta * \gamma) - b) \circ c'.$$

As $B * C$ is a strong left ideal, it is sufficient to show that $B * C$ is closed under conjugation of $(C, \circ)$. Let $b \in B$ and $c, \gamma \in C$. Then, as $C$ is a trivial skew left brace, it follows that

$$\gamma \circ b * c \circ \gamma' = \gamma + b * c - \gamma.$$

As $(B * C, +)$ is normal in $(A, +)$, this shows that $B * C$ is an ideal of $A$. If this is non-zero, then the theorem follows. If $B * C = 0$, then $A^{(2)} = C * B$. This shows that in this case $C * B$ is an ideal. If this is also zero, then $A^{(2)} = 0$ and hence $A$ is a trivial skew brace, $B$ and $C$ are ideals of $A$. $\square$

The conditions in the statement of Theorem 2.9 cannot be relaxed:

**Example 2.10.** There exists a skew left brace $A$ with $(A, +) \cong (C_3 \times C_3) \rtimes C_2$ and $(A, \circ) \cong C_3 \times S_3$. The skew brace $A$ can be written as the sum of two left ideals $X$ and $Y$, which are trivial as skew left braces, where $|X| = 6$ and $|Y| = 3$. However, no ideal of $A$ is contained in $X$ or $Y$.

**Corollary 2.11.** *Let $A = B + C$ be a skew left brace with a factorization through the left ideals $B$ and $C$, which are trivial as skew left braces. If $B$ is a strong left ideal of $A$, then $A$ is right nilpotent of class at most four.*

*Proof.* Notice that, by the proof of Theorem 2.9, $B * C$ is an ideal of $A$. Assume first that $B * C = 0$. Then $B * A = 0$. Moreover, $A^{(2)} = C * B \subseteq B$ by Lemma 2.4(3). Thus $A^{(3)} \subseteq B * A = 0$. Assume now that $B * C \neq 0$. Then the skew left brace $A/B * C$ is right nilpotent of class at most three by the previous case. Hence $A^{(3)} \subseteq B * C$. As, by the proof of Theorem 2.5, $B * C$ acts trivially on $A$, it follows that $A^{(4)} = 0$. $\square$

Our results on factorizations of skew left braces have applications to involutive non-degenerate solutions of the Yang–Baxter equation. Let $(X, r)$ be an involutive non-degenerate solution and write $r(x, y) = (\sigma_x(y), \tau_y(x))$. On $X$ one considers the equivalence relation given by

$$x \sim y \iff \sigma_x = \sigma_y.$$

Then $\sim$ induces an involutive non-degenerate solution on the set of equivalence classes of $X$ known as the *retraction* $\mathrm{Ret}(X, r)$ of $(X, r)$, see [13]. One defines inductively:

$$\mathrm{Ret}^0(X, r) = (X, r),$$
$$\mathrm{Ret}^1(X, r) = \mathrm{Ret}(X, r),$$
$$\mathrm{Ret}^n(X, r) = \mathrm{Ret}(\mathrm{Ret}^{n-1}(X, r)), \quad n \geqslant 2.$$

A solution $(X, r)$ is said to be *multipermutation* of level $m$ if $\mathrm{Ret}^m(X, r)$ has size one and $\mathrm{Ret}^{m-1}(X, r)$ has more than one element. Multipermutation solutions can be characterized in terms of left orderability of the structure group $G(X, r)$ of $(X, r)$, see [4, 12, 19]. This group is defined as the group generated by the elements of $X$ with relations

$$x \circ y = u \circ v \quad \text{whenever } r(x, y) = (u, v).$$

The group $G(X, r)$ is a left brace with $\circ$ as the multiplicative operation and the quotient left brace

$$\mathcal{G}(X, r) = G(X, r) / \mathrm{Soc}(G(X, r))$$

has multiplicative group isomorphic to the subgroup of $\mathrm{Sym}(X)$ generated by all $\lambda_x$ for $x \in X$, for details see [5, 8].

It is known [6, Proposition 6] that a non-zero left brace $A$ is right nilpotent of class $m$ if and only if its associated solution of the Yang–Baxter equation $(A, r_A)$ is a multipermutation solution of level $m - 1$. It is also known [14, Theorem 5.15] that an involutive non-degenerate (not necessarily finite) solution of the Yang–Baxter equation $(X, r)$ with $|X| \geqslant 2$ is a multipermutation solution of level not exceeding $m$ provided the solution $(G, r_G)$, where $G = G(X, r)$, is a multipermutation solution of level $m$. Both these results together with our Theorem 2.5 lead to an interesting information on involutive non-degenerate solutions of the Yang–Baxter equation.

**Corollary 2.12.** *Let $(X, r)$ be an involutive non-degenerate (not necessarily finite) solution of the Yang–Baxter equation with $|X| \geqslant 2$. If the left brace $\mathcal{G}(X, r)$ admits a factorization through left ideals, which are trivial as left braces, then $(X, r)$ is a multipermutation solution of level at most three.*

*Proof.* Let $A = \mathcal{G}(X, r)$ and $G = G(X, r)$. Then Theorem 2.5 yields $A^{(m)} = 0$ for some $m \leqslant 3$. Because $G / \mathrm{Soc}(G) \cong A$ as left braces, we get $G^{(m)} \subseteq \mathrm{Soc}(G)$, and thus $G^{(m+1)} = 0$. Hence $G$ is a right nilpotent left brace of class at most four and, by [6, Proposition 6], $(G, r_G)$ is a multipermutation solution of level at most three. Therefore, by [14, Theorem 5.15], $(X, r)$ is a multipermutation solution of level at most three. $\square$

This shows that properties of the involutive non-degenerate set-theoretic solution $(X, r)$ are not completely determined by the group theory of the additive and multiplicative groups of the left brace $\mathcal{G}(X, r)$. The following examples clarify this.

**Example 2.13.** Let $X = \{1, 2, 3, 4\}$ and $r(x, y) = (\sigma_x(y), \tau_y(x))$ be the irre-tractable involutive non-degenerate solution given by

$$\sigma_1 = (34), \quad \sigma_2 = (1324), \quad \sigma_3 = (1423), \quad \sigma_4 = (12),$$
$$\tau_1 = (24), \quad \tau_2 = (1432), \quad \tau_3 = (1234), \quad \tau_4 = (13).$$

The associated left brace $\mathcal{G}(X, r)$ is $B(8, 27)$ and has additive group $C_2^3$ and multiplicative group $D_8$. Furthermore, $\mathcal{G}(X, r)$ is not right nilpotent. Hence it is impossible to decompose the left brace $\mathcal{G}(X, r)$ as in Corollary 2.12.

**Example 2.14.** The left brace $B(8, 26)$ has the same additive and multiplicative groups as the brace $\mathcal{G}(X, r)$ of Example 2.13 but it has a factorization as in Corollary 2.12. This shows that $B(8, 26)$ is right nilpotent.

As a counterpart to Theorem 2.5, an analog of Itô's theorem on metabelian groups [18], it is natural to ask if we can extend this analogy. A natural candidate is the celebrated Kegel–Wielandt theorem [17, 20, 28], which states that a finite group which is factorized by two nilpotent subgroups is solvable. In the following example we show that we cannot expect a naive analog of this theorem for skew left braces. Recall that a skew left brace is said to be *simple* if is contains no non-trivial proper ideals.

**Example 2.15.** Consider the left brace $B(72, 475)$, a simple left brace of size 72. This left brace admits a factorization through non-trivial left braces $B$ and $C$ with $|B| = 9$ and $|C| = 8$ that are both left and right nilpotent (strong) left ideals.

Moreover, as $72 = 2^3 3^2$, Example 2.15 shows also that the $p^a q^b$-theorem of Burnside does not have an analog for skew left braces. This also follows directly from work of Cedó, Jespers, and Okniński [9]. As the construction of simple left braces has received a lot of attention [1, 3, 9] and because every left brace is a matched product of left ideals [1, 3] (if it is not of prime power order) we mention the following:

**Corollary 2.16.** *Let $A$ be a skew left brace. If $A$ is the matched product of trivial skew left braces $B$ and $C$, then $A$ cannot be a simple skew left brace.*

*Proof.* By definition of the matched product, it is clear that both $B$ and $C$ are strong left ideals of $A$ and that $A = B + C$. Hence Theorem 2.9 shows that $A$ will contain a non-trivial ideal. □

**Definition 2.17.** Let $A = B + C$ be a factorization of a skew left brace $A$ through left ideals $B$ and $C$. A left ideal $I$ of $A$ is said to be *factorized* if $I = (I \cap A) + (I \cap B)$.

If $A$ is a skew left brace, then

$$\mathrm{Fix}(A) = \{a \in A : \lambda_b(a) = a \text{ for all } b \in A\}$$

is a left ideal of $A$.

**Corollary 2.18.** *Let $A = B + C$ be factorization of a skew left brace $A$ through left ideals $B$ and $C$. If $B$ and $C$ are both trivial as skew left braces, then $\mathrm{Fix}(A)$ is a factorized left ideal of $A$.*

*Proof.* Suppose $b + c \in \mathrm{Fix}(A)$ for some $b \in B$ and $c \in C$. Then, for any $\beta \in B$, we have $b + c = \lambda_\beta(b + c) = b + \lambda_\beta(c)$ because $\lambda_\beta$ is a homomorphism and $B$ is a trivial skew left brace. Hence $\lambda_\beta(c) = c$. Because $A = C \circ B$ and $C$ is a trivial skew left brace, it follows that $c \in \mathrm{Fix}(A) \cap C$. By symmetry, we have that $b \in \mathrm{Fix}(A) \cap B$. □

Recall that a *left brace* is a skew left brace with abelian additive group. For left braces, $\mathrm{Soc}(A) = \mathrm{Ker}\,\lambda$.

**Corollary 2.19.** *Let $A$ be a left brace. If $A = B + C$ is a factorization through the left ideals $B$ and $C$, where both are trivial as skew left braces, then $\mathrm{Soc}(A)$ is a factorized ideal of $A$.*

*Proof.* Let $s \in \mathrm{Soc}(A)$. Then $s = b + c$, where $b \in B$ and $c \in C$. We show that $b \in \mathrm{Ker}\,\lambda$. For that purpose, let $\gamma \in C$. As $C$ is a left ideal and trivial as skew left braces,

$$\lambda_b(\gamma) = \lambda_{b \circ \lambda_{b'}(c)}(\gamma) = \lambda_{b+c}(\gamma) = \lambda_s(\gamma) = \gamma.$$

Hence $b$ acts trivially on both $B$ and $C$ and therefore $b \in \mathrm{Ker}\,\lambda = \mathrm{Soc}(A)$. This implies that $c = s - b \in \mathrm{Soc}(A)$. □

In [27], it is shown that exact factorizations of groups produce non-trivial solutions of the Yang–Baxter equation. Such factorizations produce skew left braces: let $G$ be a finite additive group with an exact factorization through subgroups $B$ and $C$, i.e., $G = B + C$. The operation

$$x \circ y = b + y + c,$$

where $x = b + c$, turns the group $G$ into a skew left brace with multiplicative group isomorphic to $B \times C$ and additive group isomorphic to $G$, see [26, Theorem 2.3]. We say that $(G, +, \circ)$ is the skew left brace obtained from this exact factorization.

**Proposition 2.20.** *Let $A$ be a skew left brace obtained from an exactly factorizable group $A = B + C$. The following statements hold:*

1. *$C$ is a left ideal of $A$.*
2. *If $(C, +)$ is normal in $(A, +)$, then $C$ is an ideal of $A$.*
3. *If $(B, +)$ is normal in $(A, +)$, then $B$ is an ideal of $A$.*

*Proof.* Let $a = b + c$ with $b \in B$ and $c \in C$. To prove that $C$ is a left ideal let $\gamma \in C$. Then

$$\begin{aligned}
\lambda_a(\gamma) &= \lambda_{b+c}(\gamma) \\
&= -(b+c) + (b+c) \circ \gamma \\
&= -c - b + b + \gamma + c \\
&= -c + \gamma + c \in C.
\end{aligned}$$

Now let $\beta \in B$. Since

$$\begin{aligned}
\lambda_a(\beta) &= \lambda_{b+c}(\beta) \\
&= -(b+c) + (b+c) \circ \beta \\
&= -c - b + b + \beta + c \\
&= -c + \beta + c,
\end{aligned}$$

the second claim follows. □

**Corollary 2.21.** *Let $A$ be a skew left brace obtained from an exactly factorizable additive group, say $A = B + C$. Assume that both $(B, +)$ and $(C, +)$ are normal in $(A, +)$. If $(C, +)$ is abelian, then $A$ is right nilpotent of class at most three. In particular, its associated solution is a multipermutation solution of level at most three.*

*Proof.* By Proposition 2.20, $B$ and $C$ are in particular strong left ideals of $A$. The definition of the circle operation implies that $B$ is a trivial skew left brace. Since $(C, +)$ is abelian, $c_1 \circ c_2 = 0 + c_2 + c_1 = c_1 + c_2$ for all $c_1, c_2 \in C$ and hence $C$ is a trivial skew left brace. By Theorem 2.5, $A$ is right nilpotent of class at most three. □

## 3. Characteristic ideals

We denote by $\mathrm{Aut}_{\mathrm{Br}}(A)$ the automorphism group of a skew left brace $A$.

**Definition 3.1.** Let $A$ be a skew left brace. An ideal $I$ of $A$ is called *characteristic* if $\sigma(I) = I$ for all $\sigma \in \mathrm{Aut}_{\mathrm{Br}}(A)$. A skew left brace $A$ is called *characteristically simple* if $0$ and $A$ are its only characteristic ideals.

As for finite groups, characteristically simple finite skew left braces can be described as a factorization into copies of a simple skew left subbrace.

**Theorem 3.2.** *Let $A$ be a finite skew left brace. Then $A$ is characteristically simple if and only if there exists a simple skew left brace $S$ and a positive integer $n$ such that $A \cong S^n$. Moreover, $A$ is solvable if and only if $S$ is trivial, and in this case $A$ is trivial.*

*Proof.* Let $I$ be a minimal ideal of $A$. Let $I_1 = I$. If $I_1, \ldots, I_j$ are defined, then define $I_{j+1} = \sigma(I)$ for some $\sigma \in \mathrm{Aut}_{\mathrm{Br}}(A)$ such that $\sigma(I) \nsubseteq I_1 + \cdots + I_j$. As $A$ is finite and characteristically simple, it follows that this procedure stops and there exists a positive integer $n$ such that $A = I_1 + \cdots + I_n$. As $I_j \cap I_k = 0$ for $j \neq k$, it follows that $A \cong I_1 \times \cdots \times I_n$. Moreover, for any $1 \leqslant k \leqslant n$, it clearly holds that $I_k \cong I$. Thus $A \cong I^n$. Let $J$ be an ideal of $I$. As $I$ is a direct factor of $A$, it follows that $J$ is an ideal of $A$. Hence either $J = I$ or $J = 0$. Thus $I$ is a simple skew left brace.

Let $S$ be a simple skew left brace and $n$ be a positive integer. Let $A = S^n$ and $I$ be a non-zero characteristic ideal of $A$. Then the projection on the $k$-th component $\pi_k \colon A \to S$ is a surjective skew left brace homomorphism. Hence $\pi_k(I)$ is an ideal in $S$. Thus either $\pi_k(I) = S$ or $\pi_k(I) = 0$. Suppose that $\pi_k(I) = S$. Let $a = (a_1, \ldots, a_n) \in I$ with $a_k \neq 0$. Then there exists an $s \in S$ such that $\lambda_s(a_k) \neq 0$ or $s + a_k - s \neq 0$ or $s \circ a_k \circ s' \neq 0$. Denote by $c$ the element of $A$ where every entry is $0$ except the $k$-th which is $s$. Then $\lambda_c(a) \neq a$ or $c + a - c \neq a$ or $c \circ a \circ c' \neq a$. Denote one of the elements different from $a$ by $d$. Then $d - a \neq 0$. Since $d - a$ only has a non-trivial element in the $k$-th component, it follows that the ideal generated by this element is the full $k$-th component. This shows that $I = C_{j_1} + \cdots + C_{j_t}$, where $C_l$ denotes the full $l$-th component. As the symmetric group $S_n$ acts on $A$ by permuting the indices and $I$ is a characteristic ideal, it follows that $I = A$.

Let $A$ be a solvable and characteristically simple skew left brace. As $S$ is a skew left subbrace of $A$, it follows that $S$ is a solvable simple skew left brace. Hence $S$ is a trivial skew left brace. On the other hand, the direct product of trivial skew left braces is trivial, so $A$ is trivial (and thus certainly solvable). $\square$

## References

[1] D. Bachiller. Extensions, matched products, and simple braces. *J. Pure Appl. Algebra*, 222(7):1670–1691, 2018.

[2] D. Bachiller. Solutions of the Yang–Baxter equation associated to skew left braces, with applications to racks. *J. Knot Theory Ramifications*, 27(8):1850055, 36, 2018.

[3] D. Bachiller, F. Cedó, E. Jespers, and J. Okniński. Iterated matched products of finite braces and simplicity; new solutions of the Yang–Baxter equation. *Trans. Amer. Math. Soc.*, 370(7):4881–4907, 2018.

[4] D. Bachiller, F. Cedó, and L. Vendramin. A characterization of finite multipermutation solutions of the Yang–Baxter equation. *Publ. Mat.*, 62(2):641–649, 2018.

[5] F. Cedó. Left Braces: Solutions of the Yang–Baxter Equation. *Adv. Group Theory Appl.*, 5:33–90, 2018.

[6] F. Cedó, T. Gateva-Ivanova, and A. Smoktunowicz. On the Yang–Baxter equation and left nilpotent left braces. *J. Pure Appl. Algebra*, 221(4):751–756, 2017.

[7] F. Cedó, E. Jespers, and J. Okniński. Retractability of set theoretic solutions of the Yang–Baxter equation. *Adv. Math.*, 224(6):2472–2484, 2010.

[8] F. Cedó, E. Jespers, and J. Okniński. Braces and the Yang–Baxter equation. *Comm. Math. Phys.*, 327(1):101–116, 2014.

[9] F. Cedó, E. Jespers, and J. Okniński. An abundance of simple left braces with multiplicative abelian Sylow subgroups. *arXiv:1807.06428*, 2018.

[10] F. Cedó, A. Smoktunowicz, and L. Vendramin. Skew left braces of nilpotent type. *Accepted for publication in Proc. London Math. Soc. (3)*, `DOI:10.1112/plms.1220`, 2018.

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

[12] F. Chouraqui. Left orders in Garside groups. *Internat. J. Algebra Comput.*, 26(7):1349–1359, 2016.

[13] P. Etingof, T. Schedler, and A. Soloviev. Set-theoretical solutions to the quantum Yang–Baxter equation. *Duke Math. J.*, 100(2):169–209, 1999.

[14] T. Gateva-Ivanova. Set-theoretic solutions of the Yang–Baxter equation, braces and symmetric groups. *Adv. Math.*, 338:649–701, 2018.

[15] T. Gateva-Ivanova and P. Cameron. Multipermutation solutions of the Yang–Baxter equation. *Comm. Math. Phys.*, 309(3):583–621, 2012.

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

[17] B. Huppert. *Endliche Gruppen. I*. Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.

[18] N. Itô. Über das Produkt von zwei abelschen Gruppen. *Math. Z.*, 62:400–401, 1955.

[19] E. Jespers and J. Okniński. Monoids and groups of *I*-type. *Algebr. Represent. Theory*, 8(5):709–729, 2005.

[20] O. H. Kegel. Produkte nilpotenter Gruppen. *Arch. Math. (Basel)*, 12:90–93, 1961.

[21] A. Konovalov, A. Smoktunowicz, and L. Vendramin. On skew braces and their ideals. *Accepted for publication in Exp. Math.*, `DOI:10.1080/10586458.2018.1492476`, 2018.

[22] H. Meng, A. Ballester-Bolinches, and R. Esteban-Romero. Left Braces and the Quantum Yang–Baxter Equation. *Proc. Edinb. Math. Soc. (2)*, 62(2):595–608, 2019.

[23] W. Rump. Braces, radical rings, and the quantum Yang–Baxter equation. *J. Algebra*, 307(1):153–170, 2007.

[24] W. Rump. The brace of a classical group. *Note Mat.*, 34(1):115–144, 2014.

[25] A. Smoktunowicz. On Engel groups, nilpotent groups, rings, braces and the Yang–Baxter equation. *Trans. Amer. Math. Soc.*, 370(9):6535–6564, 2018.

[26] A. Smoktunowicz and L. Vendramin. On skew braces (with an appendix by N. Byott and L. Vendramin). *J. Comb. Algebra*, 2(1):47–86, 2018.

[27] A. Weinstein and P. Xu. Classical solutions of the quantum Yang–Baxter equation. *Comm. Math. Phys.*, 148(2):309–343, 1992.

[28] H. Wielandt. Über produkte von nilpotenten gruppen. *Illinois Journal of Mathematics*, 2(4B):611–618, 1958.

(E. Jespers, Ł. Kubat, A. Van Antwerpen) Department of Mathematics, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussel

*E-mail address*: `eric.jespers@vub.be`

*E-mail address*: `lukasz.kubat@vub.be`

*E-mail address*: `arne.van.antwerpen@vub.be`

(L. Vendramin) IMAS–CONICET and Departamento de Matemática, FCEN, Universidad de Buenos Aires, Pabellón 1, Ciudad Universitaria, C1428EGA, Buenos Aires, Argentina; and NYU-ECNU Institute of Mathematical Sciences at NYU Shanghai, 3663 Zhongshan Road North, Shanghai, 200062, China

*E-mail address*: `lvendramin@dm.uba.ar`