On Skew Braces (with an appendix by N. Byott and L. Vendramin)

ON SKEW BRACES (WITH AN APPENDIX BY N. BYOTT AND L. VENDRAMIN)

A. SMOKTUNOWICZ AND L. VENDRAMIN

Abstract. Braces are generalizations of radical rings, introduced by Rump to study involutive non-degenerate set-theoretical solutions of the Yang–Baxter equation (YBE). Skew braces were also recently introduced as a tool to study not necessarily involutive solutions. Roughly speaking, skew braces provide group-theoretical and ring-theoretical methods to understand solutions of the YBE. It turns out that skew braces appear in many different contexts, such as near-rings, matched pairs of groups, triply factorized groups, bijective 1-cocycles and Hopf–Galois extensions. These connections and some of their consequences are explored in this paper. We produce several new families of solutions related in many different ways with rings, near-rings and groups. We also study the solutions of the YBE that skew braces naturally produce. We prove, for example, that the order of the canonical solution associated with a finite skew brace is even: it is two times the exponent of the additive group modulo its center.

Contents

Introduction

In [19] Drinfeld posed the problem of studying set-theoretical solutions of the Yang–Baxter equation. Such solutions are pairs (X, r), where X is a set and

$$r\colon X \times X \to X \times X, \quad r(x, y) = (\sigma_x(y), \tau_y(x))$$

Key words and phrases. Braces, Yang–Baxter, Rings, Near-rings, Triply factorized groups, Matched pair of groups, Bijective 1-cocycles, Hopf–Galois extensions .

is a bijective map such that

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

The first two papers addressing this combinatorial problem were those of Etingof, Schedler, Soloviev [22] and Gateva-Ivanova and Van den Bergh [31]. Both papers considered involutive and non-degenerate solutions. A solution is said to be *involutive* if $r^2 = \mathrm{id}_{X\times X}$ and it is said to be *non-degenerate* if all the maps $\sigma_x, \tau_x \colon X \to X$ are bijective.

In [22], Etingof, Schedler and Soloviev introduced the *structure group* $G(X, r)$ of a solution (X, r) as the group with generators in $\{e_x : x \in X\}$ and relations $e_x e_y = e_{\sigma_x(y)} e_{\tau_y(x)}$, $x, y \in X$. They proved that $G(X, r)$ acts on X and there is a bijective 1-cocycle $G(X, r) \to \mathbb{Z}^{(X)}$ where $\mathbb{Z}^{(X)}$ is the free abelian group on X. Bijective 1-cocycles are a powerful tool for studying involutive set-theoretical solutions of the Yang–Baxter equation; see for example [22, 23].

Involutive solutions have been intensively studied; see for example [14, 18, 25, 26, 28, 29, 30]. In [44], Rump introduced braces, a new algebraic structure that turns out to be equivalent to bijective 1-cocycles; see [13, 27, 47]. According to the definition given by Cedó, Jespers and Okniński in [15], a brace is a triple $(A, \cdot, +)$, where $(A, \cdot)$ is a group, $(A, +)$ is an abelian group and

$$a(b + c) + a = ab + ac$$

holds for all $a, b, c \in A$. In this paper these braces will be called *classical* braces. It was observed by Rump that radical rings form an important family of examples of braces. This observation suggests using ring-theoretical methods to study involutive set-theoretical solutions. Rump also observed that a classical brace A produces an involutive non-degenerate solution:

$$r_A \colon A \times A \to A \times A, \quad r_A(a, b) = \left(ab - a, (ab - a)^{-1} ab\right).$$

Moreover, the structure group $G(X, r)$ admits a canonical brace structure. This brace structure over $G(X, r)$ is extremely important for understanding the structure of involutive set-theoretical solutions.

The study of non-involutive solutions of the Yang–Baxter equation is also an interesting problem with several applications in algebra and topology. Lu, Yan and Zhu [38] and Soloviev [49] extended the main results of [22] to non-involutive solutions. As in the involutive setting, one defines the structure group $G(X, r)$ and proves that there is a bijective 1-cocycle with domain $G(X, r)$ (now with values in a group which is in general not isomorphic to a free abelian group). These results suggest a generalization of classical braces known as *skew braces*; see [33].

Skew braces produce non-degenerate set-theoretical solutions; see Theorem 3.1. Moreover, the results of [38, 49] can now be translated into the language of skew braces. In particular, one obtains that $G(X, r)$ admits a canonical skew brace structure and its associated solution $r_{G(X,r)}$ satisfies a universal property; see Theorem 3.5.

It is remarkable that skew braces have connections with other algebraic structures such as groups with exact factorizations, Zappa–Szép products, triply factorized groups, rings and near-rings, regular subgroups, Hopf–Galois extensions. As skew braces produce non-degenerate solutions, these connections yield several new families of examples of solutions of the Yang–Baxter equation associated with rings, near-rings and groups.

This paper is organized as follows. In Section 1 we review the definition and some basic properties of skew braces and some elementary examples are given. In Section 2 connections to other topics in algebra are explored. We prove in Theorem 2.3 that factorizable groups are skew braces. As a corollary we prove that Zappa-Szép product of groups and semidirect products of groups are skew braces. Theorem 2.3 is also used to construct skew braces from Jacobson radical rings. In Theorem 2.12 we prove that skew braces provide examples of triply factorized groups. In Theorem 2.17 we translate a result of Sysak for triply factorized groups into the language of skew braces. Based on this theorem, one easily finds a connection between near-rings and skew braces; see Proposition 2.20. Several general constructions of skew braces are stated, for example semidirect products, Zappa–Szép products and wreath products of skew braces. The first two sections contain several new examples of skew braces. We summarize these examples in the following table:

Additive group	Multiplicative group	Reference
$\mathbb{S}_3$	C_6	Example 1.13
dihedral group	quaternion group	Example 1.18
$\mathbb{A}_4$	$C_3 \rtimes C_4$	Example 1.20
$\mathrm{GL}(n, C)$	$U(n) \times T(n)$	Example 2.4
$\mathbb{A}_5$	$\mathbb{A}_4 \times C_5$	Example 2.5
$\mathrm{PSL}(2, 7)$	$\mathbb{S}_4 \times C_7$	Example 2.6

In Section 3 the canonical non-degenerate solution associated to a skew brace (constructed in Theorem 3.1) is studied. We prove in Corollary 3.3 that the solutions associated with skew braces are biquandles; hence skew braces could be used to construct combinatorial invariants of knots. In Theorem 3.13 it is proved that the solution associated to a finite skew brace is always a permutation of even order; and the order of this permutation is computed explicitly in terms of the exponent of a certain quotient the additive group of the skew brace. In Section 4 ideals of skew braces simple skew braces and skew braces of finite multipermutation level are introduced. Finally, in Section 5 it is proved that skew braces are related to other algebraic structures such as cycle sets (Theorem 5.8) and matched pairs of groups (Theorem 5.11).

Notations and conventions. If X is a set, we write $|X|$ to denote the cardinality of X and $\mathbb{S}_X$ to denote the group of bijective maps $X \to X$.

For $n \in \mathbb{N}$ the symmetric group in n letters will be denoted by $\mathbb{S}_n$, the alternating group in n letters by $\mathbb{A}_n$ and the cyclic group of order n by C_n. Usually we simply write ab to denote the product $a \cdot b$.

1. Preliminaries

Skew braces were first defined in [33]. In this section we recall the basic notions and properties of skew braces.

Definition 1.1. *A* skew brace *is a triple $(A, \cdot, \circ)$, where $(A, \cdot)$ and $(A, \circ)$ are groups and the compatibility condition*

$$a \circ (bc) = (a \circ b)a^{-1}(a \circ c) \tag{1.1}$$

holds for all $a, b, c \in A$, where a^{-1} denotes the inverse of a with respect to the group $(A, \cdot)$. The group $(A, \cdot)$ will be the additive group *of the brace and $(A, \circ)$ will be the* multiplicative group *of the brace. A skew brace is said to be* classical *if its additive group is abelian.*

Definition 1.2. *Let A and B be skew braces. A map $f\colon A \to B$ is said to be a* brace homomorphism *if $f(aa') = f(a)f(a')$ and $f(a \circ a') = f(a) \circ f(a')$ for all $a, a' \in A$.*

Remark 1.3. Skew braces form a category.

Remark 1.4. It follows from (1.1) that in every brace A the neutral elements of $(A, \cdot)$ and $(A, \circ)$ concide.

Example 1.5. *Let A be a group. Then $a \circ b = ab$ gives a skew brace. Similarly, the operation $a \circ b = ba$ turns A into a skew brace.*

Example 1.6. *Let A and M be groups and let $\alpha\colon A \to \operatorname{Aut}(M)$ be a group homomorphism. Then $M \times A$ with*

$$(x, a)(y, b) = (xy, ab), \quad (x, a) \circ (y, b) = (x\alpha_a(y), ab)$$

is a skew brace. Similarly, $M \times A$ with

$$(x, a)(y, b) = (x\alpha_a(y), ab), \quad (x, a) \circ (y, b) = (xy, ba)$$

is a skew brace.

Example 1.7. *Let A and B be skew braces. Then $A \times B$ with*

$$(a, b)(a', b') = (aa', bb'), \quad (a, b) \circ (a', b') = (a \circ a', b \circ b'),$$

is a skew brace.

Lemma 1.8. [33, Corollary 1.10] *Let A be a skew brace. The map*

$$\lambda\colon (A, \circ) \to \operatorname{Aut}(A, \cdot), \quad \lambda_a(b) = a^{-1}(a \circ b),$$

is a group homomorphism.

Remark 1.9. If A is a skew brace and $a \in A$, the inverse of a with respect to $\circ$ is the element $\overline{a} = \lambda_a^{-1}(a^{-1})$.

Lemma 1.8 justifies the following definition:

Definition 1.10. *Let A be a skew brace. The* crossed group *of A is defined as the group $\Gamma(A) = (A, \cdot) \rtimes (A, \circ)$ with multiplication*

$$(a, x)(b, y) = (a\lambda_x(b), x \circ y).$$

Lemma 1.11. [3, Lemma 2.4] *Let A be a skew brace and let*

$$\mu \colon (A, \circ) \to \mathbb{S}_A, \quad \mu_b(a) = \overline{\lambda_a(b)} \circ a \circ b.$$

Then $\mu_1 = \mathrm{id}$ and $\mu_{a \circ b} = \mu_b \mu_a$ for all $a, b \in A$.

The following lemma was proved by Bachiller for classical braces, see [4, Proposition 2.3]. The same proof also works for skew braces.

Lemma 1.12. [5, Lemma 1.1.17] *Let A be a group and $\lambda \colon A \to \mathrm{Aut}(A)$ be a map such that*

$$\lambda_{a\lambda_a(b)} = \lambda_a \lambda_b, \quad a, b \in A. \tag{1.2}$$

Then A with $a \circ b = a\lambda_a(b)$ is a skew brace.

Proof. The first claim is [33, Corollary 1.10]. For the second claim see [5, Lemma 1.1.17]. □

Example 1.13. *Let $A = \mathbb{S}_3$ and $\lambda \colon A \to \mathbb{S}_A$ be given by*

$$\lambda_{\mathrm{id}} = \lambda_{(123)} = \lambda_{(132)} = \mathrm{id},$$
$$\lambda_{(12)} = \lambda_{(23)} = \lambda_{(13)} = \textit{conjugation by } (23).$$

It is easy to check that $\lambda_{a\lambda_a(b)} = \lambda_a \lambda_b$ for all $a, b \in A$. Hence A is a skew brace by Lemma 1.12. Since the transposition (12) has order six in the group $(A, \circ)$, it follows that $(A, \cdot) \simeq \mathbb{S}_3$ and $(A, \circ) \simeq C_6$.

The following lemma provides another useful tool for constructing skew braces.

Lemma 1.14. *Let $(A, \circ)$ be a group and $\lambda \colon A \to \mathbb{S}_A$ be a group homomorphism. Assume that $\lambda_a(1) = 1$ for all $a \in A$ and that*

$$\lambda_a(b \circ \lambda_b^{-1}(c)) = \lambda_a(b) \circ \lambda_{\lambda_a(b)}^{-1} \lambda_a(c) \tag{1.3}$$

for all $a, b, c \in A$. Then A with $ab = a \circ \lambda_a^{-1}(b)$ is a skew brace.

Proof. Note that Equation (1.3) is equivalent to

$$\lambda_a^{-1}(bc) = \lambda_a^{-1}(b) \lambda_a^{-1}(c). \tag{1.4}$$

We prove that the operation is associative:

$$\begin{aligned} a(bc) &= a \circ \lambda_a^{-1}(bc) = a \circ (\lambda_a^{-1}(b) \lambda_a^{-1}(c)) \\ &= a \circ \lambda_a^{-1}(b) \circ \lambda_{a \circ \lambda_a^{-1}(b)}^{-1}(c) = (ab) \circ \lambda_{ab}^{-1}(c) = (ab)c. \end{aligned}$$

The neutral element 1 of A is a right identity: $a1 = a \circ \lambda_a^{-1}(1) = a \circ 1 = a$. The element $a^{-1} = \lambda_a(\overline{a})$ is a right inverse of A since

$$aa^{-1} = a \circ \lambda_a^{-1}(a^{-1}) = a \circ \lambda_a^{-1} \lambda_a(\overline{a}) = a \circ \overline{a} = 1.$$

Therefore $(A, \cdot)$ is a group by [42, §1.1.2].

The brace compatibility condition follows from Equation (1.4):

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

The lemma is proved. □

Definition 1.15. *A skew brace A is said to be a* two-sided *skew brace if*

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

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

Example 1.16. *Let A be a skew brace with abelian multiplicative group. Then A is a two-sided skew brace.*

Example 1.17. *Let $n \in \mathbb{N}$ be such that $n = p_1^{a_1} \cdots p_k^{a_k}$, where the p_j are distinct primes, all $a_j \in \{0, 1, 2\}$ and $p_i^m \not\equiv 1 \pmod{p_j}$ for all i, j, m with $1 \leq m \leq a_i$. Then every skew brace of size n is a two-sided classical brace, since every group of order n is abelian, see for example* [41].

Example 1.18. *Let*

$$A = \langle r, s : r^4 = s^2 = 1, srs = r^{-1} \rangle$$

be the dihedral group of eight elements and let

$$B = \{1, -1, i, -i, j, -j, k, -k\}$$

be the quaternion group of eight elements. Let $\pi : B \to A$ be the bijective map given by

$$\begin{aligned} 1 &\mapsto 1, & -1 &\mapsto r^2, & -k &\mapsto r^3 s, & k &\mapsto rs, \\ i &\mapsto s, & -i &\mapsto r^2 s, & j &\mapsto r^3, & -j &\mapsto r. \end{aligned}$$

A straightforward calculation shows that A with

$$x \circ y = \pi(\pi^{-1}(x)\pi^{-1}(y))$$

is a skew brace with additive group A and multiplicative group isomorphic to B. This skew brace is two-sided.

The following proposition provides other examples:

Proposition 1.19. *Let A be a skew brace such that $\lambda_a(a) = a$ for all $a \in A$. Then A is a two-sided skew brace.*

Proof. First we notice that $a^{-1} = \overline{a}$ since $\overline{a} = \lambda_a^{-1}(a^{-1}) = \lambda_a^{-1}(a)^{-1} = a^{-1}$. In particular,

$$x \circ y = \overline{\overline{y} \circ \overline{x}} = (y^{-1} \circ x^{-1})^{-1} \tag{1.5}$$

for all $x, y \in A$. Using (1.1) and (1.5) one obtains that

$$\begin{aligned}(ab) \circ c &= (c^{-1} \circ (b^{-1}a^{-1}))^{-1} \\ &= \big((c^{-1} \circ b^{-1})c(c^{-1} \circ a^{-1})\big)^{-1} \\ &= (c^{-1} \circ a^{-1})^{-1}c^{-1}(c^{-1} \circ b^{-1})^{-1} \\ &= (a \circ c)c^{-1}(b \circ c).\end{aligned}$$

This completes the proof. □

Now we show a non-classical skew brace that is not two-sided:

Example 1.20. *Let G be the group generated by the permutations*

$$(1263)(48ba)(57c9), \quad (145)(278)(39a)(6bc).$$

Then G is a group of order twelve isomorphic to $C_3 \rtimes C_4$. Let $\pi\colon G \to \mathbb{A}_4$ be the bijective map given by

$$\begin{aligned}
&\mathrm{id} \mapsto \mathrm{id}, && (16)(23)(4b)(5c)(79)(8a) \mapsto (14)(23),\\
&(145)(278)(39a)(6bc) \mapsto (234), && (1b564c)(29837a) \mapsto (143),\\
&(154)(287)(3a9)(6cb) \mapsto (243), && (1c465b)(2a7389) \mapsto (142),\\
&(1362)(4ab8)(59c7) \mapsto (13)(24), && (1263)(48ba)(57c9) \mapsto (12)(34),\\
&(1a68)(253c)(49b7) \mapsto (132), && (186a)(2c35)(47b9) \mapsto (124),\\
&(1967)(243b)(5ac8) \mapsto (134), && (1769)(2b34)(58ca) \mapsto (123).
\end{aligned}$$

A straightforward calculation shows that $\mathbb{A}_4$ with the operation

$$\sigma \circ \tau = \pi(\pi^{-1}(\sigma)\pi^{-1}(\tau))$$

is a skew brace.

Let $a = (14)(23)$ and $b = c = (234)$. Then

$$(12)(34) = (ab) \circ c \neq (a \circ c)c^{-1}(a \circ b) = (123),$$

hence it is not two-sided.

1.1. **Skew braces with nilpotent additive group.** Skew braces with nilpotent additive group are similar to classical braces. It was observed in [48] Sylow subgroups of the additive group of finite classical braces are also braces.

Theorem 1.21. *Let A be a finite skew brace whose additive group $(A, \cdot)$ is nilpotent and decomposes as $A = A_1 \cdots A_k$, where A_j is a Sylow subgroup of order $p_j^{\alpha_j}$, p_j is a prime number and $\alpha_j \geq 1$. Then each A_i is a skew brace.*

Proof. It is enough to prove that the subgroup A_1 of $(A, \cdot)$ is a subgroup of $(A, \circ)$. Remark 1.4 implies that $A_1 \neq \emptyset$. Let $a \in A$ and $b \in A_1$. Since $p_1^{\alpha_1}b = 0$ and λ_a is a group automorphism of $(A, \cdot)$, $0 = \lambda_a(p_1^{\alpha_1}b) = p_1^{\alpha_1}\lambda_a(b)$. Hence $\lambda_a(b) \in A_1$ and $\lambda_a^{-1}(b) = \lambda_{\overline{a}}(b) \in A_1$. Therefore $a \circ b = a\lambda_a(b) \in A_1$ and $\overline{a} = \lambda_a^{-1}(a^{-1}) \in A_1$ for all $a, b \in A_1$. □

Corollary 1.22. *Let A be a finite skew brace whose additive group $(A,\cdot)$ is nilpotent and decomposes as $A = A_1 \cdots A_k$, where A_j is a Sylow subgroup of order $p_j^{\alpha_j}$, p_j is a prime number and $\alpha_j \geq 1$. Then each $A_{i_1} \cdots A_{i_l}$ is a skew brace.*

Proof. It follows from Theorem 1.21 and induction on k. □

Corollary 1.23. *Let A be a finite skew brace whose additive group $(A,\cdot)$ is nilpotent. Then $(A,\circ)$ is solvable.*

Proof. By Corollary 1.22, for each prime p there exists subgroup of $(A,\cdot)$ of order coprime with p. Thus the claim follows from Hall Theorem; see for example [42, §9.1.8]. □

Remark 1.24. Corollary 1.23 was proved by Byott in the context of Hopf–Galois extensions; see [11, Theorem 1].

We recall some questions from [5], see also [11, §1].

Question 1.25. *Let A be a finite skew brace with solvable additive group. Is the multiplicative group solvable?*

Question 1.26. *Let A be a finite skew brace with nilpotent multiplicative group. Is the additive group solvable?*

Remark 1.27. Partial results to Questions 1.25 and 1.26 can be found in the context of Hopf–Galois extensions; see for example [9, 11].

1.2. **Bijective 1-cocycles.** In this subsection we review the equivalence between skew braces and bijective 1-cocycles.

Let G and A be groups such that G acts on A by automorphisms. Recall that a *bijective 1-cocycle* is an invertible map $\pi\colon G \to A$ such that

$$\pi(gh) = \pi(g)(g \cdot \pi(h))$$

for all $g, h \in G$.

Example 1.28. *The maps of Examples 1.18 and 1.20 are bijective 1-cocycles.*

Let $\pi\colon G \to A$ and $\eta\colon H \to B$ be bijective 1-cocycles. A *homorphism* between these bijective 1-cocycles is a pair (f, g) of group homomorphisms $f\colon G \to H$, $g\colon A \to B$ such that

$$\begin{aligned} &\eta f = g\pi, \\ &g(h \cdot a) = f(h) \cdot g(a), \qquad\qquad a \in A,\ h \in G. \end{aligned}$$

Bijective 1-cocycles form a category.

For a given group A let $\mathfrak{C}(A)$ be the full subcategory of the category of bijective 1-cocycles with objects $\pi\colon G \to A$ and let $\mathfrak{B}_{\mathrm{add}}(A)$ be the full subcategory of the category of skew braces with additive group A.

Theorem 1.29. [33, Proposition 1.11] *Let A be a group. The categories $\mathfrak{B}_{\mathrm{add}}(A)$ and $\mathfrak{C}(A)$ are equivalent.*

Remark 1.30. In the context of classical braces, Theorem 1.29 was implicit in the work of Rump; see [44, 47] or [27].

Remark 1.31. In [20] Etingof and Gelaki give a method of constructing finite-dimensional complex semisimple triangular Hopf algebras. They show how any non-abelian group which admits a bijective 1-cocycle gives rise to a semisimple minimal triangular Hopf algebra which is not a group algebra.

2. Examples and constructions

2.1. **Factorizable groups.** For an introduction to the theory of factorizable groups we refer to [1]. Recall that a group A *factorizes* through two subgroups B and C if $A = BC = \{bc : b \in B, c \in C\}$. The factorization is said to be *exact* if $B \cap C = 1$.

The following proposition produces factorizable groups from classical and skew braces:

Proposition 2.1. *Let A be a skew brace. Assume that there exist subbraces B and C such that $(A, \cdot)$ admits an exact factorization through $(B, \cdot)$ and $(C, \cdot)$. If $\lambda_b(c) \in C$ for all $b \in B$ and $c \in C$, then $(A, \circ)$ admits an exact factorization through $(B, \circ)$ and $(C, \circ)$.*

Proof. The claim follows from the equality $a = bc = b \circ \lambda_b^{-1}(c)$. □

Example 2.2. *Let A be a classical brace (or more generally, a skew brace with nilpotent additive group). Assume that the group $(A, \cdot)$ decomposes as $A_1 \cdots A_k$, where the A_j are the Sylow subgroups of $(A, \cdot)$. Let $I \subseteq \{1, \dots, k\}$, $B = \prod_{i \in I} A_i$ and $C = \prod_{i \notin I} A_i$. Then $(A, \circ)$ admits an exact factorization through B and C by Corollary 1.22 and Proposition 2.1.*

Theorem 2.3. *Let A be a group that admits an exact factorization through two subgroups B and C. Then A with*

$$a \circ a' = ba'c, \quad a = bc \in BC,\ a' \in A,$$

is a skew brace with multiplicative group isomorphic to $B \times C$ and additive group isomorphic to A.

Proof. The map $\eta\colon B \times C \to A$, $\eta(b, c) = bc^{-1}$, is bijective. Since η is bijective and $a \circ a' = \eta(\eta^{-1}(a)\eta^{-1}(a'))$, it follows that $(A, \circ)$ is a group isomorphic to the direct product $B \times C$. To prove that A is a skew brace it remains to show (1.1). Let $a = bc \in BC$ and $a', a'' \in A$. Then

$$\begin{aligned}(a \circ a')a^{-1}(a \circ a'') &= (ba'c)a^{-1}(ba''c)\\ &= ba'c(c^{-1}b^{-1})ba''c\\ &= ba'a''c\\ &= a \circ (a'a'').\end{aligned}$$

This completes the proof. □

Example 2.4 (QR decomposition)**.** *Let $n \in \mathbb{N}$. The group $\mathrm{GL}(n,\mathbb{C})$ admits an exact factorization as through the subgroups $U(n)$ and $T(n)$, where $U(n)$ is the unitary group and $T(n)$ is the group of upper triangular matrices with positive diagonal entries. Therefore there exists a skew brace A with $(A,\cdot) \simeq \mathrm{GL}(n,\mathbb{C})$ and $(A,\circ) \simeq U(n) \times T(n)$.*

Example 2.5. *The alternating simple group $\mathbb{A}_5$ admits an exact factorization through the subgroups*

$$A = \langle (123), (12)(34) \rangle \simeq \mathbb{A}_4, \quad B = \langle (12345) \rangle \simeq C_5.$$

By Theorem 2.3, there exists a skew brace with additive group $\mathbb{A}_5$ and multiplicative group $\mathbb{A}_4 \times C_5$. Compare with [11, Corollary 1.1(i)].

Example 2.6. *The simple group $\mathrm{PSL}(2,7)$ admits an exact factorization through the subgroups $A \simeq \mathbb{S}_4$ and $B \simeq C_7$. By Theorem 2.3, there exists a skew brace with additive group $\mathrm{PSL}(2,7)$ and multiplicative group $\mathbb{S}_4 \times C_7$. Compare with* [11, Corollary 1.1(ii)].

Recall from [36] that a pair (A,B) of groups is said to be *matched* if there are two actions

$$B \overset{\leftharpoonup}{\curvearrowright} B \times A \overset{\rightharpoonup}{\curvearrowright} A$$

such that

$$b \rightharpoonup (aa') = (b \rightharpoonup a)\left((b \leftharpoonup a) \rightharpoonup a'\right), \tag{2.1}$$

$$(bb') \leftharpoonup a = (b \leftharpoonup (b' \rightharpoonup a))(b' \leftharpoonup a) \tag{2.2}$$

for all $a, a' \in A$ and $b, b' \in B$. If the quadruple $(A, B, \rightharpoonup, \leftharpoonup)$ form a matched pair of groups, then $A \times B$ is a group with multiplication

$$(a,b)(a',b') = \left(a(b \rightharpoonup a'), (b \leftharpoonup a')b'\right),$$

where $a, a' \in A$ and $b, b' \in B$. The inverse of (a,b) is

$$(a,b)^{-1} = (b^{-1} \rightharpoonup a^{-1}, (b \leftharpoonup (b^{-1} \rightharpoonup a^{-1}))^{-1}).$$

This group will be denoted by $A \bowtie B$ and it is known as the *biproduct* or the *Zappa–Szép product* of A and B.

Corollary 2.7. *Let A and B be a matched pair of groups. Then the biproduct $A \bowtie B$ is a skew brace with*

$$(a,b)(a',b') = (a(b \rightharpoonup a'), (b \leftharpoonup a')b'), \quad (a,b) \circ (a',b') = (aa', b'b),$$

where $a, a' \in A$ and $b, b' \in B$.

Proof. It follows from Theorem 2.3 since the biproduct $A \bowtie B$ admits an exact factorization through the subgroups $A \bowtie 1 \simeq A$ and $1 \bowtie B \simeq B$. □

Theorem 2.3 is useful to construct skew braces associated with rings.

Proposition 2.8. *Let R be a ring (associative, noncommutative), let S be a subring of R and let I be a left ideal in R such that $S \cap I = 0$ and $R = S + I$. Assume that S and I are Jacobson radical rings (for example nilpotent rings). Then R with the operation*

$$a \circ b = a + b + ab$$

is a group and $R = S \circ I$ is an exact factorization.

Proof. It is easy to prove that $\circ$ is associative. Moreover, since S and I are Jacobson radical rings, it follows that $(S, \circ)$ and $(I, \circ)$ are groups.

We claim that each $r \in R$ can be written as $r = a \circ b$ for some $a \in S$ and $b \in I$. Since $R = I + S$, one writes $r = i + s$ for some $s \in S$ and $i \in I$. Now let $\overline{s}$ be the inverse of s in the group $(S, \circ)$. Then

$$r = s \circ (\overline{s} \circ r)$$

with $s \in S$ and $\overline{s} \circ r = \overline{s} \circ (i + s) = i + \overline{s}i \in I$. Since $(S, \circ)$ and $(I, \circ)$ are groups and $R = S \circ I$, it follows that $(R, \circ)$ is a group. The factorization $R = S \circ I$ is exact since $I \cap S = 0$. □

Particular cases of Proposition 2.8 can be easily obtained as factors of free algebras or as factors of differential polynomial rings.

Example 2.9. *Let F be a field and let $P = F\langle x_1, \ldots, x_n\rangle$ be the noncommutative (associative) polynomial ring in n noncommuting variables, and let A be the subalgebra of P consisting of polynomials which have zero constant term. Let V be the linear space over F spanned by $x_1, \ldots, x_n$ and let V_1 and V_2 be linear subspaces of A such that $V = V_1 \oplus V_2$. Let $Q \subseteq A$ be an ideal in A such that $A^m \subseteq Q$ for some m, and denote $J = QA$ (note that J is an ideal in P). Let $R = A/J$. Then*

$$S = \{a + J : a \in PV_1\} \subseteq R, \quad I = \{a + J : a \in PV_2\} \subseteq R,$$

satisfy the assumptions of Proposition 2.8 and hence $(R, \circ)$ admits an exact factorization $R = S \circ I$.

Example 2.10. *Let N be a nilpotent ring and M be a left N-module. Let R be the ring of matrices*

$$\begin{pmatrix} N & M \\ 0 & 0 \end{pmatrix} = \left\{ \begin{pmatrix} n & m \\ 0 & 0 \end{pmatrix} : n \in N,\, m \in M \right\},$$

and

$$S = \begin{pmatrix} N & 0 \\ 0 & 0 \end{pmatrix} \subseteq R, \quad I = \begin{pmatrix} 0 & M \\ 0 & 0 \end{pmatrix} \subseteq R.$$

Then R, I and S satisfy the assumptions of Proposition 2.8 and the group $(R, \circ)$ admits an exact factorization as $R = S \circ I$.

Remark 2.11. Exactly factorizable groups give rise to a special class of Hopf algebras, see for example [6, 21, 35, 52].

2.2. **Triply factorized groups.** In [50] Sysak observed an interesting connection between radical rings and triply factorized groups. This idea shows that skew braces produce triply factorized groups.

Recall that a *triply factorized group* is tuple (G, A, B, M), where G is a group with subgroups A, B and M and such that $G = AM = BM = AB$ and $A \cap M = B \cap M = 1$.

Theorem 2.12. *Let X be a skew brace. Let $G = \Gamma(X)$, $A = (X, \cdot) \times 1$, $M = 1 \times (X, \circ)$ and $B = \{(x, x) : x \in X\}$. Then (G, A, B, M) is a triply factorized group such that $A \cap B = 1$.*

Proof. Clearly $G = AM$ and $A \cap M = A \cap B = B \cap M = 1$. Let us prove that B is a subgroup of G. Clearly B is nonempty. For $x, y \in X$, using that $\overline{y} = \lambda_y^{-1}(y^{-1})$, one obtains

$$(x, x)(y, y)^{-1} = (x, x)(\overline{y}, \overline{y}) = (x \circ \overline{y}, x \circ \overline{y}) \in B.$$

To prove that $G = BM$ notice that $(x, y) = (x, x)(1, \overline{x} \circ y) \in BM$. Similarly $(x, y) = (xy^{-1}, 1)(y, y) \in AB$, proves that $G = AB$. □

Example 2.13. *Let R be a nilpotent ring (associative, noncommutative), let S be a subring of R and let I_1 and I_2 be left ideals of R such that*

$$S \cap I_1 = S \cap I_2 = I_1 \cap I_2 = 0, \quad R = S + I_1 = S + I_2 = I_1 + I_2.$$

Proposition 2.8 with $A = S$, $B = I_1$ and $M = I_2$ implies that $(R, \circ)$ is a triply group factorized group:

$$R = A \circ B = A \circ M = B \circ M, \quad A \cap B = 0.$$

Let us show a particular case of Example 2.13.

Example 2.14. *Recall the notation from Example 2.9. Let $n = 2m$ for some $m \in \mathbb{N}$ and let*

$$V_1 = \sum_{i=1}^{m} Fx_i, \qquad V_2 = \sum_{i=m+1}^{2m} Fx_i, \qquad V_3 = \sum_{i=1}^{m} F(x_i + x_{m+i}).$$

Now let

$$A = \{a + J : a \in PV_1\}, \quad B = \{a + J : a \in PV_2\}, \quad M = \{a + J : a \in PV_3\}.$$

Proposition 2.8 implies that $(R, \circ)$ is a triply factorized group:

$$R = A \circ B = A \circ M = B \circ M, \quad A \cap B = 0.$$

Remark 2.15. Let A be a skew brace. The multiplicative group $(A, \circ)$ with actions $x \rightharpoonup y = \lambda_x(y)$ and $x \leftharpoonup y = \mu_y(x)$ form a matched pair of groups, see Lemma 5.9. The biproduct $(A, \circ) \bowtie (A, \circ)$ has multiplication

$$(x, y)(x', y') = (x \circ \lambda_y(x'), \mu_{x'}(y) \circ y')$$

and it is a triply factorizable group with $A = (A, \circ) \times 1$, $M = 1 \times (A, \circ)$ and $\Delta = \{(x, \overline{x}) : x \in A\}$. The multiplication on Δ is given by

$$(a, \overline{a})(b, \overline{b}) = (a \circ \lambda_{\overline{a}}(b), \mu_b(\overline{a}) \circ \overline{b}) = (ab, \overline{ab})$$

since $ab = a \circ \lambda_{\overline{a}}(b)$ and $a \circ \lambda_{\overline{a}}(b) \circ \mu_b(\overline{a}) \circ \overline{b} = 1$. There is a left action of $(A, \circ)$ on Δ given by

$$a \cdot (b, \overline{b}) = (1, a)(b, \overline{b})(1, a)^{-1} = (\lambda_a(b), \overline{\lambda_a(b)})$$

and the map $\Delta \rtimes (A, \circ) \to (A, \circ) \bowtie (A, \circ)$ given by $((a, \overline{a}), b) \mapsto (a, \overline{a} \circ b)$ is a group isomorphism.

Lemma 2.16. *Let (G, A, B, M) be a triply factorized group with M normal in G and $A \cap B = 1$. For each $m \in M$ there exists a unique $\gamma(m) \in A$ such that $m\gamma(m) \in B$. Moreover, the map $m \mapsto \gamma(m)$ is bijective.*

Proof. Since $G = AB = BA$ and $A \cap B = 1$, for each $m \in M$ there is a unique $\gamma(m) \in A$ such that $m\gamma(m) \in B$, i.e. if $m = ba$, then $\gamma(m) = a^{-1}$. Similarly, $A \subseteq MB = BM$ and $M \cap B = 1$ imply that for each $a \in A$ there is a unique $\pi(a) \in M$ such that $\pi(a)a \in B$, i.e. if $a = b_1 m_1$, then $\pi(a) = b_1 m_1^{-1} b_1^{-1}$. Now it follows $\pi(\gamma(m)) = m$ for all $m \in M$ and that $\gamma(\pi(a)) = a$ for all $a \in A$. □

The following result is [51, Proposition 21] in the language of skew braces:

Theorem 2.17 (Sysak)**.** *Let (G, A, B, M) be a triply factorized group such that M is normal in G and $A \cap B = 1$. Then M with*

$$m \circ m' = \gamma^{-1}(\gamma(m)\gamma(m')),$$

where γ is the map of Lemma 2.16, is a skew brace such that $\Gamma(M) \simeq G$.

Proof. For $m, m' \in M$ write $a = \gamma(m)$ and $a' = \gamma(m')$. By Lemma 2.16, $m \circ m' = \gamma^{-1}(\gamma(m)\gamma(m'))$ defines a group structure over M isomorphic to that of A. Since $m(am'a^{-1})(aa') = (ma)(m'a') \in B$, it follows that

$$m \circ m' = m(am'a^{-1}).$$

Now M is a skew brace since

$$\begin{aligned}(m \circ m')m^{-1}(m \circ m'') &= m(am'a^{-1})m^{-1}m(am''a^{-1}) \\ &= mam'm''a^{-1} \\ &= m \circ (m'm'').\end{aligned}$$

Since $G = MA = AM$, a routine calculation proves $\Delta\colon \Gamma(M) \to G$, $(m, x) \mapsto m\gamma(x)$, is a bijective group homomorphism:

$$\begin{aligned}\Delta((m, x)(n, y)) &= \Delta(m\lambda_x(n), x \circ y) \\ &= m\lambda_x(n)\gamma(x \circ y) \\ &= m\lambda_x(n)\gamma(x)\gamma(y) \\ &= mx^{-1}(x \circ n)\gamma(x)\gamma(y) \\ &= mx^{-1}(x\gamma(x)n\gamma(x)^{-1})\gamma(x)\gamma(y) \\ &= m\gamma(x)n\gamma(y) \\ &= \Delta(m, x)\Delta(n, y).\end{aligned}$$

This completes the proof. □

2.3. **Near-rings.** This section is based on the work of Sysak on near-rings; see for example [51, §10]. However, the connection with skew braces and all the examples in this section are new.

We refer to [39] for the basic theory of near-rings. Recall that *near-ring* is a set N with two binary operations

$$(x, y) \mapsto x + y, \quad (x, y) \mapsto x \cdot y,$$

such that $(N, +)$ is a (not necessarily abelian) group, $(N, \cdot)$ is a semigroup, and $x \cdot (y+z) = x \cdot y + x \cdot z$ for all $x, y, z \in N$. We assume that our near-rings contain a multiplicative identity, denoted by 1.

Example 2.18. *Let G be a (not necessarilly abelian) additive group and $M(G)$ be the set of maps $G \to G$. Then $M(G)$ is a near-ring under the following operations:*

$$(f + g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = g(f(x)), \quad f, g \in M(G), x \in G.$$

A subgroup M of $(N, +)$ is said to be a *construction subgroup* if $1 + M$ is a subgroup of the multiplicative subgroup $N^\times$ of units of N.

Lemma 2.19. *Let N be a near-ring and M be a construction subgroup of N. Then $(1 + M) \cdot M \subseteq M$. In particular, $1 + M$ acts on M by left multiplication.*

Proof. Let $a, a' \in 1 + M$. Then

$$-a' + a = -a' + 1 - 1 + a = -(-1 + a') + (-1 + a) \in M$$

since $-1 + a' \in M$ and $-1 + a \in M$. Let $m, m' \in M$ and write $m = -1 + a$ and $m' = -1 + a'$ for some $a, a' \in 1 + M$. Then

$$(1 + m) \cdot m' = a \cdot (-1 + a') = -a + a \cdot a' \in M$$

since $a \in 1 + M$ and $a \cdot a' \in 1 + M$. □

Proposition 2.20. *Let N be a near-ring and M be a construction subgroup. Then M is a skew brace with*

$$mm' = m + m', \quad m \circ m' = m + (1 + m) \cdot m'.$$

Proof. By Lemma 2.19, the operations are well-defined. For each $m \in M$ let λ_m be the map $n \mapsto (1+m) \cdot n$. It is routine to verify that $\lambda \colon M \to \mathrm{Aut}(M)$, $m \mapsto \lambda_m$, is a well-defined map such that $\lambda_{m+\lambda_m(n)} = \lambda_m \lambda_n$. By applying Lemma 1.12, the proposition is proved. □

Remark 2.21. Proposition 2.20 shows a connection between near-rings and skew braces. This connection then answers [12, Question 1].

If N is a near-ring and M is a construction subgroup of N, Proposition 2.20 implies that M is a skew brace. The following is the translation of a theorem of Hubert in the language of skew braces:

Theorem 2.22 (Hubert)**.** *Let A be a skew brace with multiplicative group isomorphic to G. The near-ring $M(G)$ contains a construction subgroup M such that $\Gamma(A) \simeq \Gamma(M)$.*

Proof. By Theorem 2.12, the group $G = \Gamma(A)$ provides a triply factorized group $G = MA = MB = AB$ with $A \cap B = 1$. Now [34, Theorem 2.9] applies. □

2.4. **Nilpotent rings.** We now construct examples of skew braces related to nilpotent rings and algebras. These examples are influenced by near ring theory and construction subgroups. The following result is inspired by [39, Example 1.6].

Lemma 2.23. *Let F be a finite field and let A be a commutative F-algebra such that $A = F + N$ where N is a nilpotent subalgebra of A. Let S be the set of all functions $A \to A$ which can be written as polynomials from $N[x]$ (where two functions are equal if they have the same values). Then S with the operation*

$$f(x) \bullet g(x) = f(x) + g(x + f(x))$$

is a group.

Proof. Direct calculations show that the operation is associative and that $f(x) = 0$ is the identity element of S. It suffices to prove that each element in S has a left inverse, i.e, for each $g(x) \in S$ there exists $f(x) \in S$ such that $f(x) = -g(x + f(x))$. The map $f(x)$ can be obtained recursively as

$$f(x) = -g(x - g(x - g(x + g(\cdots(x - g(x))\cdots)))),$$

where the number of brackets is equal to n and $N^n = 0$. Indeed, for any $p \in N[x]$, $-g(x - g(x - g(x + g(\cdots(x - g(x + p))\cdots)))) = f(x)$ because the element p will be multiplied by at least n elements from N in the left hand-side of this equation. Hence it will have zero value (where the left hand side has n brackets). By substituting $p = -g(x)$ we get that

$$f(x) = -g(x - g(x - g(x + g(\cdots(x - g(x))\cdots)))),$$

where the number of brackets is $n + 1$. Therefore, $-g(x + f(x)) = f(x)$, as required. □

Remark 2.24. The same construction of Lemma 2.23 works when A is a noncommutative associative algebra. In this case instead of the polynomial ring $A[x]$ one takes the noncommutative polynomial ring, where the variable x does not commute with the elements of A.

We are now ready to present some examples of skew braces inspired by the near-ring of functions $M(G)$ over a group G.

Proposition 2.25. *Let F be a finite field and let A be a commutative F-algebra such that $A = F + N$ where N is a nilpotent subalgebra of A. Let S*

be the set of all functions $A \to A$ which can be written as polynomials from $N[x]$. Then S with the usual addition and

$$f(x) \bullet g(x) = f(x) + g(x + f(x)),$$

is a classical brace.

Proof. By Lemma 2.23 it remains to show the brace compatibility condition:

$$\begin{aligned} f(x) \bullet (g(x) + h(x)) - f(x) &= g(x + f(x)) + h(x + f(x)) \\ &= f(x) \bullet g(x) - f(x) + f(x) \bullet h(x). \end{aligned}$$

This completes the proof. □

Remark 2.26. Notice that if we consider S to be the set of polynomial functions from $N[x]$ with zero constant terms, then Proposition 2.25 has a very short proof: since S is nilpotent in the near-ring $M(A, +)$, it is a construction subgroup hence a skew brace by Proposition 2.20. As the polynomial function x is the identity map, and hence the identity in the near-ring $M(A, +)$, we get $(f \bullet g)(x) = f(x) + g(x + f(x))$.

Corollary 2.27. *The sets $T = \{f \in S : f(1) = 0\}$ and $\{f \in T : f(0) = 0\}$ are subbraces of S.*

Proof. It follows from Proposition 2.25. □

Lemma 2.28. *Let F be a finite field and let A be a commutative F-algebra such that $A = F + N$ where N is a nilpotent subalgebra of A. Let S be the set of all functions $A \to A$ which can be written as polynomials from $N[x]$ (where two functions are equal if they have the same values). Then S with the operation*

$$f(x) \odot g(x) = f(x) \circ g(x \circ f(x)),$$

where $a \circ b = a + b + ab$, $a, b \in A$, is a group.

Proof. It is easy to prove that $\odot$ is associative and that $f(x) = 0$ is the identity element of S. To prove that S is a group it suffices to show that every element in S has a left inverse, i.e. that for every $g(x) \in S$ there is $f(x) \in S$ such that $f(x) \circ g(x \circ f(x)) = 0$, so

$$f(x) = -g(x \circ f(x)) - f(x) \cdot g(x \circ f(x)).$$

Let n be such that $N^n = 0$ and let $t(x) = \sum_{i=1}^{n} (-1)^i g(x)^i$. Then

$$g(x) \circ t(x) = t(x) \circ g(x) = 0,$$

and hence

$$g(x \circ f(x)) \circ t(x \circ f(x)) = t(x \circ f(x)) \circ g(x \circ f(x)) = 0.$$

Therefore, the equation $f(x) \circ g(x \circ f(x)) = 0$ is equivalent to

$$f(x) = t(x \circ f(x))$$

Now $f(x) = t(x \circ t(x \circ t(\cdots (x \circ t(x)) \cdots)))$, where the number of brackets is equal to n. □

Remark 2.29. The same construction of Lemma 2.28 works when A is a noncommutative associative algebra. In this case instead of the polynomial ring $A[x]$ one takes the noncommutative polynomial ring, where the variable x does not commute with the elements of A.

Proposition 2.30. *Let F be a finite field and let A be an F-algebra such that $A = F + N$ where N is a nilpotent subalgebra of A. Let S be the set of all functions $A \to A$ which can be written as a noncommutative polynomials from $N[x]$. Then S with the operations*

$$f(x) \odot g(x) = f(x) \circ g(x \circ f(x)), \quad (f \circ g)(x) = f(x) \circ g(x),$$

is a skew brace.

Proof. By Lemma 2.28 it suffices to prove the compatibility condition. Let $f(x)^{-1}$ denote the inverse of $f(x)$ in the group $(S, \circ)$.

$$\begin{aligned}(f \odot (g \circ h))(x) &= f(x) \circ (g \circ h)(x \circ f(x)) \\ &= f(x) \circ g(x \circ f(x)) \circ h(x \circ f(x)) \\ &= (f \odot g)(x) \circ f(x)^{-1} \circ (f \odot h)(x).\end{aligned}$$

This completes the proof. □

Remark 2.31. Proposition 2.30 can be obtained from Proposition 2.20 when S is the set of functions which are polynomial functions from $N[x]$ with zero constant term.

2.5. **Matched pair of skew braces.** The construction of matched pair of braces was first considered by Bachiller [2] for classical braces.

Definition 2.32. *A pair of skew braces (A, B) is said to be* matched *if there are group homomorphisms $\alpha\colon (A, \circ) \to \mathrm{Aut}(B, \cdot)$ and $\beta\colon (B, \circ) \to \mathrm{Aut}(A, \cdot)$ such that*

$$\lambda^A_a \beta_b = \beta_{\alpha_a(b)} \lambda^A_{\beta^{-1}_{\alpha_a(b)}}(a), \tag{2.3}$$

$$\lambda^B_b \alpha_a = \alpha_{\beta_b(a)} \lambda^B_{\alpha^{-1}_{\beta_b(a)}}(b), \quad a \in A, b \in B, \tag{2.4}$$

where λ^A is the map of A and λ^B is the map of B.

Definition 2.33. *Given a matched pair (A, B, α, β) of skew braces, define the* biproduct *$A \bowtie B$ as the set of ordered pairs $(a, b) \in A \times B$ with the operations*

$$(a, b)(a', b') = (aa', bb'), \tag{2.5}$$

$$(a, b) \circ (a', b') = (\beta_b(\beta_b^{-1}(a) \circ a'), \alpha_a(\alpha_a^{-1}(b) \circ b')). \tag{2.6}$$

Proposition 2.34. *Given a matched pair (A, B, α, β) of skew braces, the biproduct $A \bowtie B$ is a skew brace.*

Proof. We claim that

$$\alpha_a(\alpha_a^{-1}(b)\circ y) = b\lambda_b^B\alpha_{\beta_b^{-1}(a)}(y) = b\circ\alpha_{\beta_b^{-1}(a)}(y), \tag{2.7}$$

$$\beta_b(\beta_b^{-1}(a)\circ x) = a\lambda_a^A\beta_{\alpha_a^{-1}(b)}(x) = a\circ\beta_{\alpha_a^{-1}(b)}(x). \tag{2.8}$$

We only prove (2.7). Since α is a group homomorphism, using (2.5) one obtains that

$$\begin{aligned}\alpha_a(\alpha_a^{-1}(b)\circ y) &= \alpha_a\left(\alpha_a^{-1}(b)\lambda^B_{\alpha_a^{-1}(b)}(y)\right)\\ &= b\alpha_a\lambda^B_{\alpha_a^{-1}(b)}(y) = b\lambda_b^B\alpha_{\beta_b^{-1}(a)}(y) = b\circ\alpha_{\beta_b^{-1}(a)}(y).\end{aligned}$$

Then

$$\lambda_{(a,b)}(a',b') = (\lambda_a^A\beta_{\alpha_a^{-1}(b)}(a'), \lambda_b^B\alpha_{\beta_b^{-1}(a)}(b')).$$

A direct calculation shows that $\lambda_{(a,b)}\in\mathrm{Aut}(A\times B)$ for all $a\in A$ and $b\in B$. Thus by Lemma 1.12 it suffices to prove that

$$\lambda_{(a,b)}\lambda_{(x,y)}(a',b') = \lambda_{(a,b)\circ(x,y)}(a',b').$$

This is equivalent to prove the following two equalities:

$$\beta_b\lambda^A_{\beta_b^{-1}(a)}\beta_y\lambda^A_{\beta_y^{-1}(x)}(a') = \beta_{\alpha_a(\alpha_a^{-1}(b)\circ x)}\lambda^A_{\beta^{-1}_{\alpha_a(\alpha_a^{-1}(b)\circ y)}\beta_b(\beta_b^{-1}(a)\circ x)}(a'), \tag{2.9}$$

$$\alpha_a\lambda^B_{\alpha_a^{-1}(b)}\alpha_x\lambda^B_{\alpha_x^{-1}(y)}(b') = \alpha_{\beta_b(\beta_b^{-1}(a)\circ y)}\lambda^B_{\alpha^{-1}_{\beta_b(\beta_b^{-1}(a)\circ y)}\alpha_a(\alpha_a^{-1}(b)\circ y)}(b'). \tag{2.10}$$

Let us prove (2.9). Let $a''=\beta_b^{-1}(a)$ and $b''=y$. We first observe that

$$\begin{aligned}\beta^{-1}_{\alpha_a(\alpha_a^{-1}(b)\circ y)}\beta_b(\beta_b^{-1}(a)\circ x) &= \beta^{-1}_{b\circ\alpha_{a''}(b'')}\beta_b(a''\circ x)\\ &= \beta^{-1}_{\alpha_{a''}(b'')}\beta_b^{-1}(\beta_b(a''\circ x))\\ &= \beta^{-1}_{\alpha_{a''}(b'')}(a''\circ x)\\ &= \beta^{-1}_{\alpha_{a''}(b'')}(a''\lambda^A_{a''}(x))\\ &= \beta^{-1}_{\alpha_{a''}(b'')}(a'')\beta^{-1}_{\alpha_{a''}(b'')}\lambda^A_{a''}(x)\\ &= \beta^{-1}_{\alpha_{a''}(b'')}(a'')\lambda_{\beta^{-1}_{\alpha_{a''}(b'')}(a'')}\beta^{-1}_{b''}(x)\\ &= \beta^{-1}_{\alpha_{a''}(b'')}(a'')\circ\beta^{-1}_{b''}(x).\end{aligned}$$

This equality and (2.7) imply that

$$\begin{aligned}\beta_b\lambda^A_{\beta_b^{-1}(a)}\beta_y\lambda^A_{\beta_y^{-1}(x)}(a') &= \beta_b\beta_{\alpha_{a''}(b'')}\lambda^A_{\beta^{-1}_{\alpha_{a''}(b'')}(a'')}\lambda^A_{\beta_{b''}^{-1}(x)}(a')\\ &= \beta_{b\circ\alpha_{a''}(b'')}\lambda^A_{\beta^{-1}_{\alpha_{a''}(b'')}(a'')\circ\beta_{b''}^{-1}(x)}(a')\\ &= \beta_{b\circ\alpha_{a''}(b'')}\lambda^A_{\beta^{-1}_{\alpha_{a''}(b'')}(a'')\circ\beta_{b''}^{-1}(x)}(a')\\ &= \beta_{b\circ\alpha_{a''}(b'')}\lambda^A_{\beta^{-1}_{\alpha_a(\alpha_a^{-1}(b)\circ y)}\beta_b(\beta_b^{-1}(a)\circ x)}(a')\\ &= \beta_{\alpha_a(\alpha_a^{-1}(b)\circ y)}\lambda^A_{\beta^{-1}_{\alpha_a(\alpha_a^{-1}(b)\circ y)}\beta_b(\beta_b^{-1}(a)\circ x)}(a').\end{aligned}$$

The proof of (2.10) is similar. □

Definition 2.35. *Let A and X be skew braces. A* left action *of A on X is a group homomorphism $(A,\circ)\to \mathrm{Aut_B}(X)$, where $\mathrm{Aut_B}(X)$ denotes the group of brace automorphisms of X.*

An easy consequence of Proposition 2.34 is the construction of semidirect product of skew braces. Semidirect products of classical braces were considered by Rump [46].

Corollary 2.36. *Let A and B be skew braces. Assume that there is a left action α of A on B. Then $A\times B$ with the operations*

$$(a,b)(a',b') = (aa', bb'),\quad (a,b)\circ(a',b') = (a\circ a', b\circ\alpha_a(b')),$$

is a skew brace. This skew brace structure over $A\times B$ will be denoted by $A\ltimes B$.

Corollary 2.37. *Let A and B be skew braces. Assume that there is a left action β of B on A. Then $A\times B$ with the operations*

$$(a,b)(a',b') = (aa', bb'),\quad (a,b)\circ(a',b') = (a\circ\beta_b(a'), b\circ b'),$$

is a skew brace.

Corollary 2.38. *Let A be a skew brace such that*

$$\lambda_a\lambda_b = \lambda_{\lambda_a(b)}\lambda_a,\quad a,b\in A. \tag{2.11}$$

Then $D(A) = A\ltimes A$ is a skew brace. The skew brace $D(A)$ will be called the double *of A.*

Proof. The brace A acts on A if and only if (2.11) holds. Thus the claim follows from Corollary 2.36. □

Wreath products of classical braces were considered in [13, Corollary 3.5]. The construction also works for skew braces:

Corollary 2.39. *Let A be a skew brace. Let $n\in\mathbb{N}$ and B be skew brace such that $(B,\circ)\subseteq\mathbb{S}_n$. Then the wreath product $A\wr B = A^{\times n}\rtimes B$ is a skew brace.*

Proof. According to Example 1.7, $A^{\times n} = A \times \cdots \times A$ (n-times) is a skew brace. Let $\delta\colon B \to \mathrm{Aut_B}(A^n)$, $b \mapsto \delta_b$, where

$$\delta_b(a_1, \dots, a_n) = (a_{b(1)}, \dots, a_{b(n)}).$$

Then B acts on A^n and hence then claim follows from Corollary 2.37. □

3. Solutions of the Yang–Baxter equation

Skew braces produce non-degenerate solution of the YBE.

Theorem 3.1. [33, Theorem 3.1] *Let A be a skew left brace. Then*

$$r_A\colon A \times A \to A \times A,$$
$$r_A(a,b) = (\lambda_a(b), \mu_b(a)) = (\lambda_a(b), \lambda^{-1}_{\lambda_a(b)}((a \circ b)^{-1} a (a \circ b)),$$

is a non-degenerate solution of the Yang–Baxter equation. Furthermore, r_A is involutive if and only if $ab = ba$ for all $a, b \in A$.

Remark 3.2. Let A be a skew brace and r_A its associated solution. If one writes $r(a,b) = (u,v)$, then $a \circ b = u \circ v$ since

$$\lambda^{-1}_{\lambda_a(b)}((a \circ b)^{-1} a (a \circ b)) = \overline{\lambda_a(b)} \circ a \circ b$$

for all $a, b \in A$.

A *biquandle* is a non-degenerate set-theoretical solution (X, r) of the YBE such that there exists a bijection $t\colon X \to X$ such that $r(t(x), x) = (t(x), x)$ for all $x \in X$. Biquandles have applications in classical and virtual knot theory, see for example [24] and [40].

Corollary 3.3. *Let A be a skew brace and r_A its associated solution of the YBE. Then (A, r_A) is a biquandle.*

Proof. Let $a \in A$. By Theorem 3.1, $b = \lambda_a^{-1}(a)$ is the unique element of A such that $r(a,b) = (a,b)$. Similarly, $\mu_a^{-1}(a) \in A$ is the unique element of A such that $r_A(\mu_a^{-1}(a), a) = (\mu_a^{-1}(a), a)$. It follows that the map $A \to A$, $a \mapsto \mu_a^{-1}(a)$, is bijective with inverse $a \mapsto \lambda_a^{-1}(a)$. □

Let (X, r) be a non-degenerate solution. Recall that the structure group of (X, r) is defined as the group $G(X, r)$ with generators in $\{e_x : x \in X\}$ and relations $e_x e_y = e_u e_v$ whenever $r(x, y) = (u, v)$. Let $\iota\colon X \to G(X, r)$ be the canonical map, i.e., $\iota(x) = e_x$. In general, ι is not injective:

Example 3.4. *Let $X = \{1, 2, 3, 4\}$, $\sigma = (12)$ and $\tau = (34)$. Then (X, r), $r(x, y) = (\sigma(y), \tau(x))$, is a non-degenerate solution of the YBE. The canonical map $\iota\colon X \to G(X, r)$, $i \mapsto e_i$, is not injective since for example*

$$e_1 e_2 = e_1 e_1$$

and hence $e_1 = e_2$.

The following result is [38, Theorem 9] in the language of skew braces, see also [49, Theorem 2.7]:

Theorem 3.5. *Let (X, r) be a non-degenerate solution of the YBE. Then there exists a unique skew left brace structure over $G(X, r)$ such that*

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

Furthermore, 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 $(\phi \times \phi)r_{G(X,r)} = r_B(\phi \times \phi)$.

Proof. By [38, Theorem 9] and the equivalence between skew braces and bijective 1-cocycles of Theorem 1.29, it remains to prove that

$$\phi(gh) = \phi(g)\phi(h)$$

for all $g, h \in G(X, r)$. Write $\lambda_B = \mu$. Since $\phi(\lambda_g(h)) = \mu_{\phi(g)}\phi(h)$,

$$\phi(gh) = \phi(g \circ \lambda_g^{-1}(h)) = \phi(g) \circ \phi(\lambda_g^{-1}(h)) = \phi(g) \circ \mu_{\phi(g)}^{-1}\phi(h) = \phi(g)\phi(h).$$

From this the claim follows. □

Example 3.6. *Let G be a group that admits an exact factorization through the subgroups A and B. By Theorem 2.3, G is a skew brace with additive group G and multiplicative group $A \times B$. Theorem 3.1 shows that the map $r\colon G \times G \to G \times G$ given by*

$$r(g, h) = (b^{-1}hb, a_1^{-1}ahbb_1^{-1}),$$

where $g = ab$ and $b^{-1}hb = a_1b_1$ for $a, a_1 \in A$ and $b, b_1 \in B$, is a non-degenerate set-theoretical solution of the YBE. This is essentially the solution constructed by Weinstein and Xu in [54, Theorem 9.2].

Example 3.7. *Let $A = \mathbb{S}_3$. Then A is a skew brace with $a \circ b = ba$. Clearly $\lambda_a(b) = a^{-1}ba$, $a, b \in A$ and the associated solution is*

$$r_A\colon A \times A \to A \times A, \quad r_A(a, b) = (a^{-1}ba, a).$$

The order of r_A is twelve and the restriction of r_A to the conjugacy class of involutions of A has order three.

Example 3.8. *The skew brace of Example 1.13 produces a solution of order twelve. This solution is isomorphic to (X, r), where $X = \{1, 2, \ldots, 6\}$ and $r(x, y) = (\sigma_x(y), \tau_y(x))$ is given by*

$$\begin{aligned}
&\sigma_1 = \mathrm{id}, && \sigma_2 = \mathrm{id}, && \sigma_3 = (263),\\
&\sigma_4 = (236), && \sigma_5 = (263), && \sigma_6 = (236),\\
&\tau_1 = \mathrm{id}, && \tau_2 = (36)(45), && \tau_3 = (36)(45),\\
&\tau_4 = \mathrm{id}, && \tau_5 = \mathrm{id}, && \tau_6 = (36)(45).
\end{aligned}$$

Example 3.9. *The skew brace of Example 1.18 produces a solution of order four. This solution is isomorphic to (X, r), where $X = \{1, 2, \ldots, 8\}$ and*

$r(x,y) = (\sigma_x(y), \tau_y(x))$ *is given by*

$$\begin{aligned}
&\sigma_1 = \mathrm{id}, && \sigma_2 = (25)(47), && \sigma_3 = (38)(47), && \sigma_4 = (25)(38),\\
&\sigma_5 = (25)(47), && \sigma_6 = \mathrm{id}, && \sigma_7 = (25)(38), && \sigma_8 = (38)(47),\\
&\tau_1 = \mathrm{id}, && \tau_2 = (25)(38), && \tau_3 = (25)(38), && \tau_4 = \mathrm{id},\\
&\tau_5 = (25)(38), && \tau_6 = \mathrm{id}, && \tau_7 = \mathrm{id}, && \tau_8 = (25)(38).
\end{aligned}$$

Definition 3.10. *Let A be a skew brace with additive group G. The* depth *of A is defined as the exponent of the group $G/Z(G)$.*

Example 3.11. *Classical braces have depth one.*

To study the depth of a skew brace we need the following lemma.

Lemma 3.12. *Let A be a skew brace and let $n \in \mathbb{N}$. Then*

$$r^{2n}(a,b) = ((a\circ b)^{-n}a(a\circ b)^n, \overline{(a\circ b)^{-n}a(a\circ b)^n}\circ a\circ b), \tag{3.1}$$

$$r^{2n+1}(a,b) = ((a\circ b)^{-n}a^{-1}(a\circ b)^{n+1}, \overline{(a\circ b)^{-n}a^{-1}(a\circ b)^{n+1}}\circ a\circ b), \tag{3.2}$$

for all $n \geq 0$. Moreover, the following statements hold:

1. *$r^{2n} = \mathrm{id}$ if and only if $ab^n = b^n a$ for all $a, b \in A$.*
2. *$r^{2n+1} = \mathrm{id}$ if and only if $\lambda_a(b) = (a\circ b)^n a(a\circ b)^{-n}$ for all $a, b \in A$.*

Proof. It suffices to prove (3.1) and (3.2). We proceed by induction on n. The case $n = 0$ is trivial for (3.1) and (3.2). Assume that the claim holds for some $n > 0$. If n is even, by applying the map r to Equation (3.1) and using Remark 3.2 we obtain that

$$\begin{aligned}
r^{2n+1}(a,b) &= r\left((a\circ b)^{-n}a(a\circ b)^n, \overline{(a\circ b)^{-n}a(a\circ b)^n}\circ a\circ b\right)\\
&= \left((a\circ b)^{-n}a^{-1}(a\circ b)^n(a\circ b), \overline{(a\circ b)^{-n}a^{-1}(a\circ b)^n(a\circ b)}\circ a\circ b\right)\\
&= \left((a\circ b)^{-n}a^{-1}(a\circ b)^{n+1}, \overline{(a\circ b)^{-n}a^{-1}(a\circ b)^{n+1}}\circ a\circ b\right).
\end{aligned}$$

Thus Equation (3.2) holds. If n is odd, a similar argument shows that (3.1) holds. □

Theorem 3.13. *Let A be a finite skew brace with more than one element. Then the order of r_A is $2d$, where d is the depth of A.*

Proof. Let n be such that $r^{2n+1} = \mathrm{id}$. By applying Lemma 3.12 one obtains that $a^{-1}(a\circ b)^{n+1} = (a\circ b)^n a$ for all $a, b \in A$. In particular, if $b = 1$, then $a = 1$, a contradiction.

Therefore we may assume that the order of the permutation r_A is $2n$, where $n = \min\{k : b^k a = ab^k \ \forall a, b \in A\}$. Now one computes

$$n = \min\{k : b^k \in Z(A) \ \forall b \in A\} = \min\{k : (bZ(A))^k = 1 \ \forall b \in A\} = d,$$

and the theorem is proved. □

Example 3.14. *Let A be a finite skew brace such that its additive group has trivial center. Then the order of r_A is equal to $2e$, where e is the exponent of the additive group of A.*

Example 3.15. *Let p be an odd prime number and let A be a non-classical skew brace of size $2p$. Then the additive group of A is isomorphic to the dihedral group $\mathbb{D}_{2p}$ of size $2p$. Since $Z(\mathbb{D}_{2p}) = 1$ and the exponent of $\mathbb{D}_{2p}$ is $2p$, the order of r_A is $4p$.*

4. Ideals and retractable solutions

Ideals of skew braces were defined in [33].

Definition 4.1. *Let A be a skew brace. A normal subgroup I of $(A, \circ)$ is said to be an* ideal *of A if $aI = Ia$ and $\lambda_a(I) \subseteq I$ for all $a \in A$.*

Example 4.2. *Let $f\colon A \to B$ be a skew brace homomorphism. Then* $\ker f$ *is an ideal of A since $f(\lambda_a(x)) = \lambda_{f(a)}(f(x)) = 1$ for all $x \in \ker f$ and $a \in A$.*

An important example of an ideal is the socle. As in the classical case, the socle is useful for studying the structure of skew braces and multpermutation solutions.

Example 4.3. *Let A be a skew brace. Then the* socle

$$\operatorname{Soc}(A) = \{a \in A : a \circ b = ab,\ b(b \circ a) = (b \circ a)b \text{ for all } b \in A\}$$

is an ideal of A contained in the center of $(A, \cdot)$; see [33, Lemma 2.5].

Lemma 4.4. *Let A be a skew brace. Then* $\operatorname{Soc}(A) = \ker \lambda \cap Z(A, \cdot)$.

Proof. By [33, Lemma 2.5] we only need to prove $\ker \lambda \cap \mathbb{Z}(A, \cdot) \subseteq \operatorname{Soc}(A)$. Let $a \in \ker \lambda \cap \operatorname{Soc}(A)$. It suffices to show that $b(b \circ a) = (b \circ a)b$ for all $b \in B$. Since a is central, $\overline{b}a = a\overline{b}$ for all $b \in A$. This implies that $\overline{b} \circ (b(b \circ a)) = \overline{b} \circ ((b \circ a)b)$ for all b and the claim follows. □

Lemma 4.5. [33, Lemma 2.3] *Let A be a skew left brace and $I \subseteq A$ be an ideal. Then the following properties hold:*

1. *I is a normal subgroup of $(A, \cdot)$.*
2. *$a \circ I = aI$ for all $a \in A$.*
3. *I and A/I are skew braces.*

Lemma 4.6. *Let $f\colon A \to B$ be a surjective homomorphism of skew braces. then $A/\ker f \simeq B$.*

Proof. A routine calculation shows that $A/\ker f \to B$, $a \ker(f) \mapsto f(a)$, is a well-defined isomorphism of skew braces. □

The following proposition is a simple application of the transfer theory. We will use the following theorem of Schur, see for example [42, §10.1.3]. If H is a central subgroup of finite index n in a group G, the map $x \mapsto x^n$ is a group homomorphism since it is the transfer of G into H.

Proposition 4.7. *Let A be a skew brace. Assume that the socle has finite index n. Then the map $A \to A$, $a \mapsto a^n$, is a group homomorphism.*

Proof. Since $\mathrm{Soc}(A) \subseteq Z(A, \cdot)$ by [33, Lemma 2.5], the claim follows since $\mathrm{Soc}(A)$ has finite index in G. □

Definition 4.8. *A skew brace is said to be* simple *if $A \neq 1$ and 1 and A are the only ideals of A.*

Example 4.9. *Skew braces with a prime number of elements are simple.*

Example 4.10. *Skew braces with simple multiplicative group are simple.*

Example 4.11. *Skew braces with simple additive group are simple.*

Example 4.12. *The skew brace of Example 1.20 is simple since a nontrivial proper normal subgroup of $C_3 \rtimes C_4$ have size three and a nontrivial proper normal subgroup of $\mathbb{A}_4$ have size four; see Lemma 4.5.*

The following problem arises naturally.

Problem 4.13. *Classify finite simple skew braces.*

Remark 4.14. The problem of classifying classical simple braces is intensively studied, see for example [2].

Definition 4.15. *Let A be a skew brace. The* socle series *of A is defined as the sequence*

$$A_1 = A, \quad A_{n+1} = A_n/\mathrm{Soc}(A_n), \quad n \geq 1.$$

Lemma 4.16. *Let A ba a skew brace. Let $S_1(A) = \mathrm{Soc}(A)$ and*

$$S_{n+1}(A) = \{a \in A : (a \circ b)^{-1}ab \in S_n(A),\ [b, b \circ a] \in S_n(A)\ \forall b \in A\}$$

for $n \geq 1$, where $[x, y] = x^{-1}y^{-1}xy$ denotes the commutator of x and y. Then $A_{n+1} = A/S_n(A)$ for all $n \in \mathbb{N}$.

Proof. Notice that $a \in S_{n+1}(A)$ if and only if $abS_n(A) = (a \circ b)S_n(A)$ and $b(b \circ a)S_n(A) = (b \circ a)S_n(A)$ for all $b \in A$. Now the claim follows by induction on n. □

Definition 4.17. *Let A be a skew brace. It is said that A has* finite multipermutation level *if there exists $n \in \mathbb{N}$ such that A_n has only one element.*

Example 4.18. *Let A be the skew brace of Example 1.18. The socle $\mathrm{Soc}(A)$ of A has two elements and hence $A_2 = A/\mathrm{Soc}(A)$ is the trivial classical brace over $C_2 \times C_2$. It follows that $\mathrm{Soc}(A_2) = A_2$ and hence A has finite multipermutation level.*

Example 4.19. *Let A be the simple skew brace of Example 4.12. Then $\mathrm{Soc}(A) = 1$ and hence A does not have finite multipermutation level.*

Recall the construction of semidirect product of skew braces of Corollary 2.36.

Theorem 4.20. *Let A and B be skew braces of finite multipermutation level. Let $C = A \ltimes B$ be a semidirect product of A and B. Then C has finite multipermutation level.*

Proof. By induction one proves that

$$1 \times S_n(B) \subseteq S_n(C)$$

for all $n \in \mathbb{N}$. Since B has finite multipermutation level, there exists $k \in \mathbb{N}$ $1 \times B \subseteq 1 \times S_k(B) \subseteq S_k(C)$. Since $\mathrm{Soc}(A) \times 1 \subseteq S_{k+1}(C)$, one proves by induction that $S_n(A) \times 1 \subseteq S_{n+k}(C)$ for all $n \in \mathbb{N}$. Now let $l \in \mathbb{N}$ be such that $S_l(A) = A$. Then $A \times 1 = S_l(A) \times 1 \subseteq S_{k+l}(C)$ and hence $S_{k+l}(C) = C$. □

Theorem 4.21. *Let A be a skew brace of finite multipermutation level. Then $(A, \cdot)$ is nilpotent.*

Proof. We proceed by induction on the size of A. If the order of A is a prime number, then $(A, \cdot)$ is nilpotent. Now assume that the result holds for all skew braces of size $< |A|$. Since $A/\mathrm{Soc}(A)$ is nilpotent by induction and $\mathrm{Soc}(A)$ is a central subgroup of $(A, \cdot)$, it follows that A is nilpotent. □

Remark 4.22. The converse of Theorem 4.21 does not hold. One example is the simple classical brace of size 24 constructed in [2, Remark 7.2]. Another example: In the list of skew braces computed in [33] one can find a non-classical brace of size 16 with trivial socle and nilpotent additive group.

5. Skew braces and other algebraic structures

In Subsection 1.2 we reviewed the equivalence between skew braces and bijective 1-cocycles. In this section we state several equivalences involving skew braces.

5.1. **Skew cycle sets.** Recall that a *cycle set* is a pair $(X, \bullet)$, where X is a set and $(a, b) \mapsto a \bullet b$ is a binary operation on X such that each map $\varphi_a \colon X \to X$, $\varphi_a(b) = a \bullet b$, is bijective, and

$$(a \bullet b) \bullet (a \bullet c) = (b \bullet a) \bullet (b \bullet c)$$

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

A *linear cycle set* is a triple $(A, +, \bullet)$, where $(A, +)$ is an abelian group, $(A, \bullet)$ is a cycle set, and

$$a \bullet (b + c) = (a \bullet b) + (a \bullet c), \quad (a + b) \bullet c = (a \bullet b) \bullet (a \bullet c)$$

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

Linear cycle sets were introduced by Rump in [43]. Classical braces are equivalent to linear cycle sets; see for example [47, Proposition 2.3].

Definition 5.1. *A* skew cycle set *is a triple $(A, \cdot, \bullet)$, where $(A, \cdot)$ is a (not necessarily abelian) group and $(a, b) \mapsto a \bullet b$ is a binary operation on A such that each map $\varphi_a \colon X \to X$, $\varphi_a(b) = a \bullet b$, is bijective, and*

$$a \bullet (bc) = (a \bullet b)(a \bullet c), \tag{5.1}$$

$$(ab) \bullet c = (a \bullet b) \bullet (a \bullet c) \tag{5.2}$$

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

Remark 5.2. Let A be a skew cycle set. It follows from (5.2) that

$$(a \bullet b) \bullet (a \bullet c) = (b \bullet (b^{-1}ab)) \bullet (b \bullet c)$$

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

Definition 5.3. *Let A and B be skew cycle sets. A* homomorphism *between A and B is a group homomorphism $f \colon A \to B$ such that*

$$f(a \bullet a') = f(a) \bullet f(a')$$

for all $a, a' \in A$.

Notation 5.4. *Let A be a skew cycle set. The inverse operation of $\bullet$ will be denoted by $*$, i.e. $a \bullet b = c$ if and only if $a * c = b$, $a, b, c \in A$.*

Lemma 5.5. *Let A be a skew cycle set. Then*

$$a * (bc) = (a * b)(a * c), \tag{5.3}$$

$$(ab) * c = a * ((a \bullet b) * c) \tag{5.4}$$

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

Proof. Let $a, b, c \in A$. Since $a \bullet ((a * b)(a * c)) = (a \bullet (a * b))(a \bullet (a * c)) = bc$, Equation (5.3) follows. Now let

$$d = (ab) \bullet c = (a \bullet b) \bullet (a \bullet c).$$

Then $(ab) * d = c = a * ((a \bullet b) * d)$ and the lemma is proved. □

Skew cycle sets form a category.

For a group A let $\mathfrak{S}(A)$ be the full subcategory of skew cycle sets whose objects are skew cycle set structures over A.

Lemma 5.6. *Let A be a skew brace. Then the group $(A, \cdot)$ with*

$$a \bullet b = \lambda_a^{-1}(b) = \overline{a} \circ (ab)$$

is a skew cycle set. Moreover, if $f \colon A \to A_1$ is a homomorphism of skew braces, then f is a homomorphism of skew cycle sets.

Proof. Each map $\varphi_a : b \mapsto a \bullet b$ is bijective. Let $a, b, c \in A$. To prove (5.1) one uses that $\lambda \colon (A, \circ) \to \mathrm{Aut}(A, \cdot)$ is a group homomorphism:

$$a \bullet (bc) = \lambda_a^{-1}(bc) = \lambda_{\overline{a}}(bc) = \lambda_{\overline{a}}(b)\lambda_{\overline{a}}(c) = (a \bullet b)(a \bullet c).$$

To prove (5.2) we compute

$$(a \bullet b) \bullet (a \bullet c) = \lambda^{-1}_{\lambda_a^{-1}(b)}(\lambda_a^{-1}(c)) = \lambda^{-1}_{a \circ \lambda_a^{-1}(b)}(c) = \lambda_{ab}^{-1}(c) = (ab) \bullet c.$$

To prove that f is a skew cycle set homomorphism one computes

$$f(a \bullet b) = f(\overline{a} \circ (ab)) = \overline{f(a)} \circ (f(a)f(b)) = f(a) \bullet f(b).$$

This finishes the proof. □

Lemma 5.7. *Let A be a skew cycle set. Then A with $\lambda_a(b) = a * b$, where $a * b = c$ if and only if $a \bullet c = b$, is a skew brace. Moreover, if $f\colon A \to A_1$ is a skew cycle set homomorphism, then f is a skew brace homomorphism.*

Proof. Let $\lambda\colon A \to \mathbb{S}_A$ be given by $a \mapsto \lambda_a$. Let $a, b, c \in A$. First we notice that $\lambda_a(bc) = \lambda_a(b)\lambda_a(c)$ since

$$\lambda_a(bc) = a * (bc) = (a * b)(a * c) = \lambda_a(b)\lambda_a(c)$$

by Lemma 5.5, Equation (5.3).

To prove that $\lambda_{a\lambda_a(b)}(c) = \lambda_a\lambda_b(c)$ holds we use Lemma 5.5, Equation (5.4) to obtain that

$$\begin{aligned}\lambda_a\lambda_b(c) = a * (b * c) &= a * ((a \bullet (a * b)) * c) \\ &= (a(a * b)) * c = (a\lambda_a(b)) * c = \lambda_{a\lambda_a(b)}(c).\end{aligned}$$

Now since $\lambda_a(bc) = \lambda_a(b)\lambda_a(c)$ and $\lambda_{a\lambda_a(b)}(c) = \lambda_a\lambda_b(c)$ hold, A is a skew brace by Lemma 1.12.

Finally the map f is a skew brace homomorphism since

$$\begin{aligned}f(a \circ b) = f(a(a * b)) &= f(a)f(a * b) \\ &= f(a)\,(f(a) * f(b)) = f(a)\lambda_{f(a)}(f(b)) = f(a) \circ f(b)\end{aligned}$$

for all $a, b \in A$. □

Lemmas 5.6 and 5.7 yield the following result:

Theorem 5.8. *Let A be a group. The categories $\mathfrak{B}_{\mathrm{add}}(A)$ and $\mathfrak{S}(A)$ are equivalent.*

5.2. **Matched pairs of groups.** For a given group $(A, \circ)$ let $\mathfrak{M}(A)$ be the category with objects the matched pairs (A, A) such that

$$a \circ b = (a \rightharpoonup b) \circ (a \leftharpoonup b) \tag{5.5}$$

for all $a, b \in A$ and morphisms all group homomorphisms $f\colon A \to A$ such that

$$f(a \rightharpoonup b) = f(a) \rightharpoonup f(b), \quad f(a \leftharpoonup b) = f(a) \leftharpoonup f(b)$$

for all $a, b \in A$.

Lemma 5.9. *Let A be a skew brace. Then $((A, \circ), (A, \circ))$ is a matched pair of groups with $a \rightharpoonup b = \lambda_a(b)$ and $a \leftharpoonup b = \mu_b(a)$, $a, b \in A$.*

Proof. Lemma 1.8 proves that λ is a left action and Lemma 1.11 proves that μ is a right action. Thus we need to prove that

$$a \rightharpoonup (b \circ b') = (a \rightharpoonup b) \circ ((a \leftharpoonup b) \rightharpoonup b'), \tag{5.6}$$

$$(a \circ a') \leftharpoonup b = (a \leftharpoonup (a' \rightharpoonup b)) \circ (a' \leftharpoonup b) \tag{5.7}$$

hold for all $a, a', b, b' \in A$.

For $a, a', b \in A$ one obtains that

$$\begin{aligned}(a \leftharpoonup (a' \rightharpoonup b)) \circ (a' \leftharpoonup b) &= \overline{\lambda_a \lambda_{a'}(b)} \circ a \circ \lambda_{a'}(b) \circ \overline{\lambda_{a'}(b)} \circ a' \circ b \\ &= \overline{\lambda_{a \circ a'}(b)} \circ a \circ a' \circ b \\ &= (a \circ a') \leftharpoonup b.\end{aligned}$$

For $a, b, b' \in A$ one obtains that

$$\begin{aligned}(a \rightharpoonup b) \circ ((a \leftharpoonup b) \rightharpoonup b') &= \lambda_a(b) \circ \left(\overline{\lambda_a(b)} \circ a \circ b \rightharpoonup b'\right) \\ &= \lambda_a(b) \circ \lambda_{\overline{\lambda_a(b)}} \lambda_{a \circ b}(b') \\ &= \lambda_a(b) \lambda_{a \circ b}(b') \\ &= a \rightharpoonup (b \circ b').\end{aligned}$$

This completes the proof. □

Lemma 5.10. *Let $(A, \circ)$ be a group and $(A, A, \rightharpoonup, \leftharpoonup)$ be a matched pair of groups such that $a \circ b = (a \rightharpoonup b) \circ (a \leftharpoonup b)$ for all $a, b \in A$. Then A with*

$$ab = a \circ (\overline{a} \rightharpoonup b)$$

is a skew brace.

Proof. For $a, b \in A$ write $\lambda_a(b) = a \rightharpoonup b$. Then $\lambda \colon A \to \mathbb{S}_A$, $a \mapsto \lambda_a$, is a well-defined group homomorphism. Equation (5.5) implies that $\lambda_a(1) = 1$ for all a. Since

$$\begin{aligned}\lambda_a(b \circ \lambda_b^{-1}(c)) &= \lambda_a(b) \circ (\lambda_{a \leftharpoonup b} \lambda_b^{-1}(c)) \\ &= \lambda_a(b) \circ \lambda_{\overline{\lambda_a(b) \circ a \circ b}} \lambda_b^{-1}(c) \\ &= \lambda_a(b) \circ \lambda_{\lambda_a(b)}^{-1} \lambda_a(c),\end{aligned}$$

the claim follows from Lemma 1.14 □

For a given group A, let $\mathfrak{B}_{\mathrm{mul}}(A)$ be the full subcategory of the category of skew braces with multiplicative group A. Combining Lemma 5.9 and Lemma 5.10 one gets the following result:

Theorem 5.11. *Let A be a group. The categories $\mathfrak{B}_{\mathrm{mul}}(A)$ and $\mathfrak{M}(A)$ are equivalent.*

Remark 5.12. Theorem 5.11 is implicit in the work of Lu, Yan and Zhu, see [38, Theorem 2] and [53]. The result for classical braces was proved by Gateva-Ivanova; see [27, Theorem 3.7]. Our proof of Theorem 5.11 is essentially that of Gateva-Ivanova.

Appendix A. Hopf–Galois extensions

(By N. Byott and L. Vendramin)

In this appendix we review the connection between skew braces and Hopf–Galois extensions. This connection was first observed by Bachiller in [4, §2].

Let K be a field and let H be a cocommutative Hopf algebra over K. An H-module algebra A over K is an H-Galois extension of K if the map

$$\theta\colon A \otimes_K A \to \mathrm{Hom}_K(H, A), \quad \theta(a \otimes b)(h) = a(h \cdot b),$$

is bijective.

Let $K \subseteq L$ be a finite extension of fields. A Hopf–Galois structure on L/K consists of a Hopf algebra H over K and an action of H on L such that L is an H-Galois extension of K. In [32], Greither and Pareigis showed how to find all Hopf-Galois structures when L/K is separable. For simplicity, we consider only the case where L/K is also normal, so that L/K is a Galois extension in the classical sense. We then have:

Theorem A.1 (Greither–Pareigis)**.** *Let $K \subseteq L$ be a finite Galois field extension with group G. Then Hopf–Galois extensions on L/K correspond bijectively to regular subgroups A of $\mathbb{S}_G$ normalized by G, where G is considered as a subgroup of $\mathbb{S}_G$ by the regular left representation.*

Recall that a subgroup A of $\mathbb{S}_G$ is *regular* if, given any g, $h \in G$, there is a unique $a \in A$ with $a \cdot g = h$. The isomorphism class of A in Theorem A.1 is known as the *type* of the Hopf-Galois structure. Note that $|A| = |G|$, but in general A and G need not be isomorphic.

In the situation of Theorem A.1, the fact that A acts regularly on G enables us to define a bijection between A and G, via which we may translate the left regular action of G on itself into an action of G on A. Thus G becomes a regular subgroup of $\mathbb{S}_A$. It was observed by Childs [16] that the condition in Theorem A.1, namely that A is normalized by G, holds if and only if G is contained in the subgroup $\mathrm{Hol}(A)$ of $\mathbb{S}_A$, where $\mathrm{Hol}(A) = A \rtimes \mathrm{Aut}(A)$ is the *holomorph* of A. The group operation in $\mathrm{Hol}(A)$ is given by

$$(a, f)(b, g) = (af(b), fg),$$

and an element $(b, g) \in H$ acts on $a \in A$ by $(b, g) \cdot a = bg(a)$. (Thus the first factor A in $\mathrm{Hol}(A)$ is identified with left multiplications by elements of A.)

Childs' observation was used in [8] to give a formula to count Hopf-Galois structures:

Proposition A.2. *The number $e(G, A)$ of Hopf–Galois structures of type A on a Galois extension L/K with group G is given by*

$$e(G, A) = \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(A)|} f(G, A),$$

where $f(G, A)$ is the number of regular subgroups of $\mathrm{Hol}(A)$ that are isomorphic to the group G.

We now sketch the proof of this, partly following the exposition in [17, §7], in order to elucidate the relationship between Hopf-Galois structures and skew braces.

To begin with, we consider G and A as abstract groups, i.e. given without any actions on each other. Let $\lambda_G : G \to \mathbb{S}_G$ be the left regular representation: $\lambda_G(g)\cdot h = gh$ for $g, h \in G$. We will call $\alpha : A \to \mathbb{S}_G$ a *regular embedding* if α is an injective group homomorphism whose image $\alpha(A) \subseteq \mathbb{S}_G$ is regular on G. A regular embedding $\alpha : A \to \mathbb{S}_G$ induces a bijection

$$\alpha_* : A \to G, \qquad \alpha_*(a) = \alpha(a) \cdot 1_G.$$

Define $\beta : G \to \mathbb{S}_A$ by $\beta(g) = \alpha_*^{-1}\lambda_G(g)\alpha_*$. Then β is also a regular embedding. In this way, we obtain a bijection from the set

$$\mathcal{A} = \{\text{regular embeddings } \alpha : A \to \mathbb{S}_G\}$$

to the set

$$\mathcal{G} = \{\text{regular embeddings } \beta : G \to \mathbb{S}_A\},$$

whose inverse is obtained by the same construction with A and G interchanged. By the observation of Childs, this restricts to a bijection from

$$\mathcal{A}_0 = \{\alpha \in \mathcal{A} : \alpha(A) \text{ is normalized by } G\}$$

to

$$\mathcal{G}_0 = \{\beta \in \mathcal{G} : \beta(G) \subseteq \mathrm{Hol}(A)\}.$$

If $\alpha \in \mathcal{A}_0$ and $\phi \in \mathrm{Aut}(A)$, then also $\alpha\phi \in \mathcal{A}_0$. Thus $\mathrm{Aut}(A)$ acts on A (from the right) by composition. This action is fixed-point-free: if $\alpha\phi = \alpha$ then $\phi = \mathrm{id}_A$. Moreover, for α, $\alpha' \in \mathcal{A}_0$, we have $\alpha'(A) = \alpha(A) \Leftrightarrow \alpha' = \alpha\phi$ for some $\phi \in \mathrm{Aut}(A)$. Thus each regular subgroup $\alpha(A) \subseteq \mathbb{S}_G$ normalized by G corresponds to an orbit of $\mathcal{A}_0$ under $\mathrm{Aut}(A)$, and each such orbit has cardinality $|\mathrm{Aut}(A)|$. By Theorem A.1, the number of these subgroups is $e(G, A)$. Hence we have $|\mathcal{A}_0| = |\mathrm{Aut}(A)|e(G, A)$. A similar argument gives $|\mathcal{G}_0| = |\mathrm{Aut}(G)|f(G, A)$. As there is a bijective correspondence between $\mathcal{A}_0$ and $\mathcal{G}_0$, Proposition A.2 follows.

The action of $\mathrm{Aut}(A)$ on $\mathcal{A}_0$ by composition translates to an action on $\mathcal{G}_0$. Explicitly, if $\alpha \in \mathcal{A}_0$ corresponds to $\beta \in \mathcal{G}_0$, and $\phi \in \mathrm{Aut}(A)$, then $\alpha' = \alpha\phi$ corresponds to β' where $\beta'(g) = \phi^{-1}\beta(g)\phi \in \mathbb{S}_A$. Thus the action of $\mathrm{Aut}(A)$ on $\mathcal{G}_0$ is by conjugation inside $\mathbb{S}_A$, and this action is again fixed-point-free. Two elements of $\mathcal{G}_0$ give rise to the same regular subgroup of $\mathrm{Hol}(A)$ if and only if they are in the same orbit under this action. Thus the Hopf-Galois structures of type A on L/K correspond bijectively to the $\mathrm{Aut}(A)$-conjugacy classes of $\mathcal{G}_0$.

One may check that the action of $\mathrm{Aut}(A)$ on $\mathcal{G}_0$ by conjugation commutes with the action of $\mathrm{Aut}(G)$ by composition.

We now turn to the classification of skew braces. We have the following result from [33, Proposition 4.3].

Proposition A.3. *Let A be a group. There exists a bijective correspondence between isomorphism classes of skew braces with additive group isomorphic to A and classes of regular subgroups of* $\mathrm{Hol}(A)$ *under conjugation by elements of* $\mathrm{Aut}(A)$.

Proof. Let $\mathcal{B}(A)$ be the set of isomorphism classes of skew braces with additive group A and let $\mathcal{R}(A)$ be the set of equivalence classes of regular subgroups of $\mathrm{Hol}(A)$ under conjugation by $\mathrm{Aut}(A)$.

Let G be a regular subgroup of $\mathrm{Hol}(A)$. The regularity of G implies that $\pi\colon G \to A$, $\pi(a, f) = a$, is bijective. Then A with the operation

$$a \circ b = \pi(\pi^{-1}(a)\pi^{-1}(b)) = af(b)$$

is a group isomorphic to G. Since

$$a \circ (bc) = af(bc) = af(b)f(c) = af(b)a^{-1}af(c) = (a \circ b)a^{-1}(a \circ c),$$

the set A is a skew brace. A routine calculation shows that this correspondence induces a map $C\colon \mathcal{R}(A) \to \mathcal{B}(A)$.

Let $B\colon \mathcal{B}(A) \to \mathcal{R}(A)$ be given by $B(A) = \{(a, \lambda_a) : a \in A\}$. Routine calculations show that the map B is well-defined and that $B \circ C = \mathrm{id}_{\mathcal{R}(A)}$ and $C \circ B = \mathrm{id}_{\mathcal{B}(A)}$. □

Remark A.4. Proposition A.3 was proved for classical braces by Bachiller [4, Proposition 2.3].

In terms of the preceding notation, the regular subgroups of $\mathrm{Hol}(A)$ which are isomorphic to G correspond to orbits of $\mathcal{G}_0$ under $\mathrm{Aut}(A)$, and the isomorphism classes of skew braces with multiplicative group G and additive group A correspond to orbits of $\mathcal{G}_0$ under $\mathrm{Aut}(G) \times \mathrm{Aut}(A)$. We summarize the above discussion in the following result.

Theorem A.5. *Let A and G be finite groups of the same order, and let $\mathcal{G}_0$ be the set of regular embeddings $G \to \mathrm{Hol}(A)$. Then $\mathcal{G}_0$ admits commuting actions (from the right) of* $\mathrm{Aut}(G)$ *by composition and of* $\mathrm{Aut}(A)$ *by conjugation in* $\mathbb{S}(A)$.

The set of Hopf-Galois structures of type A on a Galois extension of fields with group G corresponds bijectively to the set of orbits $\mathcal{G}_0/\mathrm{Aut}(G)$, while the set of isomorphism classes of skew braces with multiplicative group G and additive group A corresponds bijectively to the set of orbits $\mathcal{G}_0/(\mathrm{Aut}(G) \times \mathrm{Aut}(A))$.

Hence there is a surjective map from this set of Hopf-Galois structures to this set of isomorphism classes of skew braces, induced by the canonical surjection

$$\mathcal{G}_0/\mathrm{Aut}(G) \twoheadrightarrow \mathcal{G}_0/(\mathrm{Aut}(G) \times \mathrm{Aut}(A)).$$

Remark A.6. While each of the groups $\mathrm{Aut}(A)$ and $\mathrm{Aut}(G)$ acts without fixed points on $\mathcal{G}_0$, this is not true for $\mathrm{Aut}(G) \times \mathrm{Aut}(A)$, and the orbits under this group need not all have the same size.

In more concrete terms, in order to count either Hopf-Galois structures or skew braces, we need to determine the regular subgroups of $\mathrm{Hol}(A)$ isomorphic to G. To obtain the number of Hopf-Galois structures, we take the number of such subgroups and adjust by the factor $|\operatorname{Aut}(G)|/|\operatorname{Aut}(A)|$ as specified in Proposition A.2. To obtain the number of skew braces (up to isomorphism), we take the number of *orbits* of such subgroups under conjugacy by $\operatorname{Aut}(A)$. In general, these orbits are of different sizes, so there is no simple relationship between the number of Hopf-Galois structures and the number of skew braces.

We illustrate the difference between counting Hopf-Galois structures and counting skew braces by means of an example.

Example A.7. *Let $G = C_{p^n}$ be the cyclic group of order p^n for an odd prime p and $n \in \mathbb{N}$. In this case, the Hopf-Galois structures were determined by Kohl* [37] *(see also* [17, Theorem 9.1]*), and the classical braces were determined by Rump* [45]*. If A is a group of order p^n (not necessarily abelian) such that $\mathrm{Hol}(A)$ contains an element of order p^n then in fact A is cyclic* [37, Theorem 4.4]*. Thus every Hopf-Galois structure on a cyclic field extension of degree p^n is of cyclic type, and every skew brace with multiplicative group C_{p^n} also has additive group C_{p^n}. In particular, there are no such skew braces beyond the classical braces found by Rump. Let σ be a generator of $A = C_{p^n}$. Then $\operatorname{Aut}(A) = \{\theta_u : u \in (\mathbb{Z}/p^n\mathbb{Z})^\times\}$, where $\theta_u(\sigma) = \sigma^u$. Now any regular subgroup G of $\mathrm{Hol}(A)$ must contain a unique element of the form (σ, θ_u), and it easy to check that this element generates G. Moreover, $u \equiv 1 \pmod{p}$ since θ_u must have p-power order. Hence there are p^{n-1} possibilities for u. This gives p^{n-1} distinct regular subgroups, and hence p^{n-1} Hopf-Galois structures. To count the skew braces, we must consider the orbits of these subgroups under conjugacy by $\operatorname{Aut}(A)$. Now if $G = \langle(\sigma, \theta_u)\rangle$ then $\theta_v G \theta_v^{-1}$ is generated by (σ^v, θ_u). This subgroup is also generated by a unique element of the form (σ, θ_w). As v varies, the possible values of w are precisely those such that $u - 1$ and $w - 1$ are divisible by the same power of p. Hence we obtain n skew braces (up to isomorphism), corresponding to $u = 1$, $1 + p^{n-1}$, $1 + p^{n-2}$, …, $1 + p$. These skew braces have socles of size p^n, p^{n-1}, …, p respectively, and the corresponding orbits of regular subgroups under the action of $\operatorname{Aut}(A)$ have sizes 1, $p-1$, $p(p-1)$, …, $p^{n-2}(p-1)$ respectively.*

Having explained the connection between skew braces and Hopf-Galois structures, we restate a couple of known results for Hopf-Galois structures in terms of skew braces. The first example is the uniqueness result [33, Theorem 1]:

Theorem A.8. *Let $n \in \mathbb{N}$. There is a unique skew brace of size n if and only if n and $\phi(n)$ are coprime, where ϕ denotes the Euler's totient function.*

The following result is [11, Theorem 2]:

Theorem A.9. *Let A be a finite skew brace with abelian multiplicative group. Then the additive group of A is solvable.*

Question A.10. *Let A be a skew brace with multiplicative group isomorphic to $\mathbb{Z}$. Is the additive group of A also isomorphic to $\mathbb{Z}$?*

In [33, Algorithm 5.1] a method to enumerate skew braces of small size appears. It is based on Proposition A.3. An easy modification of the Magma [7] implementation of [33, Algorithm 5.1] allows us to enumerate Hopf–Galois extensions of small degree using Proposition A.2.

Example A.11. *In* [10, Corollaries 6.3 and 6.4] *one finds that*

$$e(\mathbb{S}_3, \mathbb{S}_3) = e(C_6, \mathbb{S}_3) = 2, \quad e(\mathbb{S}_3, C_6) = 3, \quad e(C_6, C_6) = 1.$$

In [10, Corollary 6.6] *one finds that*

$$e(C_7 \rtimes C_3, C_7 \rtimes C_3) = 16, \qquad e(C_7 \rtimes C_3, C_{21}) = 7,$$
$$e(C_{21}, C_7 \rtimes C_3) = 4, \qquad e(C_{21}, C_{21}) = 1.$$

Let $n \in \mathbb{N}$. Let $G_1, \ldots, G_m$ be a complete set of representatives of isomorphism classes of groups of order n. To record the number of Hopf–Galois extensions of degree n, we constuct an $m \times m$ array $E(n)$ in which the (i, j)-entry is the number $e(G_i, G_j)$.

Example A.12. *The arrays $E(8)$ and $E(12)$ are shown in Tables A.1 and A.2, respectively.*

TABLE A.1. The number of Hopf–Galois extensions of fields of degree eight.

	C_8	$C_4 \times C_2$	$C_4 \rtimes C_2$	Q_8	C_2^3
C_8	2	0	2	2	0
$C_4 \times C_2$	4	10	6	2	4
$C_4 \rtimes C_2$	2	14	6	2	6
Q_8	6	6	6	2	2
C_2^3	0	42	42	14	8

TABLE A.2. The number of Hopf–Galois extensions of fields of degree twelve.

	$C_3 \rtimes C_4$	C_{12}	$\mathbb{A}_4$	$C_6 \rtimes C_2$	$C_6 \times C_2$
$C_3 \rtimes C_4$	2	3	12	2	3
C_{12}	2	1	0	2	1
$\mathbb{A}_4$	0	0	10	0	4
$C_6 \rtimes C_2$	14	9	0	14	3
$C_6 \times C_2$	6	3	4	6	1

The number $h(n)$ of Hopf–Galois structures of degree n is

$$h(n) = \sum_{i=1}^{m} \sum_{j=1}^{m} e(G_i, G_j).$$

Some values of $h(n)$ are shown in Table A.3.

TABLE A.3. The number $h(n)$ of Hopf–Galois extensions of fields of degree n.

n	6	8	10	12	14	16	18	20
$h(n)$	8	190	10	102	12	25168	289	166
n	21	22	24	25	26	27	28	30
$h(n)$	28	16	5618	30	18	4329	128	80
n	34	36	38	40	42	44	45	46
$h(n)$	22	5980	24	8556	374	184	12	28

Problem A.13. *Compute* $h(32)$.

ACKNOWLEDGEMENTS

This research was supported with ERC advanced grant 320974. The second-named author is partially supported by PICT-2014-1376, MATH-AmSud 17MATH-01, ICTP and the Alexander Von Humboldt Foundation. The authors thank Nigel Byott, Martín González Yamone, Timothy Kohl, Victoria Lebed, Michael West and the referees for comments and corrections.

REFERENCES

[1] B. Amberg, S. Franciosi, and F. de Giovanni. *Products of groups*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1992. Oxford Science Publications.

[2] D. Bachiller. Extensions, matched products, and simple braces. *arXiv:1511.08477*.

[3] D. Bachiller. Solutions of the Yang-Baxter equation associated to skew left braces, with applications to racks. *arXiv:1611.08138*.

[4] D. Bachiller. Counterexample to a conjecture about braces. *J. Algebra*, 453:160–176, 2016.

[5] D. Bachiller. *Study of the Algebraic Structure of Left Braces and the Yang-Baxter Equation*. PhD thesis, Universitat Autònoma de Barcelona. Departament de Matemàtiques, `https://ddd.uab.cat/record/165965`, 2016.

[6] E. J. Beggs, J. D. Gould, and S. Majid. Finite group factorizations and braiding. *J. Algebra*, 181(1):112–151, 1996.

[7] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[8] N. P. Byott. Uniqueness of Hopf Galois structure for separable field extensions. *Comm. Algebra*, 24(10):3217–3228, 1996.

[9] N. P. Byott. Hopf-Galois structures on field extensions with simple Galois groups. *Bull. London Math. Soc.*, 36(1):23–29, 2004.

[10] N. P. Byott. Hopf-Galois structures on Galois field extensions of degree pq. *J. Pure Appl. Algebra*, 188(1-3):45–57, 2004.
[11] N. P. Byott. Solubility criteria for Hopf-Galois structures. *New York J. Math.*, 21:883–903, 2015.
[12] 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.
[13] F. Cedó, E. Jespers, and Á. del Río. Involutive Yang-Baxter groups. *Trans. Amer. Math. Soc.*, 362(5):2541–2558, 2010.
[14] F. Cedó, E. Jespers, and J. Okniński. Retractability of set theoretic solutions of the Yang-Baxter equation. *Adv. Math.*, 224(6):2472–2484, 2010.
[15] F. Cedó, E. Jespers, and J. Okniński. Braces and the Yang-Baxter equation. *Comm. Math. Phys.*, 327(1):101–116, 2014.
[16] L. N. Childs. On the Hopf Galois theory for separable field extensions. *Comm. Algebra*, 17(4):809–825, 1989.
[17] L. N. Childs. *Taming wild extensions: Hopf algebras and local Galois module theory*, volume 80 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2000.
[18] P. Dehornoy. Set-theoretic solutions of the Yang–Baxter equation, RC-calculus, and Garside germs. *Adv. Math.*, 282:93–127, 2015.
[19] 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.
[20] P. Etingof and S. Gelaki. A method of construction of finite-dimensional triangular semisimple Hopf algebras. *Math. Res. Lett.*, 5(4):551–561, 1998.
[21] P. Etingof, S. Gelaki, R. Guralnick, and J. Saxl. Biperfect Hopf algebras. *J. Algebra*, 232(1):331–335, 2000.
[22] P. Etingof, T. Schedler, and A. Soloviev. Set-theoretical solutions to the quantum Yang-Baxter equation. *Duke Math. J.*, 100(2):169–209, 1999.
[23] P. Etingof, A. Soloviev, and R. Guralnick. Indecomposable set-theoretical solutions to the quantum Yang-Baxter equation on a set with a prime number of elements. *J. Algebra*, 242(2):709–719, 2001.
[24] R. Fenn. Biquandles and their application to virtual knots and links. *J. Knot Theory Ramifications*, 18(6):785–789, 2009.
[25] T. Gateva-Ivanova. A combinatorial approach to the set-theoretic solutions of the Yang-Baxter equation. *J. Math. Phys.*, 45(10):3828–3858, 2004.
[26] T. Gateva-Ivanova. Quadratic algebras, Yang-Baxter equation, and Artin-Schelter regularity. *Adv. Math.*, 230(4-6):2152–2175, 2012.
[27] T. Gateva-Ivanova. Set-theoretic solutions of the Yang-Baxter equation, Braces, and Symmetric groups. *arXiv:1507.02602*, 2015.
[28] T. Gateva-Ivanova and P. Cameron. Multipermutation solutions of the Yang-Baxter equation. *Comm. Math. Phys.*, 309(3):583–621, 2012.
[29] T. Gateva-Ivanova and S. Majid. Set-theoretic solutions of the Yang-Baxter equation, graphs and computations. *J. Symbolic Comput.*, 42(11-12):1079–1112, 2007.
[30] T. Gateva-Ivanova and S. Majid. Matched pairs approach to set theoretic solutions of the Yang-Baxter equation. *J. Algebra*, 319(4):1462–1529, 2008.
[31] T. Gateva-Ivanova and M. Van den Bergh. Semigroups of I-type. *J. Algebra*, 206(1):97–112, 1998.
[32] C. Greither and B. Pareigis. Hopf Galois theory for separable field extensions. *J. Algebra*, 106(1):239–258, 1987.
[33] L. Guarnieri and L. Vendramin. Skew braces and the Yang–Baxter equation. *Math. Comp.*, 86(307):2519–2534, 2017.

[34] P. Hubert. Triply factorised groups and nearrings. In *Groups St. Andrews 2005. Vol. 2*, volume 340 of *London Math. Soc. Lecture Note Ser.*, pages 496–503. Cambridge Univ. Press, Cambridge, 2007.
[35] G. I. Kac. Group extensions which are ring groups. *Mat. Sb. (N.S.)*, 76 (118):473–496, 1968.
[36] C. Kassel. *Quantum groups*, volume 155 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.
[37] T. Kohl. Classification of the Hopf Galois structures on prime power radical extensions. *J. Algebra*, 207(2):525–546, 1998.
[38] J.-H. Lu, M. Yan, and Y.-C. Zhu. On the set-theoretical Yang-Baxter equation. *Duke Math. J.*, 104(1):1–18, 2000.
[39] J. D. P. Meldrum. *Near-rings and their links with groups*, volume 134 of *Research Notes in Mathematics*. Pitman (Advanced Publishing Program), Boston, MA, 1985.
[40] S. Nelson. The combinatorial revolution in knot theory. *Notices Amer. Math. Soc.*, 58(11):1553–1561, 2011.
[41] J. Pakianathan and K. Shankar. Nilpotent numbers. *Amer. Math. Monthly*, 107(7):631–634, 2000.
[42] D. J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.
[43] W. Rump. A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation. *Adv. Math.*, 193(1):40–55, 2005.
[44] W. Rump. Braces, radical rings, and the quantum Yang-Baxter equation. *J. Algebra*, 307(1):153–170, 2007.
[45] W. Rump. Classification of cyclic braces. *J. Pure Appl. Algebra*, 209(3):671–685, 2007.
[46] W. Rump. Semidirect products in algebraic logic and solutions of the quantum Yang-Baxter equation. *J. Algebra Appl.*, 7(4):471–490, 2008.
[47] W. Rump. The brace of a classical group. *Note Mat.*, 34(1):115–144, 2014.
[48] A. Smoktunowicz. On Engel groups, nilpotent groups, rings, braces and the Yang-Baxter equation. *Accepted for publication in Trans. Amer. Math. Soc, arXiv:1509.00420*.
[49] A. Soloviev. Non-unitary set-theoretical solutions to the quantum Yang-Baxter equation. *Math. Res. Lett.*, 7(5-6):577–596, 2000.
[50] Y. P. Sysak. Products of infinite groups. *Akad. Nauk Ukrain. SSR Inst. Mat. Preprint*, (53):36, 1982.
[51] Y. P. Sysak. Products of groups and local nearrings. *Note Mat.*, 28(suppl. 2):181–216 (2009), 2008.
[52] M. Takeuchi. Matched pairs of groups and bismash products of Hopf algebras. *Comm. Algebra*, 9(8):841–882, 1981.
[53] M. Takeuchi. Survey on matched pairs of groups—an elementary approach to the ESS-LYZ theory. In *Noncommutative geometry and quantum groups (Warsaw, 2001)*, volume 61 of *Banach Center Publ.*, pages 305–331. Polish Acad. Sci., Warsaw, 2003.
[54] A. Weinstein and P. Xu. Classical solutions of the quantum Yang-Baxter equation. *Comm. Math. Phys.*, 148(2):309–343, 1992.

School of Mathematics, The University of Edinburgh, James Clerk Maxwell Building, The Kings Buildings, Mayfield Road EH9 3JZ, Edinburgh
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

Department of Mathematics, College of Engineering, Mathematics and Physical Sciences, University of Exeter, Exeter EX4 4QF U.K.
E-mail address: N.P.Byott@exeter.ac.uk