On skew braces and their ideals

Digital Object Identifier (DOI):
10.1080/10586458.2018.1492476

ON SKEW BRACES AND THEIR IDEALS

A. KONOVALOV, A. SMOKTUNOWICZ, AND L. VENDRAMIN

Abstract. We define combinatorial representations of finite skew braces and use this idea to produce a database of skew braces of small size. This database is then used to explore different concepts of the theory of skew braces such as ideals, series of ideals, prime and semiprime ideals, Baer and Wedderburn radicals and solvability. The paper contains several questions.

Contents

Introduction 1
1. Combinatorial representations of finite skew braces 3
2. Ideals of skew braces 5
3. Series of ideals 6
4. Prime ideals and prime skew braces 7
5. Solvable ideals 11
Acknowledgements 13
References 14

Introduction

In this work we explore some algebraic structures related to solutions to the celebrated Yang–Baxter equation. Following Drinfeld [23], a *set-theoretic solution of the Yang–Baxter equation* is defined as a pair (X,r), where X is a set and $r\colon X\times X\to X\times X$ is a bijection such that

$$r_1r_2r_1=r_2r_1r_2,\quad r_1=r\times\mathrm{id},\quad r_2=\mathrm{id}\times r.$$

We will be interested in *non-degenerate* solutions, that is solutions (X,r) where r can be written as $r(x,y)=(\sigma_x(y),\tau_y(x))$ for permutations σ_x and τ_x of X.

Rump found that there is a deep connection between radical rings and set-theoretic solutions of the Yang–Baxter equation. The key observation is the following. Let R be a radical ring, that is an associative ring R such that for each $x\in R$ there exists $y\in R$ such that $x+y+xy=0$. Then the operation $x\circ y=x+y+xy$ turns R into a group and

$$r\colon R\times R\to R\times R,\quad r(x,y)=(xy+y,(xy+y)'\circ x\circ y),$$

where z' denotes the inverse of z with respect to the circle operation $\circ$, is a non-degenerate solution of the Yang–Baxter equation such that $r^2=\mathrm{id}_{R\times R}$. A natural question arises: do we really need radical rings to construct such solutions?

Key words and phrases. Braces, Yang–Baxter equation, Radical rings.

In [30] Rump introduced braces, a generalization of radical rings that produces involutive solutions. There is a rich theory of braces, see for example [5, 6, 7, 8, 10, 13, 16, 17, 18, 19, 22, 25, 29, 31, 32]. Later braces were generalized to *skew braces* to allow the construction of non-involutive solutions [26]. A *skew brace* is a triple $(A,\circ,+)$, where $(A,+)$ and $(A,\circ)$ are (not necessarily abelian) groups and the compatilibity condition

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

holds for all $a,b,c\in A$.

If $\mathcal{X}$ is a property of groups, a skew brace is said to be of $\mathcal{X}$-type if its additive group belongs to $\mathcal{X}$. For example, skew braces of abelian type are those braces introduced by Rump in [30] to study involutive set-theoretic solutions. Such braces will be also called either *classical braces* or *braces*.

Skew braces have connections to several different topics, see for example [4, 12, 14, 20, 21, 27, 33]. In particular, skew braces provide the right algebraic framework to study set-theoretic solutions to the Yang–Baxter equation. The connection between set-theoretic solutions and skew braces is explained in the following theorems. The first one shows that skew braces produce set-theoretic solutions:

Theorem. [26, Theorem 3.1] *Let A be a skew brace. The map*

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

is a non-degenerate set-theoretic solution of the Yang–Baxter equation.

The second theorem shows that solutions associated to skew braces are, in some sense, universal. Similar results are [24, Theorem 2.9] for involutive solutions, and [28, Theorem 9] and [34, Theorem 2.7] for non-involutive solutions. Recall that the *structure group* of a solution (X,r) is the group $G(X,r)$ generated by $\{x:x\in X\}$ with relations $xy=uv$ whenever $r(x,y)=(u,v)$.

Theorem. [33, Theorem 4.5] *Let (X,r) be a non-degenerate solution of the Yang–Baxter equation. Then there exists a unique skew left brace structure over the group $G=G(X,r)$ such that*

$$(\iota\times\iota)r=r_{G(x,r)}(\iota\times\iota),$$

where $\iota\colon X\to G(X,r)$ is the canonical map. Moreover, the pair $(G(X,r),\iota)$ has the following universal property: if B is a skew left brace and $f\colon X\to B$ is a map such that $(f\times f)r=r_B(f\times f)$, then there exists a unique skew brace homomorphism $\phi\colon G(X,r)\to B$ such that $f=\phi\iota$ and $(\phi\times\phi)r_{G(X,r)}=r_B(\phi\times\phi)$.

This theorem allows us to define $G(X,r)$ as the structure skew brace of the solution (X,r). Clearly, skew braces are useful for understanding non-degenerate set-theoretic solutions of the Yang–Baxter equation. Moreover, to study finite solutions one only needs finite skew braces, see [4, Theorem 3.11]. Hence, since skew braces generalize radical rings, tools and ideas from ring theory can be used to study the Yang–Baxter equation.

Braces and skew braces have a strong connection with regular subgroups, see for example [6, Proposition 2.3], [15, Theorem 1] and [26, Theorem 4.2]. Based on this fact, an algorithm for constructing all skew braces of a given size was developed in [26]. Using it, one produces a huge database of all (skew) braces of a given order.

The first and the third author produced the GAP package YangBaxter that implements several methods for studying skew braces and other structures related to the set-theoretic Yang–Baxter equation. The package contains a database of classical and skew braces of small orders and it is freely available at `https://github.com/gap-packages/YangBaxter`.

The paper is organized as follows. In Section 1 we introduce combinatorial representations of skew braces; this concept is needed to store small skew braces in a database. In Sections 2 and 3 we study ideals and some particular series of ideals of skew braces; these sections contain several examples that answer some natural questions. Section 4 is devoted to study prime and semiprime ideals and related concepts such as the Baer radical and the Wedderburn radical of a skew brace. This section contains some of our main results. In Theorem 4.21 we prove that a skew brace is semiprime if and only if its Baer radical is zero. Theorem 4.22 proves that the Baer radical of a skew brace is the intersection of all its prime ideals. In Theorem 4.24 we prove that every semiprime skew brace is a subdirect product of prime skew braces. A relation between the Wedderburn and the Baer radical is stated in Theorem 4.28. Solvable ideals of skew braces are studied in Section 5. One of our main results is Theorem 5.6, where it is proved that a finite skew brace is solvable if and only if it is Baer radical.

1. Combinatorial representations of finite skew braces

When storing skew braces in a database, an obvious question is how to represent them efficiently. Obviously, each skew brace can be given by the tables for addition and multiplication, but that would cause a substantial overhead. On the other hand, one can substantially reduce the storage size by keeping only generators for the additive and multiplicative groups of a skew brace, and recording a way to reconstruct its full structure. This process should be deterministic and should not depend on some randomized algorithms. If we store additive and multiplicative groups as permutation groups, we can rely on the lexicographic ordering of permutations and store skew braces as explained below.

Definition 1.1. *For permutations f and g, $f < g$ if and only if the image of f on the range from 1 to the degree of f is lexicographically smaller than the corresponding image for g.*

Recall from [26, Proposition 1.11] that a skew brace of size n with additive group A is equivalent to a pair (G, π) where G is a group acting by automorphisms on A and $\pi\colon G \to A$ is a bijective 1-cocycle. Without loss of generality we can write $G = \{g_1, g_2, \dots, g_n\}$ and $A = \{a_1, a_2, \dots, a_n\}$ as permutation groups and assume that $\pi(g_j) = a_j$ for all $j \in \{1, \dots, n\}$. Then the skew brace is the additive group $A = \{a_1, \dots, a_n\}$ with the multiplication

$$a_i \circ a_j = a_k,$$

where $g_i g_j = g_k$. This means that to store our skew brace we only need these two tuples of permutations $(a_1, a_2, \dots, a_n)$ and $(g_1, g_2, \dots, g_n)$. Observe the use of tuples is very important because it implies that elements of G and A are listed in a particular order, determined by the bijection π.

This way, we will need $2n$ permutations to store a brace of size n. We can try to be more efficient by storing generating sets of groups G and A, together with the

TABLE 1.1. Number of skew and classical braces for $n \leq 16$.

n	1	2	3	4	5	6	7	8
$s(n)$	1	1	1	4	1	6	1	47
$b(n)$	1	1	1	4	1	2	1	27
n	9	10	11	12	13	14	15	16
$s(n)$	4	6	1	38	1	6	1	1605
$b(n)$	4	2	1	10	1	2	1	357

data needed to recover the tuples $(a_1, a_2, \dots, a_n)$ and $(g_1, g_2, \dots, g_n)$. To recover these tuples, first we use an algorithm that constructs the lists of all elements of the groups G and A from the chosen generating sets, and then sort each of the resulting lists in lexicographic order (see Definition 1.1). So we obtain

$$a_{\sigma(1)} < a_{\sigma(2)} < \cdots < a_{\sigma(n)}, \quad g_{\tau(1)} < g_{\tau(2)} < \cdots < g_{\tau(n)},$$

where σ and τ are some permutations of $\{1, \dots, n\}$. These translate into two tuples $(a_{\sigma(1)}, a_{\sigma(2)}, \cdots, a_{\sigma(n)})$ and $(g_{\tau(1)}, g_{\tau(2)}, \cdots, g_{\tau(n)})$. Acting with the inverses of σ and τ we recover the tuples $(a_1, a_2, \dots, a_n)$ and $(g_1, g_2, \dots, g_n)$ respectively.

Note that the generating sets of G and A do not have to be of a minimal size, although for practical purposes it is useful to choose them as small as possible.

A database of small skew braces. Motivated by [11] and using the algorithm described in [26], one constructs a database of small (skew) braces. Thanks to the representation described in the previous section, we were able to reduce the size of the database from more than 300 MB in the initial representation (which kept full lists of elements of permutation representation of the additive and multiplicative group of a skew brace) to less than 30 MB.

At the present moment, the database contains all (up to isomorphism) skew braces of sizes up to 85 except some orders including large prime powers, e.g. 32, 64, etc. and all (up to isomorphism) classical braces of sizes up to 127 except 32, 64, 81 and 96. In total, it included 7797 skew braces and 8312 classical braces.

Each classical brace (respectively skew brace) is named by their library index as $B_{n,k}$ (resp. $S_{n,k}$), where n is its size and k is its index in the database of braces of size n. For example, the list of skew braces of size eight is $S_{8,1}, S_{8,2}, \dots, S_{8,47}$, and the list of classical ones is $B_{8,1}, B_{8,2}, \dots, B_{8,27}$.

The number $s(n)$ of isomorphism classes of skew braces and $b(n)$ of classical braces for $n \leq 16$ is given in Table 1.1.

An application to two-sided skew braces. In [16, Question 2.1(2)] one finds the following interesting question: Is it true that any brace such that the operation $a * b = -a + a \circ b - b$ is associative is a two-sided brace? We check that the answer is affirmative for all the classical braces of our database. We know from [16, Proposition 2.2] that we only need to check classical braces of even size. We have tested all such classical braces in our database and we found no answer to this question.

What happens if we ask the same question for skew braces? Now it turns out that indeed we have an answer! The smallest skew braces which are not two-sided and have an associative $*$ operation are

$$S_{16,j}, \quad j \in \{230, 235, 424, 429, 547, 554, 556, 561\}.$$

It is interesting to observe that the additive groups of these skew braces are nilpotent. Since skew braces with nilpotent additive groups are almost like classical braces, these examples of size 16 suggest that one should expect an answer to Question [16, Question 2.1(2)] in the positive.

2. Ideals of skew braces

Since skew braces are generalizations of radical rings, one can try to exploit ideas from ring theory. Let us first recall a very useful lemma:

Lemma 2.1. *Let A be a skew brace. Then $\lambda\colon (A,\circ)\to \operatorname{Aut}(A,+)$ given by $a\mapsto\lambda_a$, where $\lambda_a(b)=-a+a\circ b$, is a well-defined group homomorphism.*

Proof. See [7, Corollary 1.10]. □

An *ideal* of a skew brace A is a normal subgroup I of the multiplicative group of A such that $\lambda_a(I)\subseteq I$ and $a+I=I+a$ for all $a\in A$. The following easy lemma is useful for computational purposes:

Lemma 2.2. *Let A be a skew brace and I be a subset of A. Then I is an ideal if and only if I is a normal subgroup of the additive group of A, $a\circ I=I\circ a$ and $\lambda_a(I)\subseteq I$ for all $a\in A$.*

Proof. Assume first that I is an ideal of A. Then the claim follows from [26, Lemma 2.3(1)]. To prove the converse we need to show that I is a subgroup of the multiplicative group of A. For $x,y\in I$,

$$x\circ y'=x\lambda_x(-\lambda_{y'}(y))\in I$$

and hence the claim follows. □

The *socle* of a skew brace A is defined as $\operatorname{Soc}(A)=\ker\lambda\cap Z(A,+)$ and it is an ideal of A. A skew brace A is said to be *trivial* if $a+b=ab$ for all $a,b\in A$.

Example 2.3. *Let $A=S_{6,1}$, the trivial skew brace over $\mathbb{S}_3$. Then $\operatorname{Soc}(A)=0$ because $\mathbb{S}_3$ has a trivial center.*

Naturally, one can quotient out skew braces by ideals to produce new skew braces. Using the map λ from Lemma 2.1 one shows that I is a normal subgroup of the additive group of A (see Lemma 2.2) and that for every $a\in A$ we have $a\circ I=a+I$. Then it follows that A/I is a skew brace.

Example 2.4. *Let $A=B_{8,5}$. This is the only classical brace of size eight with additive group is isomorphic to C_8 and multiplicative group isomorphic to $C_4\times C_2$. It has four ideals which are isomorphic to 0, $B_{2,1}$, $B_{4,1}$ and $B_{8,5}$. The quotients of A are then isomorphic to $B_{8,5}$, $B_{4,2}$, $B_{2,1}$ and 0.*

A *left ideal* I of A is a subgroup I of the additive group of A such that $\lambda_a(I)\subseteq I$ for all $a\in A$.

Example 2.5. *Let $A=B_{6,2}$, the only classical brace of size six with additive and multiplicative groups isomorphic to C_6. It has four left ideals which are isomorphic to 0, $B_{2,1}$, $B_{3,1}$ and $B_{6,2}$ (in fact, all of them are two sided ideals in A).*

Example 2.6. *Let $A=B_{6,1}$, the only non-trivial classical brace of size six with additive group isomorphic to C_6 and multiplicative groups isomorphic to S_3. It has one left ideal of size two, which is not a two-sided ideal.*

Let I and J be ideals of a skew brace A. Then $I \cap J$ is an ideal of A. The sum $I+J$ of I and J is defined as the additive subgroup of A generated by all the elements of the form $u+v$, $u \in I$ and $v \in J$.

Lemma 2.7. *Let A be a skew brace and let I and J be ideals of A. Then $I+J$ is an ideal of A.*

Proof. Let $a \in A$, $u \in I$ and $v \in J$. Then $\lambda_a(u+v) \in I+J$ and hence it follows that $\lambda_a(I+J) \subseteq I+J$. Moreover,

$$(u+v)*a = (u \circ \lambda_u^{-1}(v))*a = u*(\lambda_u^{-1}(v)*a) + \lambda_u^{-1}(v)*a + u*a \in I+J.$$

This formula implies that

$$a \circ (u+v) \circ a' = a + \lambda_a((u+v)+(u+v)*a') - a \in I+J.$$

Thus it follows that $a \circ (I+J) \circ a' \subseteq I+J$.

Finally $I+J$ is a normal subgroup of $(A,+)$ since

$$a + \left(\sum_k u_k + v_k\right) - a = \sum_k ((a+u_k-a)+(a+v_k-a)) \in I+J$$

whenever $u_k \in I$ and $v_k \in J$ for all k. □

For $a,b \in A$ we write $a*b = \lambda_a(b)-b$. For subsets X and Y of A we write $X*Y$ to denote the subgroup of $(A,+)$ generated by $\{x*y : x \in X, y \in Y\}$.

Example 2.8. *Let $A = B_{8,18}$. It has three ideals which are isomorphic to 0, $B_{4,3}$ or A. Let I be the ideal isomorphic to $B_{4,3}$. Since A has no ideals of size two, the subset $A*I$ of size two cannot be an ideal of A.*

3. Series of ideals

Following Rump [30], one defines the *left series* of a skew brace A recursively by $A^1 = A$ and $A^{n+1} = A*A^n$ for $n \geq 1$. Each A^n is a left ideal of A. The following example shows that in general A^n is not a normal subgroup of the additive group of A:

Example 3.1. *Let $A = S_{36,191}$. The left series of A is $A^1 = A$, $A^2 \simeq S_{18,22}$ and $A^3 \simeq B_{3,1}$. Then the additive group A^3 is not normal in the additive group of A. Indeed, the additive group of A contains no normal subgroup of order three.*

Similarly the *right series* of A is defined by $A^{(1)} = A$ and $A^{(n+1)} = A^{(n)} * A$ for $n \geq 1$. Each $A^{(n)}$ is an ideal of A. A skew brace A is said to be *left nilpotent* (resp. *right nilpotent*) if $A^n = 0$ (resp. $A^{(n)} = 0$) for some $n \in \mathbb{N}$. See [9] or [30] for examples.

Example 3.2. *Let $A = B_{16,73}$. Up to isomorphism, the ideals of A are*

$$0, B_{2,1}, B_{4,1}, B_{4,2}, B_{4,3}, B_{8,10}, B_{8,13}, B_{8,19}, B_{16,73}.$$

Let I be the ideal isomorphic to $B_{8,10}$. Then $I*I$ is a subset of size two which is not an ideal of A.

Simple skew braces. Recall that a skew brace A is said to be *simple* if its only ideals are $\{0\}$ and A. Simple skew braces are intensively studied, in particular simple classical braces [7, 9].

Example 3.3. *Let $A = S_{12,22}$. Then $(A,+) \simeq \mathbb{A}_4$ and $(A,\circ) \simeq C_3 \rtimes C_4$. The skew brace A is a simple skew brace and $A = A^n = A^{(n)}$ for all $n \in \mathbb{N}$.*

Example 3.4. *Let $A = S_{24,50}$. Then $(A,+) \simeq \mathrm{SL}_2(3)$ and $(A,\circ) \simeq C_3 \rtimes C_8$. Furthermore $A = A^n = A^{(n)}$ for all $n \in \mathbb{N}$. This skew brace is not simple since for example* $\mathrm{Soc}(A) \simeq B_{2,1}$.

Let us count how many simple classical braces appear in our database. It is known that classical braces of prime-power size are not simple. Computer calculations show the following results:

Proposition 3.5. *Let A be a simple brace of order n, where $1 \leq n \leq 127$ and $n \neq 96$. Then A is isomorphic to $B_{24,94}$ or $B_{72,475}$.*

For skew braces we can prove the following proposition:

Proposition 3.6. *Let A be a simple skew brace of order n, where $1 \leq n \leq 63$ and $n \notin \{32, 48, 54\}$. Then A is isomorphic to $S_{12,22}$, $S_{12,23}$, $S_{24,853} \cong B_{24,94}$ or to one of the skew braces $S_{60,k}$, where $145 \leq k \leq 152$, which are the only skew braces with additive group isomorphic to $\mathbb{A}_5$.*

Question 3.7. *Are there simple two-sided skew braces of nilpotent type?*

4. Prime ideals and prime skew braces

In the conference "Groups, rings and the Yang–Baxter equation", Spa, 2017, Louis Rowen suggested that it could be interesting to study prime ideals of skew braces.

Definition 4.1. *A skew brace A is said to be* prime *if for all non-zero ideals I and J one has $I * J \neq 0$.*

Simple non-trivial skew braces are prime. The converse does not hold:

Example 4.2. *The skew brace $A = S_{24,708}$ is not simple and it is prime. The additive group of A is not nilpotent since it is isomorphic to $\mathbb{S}_4$.*

We found several examples of non-simple prime skew braces; in all cases the additive group is not nilpotent. Therefore it seems natural to ask the following questions:

Question 4.3. *Let A be a finite prime skew brace of nilpotent type. Is A simple?*

Question 4.4. *Let A be a finite classical prime brace. Is A simple?*

Question 4.5. *Are there prime two-sided skew braces of nilpotent type?*

Definition 4.6. *A skew brace A is said to be* semiprime *if for each non-zero ideal I of A one has $I * I \neq 0$.*

Of course, prime skew braces are semiprime. The converse does not hold:

Example 4.7. *Let $A = S_{12,22}$. Since A is a simple skew brace, A is prime. The direct product $A \times A$ is semiprime and not prime.*

Definition 4.8. *We say that an ideal I of a skew brace A is* prime *(resp. semiprime) if A/I is a prime (resp. semiprime) skew brace.*

In non-commutative ring theory there is a strong connection between prime ideals and the Baer radical of the ring. Recall that the Baer radical of a ring R (also called the prime radical) equals the intersection of all prime ideals in R. Solvable and Baer radicals were also considered for non-associative algebras, loop algebras and semigroups by Amitsur in [1, 2, 3]. Below, we generalize some classical results which hold for rings to skew braces. Our definitions are similar to those of ring theory but not identical.

Let A be a skew brace and $a \in A$. By $\langle a\rangle$ we will denote the smallest ideal of A which contains a (i.e., the ideal generated by a in A).

Definition 4.9. *Let A be a skew brace. We say that $a_1, a_2, a_3, \dots \in A$ is an* n-sequence *if $a_{i+1} \in \langle a_i\rangle * \langle a_i\rangle$ for $i \geq 1$.*

Definition 4.10. *A skew brace A is said to be* Baer radical *if for each $a \in A$, every n-sequence starting with a reaches zero at some point. An ideal I of A is said to be Baer radical if I is a Baer radical skew brace.*

Lemma 4.11. *Let A be a skew brace and J be an ideal in A. Let $a, b \in A$ such that $a - b \in J$ and $c \in \langle a\rangle$. Then there exists $c' \in \langle b\rangle$ such that $c - c' \in J$.*

Proof. It follows from using the canonical map $A \to A/J$. □

Lemma 4.12. *Let A be a skew brace and let I and J be ideals of A. Let $a_1, a_2, \dots$ be an n-sequence such that $a_k \in I + J$ for all k. Then there exist an n-sequence $i_1, i_2, \dots$ in I and $j_1, j_2 \dots \in J$ such that $a_k = i_k + j_k$ for all k.*

Proof. We proceed by induction on the length l of the n-sequence $a_1, a_2, \dots a_l$. The case $l = 1$ is trivial, so let us assume that the result holds for some $l \geq 1$. Since $a_{l+1} \in \langle a_l\rangle * \langle a_l\rangle$, there exist $c_i, d_i \in \langle a_l\rangle$ such that $a_{l+1} = \sum c_i * d_i$. By applying Lemma 4.11 with $a = a_l$, $b = i_l$ and $c = c_i$ or $c = d_i$, there exist $c_i' \in \langle i_l\rangle$ and $d_i' \in \langle i_l\rangle$ such that $c_i - c_i' \in J$ and $d_i - d_i' \in J$. Let $i_{l+1} = \sum c_i' * d_i' \in \langle i_l\rangle * \langle i_l\rangle \subseteq I$. Then $\pi(a_{l+1} - i_{l+1})$, where $\pi\colon A \to A/J$ is the canonical map. This implies that $a_{l+1} - i_{l+1} \in J$ and the lemma follows. □

Lemma 4.13. *Let A be a skew brace. The sum of any number of Baer radical ideals in A is a Baer radical ideal in A.*

Proof. Let I and J be two Baer radical ideals in A. Since every ideal is a normal subgroup of the additive group of A, $I + J = \{i + j : i \in I, j \in J\}$. Consider an n-sequence $a_1, a_2, \dots$ starting with an element $a_1 = i + j$ where $i \in I, j \in J$. By Lemma 4.12, $a_m \in J$ for some m. Now, since J is Baer radical, every n-sequence starting with a_m will reach zero, therefore the n-sequence $a_m, a_{m+1}, a_{m+2}, \dots$ will reach zero, as required. Similarly, the sum of any number of Baer radical ideals is an ideal (as any element in this sum belongs to a sum of a finite number of these ideals). □

Lemma 4.13 implies that the sum of all Baer radical ideals in A is the largest Baer radical ideal in A. Thus a skew brace A contains largest Baer radical ideal. This justifies the following definition:

Definition 4.14. *Let A be a skew brace. The* Baer radical *$B(A)$ of A is the largest Baer radical ideal of A.*

Lemma 4.15. *Let A be a skew brace and let I be an ideal in A. If I and A/I are Baer radical skew braces, then A is a Baer radical skew brace.*

Proof. Let $a_1, a_2, \dots$ be an n-sequence in A. Because A/I is Baer radical we get that $a_m \in I$ for some m. Now, since I is a Baer radical ideal, every n-sequence starting with a_m will reach zero. Therefore the n-sequence $a_m, a_{m+1}, a_{m+2}, \dots$ will reach zero. □

Lemma 4.16. *Let A be a skew brace, and J be an ideal in A, and let I be an ideal in the skew brace A/J. Then $\bar{I} = \{a \in A : a + J \in I\}$ is an ideal in A.*

Proof. Note that $a \in \bar{I}$ if and only if $a + J \in I$. Let $a, b \in \bar{I}$. Since $a + J \in I$ and $b + J \in I$, $a + b + J = (a + J) + (b + J) \in I$. Hence $a + b \in \bar{I}$. Similarly, if $a \in \bar{I}$ and $c \in A$, then $a + J \in I$. Therefore $\lambda_c(a) + J = \lambda_{c+J}(a + J) \in I$ and hence $\lambda_c(a) \in \bar{I}$. Observe also that $c' \circ a \circ c + J = (c' + J) \circ (a + J) \circ (c + J) \in I$, therefore $c' \circ a \circ c \in \bar{I}$. □

Theorem 4.17. *Let A be a skew brace. Then $B(A/B(A)) = 0$.*

Proof. By Lemma 4.16, if the Baer radical $B(A/B(A))$ of $A/B(A)$ is nonzero, then

$$I = \{a \in A : a + B(A) \in B(A/B(A))\}$$

is an ideal of A. Notice that $B(A) \subseteq I$ and $I/B(A) = B(A/B(A)) \neq 0$. Since $I/B(A)$ and $B(A)$ are Baer radical, by Lemma 4.15 one obtains that I is a Baer radical ideal in A and thus $I \subseteq B(A)$. Hence $I/B(A) = 0$, a contradiction. □

Lemma 4.18. *If $J \subseteq I$ are ideals in a skew brace A, then I/J is an ideal in A/J.*

Proof. Let $a + J, b + J \in I/J$ and $c \in A$. Then $a \in I$ and $b \in I$. Moreover, since J is an ideal, $(a + J) + (b + J) = a + b + J \in I/J$, $\lambda_{c+J}(a + J) = \lambda_c(a) + J \in I/J$ and $(c + J)' \circ (a + J) \circ (c + J) = c' \circ a \circ c + J \in I/J$. □

Proposition 4.19. *Let A be a skew brace and I, J be ideals in A, then $(I + J)/J$ is an ideal in A/J.*

Proof. Since $I + J$ is an ideal, the claim follows from Lemma 4.18. □

Lemma 4.20. *Let A be a skew brace such that $B(A) \neq 0$. Then there is a non-zero ideal $I \subseteq B(A)$ in A such that $I * I = 0$.*

Proof. Let $a \in B(A)$. We construct an n-sequence of elements of A starting with a. Suppose that we defined elements $a_1, a_2, \dots, a_i$ of our sequence and they are all non-zero. If $\langle a_i \rangle * \langle a_i \rangle$ is nonzero, we can add a non-zero element a_{i+1} to this n-sequence. Since $a \in B(A)$, every n-sequence starting with a will reach zero. Therefore there exists j such that $a_j \neq 0$ and $\langle a_j \rangle * \langle a_j \rangle = 0$. Now take $I = \langle a_j \rangle$. Since $I \neq 0$ and $I \subseteq B(A)$, the lemma is proved. □

Theorem 4.21. *Let A be a skew brace. Then A is semiprime if and only if the Baer radical of A is zero.*

Proof. If $B(A) \neq 0$, then the claim follows from Lemma 4.20. Conversely, assume that $B(A) = 0$ and that A is not semiprime. Then there is a non-zero ideal I such that $I * I = 0$. Since every n-sequence starting with elements from I reaches zero at the second place, it follows that $0 \neq I \subseteq B(A) = 0$. Since this is a contradiction, A is semiprime. □

Theorem 4.22. *Let A be a skew brace. Then $B(A)$ equals the intersection of all prime ideals of A.*

Proof. Let I be the intersection of all prime ideals in A. Then I is an ideal of A. To prove that $I \subseteq B(A)$ we need to show that every n-sequence starting with any element of I reaches zero. Let $a_1 \in I$ and $a_1, a_2, \dots$ be an n-sequence. Suppose on the contrary that this n-sequence contains only non-zero elements. Let J be a maximal ideal which does not contain any element from this n-sequence (it may be the zero ideal) and let $\pi\colon A \to A/J$ be the canonical map. Note that every ideal in A/J is of the form $\pi(L)$ for some ideal L in A. We claim that J is a prime ideal. Indeed, if P and Q are ideals of A properly containing J, the maximality of J implies that there are $n, m \in \mathbb{N}$ such that $a_n \in P$ and $a_m \in Q$. Hence there exists $N \geq \max\{n, m\}$ such that $a_N \in P \cap Q$. Since $0 \neq a_{N+1} \in P * Q$ and $a_{N+1} \notin J$, the non-zero ideals $\pi(P)$ and $\pi(Q)$ are such that $\pi(P) * \pi(Q) \neq 0$. Therefore J is prime and hence $I \subseteq J$, a contradiction.

It remains to show that the Baer radical of A is contained in every prime ideal in A. Suppose on the contrary, let P be a prime ideal in A such that P does not contain $B(A)$. Then the factor brace A/P has an element $a + P \neq 0 + P$ such that $a \in B(A)$. We construct an n-sequence of elements of A starting with element $a \in B(A) \setminus P$. Suppose that we defined elements $a_1, a_2, \dots, a_i \notin P$ of our sequence and they are all non-zero. Observe that if $\langle a_i \rangle * \langle a_i \rangle$ is not a subset of P, then we can add a non-zero element $a_{i+1} \notin P$ to this n-sequence. Since $a \in B(A)$ then every n-sequence starting with a will reach zero, therefore every n-sequence starting with a will reach an element in P. Therefore, there is j in our n-sequence such that $a_j \notin P$ and $\langle a_j \rangle * \langle a_j \rangle \subseteq P$. Note that since $a_1 \in B(A)$ then $a_2, a_3, \dots, a_j \in B(A)$. By Lemma 4.18, $L = \langle a_j + P \rangle / P$ is an ideal in A/P. Note that $L * L = 0$ hence A/P is not a prime skew brace, a contradiction since by assumption P is a prime ideal in A. □

Corollary 4.23. *Let A be a skew brace. Then A is Baer radical if and only if A has no prime ideals except A. In other words every n-sequence in a skew brace A has zero element if and only if A has no prime ideals except A.*

Proof. It follows from Theorem 4.22 □

Theorem 4.24. *Every semiprime skew brace embeds as a skew brace in a direct product of prime skew braces.*

Proof. Let A be a skew brace and $\{P_i : i \in T\}$ be the set of its prime ideals. Then $B(A) = \bigcap_{i \in T} P_i$. Consider the skew brace Q which is direct product of skew braces A/P_i, for $i \in T$. Consider the map $f : A \to Q$ where $f(a) = \{a + P_i\}_{i \in T}$, then this is a homomorphism of skew braces. Observe, that the kernel of this map f equals the set of these elements which are in all prime ideals of A, hence it equals $B(A)$. It follows that the kernel of f is zero. □

Definition 4.25. *Let A be a skew brace and let I be an ideal of A. We say that an ideal I in A is a left (resp. right) nilpotent ideal if I is a left nilpotent (resp. right nilpotent) skew brace.*

Definition 4.26. *Let A be a skew brace. The* Wedderburn radical $W(A)$ *of A is defined as the sum of all the ideals of A that are either left nilpotent or right nilpotent.*

Lemma 4.27. *Let A be a skew brace, then the Baer radical of A contains every left nilpotent ideal in A, and every right nilpotent ideal in A. Therefore $W(A) \subseteq B(A)$.*

Proof. If I is a nilpotent ideal, then $I \subseteq B(A)$ since every n-sequence reaches zero. The result now follows from Lemma 4.13. □

Theorem 4.28. *Let A be a skew brace. Then $B(A) = 0$ if and only if $W(A) = 0$.*

Proof. By Lemma 4.27, if $B(A) = 0$ then $W(A) = 0$. Suppose that $B(A) \neq 0$ then $W(A) \neq 0$ by Lemma 4.20. □

Corollary 4.29. *A skew brace with a non-zero Baer radical is not prime and not semiprime. In particular, a skew brace which is either left nilpotent or right nilpotent is not prime and not semiprime.*

Proof. The first assertion follows from Lemma 4.20. The second assertion follows from the fact that if a skew brace A is either left or right nilpotent, $A \subseteq W(A)$. □

It is known that in finite rings the Wedderburn and the Baer radical are equal. This does not happen for infinite rings. Therefore, for infinite skew braces, the Baer and the Wedderburn radical are not in general equal. This follows from the following lemma:

Lemma 4.30. *Let $(A, +, \cdot)$ be a Jacobson radical ring and $(A, +, \circ)$ be the associated two-sided brace (this means that $a \circ b = a + b + a \cdot b$ for all $a, b \in A$). Then the Baer radical of the brace $(A, +, \circ)$ equals the Baer radical of the ring $(A, +, \cdot)$.*

Proof. It follows from the fact that the intersection of prime ideals in any ring equals the Baer radical of this ring. So the Baer radical of the Jacobson radical ring $(A, +, \cdot)$ will be equal to the intersection of all its prime ideals. This equals the intersection of all prime ideals in the corresponding brace $(A, +, \circ)$. By Theorem 4.22, this is equal to the Baer radical of the brace $(A, +, \circ)$. To finish the argument, one uses a result of Cedó, Jespers and Okniński [18, Proposition 1] stating that every ideal I in a two-sided brace A comes from the associated Jacobson radical ring and gives a two-sided factor brace A/I. □

The Baer and the Wedderburn radical might be different even in the case of finite skew braces:

Example 4.31. *Let $A = S_{6,2}$ be the unique non-trivial skew brace with additive and multiplicative group isomorphic to $\mathbb{S}_3$. Then $W(A) \simeq B_{3,1}$ and $B(A) = A$.*

5. Solvable ideals

Motivated by the theory of groups, Bachiller, Cedó, Jespers and Okniński introduced solvable braces [9]. The definition not only works in the case of classical braces. For a skew brace A we define $A_1 = A$ and inductively $A_{i+1} = A_i * A_i$ for $i \geq 1$. Recall that A is said to be *solvable* if $A_n = 0$ for some n. By induction one proves that $A_{i+1} \subseteq A_i$ for all i. An ideal I in a skew brace A is *solvable*, if I is a solvable skew brace. Clearly every solvable skew brace is Baer radical as every n-sequence will reach zero.

Lemma 5.1. *Let A be a skew brace. For each j, A_{j+1} is an ideal of A_j. In particular, each A_j is a sub skew brace of A.*

Proof. It follows since $A_{j+1} = A_j * A_j = (A_j)^{(2)}$ for all j. □

Example 5.2. *Let $A = B_{48,396}$. Then $A_1 = A$, $A_2 \simeq B_{24,58}$, $A_3 \simeq B_{6,1}$, $A_4 \simeq B_{3,1}$ and $A_5 = 0$. The sub skew brace A_3 is not an ideal.*

The aim of this section is to show that for finite skew braces the Baer radical equals the largest solvable ideal. For that purpose, we need some preliminary results. Some of these results were proved by Cedó, Jespers and Okniński in [9] for classical braces.

Lemma 5.3. *A sum of a finite number of solvable ideals in a skew brace is solvable.*

Proof. Let I and J be solvable ideals in A, $T = I + J$, $T_1 = T$ and $T_{n+1} = T_n * T_n$ for $n \geq 1$. Similarly, let $I_1 = I$ and $I_{n+1} = I_n * I_n$ for $n \geq 1$. Notice that $I_m = 0$ and $J_{m'} = 0$ for some m, m' since I and J are solvable. It can be proved by induction that for every i, $T_i \subseteq J_i + I$ (by showing that $T_i/I \subseteq (J_i + I)/I$ in the skew brace A/I). It follows that $T_{m'} \subseteq I$, and therefore $T_{m+m'} = 0$. Therefore a sum of two solvable ideals is solvable. By using induction on the number of ideals we can show that sum of any finite number of solvable ideals is solvable. □

Lemma 5.4. *Let A be a skew brace and let I be a solvable ideal in A. If A/I is a solvable skew brace, then A is a solvable skew brace.*

Proof. Denote inductively $T = A/I$, $T_1 = T, T_{n+1} = T_n * T_n$, $I_1 = I, I_{n+1} = I_n * I_n$. Notice that $I_m = 0$ and $T_{m'} = 0$ for some m, m' since I and T are solvable. It can be proved by induction that, for every i, $A_i + I = T_i$ in A/I. Therefore $A_{m'} \subseteq I$. Consequently $A_{m+m'} \subseteq I_m = 0$. □

Lemma 5.5. *Let A be a finite skew brace. Then the Wedderburn radical of A is a solvable ideal in A.*

Proof. Let I be a left of right nilpotent ideal of A, it can be shown by induction that $I_n \subseteq I^n$ and $I_n \subseteq I^{(n)}$, therefore I is solvable. Our result now follows from Lemma 5.3. □

Now we are ready to prove the main result of the section:

Theorem 5.6. *Let A be a finite skew brace. Then A is Baer radical if and only if A is solvable.*

Proof. Clearly every solvable skew brace is a Baer radical skew brace since every n-sequence will reach zero. Suppose now that A is a Baer radical skew brace, so $A \subseteq B(A)$. We will prove that A is solvable by induction on the number of elements in A. If A has only one element then A is a trivial brace and the result holds. Suppose the result holds for all skew braces of cardinality smaller than i, and suppose that A has cardinality $i + 1$. Since $B(A) \neq 0$ we get $W(A) \neq 0$ (by Theorem 4.28). By Lemma 5.5, $W(A)$ is a solvable ideal in A. Since A is Baer radical it follows that $A/W(A)$ is Baer radical. By the inductive assumption $A/W(A)$ is solvable. By Lemma 5.4 applied for $I = W(A)$ we get that A is solvable. □

Corollary 5.7. *Let A be a finite skew brace and I be an ideal in A. Then I is solvable if and only if I is Baer radical. In particular, the Baer radical of A equals the largest solvable ideal. Moreover, if A has a nonzero solvable ideal then A has a non-zero ideal I such that $I * I = 0$.*

Proof. Every Baer radical ideal is solvable, hence $B(A)$ is solvable. On the other hand every solvable ideal is Baer radical by Theorem 5.6. The rest follows from Lemma 4.20. $\square$

Corollary 5.8. *There exists an infinite brace such that its Baer radical is not solvable.*

Proof. It follows from the fact that there are Baer radical rings which are not nilpotent. $\square$

Remark 5.9. Question 4.5 asks for two-sided braces that are prime. Note that there exists an infinite prime and not simple Jacobson radical ring. Thus, by Lemma 4.30, there exists a prime and not simple infinite two-sided brace.

The results in this section allow us to answer the following question: Is it true that a product of any number of non-zero ideals in A (in any order) is nonzero?

Lemma 5.10. *Let A be a prime skew brace and let I and J be non-zero ideals in A. Then $I \cap J$ is a non-zero ideal in A. Moreover, the intersection of any finite number of non-zero ideals in A is a non-zero ideal in A.*

Proof. The intersection of any two ideals is an ideal. Notice that $I * J \subseteq I \cap J$, therefore $I \cap J \neq 0$. The last assertion can be proved by induction on the number of ideals. $\square$

Lemma 5.11. *Let A be a semiprime skew brace and I be a non-zero ideal in A. Then the product of any number of copies of I, multiplied in any order, is non-zero. Moreover, any product of copies of I contains some I_n.*

Proof. We use an induction on i, the number of copies of I used in our product. If $i = 1$ then our product equals $I = I_1 \neq 0$. Suppose now that any product of any number of at most i copies of I contains I_n for some n. Let P be a product of $i+1$ copies of I, for some $i > 0$. Then $P = P_1 * P_2$ where P_1 and P_2 are products of at most i copies of I. By the inductive assumption, $I_n * I_n = I_{n+1} \subseteq P_1 * P_2 = P$ for some n. Notice that $I_n \neq 0$ for every n. Indeed if $I_n = 0$ then I is solvable and consequently I is Baer radical. A contradiction with Theorem 4.21 since A is semiprime. $\square$

Theorem 5.12. *If A is a prime skew brace, then a product of any number of non-zero ideals, multiplied in any order, in A is non-zero.*

Proof. Denote our product of ideals as P. Let $I_1, \dots, I_m$ be ideals used in the product P. By Lemma 5.10, $T = \bigcap_{k=1}^{m} I_k$ is a nonzero ideal in A. Let Q be a product of copies of ideal T obtained by exchanging any ideal among $I_1, \dots, I_m$ appearing in the product P by ideal T. Clearly $Q \subseteq P$. Note that A is semiprime since it is prime. By Lemma 5.11, $Q \neq 0$. $\square$

Acknowledgements

The first-named author is partially supported by CCP CoDiMa (EP/M022641/1) and the OpenDreamKit Horizon 2020 European Research Infrastructures project (#676541). The second-named author is supprted by the ERC Advanced grant 320974. The third-named author is supported by PICT-201-0147, MATH-AmSud 17MATH-01 and ERC Advanced grant 320974. We thank Emiliano Acri, Ferran

Cedó, Rofoldo Cossalter, Louis Rowen and Ivan Shestakov for comments and corrections.

References

[1] S. A. Amitsur. A general theory of radicals. I. Radicals in complete lattices. *Amer. J. Math.*, 74:774–786, 1952.
[2] S. A. Amitsur. A general theory of radicals. II. Radicals in rings and bicategories. *Amer. J. Math.*, 76:100–125, 1954.
[3] S. A. Amitsur. A general theory of radicals. III. Applications. *Amer. J. Math.*, 76:126–136, 1954.
[4] D. Bachiller. Solutions of the Yang-Baxter equation associated to skew left braces, with applications to racks. *arXiv:1611.08138*.
[5] D. Bachiller. Classification of braces of order p^3. *J. Pure Appl. Algebra*, 219(8):3568–3603, 2015.
[6] D. Bachiller. Counterexample to a conjecture about braces. *J. Algebra*, 453:160–176, 2016.
[7] D. Bachiller. Extensions, matched products, and simple braces. *J. Pure Appl. Algebra*, 222(7):1670–1691, 2018.
[8] D. Bachiller, F. Cedó, and E. Jespers. Solutions of the Yang-Baxter equation associated with a left brace. *J. Algebra*, 463:80–102, 2016.
[9] D. Bachiller, F. Cedó, E. Jespers, and J. Okniński. Asymmetric product of left braces and simplicity; new solutions of the Yang-Baxter equation. *arXiv:1705.08493*.
[10] D. Bachiller, F. Cedó, E. Jespers, and J. Okninski. Iterated matched products of finite braces and simplicity; new solutions of the Yang-Baxter equation. *Accepted for publication in Trans. Amer. Math. Soc. arXiv:1610.00477*.
[11] H. U. Besche, B. Eick, and E. A. O'Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.*, 12(5):623–644, 2002.
[12] T. Brzeziński. Trusses: between braces and rings. *arXiv:1710.02870*.
[13] F. Catino, I. Colazzo, and P. Stefanelli. Regular subgroups of the affine group and asymmetric product of radical braces. *J. Algebra*, 455:164–182, 2016.
[14] F. Catino, I. Colazzo, and P. Stefanelli. Semi-braces and the Yang-Baxter equation. *J. Algebra*, 483:163–187, 2017.
[15] F. Catino and R. Rizzo. Regular subgroups of the affine group and radical circle algebras. *Bull. Aust. Math. Soc.*, 79(1):103–107, 2009.
[16] F. Cedó, T. Gateva-Ivanova, and A. Smoktunowicz. Braces and symmetric groups with special conditions. *arXiv:1703.08766, accepted for publication in J. Pure Appl. Alg.*
[17] 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.
[18] F. Cedó, E. Jespers, and J. Okniński. Braces and the Yang-Baxter equation. *Comm. Math. Phys.*, 327(1):101–116, 2014.
[19] F. Cedó, E. Jespers, and J. Okniński. Nilpotent groups of class three and braces. *Publ. Mat.*, 60(1):55–79, 2016.
[20] L. N. Childs. Left skew braces and the Galois correspondence for Hopf Galois structures. *arXiv:1802.03448*.
[21] K. De Commer. Actions of skew braces and set-theoretic solutions of the reflection equation. *arXiv:1803.05826*.
[22] C. Dietzel. Braces of order p^2q. *arXiv:1801.06911*.
[23] V. G. Drinfel′d. On some unsolved problems in quantum group theory. In *Quantum groups (Leningrad, 1990)*, volume 1510 of *Lecture Notes in Math.*, pages 1–8. Springer, Berlin, 1992.
[24] P. Etingof, T. Schedler, and A. Soloviev. Set-theoretical solutions to the quantum Yang-Baxter equation. *Duke Math. J.*, 100(2):169–209, 1999.
[25] T. Gateva-Ivanova. Set-theoretic solutions of the Yang-Baxter equation, Braces, and Symmetric groups. *arXiv:1507.02602*, 2015.
[26] L. Guarnieri and L. Vendramin. Skew braces and the Yang–Baxter equation. *Math. Comp.*, 86(307):2519–2534, 2017.
[27] E. Jespers and A. Van Antwerpen. Left semi-braces and solutions to the Yang-Baxter equation. *arXiv:1802.09993*.

[28] J.-H. Lu, M. Yan, and Y.-C. Zhu. On the set-theoretical Yang-Baxter equation. *Duke Math. J.*, 104(1):1–18, 2000.
[29] W. Rump. Classification of cyclic braces, II. *Accepted for publication in Trans. Amer. Math. Soc.*
[30] W. Rump. Braces, radical rings, and the quantum Yang-Baxter equation. *J. Algebra*, 307(1):153–170, 2007.
[31] W. Rump. Classification of cyclic braces. *J. Pure Appl. Algebra*, 209(3):671–685, 2007.
[32] W. Rump. The brace of a classical group. *Note Mat.*, 34(1):115–144, 2014.
[33] 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.
[34] A. Soloviev. Non-unitary set-theoretical solutions to the quantum Yang-Baxter equation. *Math. Res. Lett.*, 7(5-6):577–596, 2000.

Centre for Interdisciplinary Research in Computational Algebra, University of St Andrews, North Haugh, St Andrews, Fife, KY16 9SX, UK
E-mail address: `alexander.konovalov@st-andrews.ac.uk`

School of Mathematics, The University of Edinburgh, James Clerk Maxwell Building, The Kings Buildings, Mayfield Road EH9 3JZ, Edinburgh, UK
E-mail address: `A.Smoktunowicz@ed.ac.uk`

IMAS–CONICET and Departamento de Matemática, FCEN, Universidad de Buenos Aires, Pabellón 1, Ciudad Universitaria, C1428EGA, Buenos Aires, Argentina
E-mail address: `lvendramin@dm.uba.ar`