Journal of Algebra 556 (2020) 725–749

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

# Affine structures of decomposable solvable groups

Wolfgang Rump

*Institute for Algebra and Number Theory, University of Stuttgart, Pfaffenwaldring 57, D-70550 Stuttgart, Germany*

ARTICLE INFO

*Article history:*
Received 5 October 2019
Available online 15 April 2020
Communicated by Nicolás Andruskiewitsch

Dedicated to B.V.M.

*MSC:*
17D99
20E22
08A05
81R50

*Keywords:*
Brace
Solvable group
Bi-crossed product
Affine structure

ABSTRACT

Bi-crossed products of groups are closely related to *braces*, a ring-like structure connected with solutions to the Yang-Baxter equation. The asymmetric product of braces, which has become useful for the construction of regular affine groups and simple braces, as well as several other product constructions, are unified, extended, and simplified. All bi-crossed products of bicyclic braces are classified.

© 2020 Elsevier Inc. All rights reserved.

## Introduction

Group factorizations $G = AB$ into proper subgroups $A, B$ have been considered since the early development of group theory. From 1933 on, they have been studied by I. Schur and his students [29,42] and descendants [20,21]. Itô [22] proved that $G$ is metabelian if $A, B$ are abelian. Contributions to the case where $A$ and $B$ are cyclic were made by

*E-mail address:* rump@mathematik.uni-stuttgart.de.

https://doi.org/10.1016/j.jalgebra.2020.04.004
0021-8693/© 2020 Elsevier Inc. All rights reserved.

Rédei [30] and Cohn [10] who settled the case where $A$ is infinite, and Douglas [11] who developed a reduction procedure for finite $A, B$. Huppert proved that $G$ is supersolvable [20], but a complete description for cyclic $A, B$ has not been carried out. Some of Douglas' results were improved later by Gorenstein and Herstein [14,15].

Miller [27,28] considered factorizations with $A \cap B = 1$ (we call them *decompositions*) for transitive permutation groups of prime power degree, which led him to state the decomposition problem as a fundamental question in group theory. Zappa [43] and Szép [40,41] showed that decompositions give rise to mutual actions between $A$ and $B$, from which $G$ can be recovered as a *bi-crossed product* $G = A \bowtie B$ of $A$ and $B$.

For decompositions $G = A_1 \cdots A_n$ into finitely many factors, it has to be assumed that the $A_i$ pairwise commute, which is granted for $n = 2$. Hall [17,18] proved that a group is solvable if and only if it admits a decomposition into Sylow subgroups. Wielandt [42] extended Hall's theorem to nilpotent factors.

In this paper, we study group decompositions $G = AB$ in connection with ring-like structures called *braces* [32], which were introduced as a tool for solving the set-theoretic Yang-Baxter equation [12,13,26,31]. Apart from this original purpose, there is an increasing tendency to study braces in their own right [32,6,7,35,8,37,36]. For a quick orientation on braces and a sketch of their relationship to mathematical topics like flat manifolds, Chevalley groups, and Lie algebras, we refer to [35]. Here we focus upon braces in the context of group decompositions.

Before explaining our results, let us elaborate how braces are related to any group decomposition $G = AB$. Each pair of elements $a \in A$ and $b \in B$ gives rise to a unique factorization

$$ba = \alpha\beta$$

with $\alpha \in A$ and $\beta \in B$. With ${}^b a := \alpha$ and $b^a := \beta$, the map $a \mapsto {}^b a$ defines a left action of the group $B$ on the set $A$, and $b \mapsto b^a$ gives a right action of the group $A$ on the set $B$. Changing the roles of $A$ and $B$, we also get a left action ${}^\alpha\beta := b$ and a right action $\alpha^\beta := a$, so that there are left and right actions of $A$ on $B$, and vice versa. If $b \mapsto a \cdot b$ denotes the inverse of $b \mapsto b^a$ and $a \mapsto b \cdot a$ the inverse of $a \mapsto a^b$, the equation $ba = ({}^b a)(b^a)$ can be rewritten as

$$(a \cdot b)a = (b \cdot a)b. \tag{0}$$

With a slight modification, this equation defines an *affine structure* [37] of a group $G$, the modification being that the equation has to be valid for all $a, b \in G$. The operation $a + b := (a \cdot b)a$ then gives an abelian group structure for $G$. By [37], Theorem 2.1, an affine structure of a group $G$ is equivalent to a *brace* $A$ with *adjoint group* $A^\circ = G$. The basic example of a brace is the Jacobson radical $J$ of any ring $R$, with $a \cdot b := b(1+a)^{-1}$. The adjoint group $J^\circ$ of $J$ is given by Jacobson's circle operation $a \circ b := ab + a + b$.

Thus any group decomposition $G = AB$ gives a part of a brace, where only the operations within $A$ and $B$ are undefined. If they can be inserted in a compatible fashion,

$G$ becomes the adjoint group of a brace, with $A$ and $B$ as right ideals, constituting a bi-crossed product representation $A \bowtie B$ for that brace [2]. On the other hand, any brace $A$ can be viewed as part of a bi-crossed product $A \bowtie A$ in a natural way (Example 2). For a finite brace, the $p$-components of the additive group give a decomposition into right ideals, hence a decomposition of the adjoint group $G$ into Sylow subgroups, which implies that $G$ must be solvable. Examples of solvable groups without an affine structure exist, but they are rare. (Bachiller's counterexample [1] is a $p$-group of order $23^{10}$.)

To understand the structure of braces, it is natural to study the possible ways to construct them as composites of smaller ones. We already mentioned the bi-crossed product $A \bowtie B$, where the adjoint group $(A \bowtie B)^\circ$ coincides with the bi-crossed product $A^\circ \bowtie B^\circ$ of groups. Special cases are the semidirect product of braces [34] and the direct product $A \times B$. However, other types of composites have been found. For example, Catino et al. [5] introduced the *asymmetric product* $A \ltimes_\circ B$ of braces, where the adjoint group is $A^\circ \ltimes B^\circ$, while the additive group is modified by a symmetric 2-cocycle. Together with Hegedüs' striking construction [19] of socle-free braces, simple braces can be obtained as asymmetric products [4]. We show that the asymmetric product is closely related to the *upper shifted semi-direct product* [37] of braces.

Our first main result in this paper provides a general way to amalgamate two braces $A, B$ to a brace $A \bowtie_\delta B$ with adjoint group $A^\circ \bowtie B^\circ$, where the additive group is modified by a 2-cocycle $\delta$ (Theorem 1). All the above mentioned constructions, and also the *lower shifted semi-direct product* [37], are special cases. Despite this generality, the conditions for $\delta$ are very simple: they are $\delta(x, y) = \delta(y, x)$ and $\delta(x, y)^a = \delta(x^a, y^a)$, and

$$\delta(x + y, z) = \delta(y \cdot x, y \cdot z)^y + \delta(y, z)$$

for $a \in A$ and $x, y \in B$, which shows that $\delta$ is almost bilinear. Note that $y \cdot (\ )$ is inverse to $(\ )^y$. Thus $\delta$ is bilinear if and only if $\delta(x, z)^y = \delta(x^y, z^y)$. The asymmetric product arises as the special case where $B$ acts trivially on $A$ (Corollary 2), while the lower shifted semi-direct product arises when $A$ acts trivially on $B$ (Corollary 3). In particular, the above equations for $\delta$ imply the 2-cocycle condition as well as a complicated extra condition (Eqs. (20) and (25) in Section 3) in case of an asymmetric product.

For $\delta = 0$ we get the bi-crossed product $A \bowtie B$ of braces. The socle of $A \bowtie_\delta B$ is determined in Proposition 5, which extends previous results for the upper and lower shifted semi-direct product. It follows that the socle of $A \bowtie B$ decreases by the passage to $A \bowtie_\delta B$, which can be used for the construction of simple braces. It should be noted that recently, several authors have constructed simple braces via product decompositions [3,9]. As non-involutive solutions to the Yang-Baxter equation are related to skew-braces [16] (where the operation $\cdot$ is replaced by two operations [36]), factorizations of skew-braces have been considered [24]. For the analysis of group decompositions, the above equation (0) shows that we are actually dealing with braces.

As a second main result, we determine the bi-crossed products $A \bowtie B$ where $A$ and $B$ are bicyclic braces, that is, with cyclic additive and adjoint group (Theorem 2). So the

adjoint group of $A \bowtie B$ is a bi-crossed product of cyclic groups. Surprisingly, the work of Douglas [11] and Rédei [30] could not provide any help, so that we had to choose a different approach. Corollary 2 gives a simple description for the case where $A$ is infinite. It turns out that some of the groups listed in [30] cannot arise from bi-crossed products of braces (Example 7). On the other hand, we show that Douglas' type reduction for bi-crossed products of cyclic groups [11,14,15] carries over to braces (Theorem 3).

## 1. Preliminaries: affine structures and braces

By $\mathfrak{S}(X)$ we denote the symmetric group over a set $X$. An *affine structure* [37] on a group $G$ is given by an action $\sigma\colon G \to \mathfrak{S}(G)$ of $G$ on its underlying set such that the binary operation $a \cdot b := \sigma(a)(b)$ satisfies

$$(a \cdot b)a = (b \cdot a)b. \tag{1}$$

In terms of the binary operation, an affine structure is given by Eq. (1) and the equation

$$ab \cdot c = a \cdot (b \cdot c). \tag{2}$$

Indeed, Eq. (2) implies that $1 \cdot (1 \cdot a) = 1 \cdot a$, which yields, since $\sigma(1)$ is bijective,

$$1 \cdot a = a.$$

Eq. (1) with $b = 1$ gives

$$a \cdot 1 = 1.$$

A group $G$ with an affine structure is equivalent to a *brace* [32]. For the geometric intuition behind this concept of affine structure, we refer to [35]. Note that Eq. (1) gives rise to a commutative operation

$$a + b := (a \cdot b)a = (b \cdot a)b$$

which makes $(G; +)$ into an abelian group. With $a^b := \sigma(b)^{-1}(a)$, the multiplication of $G$ is given by the equation $ab = a^b + b$. This leads to another equivalent description ([32], Proposition 5) of a brace as an abelian group $A = (G; +)$ with a binary operation $\cdot$ satisfying

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \tag{3}$$

$$(a + b) \cdot c = (a \cdot b) \ \cdot \ (a \cdot c). \tag{4}$$

The group $A^\circ := G$ associated to a brace $A$ is called the *adjoint group* of $A$. For example, the Jacobson radical $J$ of a ring $R$ is a brace with adjoint multiplication

$$a \circ b = ab + a + b. \tag{5}$$

Therefore, we write $\circ$ for the multiplication in the adjoint group $A^\circ$ of any brace. Similarly, we use Jacobson's notation $a'$ (see [23]) for the inverse of an element $a \in A^\circ$. Eq. (4) yields

$$(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z) \tag{6}$$

for all $x, y, z \in G$. A set $X$ with a binary operation $\cdot$ satisfying Eq. (6) such that the map $\sigma\colon X \to \mathfrak{S}(X)$ with $\sigma(x)(y) := x \cdot y$ is bijective is said to be a *cycle set* [31]. By [31], Proposition 1, every cycle set is equivalent to a left non-degenerate involutive set-theoretic solution [13] to the Yang-Baxter equation.

Like in a Jacobson radical ring, Eq. (5) defines a ring-like multiplication (given by juxtaposition) for any brace $A$. The associativity of $A^\circ$ then turns into the equation

$$a(bc + b + c) = (ab)c + ab + ac. \tag{7}$$

Using the right multiplication $R_a \in \mathrm{End}(A;+)^{\mathrm{op}}$, that is, $b \mapsto ba$, viewed as a right action on the additive group of $A$, Eq. (7) can be written as

$$R_{bc+b+c} = R_b R_c + R_b + R_c.$$

Using the circle operation (5) in $\mathrm{End}(A;+)^{\mathrm{op}}$, this gives a homomorphism

$$R\colon A^\circ \to \big(\mathrm{End}(A;+)^{\mathrm{op}};\circ\big),$$

the *(right) regular representation* of the brace $A$.

More generally, a *module* [32] over a brace $A$ is an abelian group $M$ with a monoid homomorphism $\varrho\colon A^\circ \to \big(\mathrm{End}(M)^{\mathrm{op}};\circ\big)$. With $xa := \varrho(a)(x)$, this means that $x0 = 0$ and

$$(x + y)a = xa + ya$$
$$x(a \circ b) = (xa)b + xa + xb$$

holds for $x, y \in M$ and $a, b \in A$. Equivalently, $x^a := xa + x$ is a right action of $A^\circ$ on $M$:

$$(x + y)^a = x^a + y^a$$
$$x^{a \circ b} = (x^a)^b.$$

Thus, if $x \mapsto a \cdot x$ denotes the inverse of $x \mapsto x^a$, every (right) module $M$ can be viewed as a *left module*, satisfying

$$a \cdot (x + y) = a \cdot x + a \cdot y$$
$$(a \circ b) \cdot x = a \cdot (b \cdot x).$$

A subgroup $I$ of a brace $A$ is said to be a *right ideal* [32] if $a \in I$ and $b \in A$ implies that $ab \in I$. If $ba \in I$ also holds, $I$ is called an *ideal* [32]. Equivalently, $I$ is a right ideal if and only if $I$ is an $A^\circ$- submodule of $A$. In particular, every right ideal $I$ is a subbrace, and $I^\circ$ is a subgroup of $A^\circ$. A right ideal $I$ is an ideal of $A$ if and only if $I^\circ$ is a normal subgroup of $A^\circ$. So the invariance under right multiplication refers to the adjoint action, while invariance under left multiplication means invariance (=normality) as a subgroup of the adjoint group. The *socle*

$$\mathrm{Soc}(A) := \{a \in A \mid \forall\, b \in A \colon a \cdot b = b\}$$

of a brace $A$ is an ideal, and the *fixator*

$$\mathrm{Fix}(A) := \{b \in A \mid \forall\, a \in A \colon a \cdot b = b\}$$

is a right ideal of $A$. If $\mathrm{Soc}(A) = A$, the brace $A$ is said to be *trivial*.

From Eq. (3) we infer that $a \cdot (b \circ c) = a \cdot (b^c + c) = a \cdot b^c + a \cdot c = \big((a \cdot c) \cdot (a \cdot b^c)\big) \circ (a \cdot c) = \big((c \cdot a) \cdot (c \cdot b^c)\big) \circ (a \cdot c)$, which yields

$$a \cdot (b \circ c) = \big((c \cdot a) \cdot b\big) \circ (a \cdot c). \tag{8}$$

For a group $G$, let $G = AB$ be a *decomposition*, that is, $G = AB$ and $A \cap B = \{1\}$. Then $B$ is said to be a *complement* of $A$. Every $g \in G$ has a unique representation $g = ab$ with $a \in A$ and $b \in B$. In particular, $g^{-1}$ has such a representation, which shows that $G = AB = BA$. For any $a \in A$ and $b \in B$, this implies that there are unique ${}^a b \in B$ and $a^b \in A$ with $ab = ({}^a b)(a^b)$. By [37], Proposition 3.2, the map $a \mapsto a^b$ defines a right action of $B$ on the set $A$, and $b \mapsto {}^a b$ gives a left action of $A$ on the set $B$. In accordance with [37], Section 3, these actions will be called the *metacommutation actions*. By $a \mapsto b \cdot a$ we denote the inverse of $a \mapsto a^b$. Then the equation $ab = ({}^a b)(a^b)$ can be rewritten as

$$(b \cdot a)b = (a \cdot b)a, \tag{9}$$

which shows that the map $(a, b) \mapsto ({}^a b, a^b)$ is an involution of $A \times B$. In particular, $b = ({}^a b)^{a^b}$, which yields

$${}^a b = a^b \cdot b. \tag{10}$$

Inverting the equation $ab = ({}^a b)(a^b)$, we obtain $b^{-1}a^{-1} = (a^b)^{-1}({}^a b)^{-1}$. Thus $({}^a b)^{-1} = (b^{-1})^{a^{-1}} = a \cdot b^{-1}$, which yields

$${}^a b = (a \cdot b^{-1})^{-1}. \tag{11}$$

For $a \in A$ and $x, y \in B$, Eq. (9) gives $(a \cdot xy)a = (xy \cdot a)xy = \big(x \cdot (y \cdot a)\big)xy = \big((y \cdot a) \cdot x\big)(y \cdot a)y = \big((y \cdot a) \cdot x\big)(a \cdot y)a$. Hence

$$a \cdot xy = \big((y \cdot a) \cdot x\big)(a \cdot y). \tag{12}$$

For any brace $A$, Eq. (10) gives a left action $b \mapsto {}^a b$ of $A^\circ$ on the set $A$. Therefore, we define ${}^a b := a^b \cdot b$ also for braces. Moreover, Eq. (11) is satisfied:

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

The following definition gives an analogue of group decompositions for braces.

**Definition 1.** We define a *decomposition* of a brace $A$ to be a decomposition $A = I \oplus J$ of the additive group into right ideals $I$ and $J$.

The connection to group decompositions is given by

**Proposition 1.** *Let $A = I \oplus J$ be a decomposition of a brace $A$ into right ideals. Then $A^\circ = I^\circ J^\circ$. The maps $I \to I$ and $J \to J$ given by $a \mapsto a^b$ and $b \mapsto {}^a b$ for $a \in I$ and $b \in J$ coincide with the metacommutation actions of $A^\circ = I^\circ J^\circ$. The action $a \mapsto a^b$ is trivial if and only if $J$ is an ideal.*

**Proof.** Any $c \in A$ is of the form $c = a + b = (a \cdot b) \circ a = (b \cdot a) \circ b$ with $a \in I$ and $b \in J$. Hence $A^\circ = I^\circ J^\circ$. Replacing $a$ by $a^b$, this gives $a \circ b = (a^b \cdot b) \circ a^b = {}^a b \circ a^b$.

Now $J$ is an ideal if and only if $a \circ b \circ a' \in B$ for all $a \in A$ and $b \in B$. Since $a \circ b = (a^b \cdot b) \circ a^b$, this condition is equivalent to $a^b \circ a' = 0$, that is, $a^b = a$. □

So the affine structure of $A^\circ$ is given by the affine structures of $I^\circ$ and $J^\circ$. Note that Eq. (11) can be written as ${}^{a'}(b') = (b^a)'$, which shows that the metacommutation actions can also be expressed by the right actions $a \mapsto a^b$ and $b \mapsto b^a$ with $a \in A$ and $b \in B$. Thus, $I$ is a brace ideal if and only if the action $b \mapsto b^a$ is trivial, or equivalently, if $b \mapsto {}^a b$ is trivial. This happens if and only if $A$ is a semidirect product $I \rtimes J$ of braces [34]. If $I$ and $J$ are ideals, both metacommutation actions are trivial. We then write $A = I \times J$ and speak of a *direct decomposition* of $A$.

## 2. Decomposable groups

Proposition 1 shows that any decomposition $G = AB$ of a group $G$ already provides a part of an affine structure, which has to be completed only within the subgroups $A$ and $B$. An extension criterion for affine structures of $A$ and $B$ to an affine structure of $G$ was given in [37], Theorem 3.5. In what follows, we mostly denote elements of $A$ by $a, b, c, \ldots$ and elements of $B$ by $x, y, z \ldots$.

**Definition 2.** Let $G$ be a group with a decomposition $G = AB$. We call an affine structure of $A$ *compatible with* $G = AB$ if $a, b \in A$ and $x, y \in B$ with $xa = by$ implies that $(c^x)^a = (c^b)^y$ holds for all $c \in A$.

Since $AB = BA$, the definition includes a concept of compatibility for $B$, where $c \in A$ has to be replaced by $c \in B$. Let us show first that this definition is left-right symmetric.

**Proposition 2.** *Let $G$ be a group with a decomposition $G = AB$. An affine structure of $B$ is compatible with $G = AB$ if and only if $a, b \in A$ and $x, y \in B$ with $xa = by$ implies that ${}^x({}^a z) = {}^b({}^y z)$ for all $z \in B$.*

**Proof.** By Eq. (11), the equation ${}^x({}^a z) = {}^b({}^y z)$ transforms into $x \cdot (a \cdot z') = b \cdot (y \cdot z')$. So the condition is

$$x \cdot (a \cdot z) = b \cdot (y \cdot z), \tag{13}$$

for all $z \in B$. Replacing $z$ by $((z)^x)^a$, the equation becomes $z = b \cdot \big(y \cdot (z^x)^a\big)$, that is, $(z^b)^y = (z^x)^a$. □

**Proposition 3.** *Let $G$ be a group with a decomposition $G = AB$. An affine structure of $B$ is compatible with $G = AB$ if and only if*

$$(a \cdot x) \cdot (a \cdot y) = (x \cdot a) \cdot (x \cdot y) \tag{14}$$

*holds for $a \in A$ and $x, y \in B$. Affine structures of $A$ and $B$ are both compatible if and only if Eq. (14) holds for $a \in A$, $x \in B$, and $y \in A \cup B$.*

**Proof.** Since $xa = ({}^x a)(x^a) = (x^a \cdot a)(x^a)$, the compatibility condition (13) for $B$ says that $x \cdot (a \cdot z') = (x^a \cdot a) \cdot (x^a \cdot z')$. With $y := z'$ and $a \cdot x$ instead of $x$, this equation turns into Eq. (14). The second statement follows by symmetry. □

**Corollary 1.** *Let $G = AB$ be a decomposition of a group $G$. Two affine structures of $A$ and $B$, respectively, are compatible with $G = AB$ if and only if they extend to an affine structure of $G$.*

**Proof.** This follows by [37], Theorem 3.5. □

**Corollary 2.** *Let $G = AB$ be a decomposition of a group $G$, and let $U$ be a generating set of $A$. An affine structure of $B$ (resp. $A$) is compatible with $G = AB$ if and only if Eq. (14) holds for $a \in U$ and $x, y \in B$ (resp. $x \in B$ and $y \in A$).*

**Proof.** Assume that Eq. (14) holds for $a \in \{a_1, a_2\}$. By Eq. (12), $(a_1 a_2 \cdot x) \cdot (a_1 a_2 \cdot y) = \big(a_1 \cdot (a_2 \cdot x)\big) \cdot \big(a_1 \cdot (a_2 \cdot y)\big) = \big((a_2 \cdot x) \cdot a_1\big) \cdot \big((a_2 \cdot x) \cdot (a_2 \cdot y)\big) = \big((a_2 \cdot x) \cdot a_1\big) \cdot \big((x \cdot a_2) \cdot (x \cdot y)\big) =$

$\big((a_2 \cdot x) \cdot a_1\big)(x \cdot a_2) \cdot (x \cdot y) = (x \cdot a_1 a_2) \cdot (x \cdot y)$. For a fixed $a \in A$, Eq. (14) yields $x \cdot y = (a \cdot x^a) \cdot (a \cdot y^a) = (x^a \cdot a) \cdot (x^a \cdot y^a)$. Hence, by Eqs. (10) and (11), we obtain $(a' \cdot x) \cdot (a' \cdot y) = x^a \cdot y^a = (x^a \cdot a)' \cdot (x \cdot y) = (x \cdot a') \cdot (x \cdot y)$. □

**Corollary 3.** *Let $G$ be a group with a decomposition $G = AB$. An affine structure of $B$ is compatible with $G = AB$ if and only if $(x + y)^a = x^a + y^a$ holds for $a \in A$ and $x, y \in B$.*

**Proof.** Since $(x + y)a = b(x + y)^a$ for some $b \in A$, and $(x + y)a = (x \cdot y)xa = (x \cdot y)({}^x a)(x^a) = c\big((x \cdot y)^{{}^x a}\big)(x^a)$ for some $c \in A$, we have $(x + y)^a = \big((x \cdot y)^{{}^x a}\big)(x^a)$. On the other hand, $x^a + y^a = (x^a \cdot y^a)(x^a)$. So the condition $(x + y)^a = x^a + y^a$ turns into $(x \cdot y)^{{}^x a} = x^a \cdot y^a$. By the preceding proof, this is equivalent to Eq. (14). □

**Remark.** Note that the compatibility of $A$ in Corollary 3 is equivalent to the equation $(a + b)^x = a^x + b^x$ for $a, b \in A$ and $x \in B$, not ${}^x(a + b) = {}^x a + {}^x b$. The latter equation need not hold in a brace. It is only valid in the associated *left brace*, with additive group given by $a +' b := (a' + b')'$.

**Example 1.** Let $G = A \ltimes B$ be a semidirect product of subgroups $A, B$. Then each pair of elements $a \in A$ and $x \in B$ satisfies $xa = a(a^{-1}xa)$. So the metacommutation action on $A$ is trivial, which implies that any affine structure of $A$ is compatible with the decomposition $G = AB$. On the other hand, an affine structure on $B$ is compatible if and only if the conjugation action $A \to \mathrm{Aut}(B)^{\mathrm{op}}$ is a brace homomorphism, in accordance with [34], Section 3, where the semidirect product of braces is defined.

**Example 2.** Let $A$ be a brace. The right action $a \mapsto a^b$ and the left action (10) define a matched pair $(A^\circ, A^\circ)$ of groups ([25], Chapter 9; [36], Remark after Definition 7), which yields a group $A^\circ \bowtie A^\circ$. Multiplication in the *bi-crossed product* $A^\circ \bowtie A^\circ$ is given by

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

Hence $(a, x) = (a, 0)(0, x)$ and $(0, x)(a, 0) = ({}^x a, x^a) = ({}^x a, 0)(0, x^a)$, which shows that the actions $a \mapsto {}^x a$ and $x \mapsto x^a$ are the metacommutation actions of the decomposition $A^\circ \bowtie A^\circ = (A^\circ, 0)(0, A^\circ)$. Since $x \circ a = {}^x a \circ x^a$, the affine structure of $A^\circ$ extends to $A^\circ \bowtie A^\circ$, in accordance with [36], Proposition 15.

**Example 3.** More generally, let $A$ and $B$ be braces, and let $(A^\circ, B^\circ)$ be a matched pair of groups. The bi-crossed product $G := A^\circ \bowtie B^\circ$ is a group with a decomposition $G = A^\circ B^\circ$. By Corollary 1 and Corollary 3, the affine structures of $A^\circ$ and $B^\circ$ extend to a brace $A \bowtie B$ with adjoint group $G$ if and only if the right metacommutation actions $x \mapsto x^a$ and $a \mapsto a^x$ with $a \in A$ and $x \in B$ are additive. This is Bachiller's criterion for matched pairs of braces ([2], Theorem 4.2). We call $A \bowtie B$ the *bi-crossed product* of the braces $A$ and $B$. The additive structure of $A \bowtie B$ is given as follows (cf. [34], Proposition 4):

$$(a,x)+(b,y)=\big((x\cdot y)\cdot a+(y\cdot x)\cdot b, x+y\big).$$

The next result refines the description of a brace by a triply factorized group [39].

**Proposition 4.** *Let $A$ be a brace, and let $A^+$ be its additive group, viewed as a trivial brace. Then $a\mapsto(a',a)$ gives an embedding $A^+\hookrightarrow A\bowtie A$ of $A^+$ as an ideal of $A\bowtie A$ such that $A\bowtie A=(A,0)\ltimes A=(0,A)\ltimes A$. For $a,b,c\in A$, we have*

$$(a,b)\circ(c',c)\circ(a,b)'=(a,b)\cdot(c',c)=\big((a\cdot(b\cdot c))',a\cdot(b\cdot c)\big). \tag{15}$$

**Proof.** For $a,b\in A$, we have $(a',a)\circ(b',b)=(a'\circ{}^a(b'),a^{b'}\circ b)=(a'\circ(a\cdot b)',(b\cdot a)\circ b)=\big(((a\cdot b)\circ a)',(a\cdot b)\circ a\big)\in A^+$. Using Eq. (8), a straightforward calculation gives

$$(a,b)\cdot(c',c)=\big(((b\cdot c)\cdot a)\cdot((c\cdot b)\cdot c'),a\cdot(b\cdot c)\big)$$

for $a,b,c\in A$. Since $(c\cdot b)\cdot c'=(c\cdot b)\cdot(c\cdot(-c))=(b\cdot c)\cdot(b\cdot(-c))$, we have $((b\cdot c)\cdot a)\cdot((c\cdot b)\cdot c')=(a\cdot(b\cdot c))\cdot(a\cdot(b\cdot(-c))=(a\cdot(b\cdot c))\cdot\big(-(a\cdot(b\cdot c))\big)=(a\cdot(b\cdot c))'$. Thus,

$$(a,b)\cdot(c',c)=\big((a\cdot(b\cdot c))',a\cdot(b\cdot c)\big)\in A^+.$$

In particular, $(b',b)\cdot(c',c)=(c',c)$, which shows that $A^+$ is a trivial right ideal of $A\bowtie A$.

Finally, we have $\big((a\cdot(b\cdot c))',a\cdot(b\cdot c)\big)\circ(a,b)=\big((a\cdot(b\cdot c))'\circ((b\cdot c)\cdot a),(b\cdot c)\circ b\big)$ and $(a,b)\circ(c',c)=(a\circ{}^b(c'),b^{c'}\circ c)=\big(a\circ(b\cdot c)',(c\cdot b)\circ c\big)$. So the first equation in (15) reduces to

$$(a\cdot(b\cdot c))'\circ((b\cdot c)\cdot a)=a\circ(b\cdot c)'.$$

Indeed, $(a\cdot(b\cdot c))\circ a\circ(b\cdot c)'=((b\cdot c)\cdot a)\circ(b\cdot c)\circ(b\cdot c)'=(b\cdot c)\cdot a$. Thus Eqs. (15) are verified, which proves that $A^+$ is a brace ideal of $A\bowtie A$. The semidirect product representations of $A\bowtie A$ follow by the formulae

$$(a,b)=(a\circ b,0)\circ(b',b)=(a,a')\circ(0,a\circ b).\quad\square$$

As the structure of *cocyclic braces*, i.e. those with cyclic adjoint group, is completely known [38], it is natural to consider bi-crossed products of cocyclic braces. Example 2 shows that two isomorphic (not necessarily cocyclic) braces determine a bi-crossed product in a natural way. On the other hand, there seems to be no practible way to amalgamate cocyclic braces by starting with the adjoint group using Douglas' results [11], because Eq. (14) would rarely be satisfied. So it becomes a challenge to find matched pairs of cocyclic braces except those of Example 2. In what follows, $C_n$ denotes the cyclic group of order $n$.

**Example 4.** $G=\langle x,y,z|x^4=y^2=z^2=1,xy=yx,yz=zy,zxz=xy\rangle\cong(C_4\times C_2)\rtimes C_2$. Thus every element $g\in G$ is of the form $g=x^iy^jz^k$ with $i\in\{0,1,2,3\}$ and $j,k\in\{0,1\}$.

Then $x^3z$ is of order 4, with $(x^3z)^2 = x^2y$ and $(x^3z)^3 = xyz$, and $G$ can be represented as a product $G = \langle x\rangle\langle x^3z\rangle$:

| | | | |
|---|---|---|---|
| 1 | $x^3z$ | $x^2y$ | $xyz$ |
| $x$ | $z$ | $x^3y$ | $x^2yz$ |
| $x^2$ | $xz$ | $y$ | $x^3yz$ |
| $x^3$ | $x^2z$ | $xy$ | $yz$ |

The metacommutation actions are obtained by representing $G$ as a product $G = \langle x^3z\rangle\langle x\rangle$:

| | | | |
|---|---|---|---|
| 1 | $x$ | $x^2$ | $x^3$ |
| $x^3z$ | $yz$ | $xz$ | $x^2yz$ |
| $x^2y$ | $x^3y$ | $y$ | $xy$ |
| $xyz$ | $x^2z$ | $x^3yz$ | $z$ |

To get a matched pair $(A, B)$ of braces $A = \langle x\rangle$ and $B = \langle x^3z\rangle$, we have to consider affine structures of the cyclic group $C_4 \cong A^\circ \cong B^\circ$. There are two possibilities: the trivial one, and an affine structure with additive group $C_2 \times C_2$. Both affine structures satisfy the equations

$$a^{-1} \cdot b = a \cdot b, \qquad a \cdot b^{-1} = (a \cdot b)^{-1}.$$

On the other hand, the above tables show that $t^x = t^{-1}$ and ${}^tx = x^t \in \{x, x^3\}$ for all $t \in B$. Hence $x \cdot t = t^{-1}$ and $t \cdot x \in \{x, x^{-1}\}$. For $s, t \in B$, this gives $(x \cdot s) \cdot (x \cdot t) = s^{-1} \cdot t^{-1} = s \cdot t^{-1} = (s \cdot t)^{-1} = (s \cdot x) \cdot (s \cdot t)$. So Corollary 2 of Proposition 3 implies that $B$ is compatible with $G = AB$. Since $(x, y, z) \mapsto (x^3z, y, z)$ extends to an automorphism of $G$, the subgroup $A$ is compatible with $G = AB$, too. Thus, each of the four possibilities to endow $A$ and $B$ with an affine structure leads to an affine structure of $G$.

## 3. Shifted bi-crossed products of braces

For most of the known constructions of braces $A$ by amalgamation, the adjoint group $A^\circ$ can be represented as a semidirect product. One of the rare exceptions is the symmetric group $S_4$ which does not admit a normal Sylow subgroup. If a semidirect product $A^\circ = H \ltimes N$ does not arise from a semidirect product of braces, it frequently happens that $A$ can be deformed into a semidirect product by an additive or multiplicative 2-cocycle. Both cases occur [37] for the braces of order 8. In this section, we extend and unify these constructions and compare them with the *asymmetric* product of braces [5,4].

Let $(A, B)$ be a matched pair of braces. So there is a bi-crossed product $A \bowtie B$ with adjoint group $A^\circ \bowtie B^\circ$ such that the affine structures of $A^\circ$ and $B^\circ$ are compatible with the decomposition $A^\circ \bowtie B^\circ = (A^\circ, 0)(0, B^\circ)$ (see Example 3). In what follows, it will be convenient to represent the elements of $A \bowtie B$ as sums $a + x$, with $a \in (A, 0)$

and $x \in (0, B)$. Accordingly, the multiplication in $(A \bowtie B)^\circ = A^\circ \bowtie B^\circ$ has to be modified. For $a, b \in A$ and $x, y \in B$, we have $(a + x) \circ (b + y) = (a + x)^{b+y} + b + y = a^{b+y} + x^{b+y} + b + y = a^{(b\cdot y)\circ b} + b + x^{(y\cdot b)\circ y} + y = a^{b\cdot y} \circ b + x^{y\cdot b} \circ y$. More generally, we define

$$[a, x] := (a, 0) + (0, x) = (x \cdot a, x).$$

So the operations in $A \bowtie B$ are given by

$$[a, x] + [b, y] = [a + b, x + y]$$
$$[a, x] \circ [b, y] = [a^{b\cdot y} \circ b, x^{y\cdot b} \circ y].$$

We modify the addition in $A \bowtie B$ by a map $\delta\colon B \times B \to A$ as follows:

$$[a, x] + [b, y] = [a + b + \delta(x, y), x + y]. \tag{16}$$

To indicate that addition has been modified via (16), we write $A \bowtie_\delta B$ instead of $A \bowtie B$.

**Theorem 1.** *Let $A \bowtie B$ be a bi-crossed product of braces, and let $\delta\colon B \times B \to A$ be a map with $\delta(0, 0) = 0$. Then $A \bowtie_\delta B$ is a brace if and only if $\delta$ satisfies*

$$\delta(x, y) = \delta(y, x) \tag{17}$$
$$\delta(x, y)^a = \delta(x^a, y^a) \tag{18}$$
$$\delta(x + y, z) = \delta(y \cdot x, y \cdot z)^y + \delta(y, z), \tag{19}$$

*for $a \in A$ and $x, y, z \in B$.*

**Proof.** Associativity of addition in $A \bowtie_\delta B$ says that

$$[a + b + \delta(x, y), x + y] + [c, z] = [a, x] + [b + c + \delta(y, z), y + z]$$

holds for $a, b, c \in A$ and $x, y, z \in B$, that is,

$$[a + b + \delta(x, y) + c + \delta(x + y, z), x + y + z] = [a + b + c + \delta(y, z) + \delta(x, y + z), x + y + z],$$

which reduces to the 2-cocycle condition

$$\delta(y, z) - \delta(x + y, z) + \delta(x, y + z) - \delta(x, y) = 0. \tag{20}$$

Commutativity of the modified addition (16) is equivalent to Eq. (17). For $z = 0$, Eq. (20) becomes $\delta(y, 0) - \delta(x + y, 0) = 0$, which yields

$$\delta(x, 0) = \delta(0, x) = 0$$

for all $x \in B$. So $[a,x] + [0,0] = [a + \delta(x,0), x] = [a,x]$, which shows that $[0,0]$ is a zero element for the modified addition. The inverse of $[a,x]$ is

$$-[a,x] = [-\delta(x,-x) - a, -x].$$

Thus Eqs. (17) and (20) state that $A \bowtie_\delta B$ is an additive group.

The remaining condition for $A \bowtie_\delta B$ to be a brace is given by the equation

$$\big([a,x] + [b,y]\big) \circ [c,z] + [c,z] = [a,x] \circ [c,z] + [b,y] \circ [c,z]. \tag{21}$$

Its left-hand side is

$$\begin{aligned}[a+b+\delta(x,y), x+y] \circ [c,z] + [c,z] &= [(a+b+\delta(x,y))^{c\cdot z} \circ c, (x+y)^{z\cdot c} \circ z] + [c,z] \\ &= [(a+b+\delta(x,y))^{c\cdot z} \circ c + c + \delta((x+y)^{z\cdot c} \circ z, z), (x+y)^{z\cdot c} \circ z + z],\end{aligned}$$

while the right-hand side of Eq. (21) amounts to $[a^{c\cdot z} \circ c, x^{z\cdot c} \circ z] + [b^{c\cdot z} \circ c, y^{z\cdot c} \circ z] = [a^{c\cdot z} \circ c + b^{c\cdot z} \circ c + \delta(x^{z\cdot c} \circ z, y^{z\cdot c} \circ z), x^{z\cdot c} \circ z + y^{z\cdot c} \circ z]$. So Eq. (21) is equivalent to the equations

$$(a+b+\delta(x,y))^{c\cdot z} \circ c + c + \delta((x+y)^{z\cdot c} \circ z, z) = a^{c\cdot z} \circ c + b^{c\cdot z} \circ c + \delta(x^{z\cdot c} \circ z, y^{z\cdot c} \circ z) \tag{22}$$

and

$$(x+y)^{z\cdot c} \circ z + z = x^{z\cdot c} \circ z + y^{z\cdot c} \circ z.$$

Since $(x+y)^{z\cdot c} = x^{z\cdot c} + y^{z\cdot c}$, the second equation is redundant. Furthermore,

$$(a+b+\delta(x,y))^{c\cdot z} \circ c + c = \big((a+b)^{c\cdot z} + \delta(x,y)^{c\cdot z}\big) \circ c + c = (a+b)^{c\cdot z} \circ c + \delta(x,y)^{c\cdot z} \circ c,$$

where $(a+b)^{c\cdot z} \circ c = a^{c\cdot z} \circ c + b^{c\cdot z} \circ c - c$. So Eq. (22) can be rewritten as

$$(\delta(x,y)^{c\cdot z})^c + \delta((x+y)^{z\cdot c} \circ z, z) = \delta(x^{z\cdot c} \circ z, y^{z\cdot c} \circ z). \tag{23}$$

For $z = 0$, this equation turns into Eq. (18). Now Eq. (18) yields $(\delta(x,y)^{c\cdot z})^c = (\delta(x,y)^{z\cdot c})^z = \delta(x^{z\cdot c}, y^{z\cdot c})^z$. Thus if we replace $x$ by $(z \cdot c) \cdot x$ and $y$ by $(z \cdot c) \cdot y$, Eq. (23) becomes

$$\delta(x,y)^z + \delta((x+y) \circ z, z) = \delta(x \circ z, y \circ z). \tag{24}$$

By Eq. (20), $\delta(x \circ z, y \circ z) - \delta((x+y) \circ z, z) = \delta(x \circ z, y^z + z) - \delta((x \circ z + y \circ z - z, z) = \delta(x \circ z, y^z + z) - \delta((x \circ z + y^z, z) = \delta(x \circ z, y^z) - \delta(y^z, z)$, which turns Eq. (24) into

$$\delta(x,y)^z = \delta(x \circ z, y^z) - \delta(y^z, z).$$

Using Eq. (17), and replacing $x$ by $z \cdot x$ and $y$ by $z \cdot y$, this is equivalent to Eq. (19). Conversely, Eqs. (17) and (19) yield $\delta(x+y,z)-\delta(y,z) = \delta(y\cdot x, y\cdot z)^y = \delta(y\cdot z, y\cdot x)^y = \delta(z+y,x)-\delta(y,x) = \delta(x,y+z)-\delta(x,y)$, that is, Eq. (20). □

We call $A \bowtie_\delta B$ the *shifted* bi-crossed product of $A$ and $B$. For $\delta = 0$ we have the ordinary bi-crossed product $A \bowtie B$, in its additive version (see [2], Definition 4.1). The equations (17)-(19) take a particularly simple form if $\delta$ is bilinear:

**Corollary 1.** *Let $A \bowtie B$ be a bi-crossed product of braces, and let $\delta\colon B \times B \to A$ be a symmetric bilinear map satisfying*

$$\delta(x,y)^c = \delta(x^c, y^c)$$

*for $x, y \in B$ and $c \in A \cup B$. Then $A \bowtie_\delta B$ is a brace.*

Another special case arises when $A \bowtie B$ is a semidirect product. By Theorem 1, there are two such cases:

Case 1: $B$ acts trivially on $A$. For $c \in A$ and $x, y \in B$, this implies that $(\delta(x,y)^{c\cdot z})^c = (\delta(x,y)^{z\cdot c})^z = \delta(x,y)^{z\cdot c}$. Thus, if we replace $z \cdot c$ by $c$, Eq. (23) reduces to

$$\delta(x,y)^c + \delta((x+y)^c \circ z, z) = \delta(x^c \circ z, y^c \circ z). \tag{25}$$

Since $\delta(x,y)^c = \delta(x,y) \circ c - c$, this condition is equivalent to the equation (1) in [5], Theorem 3, where the *asymmetric product* of braces has been introduced. So [5], Theorem 3, says that for a semidirect product $A \ltimes B$ of braces $A, B$, the modified addition (16) gives a brace $A \bowtie_\delta B$ if and only if $\delta$ is a symmetric 2-cocycle which satisfies Eq. (25). The authors of [5] use $A \ltimes_\circ B$ for the asymmetric product. By Theorem 1, the equations (17), (20), and (25), which characterize the asymmetric product $A \ltimes_\circ B$ can be replaced by the more appealing equations (17)-(18) and $\delta(x+y,z) = \delta(y\cdot x, y\cdot z) + \delta(y,z)$. Note that for $y = z = 0$ the latter equation implies that $\delta(0,0) = 0$. Hence

**Corollary 2.** *The asymmetric product $A \ltimes_\circ B$ of braces is equivalent to a shifted bi-crossed product $A \bowtie_\delta B$ where $B$ acts trivially on $A$.*

A multiplicative version of Eq. (19) was considered in [37], Proposition 4.1. Replacing $x$ by $x^y$, the equation becomes $\delta(x \circ y, z) = \delta(y,z) + \delta(x, y\cdot z)$. Thus, if the image of $\delta$ is in the socle of $A$, Eq. (19) turns into Eq. 4.7 of [37]:

$$\delta(x \circ y, z) = \delta(y,z) \circ \delta(x, y\cdot z).$$

So the *upper shifted* semidirect product $A \ltimes^\delta B$ of [37], Proposition 4.1, can be viewed as an asymmetric product of braces.

Again, the situation further simplifies when $\delta$ is bilinear. In particular, the construction is still useful if $A$ and $B$ are trivial braces. Then Eqs. (17)-(19) just say that $\delta\colon B\times B\to A$ is an $A$-invariant symmetric bilinear map. Let $V$ be a vector space over a finite field $\mathbb{F}_q$, with a symmetric bilinear form $\delta\colon V\times V\to\mathbb{F}_q$. Any automorphism $\alpha$ of $V$ of order $q$ gives rise to a semidirect product $\mathbb{F}_q\ltimes V$ of trivial braces, with

$$[\lambda,x]\circ[\mu,y]=[\lambda\mu,x^\mu+y],$$

where $x^\mu:=\alpha^\mu(x)$. Thus $\mathbb{F}_q\ltimes^\delta V$ is a brace if and only if $\delta$ is invariant under $\alpha$, that is,

$$\delta(\alpha(x),\alpha(y))=\delta(x,y).$$

For $\dim V<\infty$, this example was first considered by Hegedüs [19].

Case 2: $A$ acts trivially on $B$. Then Theorem 1 gives the *lower shifted* semidirect product $A\rtimes_\delta B$ of braces ([37], Proposition 4.4):

**Corollary 3.** *Let $A\rtimes B$ be a semidirect product of braces, and let $\delta\colon B\times B\to\mathrm{Fix}(A)$ be a map satisfying $\delta(x,y)=\delta(y,x)$ and*

$$\delta(x+y,z)=\delta(y\cdot x,y\cdot z)^y+\delta(y,z) \tag{26}$$

*for $x,y,z\in B$. With the modified addition (16), $A\rtimes B$ turns into the brace $A\rtimes_\delta B$.*

**Proof.** For $y=z=0$, Eq. (26) gives $\delta(0,0)=0$. Eq. (4.18) of [37] states that the image of $\delta$ is in $\mathrm{Fix}(A)$, while [37], Eq. (4.16), holds in the semidirect product of braces. With $x^y$ instead of $x$, Eq. (26) turns into [37], Eq. (4.17). □

The following result generalizes [37], Corollary 4.3 and Corollary 4.6.

**Proposition 5.** *Let $A\bowtie_\delta B$ be a shifted bi-crossed product of braces. For $a,b\in A$ and $x,y\in B$,*

$$[a,x]\cdot[b,y]=[(a\cdot x)\cdot\big(a\cdot(b+\delta(x,y))\big),(x\cdot a)\cdot(x\cdot y)]. \tag{27}$$

*The socle of $A\bowtie_\delta B$ consists of the $[a,x]\in\mathrm{Soc}(A\bowtie B)$ with $\delta(x,y)=0$ for all $y\in B$.*

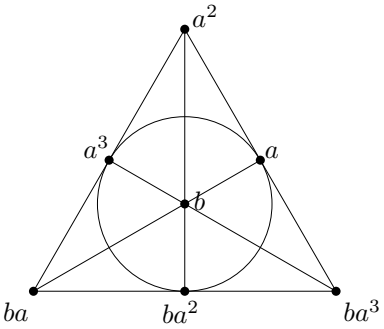
**Proof.** With $[c,z]:=[a,x]\cdot[b,y]$, we have $[c^{a\cdot x}\circ a,z^{x\cdot a}\circ x]=[c,z]\circ[a,x]=[a,x]+[b,y]=[a+b+\delta(x,y),x+y]$. Hence $(c^{a\cdot x})^a=b+\delta(x,y)$ and $(z^{x\cdot a})^x=y$, which yields $z=(x\cdot a)\cdot(x\cdot y)$ and $c=(a\cdot x)\cdot\big(a\cdot(b+\delta(x,y))\big)$. This proves Eq. (27).

Thus $[a,x]\in\mathrm{Soc}(A\bowtie B)$ if and only if $(a\cdot x)\cdot\big(a\cdot(b+\delta(x,y))\big)=b$ and $(x\cdot a)\cdot(x\cdot y)=y$ for all $b\in A$ and $y\in B$. For $b=0$, this implies that $\delta(x,y)=0$ for all $y\in B$. So the remaining condition says that $[a,x]\in\mathrm{Soc}(A\bowtie B)$. □

**Example 5.** Bachiller [2] constructed a simple brace $A$ with adjoint group $S_4$ (see also [37], Example 4). The adjoint group of its 2-component $A_2$ is a dihedral group $\langle a, b \,|\, a^4 = b^2 = 1,\ bab = a^3\rangle$ with $a := (1234)$ and $b := (13)$, while the 3-component $A_3$ is a trivial brace, generated by $c := (123)$. So $\langle a, b\rangle = A_2^\circ$ and $\langle c\rangle = A_3^\circ$ form a Sylow basis of $S_4$. The subgroup $V := \{1, a^2, ba, ba^3\}$ of $A_2^\circ$ acts trivially on $A_3$ and is invariant under the metacommutation action of $A_3^\circ$. By Eqs. (5.6) of [37], the action of $c$ on $A_2$ consists of two cycles:

$$\begin{array}{lll} c \cdot a = a^3 & c \cdot a^3 = ba^2 & c \cdot ba^2 = a \\ c \cdot a^2 = ba & c \cdot ba = ba^3 & c \cdot ba^3 = a^2. \end{array} \tag{28}$$

Addition in $A_2$ is given by the following labelling of the Fano plane:




In this representation, the automorphism (28) can be visualized as a one-third counter-clockwise rotation. Conjugation by $c$ is given by

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

where $x \in A_2$, and $i(x) = 0$ if $x \in V$ and $i(x) = 1$ otherwise. For $x, y \in A_2$, this yields

$$c \circ (x + y) \circ c^{-1} = c \circ x \circ c^{-1} + c \circ x \circ c^{-1} + \delta(x, y),$$

where $\delta(x, y) := c^{i(x+y)-i(x)-i(y)}$ is a symmetric 2-cocycle which satisfies Eqs. (17)-(18). Eq. (19) follows since

$$i(x + y) - i(x) = (-1)^{i(x)} i(x \cdot y)$$

holds for all $x, y \in A_2$, which is easily checked. Similarly, conjugation with $c^2$ gives the 2-cocycle $-\delta$. Since conjugation with $c$ is an automorphism of $S_4$ which fixes the Sylow 3-subgroup, the shifted bi-crossed products $A_3 \bowtie_\delta A_2$ and $A_3 \bowtie_{-\delta} A_2$ are isomorphic to $A$. We remark that there are no other non-zero maps $\delta\colon A_2 \times A_2 \to A_3$ which satisfy Eqs. (17)-(19). Moreover, any map $\delta\colon A_3 \times A_3 \to A_2$ which satisfies Eqs. (17)-(19) must be zero. Indeed, Eq. (18) implies that $V$ acts trivially on the image of $\delta$. Hence

$\delta(A_3 \times A_3) \subset \{0, b\}$. By Eq. (19), this implies that $\delta(c^2, c) = \delta(c+c, c) = \delta(c, c)^c + \delta(c, c) = \delta(c, c) + \delta(c, c) = 0$, and similarly, $\delta(c, c) = \delta(c^2, c^2) = 0$.

## 4. Bi-crossed products of cyclic braces

Although the structure of bi-crossed products of cyclic groups is fairly well understood [11,20,14,15], and the affine structures of cyclic groups are completely known, there seems to be no reasonable way to understand bi-crossed products of cocyclic braces $A$ and $B$ by fixing the adjoint group $A^\circ \bowtie B^\circ$. To circumvent this obstacle, we focus upon the additive groups of $A$ and $B$. The following proposition gives a converse to Proposition 3 (cf. [2], Theorem 4.2).

**Proposition 6.** *A matched pair of braces $A, B$ is equivalent to an $A$-module structure of $B$ together with a $B$-module structure of $A$ such that Eq. (14) holds for $a \in A$ and $x \in B$, and $y \in A \cup B$.*

**Proof.** By Proposition 3 and its Corollary 3, we only have to verify that the module actions between $A$ and $B$ define a matched pair of adjoint groups, that is, $(x \circ y)^a = (x^{y\,a}) \circ (y^a)$ and ${}^x(a \circ b) = ({}^x a) \circ ({}^{x^a} b)$ for all $a, b \in A$ and $x, y \in B$. With $({}^x a)' = (a')^{x'}$, the second condition turns into $(a \circ b)^x = (a^{\,{}^b x}) \circ (b^x)$. Thus, by symmetry, it is enough to verify the first equation, which can be rewritten as $a' \cdot (x \circ y) = \big((a')^{y'} \cdot x\big) \circ (a' \cdot y)$. Since $a' \cdot (x \circ y) = a' \cdot (x^y + y) = a' \cdot x^y + a' \cdot y$ and $\big((a')^{y'} \cdot x\big) \circ (a' \cdot y) = ((y \cdot a') \cdot x)^{a' \cdot y} + a' \cdot y$, the equation reduces to $a' \cdot x^y = ((y \cdot a') \cdot x)^{a' \cdot y}$, that is, $(a' \cdot y) \cdot (a' \cdot x^y) = (y \cdot a') \cdot x = (y \cdot a') \cdot (y \cdot x^y)$. This is equivalent to Eq. (14). □

By [38], Proposition 10, almost every cocyclic brace is *cyclic* [33], which means that it has a cyclic additive group. The only exceptions are braces with a special direct factor of order 4, which may be called the *exceptional* cocyclic brace. Its adjoint group is cyclic, while its additive group is a Klein Four group. On the other hand, there is a hierarchy of *exceptional* cyclic braces [33], including those which are not cocyclic. Here we restrict ourselves to bi-crossed products of braces which are *bicyclic* [33], that is, cocyclic and cyclic.

Let $A$ and $B$ be bicyclic braces. We identify their additive groups with $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$, respectively, where $n, m \in \mathbb{N}$. Thus $n = |A|$ if $A$ is finite, and $n = 0$ otherwise. Similarly for $B$. We call $o(A) := n$ the *order* of $A$. For simplicity, we represent the elements of $A$ and $B$ by integers (instead of residue classes). For example, $A = \{0, 1, \dots, n-1\}$ if $A$ is finite. To distinguish $A$ from $B$, we write $1_A$ and $1_B$, respectively, for the generator 1 of the additive group.

By [33], Theorem 1, $A, B$ are determined, up to isomorphism, by their socle order $d = o(\mathrm{Soc(A)})$ and $e = o(\mathrm{Soc(B)})$. We set

$$q := d + 1, \qquad t := e + 1,$$

and choose the generators $1_A$ and $1_B$ so that the affine structures of $A$ and $B$ are the canonical ones:

$$q = 1'_A \cdot 1_A, \qquad t = 1'_B \cdot 1_B.$$

Recall that the possible socle orders for a given order $n$ are the divisors $d$ of $n$ such that each prime divisor of $n$ also divides $d$, and $4|n$ implies that $4|d$ (see [33], Proposition 6). Hence $q$ is relatively prime to $n$, and $t$ is relatively prime to $m$. Moreover, $A$ must be trivial if $A$ is infinite. Let us write $A^\times$ for the group of invertible elements in the ring $A = \mathbb{Z}/n\mathbb{Z}$ and $o(a)$ for the order of an element $a \in A^\times$ in this group. The group $B^\times$ and the order $o(x)$ for $x \in B^\times$ are defined similarly. Then

$$q \in A^\times, \qquad t \in B^\times.$$

As before, we denote elements of $A$ by $a, b, c, \dots$ and elements of $B$ by $x, y, z \dots$. Using the ring structures of $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$, the affine structures of $A$ and $B$ are given by

$$b^a = b(1 + ad), \qquad y^x = y(1 + ex). \tag{29}$$

For $a = 1_A \circ \cdots \circ 1_A$ ($k$ factors), this implies that $b^a = bq^k$. Therefore, the action of $1_A$ on $(A; +)$ splits $A$ into cycles of equal length $o(q)$. Hence

$$o(q)|o(A), \qquad o(t)|o(B). \tag{30}$$

By Proposition 6, a bi-crossed product $A \bowtie B$ is determined by the metacommutation actions, hence by the two elements

$$u := 1'_B \cdot 1_A, \qquad v := 1'_A \cdot 1_B. \tag{31}$$

For $a \in A$ and $x \in B$, this implies that

$$a^{1_B} = ua, \qquad x^{1_A} = vx. \tag{32}$$

Hence $u \in A^\times$ and $v \in B^\times$, and

$$o(u)|o(B), \qquad o(v)|o(A). \tag{33}$$

Since $A$ is bicyclic, the adjoint group of $A$ is given by the quantum integers

$$[a]_q := 1 + q + q^2 + \cdots + q^{a-1} = \underbrace{1_A \circ \cdots \circ 1_A}_{a}.$$

Therefore, Eqs. (32) imply that the metacommutation actions have to be

$$[a]_q \cdot x = v^{-a}x, \qquad [x]_t \cdot a = u^{-x}a. \tag{34}$$

**Caution.** Throughout the rest of this section, exponents of the elements $q, u \in A^\times$ or $t, v \in B^\times$ will always be regarded as integers. For example, $q^a$ should never be confused with $a' \cdot q$.

**Theorem 2.** *Let $A, B$ be bicyclic braces with $q := o(\mathrm{Soc}(A)) + 1$ and $t := o(\mathrm{Soc}(B)) + 1$. Eqs. (31) with $u \in A^\times$ and $v \in B^\times$ determine a bi-crossed product $A \bowtie B$ of braces if and only if (33) holds, such that for all $a \in A$ and $x \in B$ there exist $b \in A$ and $y \in B$ with*

$$u^{-x}[a]_q = [b]_q \qquad v^{-a}[x]_t = [y]_t \tag{35}$$

$$q^{-a}(u^x - 1) = u^y - 1 \qquad t^{-x}(v^a - 1) = v^b - 1. \tag{36}$$

**Proof.** The conditions (33) state that (31) makes $A$ into a $B$-module and $B$ into an $A$-module. Thus, by Proposition 6, we only have to deal with the compatibility condition (14), which can be written in the form

$$([a]_q \cdot [x]_t) \cdot ([a]_q \cdot 1) = ([x]_t \cdot [a]_q) \cdot ([x]_t \cdot 1), \tag{37}$$

where $a \in A$ and $x \in B$, and $1 \in \{1_A, 1_B\}$. By Eqs. (34), we have $[a]_q \cdot [x]_t = v^{-a}[x]_t$ and $[x]_t \cdot [a]_q = u^{-x}[a]_q$. So there are unique $b \in A$ with $u^{-x}[a]_q = [b]_q$ and $y \in B$ with $v^{-a}[x]_t = [y]_t$. This gives Eqs. (35).

Case 1: $1 = 1_A$. Then Eqs. (29) and (34) give $[a]_q \cdot 1 = (1_A \circ \cdots \circ 1_A) \cdot 1_A = q^{-a}$ and $[x]_t \cdot 1 = u^{-x}$. So we obtain $([a]_q \cdot [x]_t) \cdot ([a]_q \cdot 1) = [y]_t \cdot q^{-a} = u^{-y}q^{-a}$, and by Eqs. (29), $([x]_t \cdot [a]_q) \cdot ([x]_t \cdot 1) = u^{-x}[a]_q \cdot u^{-x} = u^{-x}(1 + u^{-x}[a]_q(q-1))^{-1}$. Thus Eq. (37) with $1 = 1_A$ becomes $u^{-y}q^{-a} = u^{-x}(1 + u^{-x}[a]_q(q-1))^{-1}$, that is, $u^{-y}q^{-a}(1 + u^{-x}[a]_q(q-1)) = u^{-x}$. Multiplying by $u^y u^x$, this equation becomes $q^{-a}(u^x + [a]_q(q-1)) = u^y$, where the left-hand side is equal to $q^{-a}(u^x + q^a - 1_A) = q^{-a}(u^x - 1) + 1$. So the equation is equivalent to the first equation of (36).

Case 2: $1 = 1_B$. Then $[a]_q \cdot 1 = v^{-a}$ and $[x]_t \cdot 1 = t^{-x}$. So Eq. (37) becomes $v^{-a}[x]_t \cdot v^{-a} = [b]_q \cdot t^{-x}$, that is, $v^{-a}(1 + v^{-a}(t^x - 1))^{-1} = v^{-b}t^{-x}$. In analogy to case 1, this gives the second equation of (36). □

**Remark.** Eqs. (36) could be equivalently stated as follows:

$$u^{x-y} = q^{a-b}, \qquad v^{a-b} = t^{x-y}. \tag{38}$$

To see this, use Eqs. (35) to obtain $([x]_t \cdot [a]_q) \cdot ([x]_t \cdot 1_A) = [b]_q \cdot u^{-x} = u^{-x}q^{-b}$. Thus Eq. (37) with $1 = 1_A$ becomes $u^{-y}q^{-a} = u^{-x}q^{-b}$, which gives the first equation of (38). The second one is obtained analogously. Our preference of Eqs. (36) will be seen from the next result.

**Corollary 1.** *Let $A$ and $B$ be bicyclic braces. If $q := o(\mathrm{Soc}(A)) + 1$ is relatively prime to $o(B)$ and $t := o(\mathrm{Soc}(B)) + 1$ relatively prime to $o(A)$, then Eqs. (31) with $u := t$ and $v := q$ determine a bi-crossed product $A \bowtie B$ of braces.*

**Proof.** By assumption, $u \in A^\times$ and $v \in B^\times$, and (33) follows by Eq. (30). Multiplying the first equation of (35) by $q - 1$, it turns into the second equation of (36). Similarly, the first equation of (36) follows by the second equation of (35). □

There are many examples of bicyclic braces which can be amalgamated in this way. For example, any pair of bicyclic braces with if $|A| = p^k$ and $|B| = p^\ell$ for some prime $p$ determines a bi-crossed product $A \bowtie B$. In particular, the corollary provides a special class of decomposable groups $A^\circ \bowtie B^\circ$ which should be investigated.

**Corollary 2.** *Let $A$ be the infinite bicyclic brace, and let $B$ be any bicyclic brace. With the notations of Theorem 2, there exists a brace $A \bowtie B$ if and only if $t, v \in B^\times$ and one of the following holds:*

(a) *$u = 1$, and the equation $(t-1)(v-1) = 0$ holds in $B$.*
(b) *$u = -1$ and $2|o(B)$, and $(v^2-1)(v-1) = (t+v)(v-1) = 0$ holds in $B$.*

**Proof.** Since $o(A) = 0$, we have $q = 1$ and $u^2 = 1$. Assume first that $u = 1$. Then (33) is satisfied for all $v \in B^\times$. For any $x \in B$, the first equation in (35) yields $b = a$. So the second equation of (36) is equivalent to $(t-1)(v-1) = 0$. Moreover, the remaining equations of (35)-(36) hold for a suitable $y \in B$.

Now assume that $u = -1$. Then (33) states that $o(B)$ is even. Hence $t$ and $v$ are odd. So the parity of $[x]_t$ is equal to the parity of $x$. Therefore, the second equation in (35) and the first equation in (36) are satisfied. For $x = -1_B$, we have $b = -a$. So the remaining equation yields $t(v-1) = v^{-1} - 1 = -v^{-1}(v-1)$ and $t(v^2-1) = v^{-2} - 1 = -v^{-2}(v^2-1)$, that is, $(t + v^{-1})(v-1) = (t + v^{-2})(v^2-1) = 0$. So the second equation can be replaced by $(v^{-1} - v^{-2})(v^2-1) = 0$ or $(v^2-1)(v-1) = 0$. Thus, $(v - v^{-1})(v-1) = 0$, which shows that $(t + v^{-1})(v-1) = 0$ can be repaced by $(t+v)(v-1) = 0$.

Conversely, assume that $t(v-1) = v^{-1}-1$ and $t(v^2-1) = v^{-2}-1$. Then $(v^2-1)(v-1) = 0$, which yields $(v^2-1)(v^{-a}-1) = 0$. To verify that $t(v^a-1) = v^{-a}-1$ holds for all $a$, we proceed by induction. Assume that $t(v^a-1) = v^{-a}-1$. Then $t(v^{a+1}-1) = t(v^a-1)v + t(v-1) = (v^{-a}-1)v + v^{-1} - 1 = v^{-a-1} - 1 + v^{-1}(v^{-a}-1)(v^2-1) = v^{-a-1} - 1$. Thus $t(v^a-1) = v^{-a}-1$ holds for all $a$. In particular, $t(v^{-a}-1) = v^a - 1$, which yields $t^2(v^a-1) = v^a - 1$. So the right-hand equation of (36) holds for all $a \in A$ and $x \in B$. □

**Example 6.** Theorem 2 can also be used for the construction of solvable groups. For instance, let $A = B$ be the trivial cyclic brace of order 4. Thus, with the above notation, $q = t = 1$. Then $u = v = -1$ satisfy Eqs. (33) and (35)-(36). So there is a brace $A \bowtie B$ with additive group $C_4 \times C_4$. The adjoint group $G = A^\circ \bowtie B^\circ$ is that of Example 4.

Indeed, the tables in Example 4 give the metacommutation rules $a^x = (-1)^x a$ and $x^a = (-1)^a x$, in accordance with Eqs. (34).

**Example 7.** Rédei [30] and Cohn [10] classified the bi-crossed products of cyclic groups where one of the group is infinite. Some of these groups cannot arise from bi-crossed products of braces. For example, let $C_0 \bowtie C_6$ be a bi-crossed product, and assume that $A, B$ are braces with $A^\circ = C_0$ and $B^\circ = C_6$. Then $A$ and $B$ must be trivial. It is easily verified that the metacommutation actions

$$ {}^x a = (-1)^x a, \qquad x^a = x + 2ai(x) \tag{39}$$

define a bi-crossed product $A^\circ \bowtie B^\circ$, where $i(x) := 0$ for even $x$ and $i(x) := 1$ otherwise. However, $v = 1'_A \cdot 1_B = 3 \notin B^\times$, which shows that Eqs. (39) don't give a matched pair of braces.

**Example 8.** The smallest bi-crossed product $A \bowtie B$ of non-trivial braces $A, B$ obtained by Corollary 1 of Theorem 2 for which $A^\circ \bowtie B^\circ$ is not a semidirect product and $A \ncong B$ occurs for $|A| = 16$ and $|B| = 8$, both with socle order 4. Thus $q = u = 5 \in A$ and $t = v = 5 \in B$, and $|A \bowtie B| = 128$. If we renumber the elements of $A^\circ$ so that $i \in \{0, 1, \dots, 15\}$ stands for $1_A \circ \cdots \circ 1_A$ ($i$ factors), and similarly for $B^\circ = \{0, 1, 2, 3, 4, 5, 6, 7\}$, the right actions (32) are given by the permutations $\sigma = (1, 13, 9, 5)(2, 10)(3, 7, 11, 15)(6, 14)$ on $A^\circ$ and $\tau = (1, 5)(3, 7)$ on $B^\circ$, which determines the adjoint group $G := A^\circ \bowtie B^\circ$. Thus $a \circ 1_B = y \circ \sigma(a)$ and $x \circ 1_A = b \circ \tau(x)$ for given $a \in A^\circ$ and $x \in B^\circ$, with $y \in B$ and $b \in A$. So $a^x = \sigma^x(a)$ and $x^a = \tau^a(x)$. The general commutation rule for $G$ is as follows:

$$ a \circ x = \big(-\tau^{-a}(-x)\big) \circ \sigma^x(a) = \begin{cases} x \circ \sigma^x(a) & \text{for } x \text{ or } a \text{ even} \\ (x+4) \circ \sigma^x(a) & \text{for } x \text{ and } a \text{ odd.} \end{cases} $$

Let $N_A$ (resp. $N_B$) be the greatest subgroup of $A^\circ$ (resp. $B^\circ$) which is normal in $G$. Then $N_A \circ N_B$ is called the *nucleus* [11,14] of $G$. Here we have $N_A = \langle 2 \rangle$ and $N_B = \langle 4 \rangle$. Thus $G/N_A N_B \cong C_2 \times C_4$. We shall see below that the nucleus is always a brace ideal.

**Proposition 7.** *Let $A$ be a bicyclic brace. Every subgroup of $A^\circ$ is an ideal of $A$.*

**Proof.** If $A$ is infinite, $A$ is a trivial brace ([38], Proposition 10). Thus let $A$ be finite. For each divisor $n > 0$ of $o(A)$, there is a unique subgroup $nA$ of the additive group of $A$, and $n$ is the index of this subgroup. Moreover, $nA$ is a right ideal of $A$, hence an ideal since $A^\circ$ is abelian. In particular, $nA$ is a subgroup of $A^\circ$. Since $A^\circ$ is cyclic, there are no other subgroups of $A^\circ$. □

**Theorem 3.** *Let $A \bowtie B$ be a bi-crossed product of bicyclic braces $A, B$, and let $N_B$ be the greatest subgroup of $B^\circ$ which is normal in $(A \bowtie B)^\circ$. Then*

$$N_B = \{x \in B \mid \forall\, a \in A\colon a \circ x \circ a' \in B\} = \{x \in B \mid \forall\, a \in A\colon a^x = a\}. \tag{40}$$

*Moreover, $N_B$ is a brace ideal of $A \bowtie B$.*

**Proof.** For $a \in A$ and $x \in B$, we have $a \circ x = {}^a x \circ a^x$. Hence $a \circ x \circ a' \in B$ if and only if $a^x = a$. Thus $N_B \subset I_B = J_B$ holds for $I_B := \{x \in B^\circ \mid \forall\, a \in A\colon a \circ x \circ a' \in B\}$ and $J_B := \{x \in B \mid \forall\, a \in A\colon a^x = a\}$. Since $I_B$ is a normal subgroup of $G := (A \bowtie B)^\circ$, this proves Eqs. (40).

By Proposition 7, $N_B$ is a brace ideal of $B$. Thus, to verify that $N_B$ is a brace ideal of $A \bowtie B$, we only have to show that $N_B$ is a right ideal. Now let $a, b \in A$ and $x \in N_B$ be given. Then Proposition 3 and its Corollary 1 imply that $(a \cdot x) \cdot (a \cdot b) = (x \cdot a) \cdot (x \cdot b) = a^{x'} \cdot b^{x'} = a \cdot b$. Hence $a \cdot x \in N_B$, and thus $N_B$ is a right ideal of $A \bowtie B$. □

**Corollary.** *Let $A \bowtie B$ be a bi-crossed product of bicyclic braces $A, B$. Then the nucleus $N_A \circ N_B$ of $A^\circ \bowtie B^\circ$ is a brace ideal of $A \bowtie B$.*

**Proof.** By Theorem 3, $N_B$ is a brace ideal of $A \bowtie B$, and by symmetry, the same is true for $N_A$. Hence $N_A \circ N_B = N_A + N_B$ is a brace ideal of $A \bowtie B$. □

**Remark.** The corollary shows that the type reduction of Douglas [11] for bi-crossed products of cyclic groups carries over to braces. Note that the inversion of this reduction process for groups is not yet fully understood. On a combinatorial level, Douglas [11] characterized the "special" permutations $\sigma$ (cf. Example 8) arising as right metacommutation actions for a matched pair of cyclic groups, and introduced a *derived* special permutation $\sigma'$ which always combines with $\sigma$ as a left counterpart to a bi-crossed product. He proved that some $n$-th derivative is trivial, which led him to define the *type* to be the minimal length $n$ of such a reduction. Gorenstein and Herstein [14] proved that all finite types actually occur.

Several further directions suggest themselves.

**Problems. 1.** Extend Theorem 2 to exceptional cyclic braces [33].

**2**. What are the shifted bi-crossed products of (bi-)cyclic braces?

**3**. Determine the adjoint groups of bi-crossed products of (bi-)cyclic braces.

We conclude with a property of cyclic braces of odd order which is useful for calculating the adjoint group in terms of the additive group.

**Proposition 8.** *Let $A$ be a cyclic brace of odd order $n$ with additive group $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$ and $q := 1^1 = |\mathrm{Soc}(A)| + 1$. Then $s := |A/\mathrm{Soc}(A)|$ satisfies $[s]_q = s$.*

**Proof.** By assumption, $d := |\mathrm{Soc}(A)| = q - 1$ and $n = ds$. So we have to show that $n$ divides $[s]_q - s = \frac{(d+1)^s - 1}{d} - s$, that is, $nd \mid (d+1)^s - 1 - n$. Since $(d+1)^s = 1 + sd + \sum_{i=2}^{s} \binom{s}{i} d^i$, this is equivalent to $nd \mid \sum_{i=2}^{s} \binom{s}{i} d^i$. So it is enough to verify

$$n \big| \tbinom{s}{i} d^{i-1}$$

for $2 \leqslant i \leqslant s$. For a prime $p$ and $m \in \mathbb{Z}$, let $v_p(a)$ be the greatest $k \in \mathbb{N}$ with $p^k | m$. Then we have to verify

$$v_p(n) \leqslant v_p\big(\tbinom{s}{i} d^{i-1}\big)$$

for odd primes $p$ and $2 \leqslant i \leqslant s$. If $p \nmid s$, this is obvious. So let us assume that $p|s$.

Case 1: $p \nmid i$. Then $v_p(i!) = v_p((i-1)!) \leqslant v_p\big((s-1)\dots(s-i+1)\big)$. Hence $v_p\big(\binom{s}{i} d^{i-1}\big) \geqslant v_p(sd^{i-1}) \geqslant v_p(sd) = v_p(n)$.

Case 2: $p|i$. Since $v_p\big(\binom{s}{i}\big) = v_p\big(\binom{s/p}{i/p}\big)$, we proceed by induction. If $i = p$, then $v_p\big(\binom{s}{i} d^{i-1}\big) = v_p(\frac{s}{p} d^{i-1}) \geqslant v_p(sd) = v_p(n)$. Otherwise, $j := \frac{i}{p} \geqslant 2$, and the inductive hypothesis gives $v_p\big(\binom{s}{i} d^{i-1}\big) = v_p\big(\binom{s/p}{i/p} d^{j-1}\big) + v_p\big(d^{i-j}\big) \geqslant v_p(\frac{n}{p}) + 2v_p(d) \geqslant v_p(n) + v_p(d) = v_p(n)$. □

**Remark.** Proposition 8 does not hold for even $n$. For example, the bicyclic brace of order 16 and socle order 4 (see [33], Section 4) satisfies $[4]_5 = 12 \neq 4$.

**Corollary.** *Let $A$ be a cyclic brace of odd order $n$ with additive group $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$ and $q := 1^1 = |\mathrm{Soc}(A)| + 1$. For $s := |A/\mathrm{Soc}(A)|$ and $a \in A$,*

$$[a+s]_q = [a]_q + s. \tag{41}$$

**Proof.** Since $s = [s]_q \in \mathrm{Soc}(A)$, we have $[a+s]_q = [a]_q \circ s = ([a]_q)^s + s = [a]_q + s$. □

**Example 9.** Let $A$ be the cyclic brace of order $n = 81$ with socle order $d = 3$. As in Proposition 8, we identify the additive group with $\mathbb{Z}/n\mathbb{Z}$ and choose $q := 1^1 = d+1 = 4$. Then $s := |A/\mathrm{Soc}(A)| = 27$. To obtain $[a]_q$ for $a \in \{1, \dots, 81\}$, formula (41) shows that it suffices to calculate $[a]_q$ for $a \in \{1, \dots, 26\}$:

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $q^a$ | 4 | 16 | 64 | 13 | 52 | 46 | 22 | 7 | 28 | 31 | 43 | 10 | 40 | 79 | 73 | 49 | 34 | 55 | 58 | 70 | 37 | 67 | 25 | 19 | 76 | 61 | 1 |
| $[a]_q$ | 1 | 5 | 21 | 4 | 17 | 69 | 34 | 56 | 63 | 10 | 41 | 3 | 13 | 53 | 51 | 43 | 11 | 45 | 19 | 77 | 66 | 22 | 8 | 33 | 52 | 47 | 27 |
| mod 27 | 1 | 5 | 21 | 4 | 17 | 15 | 7 | 2 | 9 | 10 | 14 | 3 | 13 | 26 | 24 | 16 | 11 | 18 | 19 | 23 | 12 | 22 | 8 | 6 | 25 | 20 | 0 |

With the powers $q^a$ the $[a]_q$ are obtained recursively since $[a+1]_q = q^a + [a]_q$. The reduction of $[a]_q$ modulo 27, given in the last line of the table, determines the adjoint group of the cyclic brace of order 27 with the same socle order 3. Since $[a]_q = \frac{q^a - 1}{q-1}$, we have

$$q^a = d[a]_q + 1. \tag{42}$$

In this formula, the factor $d$ implies that $[a]_q$ enters only modulo 27. Thus, if the brace of order 27 is given, Eq. (42) can be used to obtain the powers $q^a$ in the above table,

which yields the brace of order 81 by virtue of Eq. (41). In this way, the bicyclic braces can be obtained with a minimum amount of calculation.

## References


[1] D. Bachiller, Counterexample to a conjecture about braces, J. Algebra 453 (2016) 160–176.
[2] D. Bachiller, Extensions, matched products, and simple braces, J. Pure Appl. Algebra 222 (7) (2018) 1670–1691.
[3] D. Bachiller, F. Cedó, E. Jespers, J. Okniński, Iterated matched products of finite braces and simplicity: new solutions of the Yang-Baxter equation, Trans. Am. Math. Soc. 370 (7) (2018) 4881–4907.
[4] D. Bachiller, F. Cedó, E. Jespers, J. Okniński, Asymmetric product of left braces and simplicity: new solutions of the Yang–Baxter equation, Commun. Contemp. Math. 21 (2019) 1850042.
[5] F. Catino, I. Colazzo, P. Stefanelli, Regular subgroups of the affine group and asymmetric product of radical braces, J. Algebra 455 (2016) 164–182.
[6] F. Cedó, E. Jespers, J. Okniński, Retractability of set theoretic solutions of the Yang-Baxter equation, Adv. Math. 224 (6) (2010) 2472–2484.
[7] F. Cedó, E. Jespers, del Río, Involutive Yang-Baxter groups, Trans. Am. Math. Soc. 362 (5) (2010) 2541–2558.
[8] F. Cedó, E. Jespers, J. Okniński, Braces and the Yang-Baxter equation, Commun. Math. Phys. 327 (1) (2014) 101–116.
[9] F. Cedó, E. Jespers, J. Okniński, An abundance of simple left braces with Abelian multiplicative Sylow subgroups, Rev. Mat. Iberoam., https://doi.org/10.4171/rmi/1168.
[10] P.M. Cohn, A remark on the general product of two infinite cyclic groups, Arch. Math. 7 (1956) 94–99.
[11] J. Douglas, On finite groups with two independent generators, I-IV, Proc. Natl. Acad. Sci. USA 37 (1951) 604–610, 677–691, 749–760, 808–813.
[12] V.G. Drinfeld, On some unsolved problems in quantum group theory, in: Quantum Groups, Leningrad, 1990, in: Lecture Notes in Math., vol. 1510, Springer-Verlag, Berlin, 1992, pp. 1–8.
[13] P. Etingof, T. Schedler, A. Soloviev, Set-theoretical solutions to the quantum Yang-Baxter equation, Duke Math. J. 100 (1999) 169–209.
[14] D. Gorenstein, I.N. Herstein, On the structure of certain factorizable groups, I, Proc. Am. Math. Soc. 10 (1959) 940–945.
[15] D. Gorenstein, I.N. Herstein, On the structure of certain factorizable groups, II, Proc. Am. Math. Soc. 11 (1960) 214–219.
[16] L. Guarnieri, L. Vendramin, Skew braces and the Yang-Baxter equation, Math. Comput. 86 (2017) 2519–2534.
[17] P. Hall, On the Sylow systems of a soluble group, Proc. Lond. Math. Soc. 43 (1937) 316–323.
[18] P. Hall, A characteristic property of soluble groups, J. Lond. Math. Soc. 12 (1937) 188–200.
[19] P. Hegedüs, Regular subgroups of the affine group, J. Algebra 225 (2) (2000) 740–742.
[20] B. Huppert, Über das Produkt von paarweise vertauschbaren zyklischen Gruppen, Math. Z. 58 (1953) 243–264.
[21] B. Huppert, Über die Auflösbarkeit faktorisierbarer Gruppen, Math. Z. 59 (1953) 1–7.
[22] N. Itô, Über das Produkt von zwei abelschen Gruppen, Math. Z. 62 (1955) 400–401.
[23] N. Jacobson, Structure of rings, Colloq. Publ. – Am. Math. Soc. 37 (1974).
[24] E. Jespers, Ł. Kubat, A. Van Antwerpen, L. Vendramin, Factorizations of skew braces, Math. Ann. 375 (2019) 1649–1663.
[25] C. Kassel, Quantum Groups, Graduate Texts in Mathematics, vol. 155, Springer-Verlag, New York, 1995.
[26] J.-H. Lu, M. Yan, Y.-C. Zhu, On the set-theoretical Yang-Baxter equation, Duke Math. J. 104 (2000) 1–18.
[27] G.A. Miller, Groups which are the products of two permutable proper subgroups, Proc. Natl. Acad. Sci. 21 (1935) 469–472.
[28] G.A. Miller, Regular subgroups of a transitive substitution group, Proc. Natl. Acad. Sci. 22 (1936) 375–377.
[29] B.H. Neumann, Decomposition of groups, J. Lond. Math. Soc. 10 (1935) 3–6.
[30] L. Rédei, Zur Theorie der faktorisierbaren Gruppen, I, Acta Math. Acad. Sci. Hung. 1 (1950) 74–98.

[31] W. Rump, A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation, Adv. Math. 193 (2005) 40–55.
[32] W. Rump, Braces, radical rings, and the quantum Yang-Baxter equation, J. Algebra 307 (2007) 153–170.
[33] W. Rump, Classification of cyclic braces, J. Pure Appl. Algebra 209 (3) (2007) 671–685.
[34] W. Rump, Semidirect products in algebraic logic and solutions of the quantum Yang-Baxter equation, J. Algebra Appl. 7 (4) (2008) 471–490.
[35] W. Rump, The brace of a classical group, Note Mat. 34 (1) (2014) 115–144.
[36] W. Rump, A covering theory for non-involutive set-theoretic solutions to the Yang-Baxter equation, J. Algebra 520 (2019) 136–170.
[37] W. Rump, Construction of finite braces, Ann. Comb. 23 (2019) 391–416.
[38] W. Rump, Classification of cyclic braces, II, Trans. Am. Math. Soc. 372 (1) (2019) 305–328.
[39] Y.P. Sysak, Products of groups and local nearrings, Note Mat. 28 (suppl. 2) (2008) 177–211.
[40] J. Szép, Über die als Produkt zweier Untergruppen darstellbaren endlichen Gruppen, Comment. Math. Helv. 22 (1949) 31–33.
[41] J. Szép, On the structure of groups which can be represented as the product of two subgroups, Acta Sci. Math. Szeged 12 (1950) 57–61.
[42] H. Wielandt, Über das Produkt paarweise vertauschbarer nilpotenter Gruppen, Math. Z. 55 (1951) 1–7.
[43] G. Zappa, Sulla costruzione dei gruppi prodotto di due dati sottogruppi permutabili traloro, in: Atti Secondo Congresso Un. Mat. Ital., Bologna, Edizioni Cremonense, Rome, 1942.