TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 372, Number 1, 1 July 2019, Pages 305–328
https://doi.org/10.1090/tran/7569
Article electronically published on September 24, 2018

CLASSIFICATION OF CYCLIC BRACES, II

WOLFGANG RUMP

Dedicated to B. V. M.

Abstract. Groups G with a bijective 1-cocycle onto a right G-module A are said to be *braces*. If the *additive group* A is finite, the *adjoint group* G of the brace is solvable. Most of the known solvable groups can be made into braces. Etingof *et al.* [Duke Math. J. 100 (1999), pp. 169–209] raised the question to classify *T-structures*, which are equivalent to *cyclic* braces. This problem is solved in the paper. The adjoint groups of finite cyclic braces are characterized as solvable, 2-nilpotent, and almost Sylow-cyclic groups. For these groups, the possible brace structures are classified.

Introduction

The concept of *brace* [24] arose in connection with nondegenerate unitary set-theoretic solutions to the Yang-Baxter equation [12, 18, 22]. A brace can be conceived as a group G with an *affine structure*, that is, a bijective 1-cocycle onto a right G-module A. Radical rings are braces where the group G is equipped with Jacobson's circle operation. So the group G of a brace A is called the *adjoint group* A° of A. Braces also arise [27] in connection with flat manifolds [1–3, 19] and Chevalley groups. Adjoint groups of finite braces, also called *involutive Yang-Baxter groups* or briefly, *IYB-groups*, have to be solvable. The converse was open for a while, but recently, certain p-groups related to Lie algebras of nilpotency class 9 were shown to be not of IYB-type. Bachiller's counterexample [5] can be regarded as a finite version of an $\mathbb{R}$-linear brace related to Benoist's nonaffine nilvariety [7] which disproves Milnor's conjecture [19] (see [27], Section 3, for details).

In this paper, we complete the classification of braces with the cyclic additive group. These so-called *cyclic* braces [25] are equivalent to the T-structures of Etingof *et al.* [12]. So our classification also settles the problem [12] to classify T-structures. In [25] the cyclic braces of order p^n for a prime p are classified. If $p = 2$, the corresponding IYB-groups admit a cyclic subgroup of index 2, while for odd primes p, the adjoint group is cyclic. These *bicyclic* braces can be regarded as quantized cyclic groups modulo a quantum integer $[n]_q = 1 + q + \cdots + q^{n-1}$ (see Section 1). The additive group of a cyclic brace A is of the form

$$B_1 \oplus \cdots \oplus B_r$$

with right ideals B_i of A such that the adjoint groups $P_i := B_i^\circ$ are Sylow subgroups of $G := A^\circ$. As the B_i are classified in [25], we have to analyze how an affine structure of G can be constructed from suitable affine structures of a Sylow basis.

Received by the editors August 12, 2017, and, in revised form, February 22, 2018.
2010 *Mathematics Subject Classification.* Primary 81R50, 20F16.
Key words and phrases. Solvable group, brace, affine structure, almost Sylow-cyclic, T-structure.

A delicate point is that isomorphic affine structures of a Sylow subgroup often lead to nonisomorphic affine structures of the whole group G.

We show first that an affine structure of G is uniquely determined by the induced affine structures of a fixed collection of Sylow subgroups (Corollary of Proposition 2). For a cyclic brace A, the adjoint group $G := A^\circ$ is *almost Sylow-cyclic* (Theorem 1), which means that the Sylow subgroups of odd order are cyclic, while a Sylow 2-subgroup $P \neq 1$ admits a cyclic subgroup of index 2. Almost Sylow-cyclic groups arise as fixed-point-free automorphism groups of finite groups ([21], 10.5.5), hence in connection with near-fields [32] and projective planes which they coordinize. They also arise as automorphism groups of regular maps on surfaces [10]. In general, almost Sylow-cyclic groups need not be solvable (see [29, 31]).

Not surprisingly, the Sylow 2-subgroup P plays a particular part. If G is the adjoint group of a cyclic brace A, we show that P has a normal complement (Proposition 13). It follows that G admits an ordered Sylow tower

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_r = 1$$

with characteristic subgroups G_i and $P_i G_i = G_{i-1}$, where $P_1, \dots, P_r$ are Sylow p_i-subgroups with $p_1 < \cdots < p_r$. We distinguish two types of primes p_i, those which are *free* in the sense that P_i is cyclic with $P_i \cap G' = 1$, where G' denotes the commutator subgroup of G, and *nonfree* primes p_i. For the nonfree odd primes p_i, the brace B_i with adjoint group P_i is unique, up to isomorphism (Proposition 5). Except for the notorious prime 2, there is no such restriction for the free primes. Any G_i of the Sylow tower is the adjoint group of a brace ideal A_i of A, and the action $P_i \to \mathrm{Aut}(A_i)$ by conjugation has its image in the subgroup of brace automorphisms (Proposition 4). Therefore, any cyclic brace is an iterated semidirect product $B_1 \ltimes \cdots \ltimes B_r$ of primary braces.

The qualitative part of our main result implies that a finite group G is the adjoint group of a cyclic brace if and only if G is solvable, 2-nilpotent, and almost Sylow-cyclic. Precisely, we give a necessary and sufficient condition for the existence of a cyclic brace with adjoint group G and prescribed socle orders of its primary components (Theorem 2).

For a complete classification of cyclic braces, the kernels K_i of the actions $P_i \to \mathrm{Aut}(A_i)$ have to be considered. In the above notation, K_i is equal to the centralizer $C_{P_i}(A_i^\circ)$ and also coincides with the *core* $(P_i)_G$ of P_i, the greatest normal subgroup of G which is contained in P_i. For groups G with a cyclic affine structure, the automorphism group of a Sylow tower, which acts on the affine structures of G, and the stabilizers of this action, can be determined (Propositions 6 and 7). Both groups depend on the cores of the Sylow subgroups. For the primary components, an additive and a multiplicative formula for the group of brace automorphisms in terms of the socle will be proved (Propositions 1 and 12). Altogether, this leads to an explicit description of the isomorphism classes of cyclic braces with adjoint group G and prescribed socle order of the primary components (Theorem 3). If the Sylow subgroups of G are cyclic, and the Sylow 2-subgroup is not of order 4, all braces with adjoint group G are cyclic, which yields a simple formula for the number of isomorphism classes of braces with adjoint group G, with or without prescribed socle orders of the primary components (Corollary 1 and Corollary 2).

For the general case, six classes of Sylow 2-subgroups P of G have to be considered. If P is dihedral, generalized quaternion, or semidihedral, there is, up to

isomorphism, a unique brace A with adjoint group P. We show that the automorphism group of P is a *central product*

$$\mathrm{Aut}(P) = \mathrm{Inn}(P) \circ \mathrm{Aut}^\flat(A) \tag{0}$$

of the group $\mathrm{Inn}(P)$ of inner automorphisms of P with the group $\mathrm{Aut}^\flat(A)$ of brace automorphisms of A; that is, $\mathrm{Inn}(P)$ and $\mathrm{Aut}^\flat(A)$ generate $\mathrm{Aut}(P)$ and intersect in the center, a subgroup of order 2 (Proposition 16). In particular, this gives a bijection between the affine structures of P and the elements of the group $\mathrm{Inn}(P)/Z(\mathrm{Aut}(P))$.

Using Eq. (0), we show that dihedral, generalized quaternion, or semidihedral Sylow 2-subgroups do not lead to braces not covered by our formula for the Sylow-cyclic case. There are two other classes of noncyclic groups to which the Sylow 2-subgroup P may belong, namely, the modular 2-group M_{2^m} and its commutator factor group M_{2^m}/M'_{2^m}. We show that the braces arising from M_{2^m} as a Sylow 2-subgroup can be handled in the same way as those arising from M_{2^m}/M'_{2^m} (Proposition 17), so that the classification problem essentially reduces to the latter case (Proposition 15). Our final enumeration of cyclic braces is collected in Theorem 4 and the corollary of Theorem 3. As an application, the cyclic braces of order 80 are classified in accordance with their adjoint groups.

In Section 3, we revisit *cocyclic* braces, that is, braces with a cyclic adjoint group. In contrast to cyclic braces, there is a single infinite cocyclic brace, and every finite cocyclic brace decomposes into its primary components (Proposition 10). Cedó *et al.* [6] have shown that with the exception of a single brace of order 4, all primary cocyclic braces are cyclic. We show that the socle of a cocyclic brace A admits a nice description (Proposition 8) in terms of a residue class modulo A^2 (Proposition 9). This leads to a description of the affine structures in terms of the adjoint group (Proposition 11). In particular, we get a simple proof of the fact that primary cocyclic braces of order $\neq 4$ are cyclic [6].

Section 4 gives an explicit formula for the socle of a cyclic brace in terms of the socles and cores of the primary components (Proposition 14). In a concluding remark of Section 7, we recall the one-to-one correspondence between cyclic braces and *T-structures* in the sense of Etingof *et al.* [12]. This shows that the cyclic braces with adjoint group G are determined by a distinguished bijection $T\colon G \to G$. We leave it to the reader to translate the classification of cyclic braces into the language of T-structures.

1. Cyclic braces

An abelian group $(A;+)$ with a multiplication $(a,b) \mapsto ab$ is said to be a *brace* [24, 25] if A is right distributive; that is,

$$(a+b)c = ac + bc,$$

and the *circle operation*

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

makes A into a group, the *adjoint group* A° of A. The associativity can be rewritten as

$$a(b \circ c) = (ab)c + ab + ac.$$

If R_a denotes the right multiplication $b \mapsto ba$, this is equivalent to the equation

$$R_{b\circ c} = R_b \circ R_c$$

in the endomorphism ring $\mathrm{End}(A)^{\mathrm{op}}$, with the Jacobson circle operation on the right-hand side. Since $0a = 0$, the neutral element of A° must be 0, which implies that $a0 = 0$ also holds in A. The inverse of an element $a \in A^\circ$ will be denoted by a' (Jacobson's original notation [17]; see also [11]). The existence of a' means that the maps $a \mapsto a^b$ with

$$a^b := ab + a$$

are bijective. The defining equations for a brace are then equivalent to

$$(a+b)^c = a^c + b^c,$$
$$(a^b)^c = a^{b\circ c},$$

where $a \circ b = a^b + b$. As usual, we denote the inverse of $b \mapsto b^a$ by $b \mapsto a \cdot b$. Then the equations become

$$a \cdot (b+c) = (a \cdot b) + (a \cdot c), \tag{1}$$

$$(a+b) \cdot c = (a \cdot b) \ \cdot \ (a \cdot c), \tag{2}$$

where Eq. (2) can also be written as

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

By Eqs. (1) and (3), the additive group of A is a left module over the adjoint group A°. Equations (1) and (2) characterize a brace as a *linear cycle set* [22]. Let

$$\mu\colon A \to \mathrm{Aut}(A) \tag{4}$$

be the map with $\mu(a)(b) := a \cdot b$. Then a brace can be viewed as an abelian group A with a map (4) satisfying the cocycle condition

$$\mu(a+b) = \mu\big(\mu(a)(b)\big)\mu(a) \tag{5}$$

for all $a, b \in A$. A map $\mu'\colon A \to \mathrm{Aut}(A)$ defines an isomorphic brace if and only if there is an automorphism $\alpha \in \mathrm{Aut}(A)$ with a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\ \mu'\ } & \mathrm{Aut}(A) \\ \big\downarrow{\scriptstyle \alpha} & & \big\downarrow{\scriptstyle \mathrm{ad}(\alpha)} \\ A & \xrightarrow{\ \mu\ } & \mathrm{Aut}(A) \end{array} \tag{6}$$

where $\mathrm{ad}(\alpha)$ denotes the conjugation $\beta \mapsto \alpha\beta\alpha^{-1}$ in $\mathrm{Aut}(A)$. By an *automorphism* of a brace A we mean an automorphism α of the additive group such that the diagram (6) commutes for $\mu' = \mu$ or, equivalently, that $\alpha(a \cdot b) = \alpha(a) \cdot \alpha(b)$ holds for $a, b \in A$.

An additive subgroup I of A is said to be a *right ideal* if $IA \subset I$; that is, I is invariant under the automorphisms $\mu(a)$ for all $a \in A$, hence a subbrace. If, in addition, $AI \subset I$, then I is called an *ideal*. By [23], Proposition 3, a right ideal of a brace A is an ideal if and only if it is a normal subgroup of A°. For example, the *socle*

$$\mathrm{Soc}(A) := \mathrm{Ker}\ \mu = \{a \in A \mid \mu(a) = 1\}$$

of A is an ideal. Furthermore, Eq. (3) shows that the image of μ is a subgroup of $\mathrm{Aut}(A)$, namely, the adjoint group of the factor brace $A/\mathrm{Soc}(A)$ (see [24] for details). In particular, $\mathrm{Soc}(A) = A$ if and only if the map (4) is trivial. By Eq. (5), this happens if and only if the adjoint group coincides with the additive group.

A brace A with $\operatorname{Soc}(A) = A$ is said to be *trivial*. Thus, any abelian group can be regarded as a trivial brace.

The cardinality of a finite brace is also called its *order*. A brace A is said to be *cyclic* [25] if its additive group is cyclic. Then A can be equipped with a ring structure such that $A \cong \mathbb{Z}/n\mathbb{Z}$, with a unique integer $n \in \mathbb{N}$, the order of A if A is finite. The ring product is closely related to brace multiplication. As there is no risk of confusion, both operations are represented by juxtaposition. The automorphism group $\operatorname{Aut}(A)$ is abelian and can be identified with the unit group $A^\times$. Thus, every automorphism $\alpha \in \operatorname{Aut}(A)$ becomes a multiplication with a fixed unit $e \in A^\times$. Since $A^\times$ is abelian, the diagram (6) reduces to

$$\mu'(a) = \mu(ae). \tag{7}$$

The structure map (4) turns into a map $\mu\colon A \to A^\times$, and Eq. (5) becomes an equation in A as a ring. Note that every right ideal of A is also an ideal with respect to this ring structure. The brace automorphisms of A form a subgroup of $A^\times$. We denote it by

$$A^\flat := \{e \in A^\times \mid a \mapsto ae \text{ brace automorphism}\}.$$

A brace A is said to be *abelian* [25] if its adjoint group is abelian. By [25], Proposition 3, this implies that A (with brace multiplication) is a commutative radical ring. If A is finite, A is a ring-direct product

$$A = \prod_{p \text{ prime}} A_p$$

of *primary* braces $A_p := \{a \in A \mid \exists\, m \in \mathbb{N}\colon p^m a = 0\}$, that is, braces of prime power order. For an arbitrary finite brace A, the primary components A_p are right ideals of A.

The primary cyclic braces are classified in [25]. A cyclic brace A is said to be *bicyclic* if its adjoint group A° is cyclic. If A is finite with $|A| = n$, then A is determined, up to isomorphism, by the socle order $d := |\operatorname{Soc}(A)|$ which has to satisfy

$$p|n \Rightarrow p|d, \qquad 4|n \Rightarrow 4|d$$

for odd primes p. For $q := d + 1 \pmod n$, the quantum integers

$$[k]_q := 1 + q + \cdots + q^{k-1}$$

with $k \in \{1, \dots, n\}$ then give a complete set of residue classes modulo n. The structure map $\mu\colon A \to A^\times$ is given by

$$\mu([k]_q) = q^{-k}.$$

If A is primary and nontrivial, that is, $n = p^k$ with p prime and $d \neq n$, it may happen either that $d = p^{k-1} \neq 1$ or that $A/\operatorname{Soc}(A)$ is not bicyclic. Then A is said to be *exceptional*. For these cyclic braces, the adjoint group is a 2-group (see [25], Section 7).

Proposition 1. *Let A be a cyclic brace. Then*

$$A^\flat = A^\times \cap (1 + \operatorname{Soc}(A)). \tag{8}$$

If A is finite and abelian with $d := |\operatorname{Soc}(A)|$, the adjoint group is given by

$$a \circ b = abd + a + b.$$

Proof. The last statement follows by [25], Theorem 1. By Eq. (7), a unit $e \in A^\times$ gives a brace automorphism if and only if $\mu(ae) = \mu(a)$ holds for all $a \in A$. In particular, $\mu(e) = \mu(1)$. Since μ is a group homomorphism on the adjoint group A° and $\mathrm{Soc}(A)$ is an ideal, the fibers of μ coincide with the residue classes of $\mathrm{Soc}(A)$ in the additive group of A. Hence $\mu(e) = \mu(1)$ is equivalent to $e - 1 \in \mathrm{Soc}(A)$. Conversely, $e - 1 \in \mathrm{Soc}(A)$ yields $a(e-1) \in \mathrm{Soc}(A)$, that is, $\mu(ae) = \mu(a)$, for all $a \in A$. □

Corollary 1. *Let A be a cyclic brace of order $n > 0$. If A has no primary component A_p such that A_p is an ideal of A and trivial as a brace, then $A^\flat = 1 + \mathrm{Soc}(A)$.*

Proof. Suppose that there is a prime p with $\mathrm{Soc}(A)_p = A_p$. Then $a \cdot b = b$ for all $a \in A_p$ and $b \in A$. Hence $b \circ a = (a \cdot b) \circ a = (b \cdot a) \circ b$, and thus $b \circ a \circ b' = b \cdot a \in A_p$. So A_p is an ideal of A which is trivial as a brace, a contradiction. This shows that $\mathrm{Soc}(A)$ is contained in the radical of the ring $A \cong \mathbb{Z}/n\mathbb{Z}$. Thus, each element of $1 + \mathrm{Soc}(A)$ is invertible. □

Note that Eq. (8) depends on the choice of a ring structure on A. To give an invariant reformulation, recall that $\mathrm{Aut}^\flat(A)$ denotes the group of brace automorphisms of A.

Corollary 2. *For any cyclic brace A, there is an exact sequence of groups:*

$$1 \to \mathrm{Aut}^\flat(A) \to \mathrm{Aut}(A) \to \mathrm{Aut}(A/\mathrm{Soc}(A)).$$

If A is finite with no trivial primary components which are ideals, the sequence is short exact.

Proof. The kernel of the homomorphism $\mathrm{Aut}(A) \to \mathrm{Aut}(A/\mathrm{Soc}(A))$ consists of the automorphisms $a \mapsto ae$ with $ae - a \in \mathrm{Soc}(A)$ for all $a \in A$, that is, $e - 1 \in \mathrm{Soc}(A)$. By Proposition 1, this is equivalent to $e \in A^\flat$. Now assume that A is finite with no trivial primary components which are ideals. Since $A/\mathrm{Soc}(A)$ is a cyclic brace, any automorphism of the abelian group $A/\mathrm{Soc}(A)$ is induced by a map $a \mapsto ae$ for some $e \in A$. Hence $Ae + \mathrm{Soc}(A) = A$, which yields $1 = ae + s$ for some $a \in A$ and $s \in \mathrm{Soc}(A)$. Thus $1 - s = ae$. By Corollary 1, $1 - s$ is invertible. Hence $a \mapsto ae$ is surjective. So we obtain $e \in A^\times$, which proves that $\mathrm{Aut}(A) \twoheadrightarrow \mathrm{Aut}(A/\mathrm{Soc}(A))$ is epic. □

Example 1. Corollary 1 does not hold for arbitrary cyclic braces. For example, the symmetric group S_3 is the adjoint group of a cyclic brace A with socle $2A$ (see [24], Example 3). Thus $1 + \mathrm{Soc}(A)$ contains a nonunit.

Example 2. Corollary 2 does not extend to noncyclic braces, even if $\mathrm{Aut}(A)$ is replaced by the subgroup $\mathrm{Aut}_{\mathrm{Soc}(A)}(A)$ of automorphisms in $\mathrm{Aut}(A)$ which leave $\mathrm{Soc}(A)$ invariant. Let F be a field. The two-dimensional F-vector space F^2 can be made into an abelian brace B with

$$\begin{pmatrix} a \\ b \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} x - yb \\ y \end{pmatrix}.$$

The socle $\mathrm{Soc}(B)$ consists of the vectors $\binom{a}{0}$ with $a \in F$. So the kernel of the map $\mathrm{Aut}_{\mathrm{Soc}(B)}(B) \twoheadrightarrow \mathrm{Aut}(B/\mathrm{Soc}(B))$ consists of the matrices $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ with $a \in F^\times$ and $b \in F$. However, the brace automorphisms are given by the unipotent matrices in this kernel.

2. Semidirect products

For the next section, we need some results on semidirect products of braces [26]. More generally, let $A \oplus B$ be a brace with right ideals A and B. If $\sigma(a)$ with $a \in A$ denotes the automorphism $b \mapsto a \cdot b$ of the additive group of B, then σ is a group homomorphism

$$\sigma\colon A^\circ \longrightarrow \mathrm{Aut}(B). \tag{9}$$

Similarly, there is a group homomorphism $\sigma'\colon B^\circ \to \mathrm{Aut}(A)$. The adjoint group $(A \oplus B)^\circ$ is determined by σ and σ'. Indeed, if $a \in A$ and $b \in B$, then $a \circ b = a^b + b$ and $b \circ a = b^a + a$, which determines $(A \oplus B)^\circ$. In practice, the following converse is more important.

Proposition 2. *Let $G = HK$ be a finite group with subgroups H, K of coprime order. For any brace C with adjoint group G, the subgroups H, K are conjugate to the adjoint groups of right ideals A, B, and the brace C is uniquely determined by the braces A, B.*

Proof. With $m := |H|$ and $n := |K|$, the order of the additive group C_{add} of C is mn. So there are subgroups $A, B \subset C_{\mathrm{add}}$ of order m and n, respectively, with $C_{\mathrm{add}} = A \oplus B$. Since A, B are characteristic subgroups of C_{add}, they are right ideals of C.

For $a \in A$ and $b \in B$, we have $b \circ a = b^a + a = (b^a \cdot a) \circ b^a$, and $A \cap B = 0$ implies that the factors $b^a \cdot a \in A$ and $b^a \in B$ are unique. So the action (9) is uniquely determined. By symmetry, this shows that C is uniquely determined by A and B. Now Hall's theorem ([21], 9.1.7) implies that H and K are conjugate to A° and B°, respectively. □

Definition 1. Let G be a group. We define an *affine structure* on G to be a binary operation $\cdot$ such that $a + b := (a \cdot b)a$ makes G into the adjoint group of a brace.

Equivalently, this means that $(G; +, \cdot)$ is a linear cycle set. The equation $a + b := (a \cdot b)a$ then shows that G is the adjoint group of the corresponding brace.

Remark. Note that $\mathrm{Aut}(G)$ acts on the affine structures of G. The orbits are the isomorphism classes of affine structures of G, and the stabilizer of an affine structure is the automorphism group $\mathrm{Aut}^\flat(A)$ of the corresponding brace A.

By induction, we obtain the following corollary of Proposition 2. Recall that by a theorem of Hall [14], a finite group G is solvable if and only if G has a *Sylow basis*, that is, a set of pairwise commuting Sylow subgroups, one for each prime which divides the order of G. Moreover, the Sylow bases of G are pairwise conjugate.

Corollary. *Up to isomorphism, a finite brace A is uniquely determined by its adjoint group A° and the primary components A_p. The primary components are right ideals of A, and their adjoint groups form a Sylow basis of A°.*

The next result contains a useful criterion for Sylow subgroups to be normal.

Proposition 3. *Let $A \oplus B$ be a brace with right ideals A, B and adjoint group G. The action $B^\circ \to \mathrm{Aut}(A)$ is trivial if and only if B° is a normal subgroup of G, and then the image $\sigma(a)$ in (9) coincides with the conjugation $b \mapsto a \circ b \circ a'$.*

Proof. For $a \in A$ and $b \in B$, we have $(a \cdot b) \circ a = b + a = (b \cdot a) \circ b$, which yields $a \cdot b = (b \cdot a) \circ b \circ a'$. If $B^\circ \to \mathrm{Aut}(A)$ is a trivial action, then $a \circ b \circ a' = a \cdot b \in B$, which shows that B° is normal. Conversely, $a \circ b \circ a' \in B$ implies that $(b \cdot a) \circ a' = (b \cdot a) \circ b \circ a' \circ (a \circ b \circ a')' \in A \cap B$, which yields $b \cdot a = a$. □

Remark. Recall [26] that an action (9) is said to be an action of braces if A° is mapped into the group $\mathrm{Aut}^\flat(B)$ of brace automorphisms of B. By [26], Proposition 4, such an action defines a *semidirect product* $A \ltimes B$ of braces.

Now let us assume that B acts trivially on A. For $a, b \in A$ and $x, y \in B$, Eq. (2) gives $(x+a)\cdot(y+b) = (x+a)\cdot y + (x+a)\cdot b = (x\cdot a)\cdot(x\cdot y) + (x\cdot a)\cdot(x\cdot b)$. Hence

$$(a + x) \cdot (b + y) = a \cdot b + a \cdot (x \cdot y). \tag{10}$$

In what follows, we consider semidirect products $A \ltimes N$ and denote elements of A by a, b, c, and elements of N by x, y, z.

Proposition 4. *Let A and N be braces with a group homomorphism $\sigma\colon A^\circ \to \mathrm{Aut}(N)$. Then* (10) *makes $A \oplus N$ into a brace with $a \cdot x := \sigma(a)(x)$ if and only if $\sigma(A^\circ) \subset \mathrm{Aut}^\flat(N)$.*

Proof. To obtain a brace, we have to check Eq. (5), that is,

$$(a + x + b + y) \cdot (c + z) = \big((a + x) \cdot (b + y)\big) \cdot \big((a + x) \cdot (c + z)\big). \tag{11}$$

By Eq. (10), the left-hand side of (11) is $(a + b) \cdot c + (a + b) \cdot \big((x + y) \cdot z\big)$, and the right-hand side of (11) is $\big(a \cdot b + a \cdot (x \cdot y)\big) \cdot \big(a \cdot c + a \cdot (x \cdot z)\big) = (a \cdot b) \cdot (a \cdot c) + (a \cdot b) \cdot \big((a \cdot (x \cdot y)) \cdot (a \cdot (x \cdot z))\big)$. Thus Eq. (11) is equivalent to

$$(a + b) \cdot \big((x + y) \cdot z\big) = (a \cdot b) \cdot \big((a \cdot (x \cdot y)) \cdot (a \cdot (x \cdot z))\big). \tag{12}$$

For $b = x = 0$, Eq. (12) reduces to

$$a \cdot (y \cdot z) = (a \cdot y) \cdot (a \cdot z). \tag{13}$$

With Eq. (13), the right-hand side of Eq. (12) becomes $(a\cdot b)\cdot\big(a\cdot((x\cdot y)\cdot(x\cdot z))\big) = (a \cdot b) \cdot \big(a \cdot ((x + y) \cdot z)\big) = \big((a \cdot b) \circ a\big) \cdot \big((x + y) \cdot z\big)$, which shows that Eq. (11) is equivalent to Eq. (13). □

To classify nonprimary cyclic braces, we have to analyze extensions $A \ltimes N$ of a primary cyclic brace N by a brace A of coprime order. We say that a semidirect product $A \ltimes N$ of braces *splits* if the action of A on N is trivial. By Proposition 3, this means that A is an ideal of the brace $A \ltimes N$. Thus, as in group theory, a semidirect product of braces splits if and only if it is a product.

Proposition 5. *Let N be a nontrivial cyclic brace of order p^n for some prime p, and let A be a brace of order m with $p \nmid m$. Then every semidirect product $A \ltimes N$ splits.*

Proof. By Corollary 1 of Proposition 1, a semidirect product $A \ltimes N$ is given by a group homomorphism $\sigma\colon A^\circ \to 1 + \mathrm{Soc}(N)$. Since $|N^\times| = p^{n-1}(p-1)$ and $p \nmid m$, any element x in the image of σ satisfies $x^{p-1} = 1$ in $N^\times$. Hence

$$(1 - x)(1 + x + \cdots + x^{p-2}) = 0.$$

Let d be the order of $\mathrm{Soc}(N)$. Then $(1-x)d = 0$. As the brace N is nontrivial, this implies that $1-x \notin N^\times$. Thus, $x \equiv 1 \pmod p$, which yields $1+x+\cdots+x^{p-2} \in N^\times$. Hence $1 - x = 0$, which shows that $A \ltimes N$ splits. □

Definition 2. Let G be a group with a subgroup N. By $\mathrm{Aut}_N(G)$ we denote the group of all automorphisms $\alpha \in \mathrm{Aut}(G)$ with $\alpha(N) = N$. If N is normal, we write $\mathrm{Aut}^N(G)$ for the group of all $\alpha \in \mathrm{Aut}_N(G)$ which are trivial modulo N.

So we have an exact sequence

$$1 \longrightarrow \mathrm{Aut}^N(G) \longrightarrow \mathrm{Aut}_N(G) \longrightarrow \mathrm{Aut}(G/N).$$

For example, if A is a cyclic brace, Corollary 2 of Proposition 1 states that $\mathrm{Aut}^\flat(A) = \mathrm{Aut}^{\mathrm{Soc}(A)}(A)$. For a subgroup H of G, let $C_H(N)$ denote the set of all $a \in H$ which commute with the elements of N. So with respect to the conjugation action of H on N, there is an exact sequence $C_H(N) \hookrightarrow H \to \mathrm{Aut}(N)$.

Proposition 6. *Let H be a Hall subgroup of a finite group G. Assume that H has a normal complement N with an abelian automorphism group. Then*

$$\mathrm{Aut}_H(G) \cong \mathrm{Aut}^{C_H(N)}(H) \times \mathrm{Aut}(N).$$

Proof. Since N consists of the elements of order dividing $|N|$, the normal complement N is unique. Hence $\mathrm{Aut}_H(G) \subset \mathrm{Aut}(H) \times \mathrm{Aut}(N)$. Let $\alpha = (\beta, \gamma) \in \mathrm{Aut}(H) \times \mathrm{Aut}(N)$ be given. For $a, b \in H$ and $x, y \in N$, we have $axby = ab(x^b)y$ with $x^b := b^{-1}xb$. Thus, an automorphism $\alpha \in \mathrm{Aut}_H(G)$ has to satisfy $\beta(ab)\gamma((x^b)y) = \beta(a)\gamma(x)\beta(b)\gamma(y) = \beta(a)\beta(b)\gamma(x)^{\beta(b)}\gamma(y)$, that is, $\gamma(x^b) = \gamma(x)^{\beta(b)}$. Since $\mathrm{Aut}(N)$ is abelian, this condition reduces to $x^b = x^{\beta(b)}$, for all $b \in H$ and $x \in N$. Furthermore, we infer that $C_H(N)$ is a normal subgroup of H. Thus $\alpha \in \mathrm{Aut}_H(G)$ if and only if β is trivial modulo $C_H(N)$. □

Proposition 7. *Let $A = B \ltimes I$ be a semidirect product of finite braces of coprime order. Assume that $\mathrm{Aut}^\flat(I)$ is abelian. Then*

$$\mathrm{Aut}^\flat(A) \cong \big(\mathrm{Aut}^{C_{B^\circ}(I^\circ)}(B^\circ) \cap \mathrm{Aut}^\flat(B)\big) \times \mathrm{Aut}^\flat(I).$$

Proof. Since B and I are invariant under brace automorphisms of A, we have $\mathrm{Aut}^\flat(A) \subset \mathrm{Aut}(B) \times \mathrm{Aut}(I)$. Let $\alpha = (\beta, \gamma) \in \mathrm{Aut}(B) \times \mathrm{Aut}(I)$ be given. For $a, b \in B$ and $x, y \in I$, Eq. (10) yields $\alpha((a + x) \cdot (b + y)) = \beta(a \cdot b) + \gamma(a \cdot (x \cdot y))$ and $\alpha(a + x) \cdot \alpha(b + y) = \beta(a) \cdot \beta(b) + \big(\beta(a) \cdot (\gamma(x) \cdot \gamma(y))\big)$. Hence $\alpha \in \mathrm{Aut}^\flat(A)$ if and only if $\beta \in \mathrm{Aut}^\flat(B)$ and $\gamma(a \cdot (x \cdot y)) = \beta(a) \cdot \big(\gamma(x) \cdot \gamma(y)\big)$ for all $a \in B$ and $x, y \in I$. For $a = 0$, this implies that $\gamma \in \mathrm{Aut}^\flat(I)$. Since $\mathrm{Aut}^\flat(I)$ is abelian, and by Proposition 4, $\gamma(a \cdot (x \cdot y)) = a \cdot \gamma(x \cdot y)$. Hence $\alpha \in \mathrm{Aut}^\flat(A)$ if and only if $\alpha \in \mathrm{Aut}^\flat(B) \times \mathrm{Aut}^\flat(I)$ and $a \cdot x = \beta(a) \cdot x$ for all $a \in B$ and $x \in I$. Now the latter condition is equivalent to $\beta \in \mathrm{Aut}^{C_{B^\circ}(I^\circ)}(B^\circ)$. □

3. The affine structures of a cocyclic brace

Cyclic braces are closely related to braces for which the adjoint group is cyclic. We call them *cocyclic*. To obtain a classification of cyclic braces in Section 4, we have to deal with the affine structures of cocyclic braces. By [25], Proposition 3, a cocyclic brace A is a commutative radical ring. Watters' theorem [30] implies that A is nilpotent. If $A \neq 0$, there is a maximal $n \in \mathbb{N}$ with $A^n \neq 0$. If A is nontrivial, A/A^2 is finite, and then A^i/A^{i+1} is finite for all $i \in \mathbb{N}$. Hence A is finite (cf. [20], Lemma 4), and splits into a direct product of its primary components.

In what follows, we fix a generator 1 of the adjoint group for any cocyclic brace A. So the elements of A are of the form $1^{\circ k} = 1 \circ \cdots \circ 1$ (k times) with $k \in \mathbb{N}$ or $1^{\circ(-k)} := (1')^{\circ k}$ if A is infinite. Since $(1 \cdot 1^{\circ k}) \circ 1 = (1^{\circ k} \cdot 1) \circ 1^{\circ k}$, we have

$$1 \cdot 1^{\circ k} = (1^{\circ k} \cdot 1) \circ 1^{\circ(k-1)}. \tag{14}$$

Proposition 8. *Let A be a cocyclic brace. Then*

$$\operatorname{Soc}(A) = \{a \in A \mid \forall\, b \in A\colon b \cdot a = a\} = \{a \in A \mid a \cdot 1 = 1\}.$$

Proof. Without loss of generality, we can assume that A is finite. Then $a \in A$ belongs to the socle if and only if $a \cdot 1^{\circ k} = 1^{\circ k}$ holds for all $k \in \mathbb{N}$, or equivalently, $(a \cdot 1^{\circ k}) \circ a = 1^{\circ k} \circ a$, that is, $(1^{\circ k} \cdot a) \circ 1^{\circ k} = a \circ 1^{\circ k}$, which proves the first equation. By Eq. (14), this yields $1^{\circ k} \in \operatorname{Soc}(A) \iff 1 \cdot 1^{\circ k} = 1^{\circ k} \iff 1^{\circ k} \cdot 1 = 1$. □

Definition 3. Let A be a brace. We call $|A/\operatorname{Soc}(A)|$ the *index* of A. If p^s is the index of a primary component A_p of A, we call $s_p(A) := s$ the *local index* at p.

If A is a cocyclic brace of index s, then $\langle 1^{\circ s}\rangle$ is the adjoint group of $\operatorname{Soc}(A)$. The permutation σ_1 of A with $\sigma_1(a) := 1 \cdot a$ determines the affine structure of A° and gives a partition of A into cycles. By Eq. (14), the affine structure of A° is already determined by the cycle $A^\sharp$ of length s which contains the generator 1, the *principal cycle*. We regard $A^\sharp$ as a cyclic group with unit element 1.

By Proposition 8, the map $1^{\circ k} \cdot 1 \mapsto \sigma_1^k$ gives an embedding $A^\sharp \hookrightarrow \operatorname{Aut}(A)$ which identifies $A^\sharp$ with the image of the structure map (4). So there is a group isomorphism

$$(A/\operatorname{Soc}(A))^\circ \cong A^\sharp. \tag{15}$$

Proposition 9. *Let A be a cocyclic brace. Then*

$$A^\sharp = 1 + A^2,$$

and $A^2 = 1A$ (with respect to the brace multiplication).

Proof. Since $1^a = 1a + 1$ for all $a \in A$, we have $A^\sharp = 1 + 1A$. By induction, it follows easily that any $1^{\circ k} \in A$ is a sum of powers if 1. Therefore, each product ab with $a, b \in A$ is a sum of products $1 \cdots 1$ with at least two factors. Whence $A^2 \subset 1A$. □

For primary cocyclic braces, the following result was proved in [6], Proposition 5.4. We give an independent, more "brace-theoretic" proof.

Proposition 10. *A cocyclic brace is either infinite and trivial or finite. If it is finite, it splits into a direct product of its primary components. A primary cocyclic brace is either bicyclic or of order 4 with a Klein Four group as an additive group.*

Proof. The nonprimary case has been treated at the beginning of this section. Thus, assume that $|A| = p^m$ for a prime p and $m \in \mathbb{N}$. By [24], Corollary of Proposition 8, the ideals of A form a chain of length m. Let I be the unique maximal ideal of A. Assume that A is not bicyclic. Suppose that I is not bicyclic, too. By induction, we can assume that I is of order 4, with a Klein Four group as an additive group. Hence $\operatorname{Soc}(A) \subsetneq I$, and $A/\operatorname{Soc}(A)$ is bicyclic. For $A^\circ = \langle u\rangle$, we have $u^2 = u \circ u - (u + u) \in \operatorname{Soc}(A)$, since $A/\operatorname{Soc}(A)$ is a trivial brace. Hence $A^2 \subset \operatorname{Soc}(A)$, a contradiction.

Thus I is bicyclic. For any $a \in A \setminus I$, this implies that pa does not generate I as an additive group. So there is an element $b \in I$ with $pa = pb$. Replacing a by $a - b$, we can assume that $pa = 0$. Therefore, the additive group of A is of the form $A = C_p \oplus I$. Since $A/\operatorname{Soc}(A)$ is trivial, this implies that $\operatorname{Soc}(A) = I$. For a generator u of A°, we obtain $u = a + b = a \circ b$ with $a \in C_p$ and $b \in I$. Hence $A^\circ = \langle a \rangle$. Now $A[p] := \{c \in A \mid pc = 0\}$ is a right ideal, hence an ideal of A. Since $a \in A[p]$, this gives $pA = 0$. Thus $|I| = p$. If p is odd, Proposition 9 yields $a^{\circ p} = \sum(a + A^2) = pa + \sum A^2 = 0$, a contradiction. Thus $p = 2$, and A is the nontrivial cocyclic brace of order 4. □

Definition 4. For a positive integer n, we call $d \in \mathbb{Z}/n\mathbb{Z}$ a *socle class* if $p|n \Rightarrow p|d$ and $8|n \Rightarrow 4|d$ holds for all primes p.

Now we have the following classification.

Proposition 11. *Let $G = \langle u \rangle$ be a cyclic group of order n.*

(a) *For a divisor s of n there exists a brace A with $A^\circ \cong G$ and index s if and only if n/s is a socle class for n. Up to isomorphism, such a brace is unique.*

(b) *An affine structure of G is uniquely determined by the element $c \in \mathbb{Z}/n\mathbb{Z}$ with $u^u = u^{\circ c}$. Such an affine structure exists if and only if $c - 1$ is a socle class. Its index is equal to the order of c in $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. By Proposition 10, we can assume that $|G| = p^m$ for some prime p. Let A be a bicyclic brace with adjoint group G and index s. We identify the additive group of A with the additive group of the ring $\mathbb{Z}/p^m\mathbb{Z}$, so that the generator $u \in G$ corresponds to the unit element of $\mathbb{Z}/p^m\mathbb{Z}$. By [25], Proposition 5, the affine structures of G correspond to the cocyclic $q \in \mathbb{Z}/p^m\mathbb{Z}$ via $q := 1^1$, and the set of cocyclic residue classes with fixed index s is $1 + (\mathbb{Z}/p^m\mathbb{Z})^\times d$, where $d := |\operatorname{Soc}(A)| = p^m/s$. Hence q is cocyclic with index s if and only if $q - 1$ is of order s in $\mathbb{Z}/p^m\mathbb{Z}$.

By [25], Proposition 7, $c - 1$ and $1^{\circ(c-1)}$ generate the same subgroup of $\mathbb{Z}/p^m\mathbb{Z}$. Hence $q - 1 = 1^{\circ c} - 1 = (1^{\circ(c-1)})^1 = (1^{\circ(c-1)})q$ implies that $q - 1$ and $c - 1$ generate the same subgroup of $\mathbb{Z}/p^m\mathbb{Z}$. So $1^1 = 1^{\circ c}$ defines an affine structure of index s if and only if $c \in \mathbb{Z}/p^m\mathbb{Z}$ is cocyclic and $c - 1$ is of order s in $\mathbb{Z}/p^m\mathbb{Z}$, or equivalently, c is of order s in $(\mathbb{Z}/p^m\mathbb{Z})^\times$ (see [28], Part 1, II.3.2). By the corollary of [25], Proposition 6, c is cocyclic if and only if $c - 1$ is a socle class. This settles the bicyclic case. Note that (a) follows by [25], Theorem 1.

By Proposition 10, it remains to consider the exceptional case $|G| = 4$. Thus, assume that $G = \{1, u, a, b\}$ with $a := u^2$ and $b := u^3$. Note first that $u^u = a$ is impossible for an affine structure of G. Indeed, this would imply that $a = u^2 = u^u + u = a + u$, a contradiction. So we are left with two cases.

Case 1. $u^u = u$. Then $u + u = a$, which implies that $a^u = u^u + u^u = u + u = a$. Hence $b = a^u + u = a + u$, and thus $b^u = a^u + u^u = b$, which gives a trivial brace.

Case 2. $u^u = b$. Then $b^b = (u^u)^b = u^1 = u$. Suppose that $b^a = a$. Then $a + a = b^a + a = u$. Hence $u + u = 1$. Thus $b + b = u^u + u^u = (u + u)^u = 1$, and similarly, $a + a = b^a + b^a = 1$, a contradiction. So we have $b^a \neq a$. Furthermore, $b^a = (u^u)^a = u^b \neq b^b = u$, which proves that $b^a = b$. Hence $b + b + u = b^a + u^u + u = b^a + a = u$, and thus $b + b = 1$. This shows that the additive group must be a Klein Four group. Furthermore, $b^a = b$ implies that the socle is $\{1, a\}$. So the affine structure is unique, and $c - 1 = 2$ is a socle class. □

Corollary 1. *The set of all socle classes which define a cocyclic brace of order n with socle order d is $(\mathbb{Z}/n\mathbb{Z})^\times d$.*

Proof. By [25], Proposition 5, the set of cocyclic residue classes which define A is $1+(\mathbb{Z}/n\mathbb{Z})^\times d$ if A is bicyclic. So the set of socle classes is $(\mathbb{Z}/n\mathbb{Z})^\times d$ in this case. If A is a nontrivial brace of order 4, then $(\mathbb{Z}/4\mathbb{Z})^\times 2 = \{2\}$, in accordance with case 2 of the preceding proof. Now the corollary follows by Proposition 10. □

Corollary 2. *The number of affine structures of a cocyclic brace of index s is $\varphi(s)$.*

Proof. This follows by Corollary 1 and part (b) of Proposition 11. □

The next result gives a multiplicative version of Proposition 1 for a cocyclic brace A. Here every $1^{\circ k} \in (A^\circ)^\times$ defines an automorphism $a \mapsto a^{\circ k}$ of the adjoint group A°. So we have a natural embedding

$$\mathrm{Aut}^\flat(A) \hookrightarrow (A^\circ)^\times.$$

Accordingly, we write $A^{\textcircled{\flat}}$ for the image of $\mathrm{Aut}^\flat(A)$ in $(A^\circ)^\times$.

Proposition 12. *Let A be a cocyclic brace. Then*

$$A^{\textcircled{\flat}} = (A^\circ)^\times \cap \big(1 \circ \mathrm{Soc}(A)\big).$$

Proof. For infinite A or $|A| = 4$, the equation is trivial. So we can assume that A is finite and bicyclic. Let $1^{\circ k} \in (A^\circ)^\times$ be given. If $1^{\circ k} \in A^{\textcircled{\flat}}$, then $1^{\circ k}$ induces an automorphism of the additive group of A. Since 1 is mapped to $1^{\circ k}$, this automorphism must be $a \mapsto a(1^{\circ k})$. Thus $1^{\circ k} \in 1+\mathrm{Soc}(A) = 1 \circ \mathrm{Soc}(A)$. Conversely, assume that $1^{\circ k} \in (A^\circ)^\times \cap \big(1 \circ \mathrm{Soc}(A)\big)$. Then $a^1 = a^{1^{\circ k}}$ holds for all $a \in A$. We have to verify $(a \cdot b)^{\circ k} = a^{\circ k} \cdot b^{\circ k}$ for $a, b \in A$. Since $(a \cdot b)^{\circ k} \circ a^{\circ k} = \big((a \cdot b) \circ a\big)^{\circ k} = (a+b)^{\circ k}$, the equation to be checked is equivalent to $(a+b)^{\circ k} = a^{\circ k} + b^{\circ k}$. To prove this, we show that

$$a^{\circ k} = a(1^{\circ k})$$

holds for all $a \in A$. For $a = 1$, this is trivial. Thus, by induction, it is enough to show that the equation implies that $(a \circ 1)^{\circ k} = (a \circ 1)(1^{\circ k})$. Now $(a \circ 1)^{\circ k} = a^{\circ k} \circ 1^{\circ k} = (a^{\circ k})^{1^{\circ k}} + 1^{\circ k}$ and $(a \circ 1)(1^{\circ k}) = (a^1 + 1)(1^{\circ k}) = (a^1)(1^{\circ k}) + 1^{\circ k}$. So we are left with the equation $(a^{\circ k})^{1^{\circ k}} = (a^1)(1^{\circ k})$. By the inductive hypothesis, we have $(a^{\circ k})^{1^{\circ k}} = (a(1^{\circ k}))^{1^{\circ k}} = (a^{1^{\circ k}})(1^{\circ k}) = (a^1)(1^{\circ k})$, which proves the claim. □

4. Almost Sylow-cyclic groups

Burnside's theorem ([21], 10.1.8) states that if a Sylow subgroup P of a finite group G is contained in the center of its normalizer, P has a *normal complement*, that is, a normal subgroup $N \lhd G$ with $G = PN$ and $P \cap N = 1$. The following definition is due to [10].

Definition 5. A finite group is said to be *almost Sylow-cyclic* if its Sylow subgroups of odd order are cyclic, while either the Sylow 2-subgroups are trivial or they contain a cyclic subgroup of index 2.

Solvable almost Sylow-cyclic groups were classified by Zassenhaus in his work on near-fields [32]. The general case was settled by Suzuki [29] and Wong [31]. If all Sylow subgroups of a finite group G are cyclic, G is a semidirect product of two cyclic groups of coprime order, and vice versa [8]. Such groups are also known as

Z-groups [29]. In accordance with Definition 5, we call them *Sylow-cyclic*. Using the classification of primary cyclic braces [25], we have the following.

Theorem 1. *The adjoint group A° of a finite cyclic brace A is solvable and almost Sylow-cyclic.*

Proof. For any prime p, the p-primary component A_p is a right ideal, hence a subbrace of A. So the adjoint groups A_p° are the Sylow subgroups of A°, and each Sylow subgroup A_p° has a complement. Thus Hall's theorem [15] implies that A° is solvable. By [25], Theorem 3, the A_p° are either cyclic, or A_p is exceptional which implies that $p = 2$ and A_p° has a cyclic subgroup of index 2. Whence A° is almost Sylow-cyclic. □

Example 3. The converse of Theorem 1 is not valid. For example, the alternating group A_4 is almost Sylow-cyclic with a unique brace structure. Indeed, $A_4 = C_3 \ltimes V$ with the Sylow 3-subgroup C_3 acting cyclically on the nontrivial elements of the normal Sylow 2-subgroup $V \cong C_2 \times C_2$. For any brace structure on A_4, the Sylow subgroups correspond to right ideals. If the brace V would be cyclic, it could not be trivial, contrary to Proposition 5. Thus V is a trivial brace, and by Proposition 2, there is a unique brace structure on A_4. However, this brace is not cyclic.

In general, the Sylow 2-subgroup of a solvable almost Sylow-cyclic group G does not have a normal complement, caused by a possible subfactor A_4 of G (see [32], Satz 7). For adjoint groups of cyclic braces, this obstruction disappears.

Proposition 13. *Let A be a finite cyclic brace. Any Sylow 2-subgroup of the adjoint group A° admits a normal complement.*

Proof. By Theorem 1, the adjoint group A° is solvable and almost Sylow-cyclic. Let P be a Sylow 2-subgroup of A°. By Hall's theorem [13], there is a complement N of P. Proposition 2 implies that there exist right ideals I and S of A with $I^\circ = N$ and $S^\circ = P$. As the additive group of S is a cyclic 2-group, N must act trivially on S. Thus N is normal by Proposition 3. □

For a group G, let G' denote the commutator subgroup of G. If G is finite, we write $\pi(G)$ for the set of primes which divide the order of G.

Definition 6. Let G be a solvable almost Sylow-cyclic group. For $p \in \pi(G)$, let $\lambda_p(G)$ denote the composition length of a Sylow p-subgroup P of G. We call $p \in \pi(G)$ *free* if P is cyclic and $P \cap G' = 1$.

Now we are ready to classify all cyclic braces. For a finite group G, the corollary of Proposition 2 shows that an affine structure of G is given by the restriction to the Sylow subgroups. So we have to determine which collections of affine structures of the Sylow subgroups extend to G. The number of isomorphism classes of affine structures can then be determined by using the results of Section 3. Recall that a finite group is said to be *p-nilpotent* (for a prime p) if any Sylow p-subgroup has a normal complement.

Theorem 2. *Let G be a finite group with a Sylow basis $\{P_1, \dots, P_r\}$ and cyclic braces B_i with adjoint group P_i. The affine structures of the P_i extend to an affine structure of G if and only if G is 2-nilpotent and B_i is trivial for the nonfree odd primes $p_i \in \pi(P_i)$.*

Proof. We order the P_i such that P_i is a p_i-group, with $p_1 < \cdots < p_r$. Assume first that the conditions of the theorem are satisfied. If $p_1 = 2$, there is a normal complement of P_1. Otherwise, let N be the normalizer of P_1. Since P_1 is cyclic, the primes in $\pi(\mathrm{Aut}(P_1))$ are $\leqslant p_1$. So the action of a complement of P_1 in N by conjugation on P_1 is trivial, which shows that P_1 is contained in the center of N. By Burnside's theorem ([21], 10.1.8), this implies that P_1 has a normal complement. Thus, in any case, there is a normal complement G_1 of P_1. By Hall's theorem ([21], 9.1.7), the complements of P_1 are conjugate. Hence $G_1 = P_2 \cdots P_r$. By induction, we get a Sylow tower

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_r = 1 \tag{16}$$

of characteristic subgroups $G_i = P_{i+1} \cdots P_r$ of G. For $1 \leqslant i < j \leqslant r$, it follows that P_j is normal in the subgroup P_iP_j of G. Thus P_i acts on P_j by conjugation.

By Proposition 2, an extension of the affine structures of the P_i to G must be unique. For $i < j$, the action of B_j° on B_i has to be trivial (Proposition 3), with

$$a \cdot b = aba^{-1} \tag{17}$$

for $a \in B_i$ and $b \in B_j$. We claim that this makes G into the adjoint group of a brace A with primary components $B_1, \ldots, B_r$.

To verify that A is a brace, we show that each G_i is the adjoint group of a brace A_i, obtained by restriction of A. Assume that this has been shown for some i with $0 < i < r$. Equation (17) gives a group homomorphism

$$P_i \longrightarrow \mathrm{Aut}(B_{i+1}) \times \cdots \times \mathrm{Aut}(B_r) = \mathrm{Aut}(A_i). \tag{18}$$

By Proposition 4, we have to prove that its image belongs to $\mathrm{Aut}^\flat(A_i)$. We show first that the image of $P_i \to \mathrm{Aut}(B_j)$ belongs to $\mathrm{Aut}^\flat(B_j)$ for all $j > i$. If p_j is not free, this follows since B_j is trivial. Thus, assume that p_j is free. For $a \in P_i$ and $b \in P_j$, this implies that $aba^{-1}b^{-1} \in P_j \cap G' = 1$. So the action of P_i on B_j is trivial. In particular, the image of $P_i \to \mathrm{Aut}(B_r)$ belongs to $\mathrm{Aut}^\flat(B_r)$.

Next we show that conjugation by an element $a \in P_i$ induces a brace automorphism of A_i. By Proposition 7 and the inductive hypothesis, we have to show that conjugation by a on P_{i+1} is trivial modulo $C_{P_{i+1}}(A_{i+1})$. As the automorphism groups $\mathrm{Aut}(B_j)$ are abelian for all $j > i$, we have $G' \cap P_{i+1} \subset C_{P_{i+1}}(A_{i+1})$. For any $b \in P_{i+1}$, this implies that $aba^{-1}b^{-1} \in C_{P_{i+1}}(A_{i+1})$. Whence $P_i \to \mathrm{Aut}(A_i)$ maps into $\mathrm{Aut}^\flat(A_i)$. Thus A is a brace.

Conversely, let A be a cyclic brace with adjoint group G. By Proposition 13, this implies that G is 2-nilpotent. Assume that p_j is not free and odd. Then P_j is cyclic, and $P_j \cap G' \neq 1$. So the kernel of the transfer map $\tau\colon G \to P_j$ intersects P_j nontrivially (see [21], 10.1.5). Since P_j is abelian, $P_j = \mathrm{Im}\,\tau \times [P_j, N_G(P_j)]$, where $N_G(P_j)$ denotes the normalizer of P_j (see [21], 10.1.6). Since $[P_j, N_G(P_j)] = P_j \cap \mathrm{Ker}\,\tau$, this implies that $P_j = [P_j, N_G(P_j)]$. So there exist $a \in N_G(P_j)$ and $b \in P_j$ with $aba^{-1}b^{-1} \neq 1$, that is, $aba^{-1} \neq b$. Thus $a = ca_0b_0$ with $c \in P_{j+1} \cdots P_r$, $a_0 \in P_1 \cdots P_{j-1}$, and $b_0 \in P_j$. Suppose that $a_0ba_0^{-1} = b$. Then $b \neq cbc^{-1} = aba^{-1} \in P_j$. Hence $(cbc^{-1})b^{-1} = c(bc^{-1}b^{-1}) \in P_j \cap (P_{j+1} \cdots P_r) = 1$, a contradiction. Thus $a_0ba_0^{-1} \neq b$, which shows that $P_1 \cdots P_{j-1}$ acts nontrivially on P_j. By Proposition 5, this proves that B_j is trivial. □

Corollary 1. *A finite group G is the adjoint group of a cyclic brace if and only if G is solvable, 2-nilpotent, and almost Sylow-cyclic.*

Proof. The necessity follows by Theorems 1 and 2. If G is solvable, 2-nilpotent, and almost Sylow-cyclic, there exists a Sylow basis $\{P_1, \dots, P_r\}$, and by [25], Theorem 3, the P_i can be endowed with affine structures which meet the requirements of the theorem. □

Corollary 2. *Let G be a finite group of square-free order. Up to isomorphism, there is a unique brace with adjoint group G.*

Proof. Existence follows by Theorem 2, and uniqueness by the corollary of Proposition 2. □

Recall that the *core* H_G of a subgroup H of a group G is given by

$$H_G := \bigcap_{g \in G} gHg^{-1}.$$

Proposition 14. *Let A be a cyclic brace with adjoint group $G = A^\circ$. If $p_1 < \cdots < p_r$ are the primes in $\pi(G)$, there are ideals*

$$A = A_0 \supset A_1 \supset \cdots \supset A_r = 0$$

and right ideals $B_1, \dots, B_r$ of A such that $P_i := B_i^\circ$ is a Sylow p_i-subgroup of G, and $A_{i-1}^\circ = P_i A_i^\circ$ for all $i \in \{1, \dots, r\}$. Furthermore, $(P_i)_G = C_{P_i}(A_i^\circ)$ holds for all i, and

$$\operatorname{Soc}(A) = \bigoplus_{i=1}^{r} \big((P_i)_G \cap \operatorname{Soc}(B_i)\big). \tag{19}$$

Proof. The adjoint groups P_i of the primary components of A form a Sylow basis $\{P_1, \dots, P_r\}$ of G. We order the p_i-groups P_i such that $p_1 < \cdots < p_r$. Then $P_{i+1} \cdots P_r$ is the adjoint group of an ideal A_i of A, and $P_i = B_i^\circ$ with right ideals B_i and $A_{i-1}^\circ = P_i A_i^\circ$. To show that $(P_i)_G = C_{P_i}(A_i^\circ)$ for all i, let $a \in (P_i)_G$ be given. For any $b \in A_i^\circ$, we have $b^{-1}ab \in P_i$. Hence $(b^{-1}ab)a^{-1} = b^{-1}(aba^{-1}) \in P_i \cap A_i^\circ = 1$, which yields $(P_i)_G \subset C_{P_i}(A_i^\circ)$. Conversely, assume that $a \in C_{P_i}(A_i^\circ)$. Then $bab^{-1} \in P_i$ for all $b \in P_j$ with $j \in \{1, \dots, r\}$. Whence $a \in (P_i)_G$.

To verify Eq. (19), we can assume that this formula holds in $B := B_1 \cdots B_{r-1} \cong A/A_{r-1}$. Let $a \in B$ and $x \in A_{r-1} = B_r$ be given. Then $a + x \in \operatorname{Soc}(A)$ if and only if $(a + x) \cdot (b + y) = b + y$ for all $b \in B$ and $y \in B_r$. By Eq. (10), this is equivalent to $a \in \operatorname{Soc}(B)$ and

$$a \cdot (x \cdot y) = y$$

for all $y \in B_r$. If $x \cdot y \neq y$, then B_r is a nontrivial brace. So Proposition 5 implies that B acts trivially on B_r. Hence $x \cdot y = a \cdot (x \cdot y) = y$, a contradiction. Thus $x \in \operatorname{Soc}(B_r)$, and $a \cdot y = y$ for all $y \in B_r$.

So we have proved that $b_1 + \cdots + b_r$ with $b_i \in B_i$ belongs to $\operatorname{Soc}(A)$ if and only if $b_1 + \cdots + b_{r-1} \in \operatorname{Soc}(B)$ and $b_r \in \operatorname{Soc}(B_r)$ such that $b_1 + \cdots + b_{r-1}$ acts trivially on B_r. As the b_i with $i < r$ map into different primary components of $\operatorname{Aut}(B_r)$, we infer that each of $b_1, \dots, b_{r-1}$ acts trivially on B_r. By induction, this completes the proof. □

Corollary. *Let A be a cyclic brace with $|A| > 1$. Then $\operatorname{Soc}(A) \neq 0$.*

Proof. With the notation of Proposition 14, $0 \neq \operatorname{Soc}(B_r) \subset \operatorname{Soc}(A)$. □

5. Classification of cyclic braces

In this section, we provide a first step toward a quantitative version of Theorem 2. For a cyclic brace A with adjoint group G and $p \in \pi(G)$ we define $\beta_p(A)$ to be the number m of double cosets in a partition

$$\mathrm{Aut}(A_p^\circ) = \bigsqcup_{i=1}^{m} \mathrm{Aut}^{(A_p^\circ)_G}(A_p^\circ)\,\alpha_i\,\mathrm{Aut}^\flat(A_p). \tag{20}$$

Theorem 3. *For a finite cyclic brace A, the number $\beta(A)$ of isomorphism classes of cyclic braces with the same adjoint group and the same local indices is $\beta(A) = \prod_{p\in\pi(G)} \beta_p(A)$.*

Proof. For $G := A^\circ$, assume that $\pi(G) = \{p_1, \dots, p_r\}$ with $p_1 < \cdots < p_r$. So the Sylow p_i-subgroups $P_i = A_{p_i}^\circ$ of G form a Sylow basis $\{P_1, \dots, P_r\}$, and by the proof of Theorem 2, they fit into a Sylow tower (16).

Now $\mathrm{Aut}(G)$ acts on the affine structures of G. By Hall's theorem [14], the Sylow bases of G are pairwise conjugate. So we can restrict ourselves to braces with the same primary components P_i. Therefore, we have to deal with the subgroup $\mathrm{Aut}'(G)$ of all $\alpha \in \mathrm{Aut}(G)$ with $\alpha(P_i) = P_i$ for all i. With $G_i := P_{i+1} \cdots P_r$, we claim that

$$\mathrm{Aut}'(G) \cong \prod_{i=1}^{r} \mathrm{Aut}^{C_{P_i}(G_i)}(P_i). \tag{21}$$

For $r = 1$, this is obvious. With $H := P_1 \cdots P_{r-1}$, Proposition 6 gives $\mathrm{Aut}_H(G) = \mathrm{Aut}^{C_H(P_r)}(H) \times \mathrm{Aut}(P_r)$. Thus, by induction, we obtain

$$\mathrm{Aut}'(G) = \left(\mathrm{Aut}^{C_H(P_r)}(H) \cap \prod_{i=1}^{r-1} \mathrm{Aut}^{C_{P_i}(P_{i+1}\cdots P_{r-1})}(P_i)\right) \times \mathrm{Aut}(P_r).$$

Now an automorphism $\alpha = (\alpha_1, \dots, \alpha_{r-1}) \in \prod_{i=1}^{r-1} \mathrm{Aut}(P_i)$ belongs to $\mathrm{Aut}^{C_H(P_r)}(H) \cap \prod_{i=1}^{r-1} \mathrm{Aut}^{C_{P_i}(P_{i+1}\cdots P_{r-1})}(P_i)$ if and only if $(a_1 \cdots a_{r-1})^{-1}\alpha_1(a_1)\cdots \alpha_{r-1}(a_{r-1}) \in C_H(P_r)$ and $a_i^{-1}\alpha_i(a_i) \in C_{P_i}(P_{i+1}\cdots P_{r-1})$ for all $a_i \in P_i$ with $i < r$. By the latter conditions, we have $a_{r-1}^{-1}\cdots a_1^{-1}\alpha_1(a_1)\cdots\alpha_{r-1}(a_{r-1}) = a_1^{-1}\alpha_1(a_1)a_{r-1}^{-1}\cdots a_2^{-1}\alpha_2(a_2)\cdots\alpha_{r-1}(a_{r-1})$, which yields $(a_1\cdots a_{r-1})^{-1}\alpha_1(a_1)\cdots \alpha_{r-1}(a_{r-1}) = a_1^{-1}\alpha_1(a_1)\cdots a_{r-1}^{-1}\alpha(a_{r-1})$. This proves (21). Similarly, an application of Proposition 7 to $A = A_{p_1} \ltimes (A_{p_2} \oplus \cdots \oplus A_{p_r})$ yields

$$\mathrm{Aut}^\flat(A) \cong \prod_{i=1}^{r} \big(\mathrm{Aut}^{C_{P_i}(G_i)}(P_i) \cap \mathrm{Aut}^\flat(A_{p_i})\big).$$

For each i, Proposition 11 and [25], Theorem 3, imply that $\mathrm{Aut}(P_i)$ acts transitively on the affine structures of P_i with fixed local index at p_i. So the affine structures of P_i correspond to the left cosets of $\mathrm{Aut}^\flat(A_{p_i})$ in $\mathrm{Aut}(P_i)$. By Theorem 2, any collection of affine structures of the P_i with local indices $s_{p_i}(A)$ extends to a unique affine structure of G. So there is a one-to-one correspondence between the isomorphism classes of braces with adjoint group G and the orbits of $\prod_{i=1}^r \mathrm{Aut}^{C_{P_i}(G_i)}(P_i)$ on the left cosets of $\prod_{i=1}^r \mathrm{Aut}^\flat(A_{p_i})$ in $\prod_{i=1}^r \mathrm{Aut}(P_i)$. By Proposition 14, $C_{P_i}(G_i) = (P_i)_G$. Therefore, these orbits correspond to the double cosets in (20). □

Definition 7. Let G be a solvable, 2-nilpotent, almost Sylow-cyclic group. For a Sylow p-subgroup P with $(P : P_G) = p^c$, we call $c_p(G) := c$ the *core index* at p. We define a *sequence of local indices* for G to be a sequence (s_p) with $0 \leqslant s_p < \lambda_p(G) + \min\{p-3, 0\}$ and $s_p = 0$ for nonfree odd primes, where $p \in \pi(G)$ runs through the primes with cyclic Sylow p-subgroups. For each s_p, we call $s'_p := \min\{s_p, c_p(G)\}$ the *reduced local index* at p.

By Theorem 2, any sequence (s_p) of local indices is realizable by a brace with adjoint group G. The value of $\beta(A)$ in Theorem 3 merely depends on the adjoint group A°, while Eq. (20) still refers to the groups $\mathrm{Aut}^\flat(A_p)$. To remove this dependence, we start with Sylow-cyclic groups G.

Corollary 1. *Let G be a Sylow-cyclic group, and let (s_p) be a sequence of local indices for G. There are $\prod_{p\in\pi(G)} \varphi(p^{s'_p})$ isomorphism classes of cyclic braces with adjoint group G and local indices s_p, where φ denotes the Euler totient function.*

Proof. By Theorem 2, there exists a cyclic brace A with adjoint group G and local indices s_p. We have to verify that $\varphi(p^{s'_p}) = \beta_p(A)$. Thus let P be a Sylow p-subgroup of G. Up to isomorphism, there is a unique cyclic brace B of index p^{s_p} with $B^\circ = P$. Identifying P with the additive group of $R := \mathbb{Z}/p^{\lambda_p(G)}\mathbb{Z}$, the automorphism group $\mathrm{Aut}(P)$ is isomorphic to the unit group $R^\times$. Since B is bicyclic, Proposition 12 implies that $\mathrm{Aut}^\flat(B) \cong B^{\textcircled{p}} = R^\times \cap \big(1 \circ \mathrm{Soc}(B)\big)$. Similarly, $\mathrm{Aut}^{P_G}(P) \cong R^\times \cap (1 \circ P_G)$. Since P_G and $\mathrm{Soc}(B)$ are comparable, $\mathrm{Aut}^{P_G}(P)\,\mathrm{Aut}^\flat(B) \cong R^\times \cap \big(1 \circ P_G\,\mathrm{Soc}(B)\big)$. Thus $\mathrm{Aut}(P)/\,\mathrm{Aut}^{P_G}(P)\,\mathrm{Aut}^\flat(B) \cong (R/P_G\,\mathrm{Soc}(B))^\times$. As the index of $P_G\,\mathrm{Soc}(B)$ in R is $p^{s'_p}$, we obtain $\beta_p(A) = \varphi(p^{s'_p})$. □

The next result shows that for Sylow-cyclic groups G, except those with Sylow 2-subgroups of order 4, *all* braces with adjoint group G are cyclic.

Corollary 2. *Let G be a Sylow-cyclic group. The number of isomorphism classes of cyclic braces with adjoint group G is $\beta(G) = \prod\{\beta_p(G) \,|\, p \in \pi(G/G'), \lambda_p(G) \geqslant 2\}$, where*

$$\beta_p(G) = \begin{cases} \lambda'_p & \text{for } c_p(G) = 0, \\ p^{c'_p - 1}\big(1 + (p-1)(\lambda'_p - c'_p)\big) & \text{for } c_p(G) > 0, \end{cases} \tag{22}$$

with $\lambda'_p := \lambda_p(G) + \min\{p-3, 0\}$ and $c'_p := \min\{c_p(G), \lambda'_p\}$. If the Sylow 2-subgroups of G are not of order 4, any brace with adjoint group G is cyclic.

Proof. Let P be a Sylow 2-subgroup of G with $|P| \neq 4$. Proposition 10 implies that every brace B with $B^\circ = P$ is cyclic. This proves the last statement of the corollary. By [21], 10.1.5 and 10.1.6, the transfer map $\tau\colon G \to P$ satisfies $P \cap \mathrm{Ker}\,\tau = P \cap G' = [P, N_G(P)]$ and $P = C_P(N_G(P)) \times [P, N_G(P)]$. Hence $P \cap G' = P$ or $P \cap G' = 1$. Thus G' is a Hall subgroup of G, and there is a cyclic complement C of G'. So $\pi(G/G') = \pi(C)$ is the set of free primes p of G. Thus, for free primes $p \in \pi(G)$, we have to show that the sum of all $\varphi(p^{s'})$ with $s' := \min\{s, c_p(G)\}$ and $0 \leqslant s < \lambda'_p$ is equal to $\beta_p(G)$. Since braces of prime order are trivial, we can restrict ourselves to the case $\lambda_p(G) \geqslant 2$.

Assume first that $c_p(G) > 0$. Then $0 < c'_p \leqslant \lambda'_p$, and

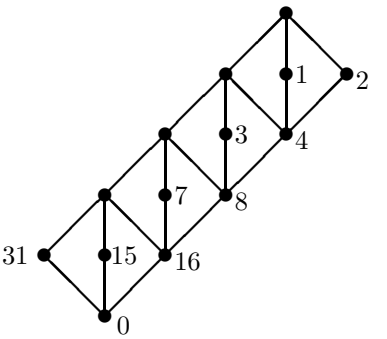
$$\begin{aligned}\sum_{s=0}^{\lambda'_p-1} \varphi(p^{s'}) &= \sum_{s=0}^{c'_p-1} \varphi(p^{s'}) + \sum_{s=c'_p}^{\lambda'_p-1} \varphi(p^{s'}) = \sum_{s=0}^{c'_p-1} \varphi(p^s) + (\lambda'_p - c'_p)\varphi(p^{c'_p}) \\ &= 1 + (p-1)\sum_{i=0}^{c'_p-2} p^i + (\lambda'_p - c'_p)p^{c'_p-1}(p-1) \\ &= p^{c'_p-1} + (\lambda'_p - c'_p)p^{c'_p-1}(p-1) \\ &= p^{c'_p-1}\big(1 + (\lambda'_p - c'_p)(p-1)\big).\end{aligned}$$

For $c_p(G) = 0$, we have $\sum_{s=0}^{\lambda'_p-1} \varphi(p^{s'}) = \lambda'_p$. □

6. The Sylow 2-subgroup

For a cyclic brace A with an exceptional 2-component, the calculation of $\beta_2(A)$ in Theorem 3 needs the classification of 2-primary cyclic braces [24].

By [25], Section 7, there are six types of exceptional cyclic braces A of order 2^n, according to the corresponding adjoint groups ([25], Proposition 11) which determine A up to isomorphism ([25], Theorem 3). Type (1a) consists of the cyclic groups A°, while (1b) stands for the abelian, noncyclic groups $A^\circ = C_2 \times C_{2^m}$. The subgroup lattice of such a group A° ($m = 4$) looks as follows:



The numbers indicate the cyclic subgroups generated by the corresponding residue class in the additive group $C_{2^5} \cong \mathbb{Z}/2^5\mathbb{Z}$ of A. Since $A^\circ = \langle -1\rangle \times \langle 1\rangle \cong \langle 31\rangle \times \langle 2\rangle$, there is a group automorphism of A° which maps $\langle 1\rangle$ to $\langle 2\rangle$ and leaves all other subgroups fixed. This cannot be a brace automorphism since $\langle 2\rangle$ is a brace ideal, in contrast to $\langle 1\rangle$. The socle is $\{0, 2^m\}$. Hence, by Proposition 1, the only nontrivial brace automorphism interchanges the subgroups $\langle -1\rangle$ and $\langle 2^m - 1\rangle$ of order 2. If $m > 1$, the socle is distinguished among the three subgroups of order 2. Hence $\mathrm{Aut}^\flat(A)$ is determined by $G := A^\circ$ in this case. Therefore, we write $\mathrm{Aut}^\flat(G) := \mathrm{Aut}^\flat(A)$.

In particular, the number $\beta_2^H(G)$ of double cosets $\mathrm{Aut}^H(G)\,\alpha\,\mathrm{Aut}^\flat(A)$ in $\mathrm{Aut}(G)$ (cf. Eq. (20) for a special subgroup H) does not depend on the affine structure of G.

Proposition 15. *Let $G = \langle b\rangle \times \langle a\rangle$ be a product of cyclic groups of order 2 and 2^m, respectively, with $m > 1$, and let H be a proper subgroup of index 2^c. Then $\beta_2^H(G) = 2$ if $H = \langle a\rangle$ or $H = \langle ba\rangle$, and $\beta_2^H(G) = 2^{c-1}$ otherwise.*

Proof. The automorphism group $\mathrm{Aut}(G)$ consists of the elements α_i and β_i with $i \in \{1, \dots, 2^m\}$, such that for odd i,

$$\begin{aligned} \alpha_i(a) &= \beta_i(a) = a^i, & \alpha_{i+1}(a) &= \beta_{i+1}(a) = ba^i, \\ \alpha_i(b) &= \alpha_{i+1}(b) = b, & \beta_i(b) &= \beta_{i+1}(b) = ba^{2^{m-1}}. \end{aligned} \tag{23}$$

Thus $|\operatorname{Aut}(G)| = 2^{m+1}$. With $a = 2$ and $b = -1$, we have $a^i = 2i$ and $ba^i = -1 + 2i$ for $i \in \mathbb{Z}/2^m\mathbb{Z}$. The nontrivial brace automorphism is given by the multiplication with $1 + 2^m$. Hence $\operatorname{Aut}^\flat(G) = \{1, \beta_1\}$. The subgroup $\operatorname{Aut}^H(G)$ consists of the automorphisms $\gamma \in \operatorname{Aut}(G)$ with $\gamma(g) \in gH$ for all $g \in G$. Therefore, we have

$$a^{2^{m-1}} \in H \iff \beta_1 \in \operatorname{Aut}^H(G) \iff \beta_{1+2^{m-1}} \in \operatorname{Aut}^H(G).$$

The 2^m left cosets of $\{1, \beta_1\}$ are $\alpha_i\{1, \beta_1\} = \beta_i\{1, \beta_1\} = \{\alpha_i, \beta_i\}$ and $\alpha_{i+1}\{1, \beta_1\} = \beta_{i+1}\{1, \beta_1\} = \{\alpha_{i+1}, \beta_{i+1}\}$. Since $\alpha_i\beta_i^{-1} = \beta_1$ and $\alpha_{i+1}\beta_{i+1}^{-1} = \beta_{1+2^{m-1}}$, this yields

$$|\operatorname{Aut}^H(G)\alpha_i \operatorname{Aut}^\flat(G)| = |\operatorname{Aut}^H(G)| \iff a^{2^{m-1}} \in H$$

for all i. If $H = \langle a \rangle$ or $H = \langle ba \rangle$, then $\operatorname{Aut}^H(G)$ consists of the α_i and β_i with odd i. Thus $\operatorname{Aut}^H(G) \operatorname{Aut}^\flat(G) = \operatorname{Aut}^H(G)$ is of index 2 in $\operatorname{Aut}(G)$. Whence $\beta_2^H(G) = 2$.

Now assume that $\langle a \rangle \neq H \neq \langle ba \rangle$. Then there is no $a^i \in H$ or $ba^i \in H$ with i odd. Hence every $h \in H$ gives rise to an automorphism $\alpha_i \in \operatorname{Aut}^H(G)$ with $\alpha_i(a) = ha$. If $a^{2^{m-1}} \in H$, the double cosets $\operatorname{Aut}^H(G)\,\alpha_i\,\operatorname{Aut}^\flat(G)$ have cardinality $|\operatorname{Aut}^H(G)| = 2|H|$. Otherwise, $\beta_1 \notin \operatorname{Aut}^H(G)$, which yields $|\operatorname{Aut}^H(G)\,\alpha_i\,\operatorname{Aut}^\flat(G)| = 2|\operatorname{Aut}^H(G)| = 2|H|$. Thus, in any case, $\beta_2^H(G) = 2^{m+1} : 2|H| = 2^{c-1}$. □

There are three 2-groups G with $|G/G'| = 4$, namely, the dihedral group D_{2^m} of order 2^{m+1} (type 2a), the generalized quaternion group Q_{2^m} of order 2^{m+2} (type 2b), and the semidihedral group SD_{2^m} of order 2^{m+1} (type 3a). The presentations are given by

$$\begin{aligned} D_{2^m} &= \{a, b \mid a^{2^m} = b^2 = 1,\ bab^{-1} = a^{-1}\} && (m \geqslant 2), \\ Q_{2^m} &= \{a, b \mid a^{2^{m+1}} = 1,\ b^2 = a^{2^m},\ bab^{-1} = a^{-1}\} && (m \geqslant 1), \\ SD_{2^m} &= \{a, b \mid a^{2^m} = b^2 = 1,\ bab^{-1} = a^{-1+2^{m-1}}\} && (m \geqslant 3). \end{aligned}$$

In all three cases, the commutator subgroup of $G := A^\circ$ is $G' = \langle a^2 \rangle$, and G/G' is the Klein Four group. For $G = D_{2^m}$ and $G = Q_{2^m}$, the brace structure is given by $a = 2$ and $b = 1$ (modulo $|G|$), and

$$x \cdot y = y^x = \begin{cases} (-1)^x y & \text{for type (2a)}, \\ (-1 + 2^{m+1})^x y & \text{for type (2b)}. \end{cases}$$

In particular, $\operatorname{Soc}(A) = \langle a \rangle = 2A$. The other two groups between G and G' are isomorphic, $\langle b, a^2 \rangle \cong \langle ba, a^2 \rangle$. Indeed, the group automorphism $b \mapsto ba$ maps $\langle b, a^2 \rangle$ to $\langle ba, a^2 \rangle$. Both groups are dihedral in case (2a) and generalized quaternion subgroups in case (2b).

For $G = SD_{2^m}$, the brace structure is given by $a = 2$ and $b = -1$, and

$$x \cdot y = y^x = \begin{cases} y & \text{for } x \equiv 0 \pmod 4, \\ (-1 + 2^m)y & \text{for } x \equiv 1 \pmod 4, \\ (1 + 2^m)y & \text{for } x \equiv 2 \pmod 4, \\ (-1)y & \text{for } x \equiv 3 \pmod 4. \end{cases}$$

So we have $\mathrm{Soc}(A) = 4A = G'$ and $\langle a\rangle = 2A$. The groups between G and G' are pairwise nonisomorphic. They are $\langle a\rangle \cong C_{2^m}$ and $\langle b, a^2\rangle \cong D_{2^{m-1}}$, and $\langle ba, a^2\rangle \cong Q_{2^{m-2}}$.

In contrast to type (1b), the group $\mathrm{Aut}^\flat(A)$ depends on the affine structure. On the other hand, the three cases share the following remarkable property.

Proposition 16. *Let A be an exceptional cyclic brace with a dihedral, generalized quaternion, or semidihedral adjoint group G. The automorphism group of G is a central product*

$$\mathrm{Aut}(G) = \mathrm{Inn}(G) \circ \mathrm{Aut}^\flat(A). \tag{24}$$

Proof. Assume first that $G = D_{2^m}$ or $G = Q_{2^m}$. Thus $|\langle a\rangle| = 2^n$ with $n \geqslant 2$. The automorphism group $\mathrm{Aut}(G)$ consists of the elements $\alpha_{i,j}$ with $\alpha_{i,j}(a) = a^i$ and $\alpha_{i,j}(b) = ba^j$, where i is odd and $i, j \in \mathbb{Z}/2^n\mathbb{Z}$. Thus $|\mathrm{Aut}(G)| = 2^{2n-1}$. Let $\alpha_{i,j}$ be in the center of $\mathrm{Aut}(G)$. Then $ba^{i+j} = \alpha_{i,j}\alpha_{1,1}(b) = \alpha_{1,1}\alpha_{i,j}(b) = ba^{j+1}$. Hence $i = 1$. Furthermore, $ba^j = \alpha_{i,j}\alpha_{-1,0}(b) = \alpha_{-1,0}\alpha_{i,j}(b) = ba^{-j}$, which yields

$$Z(\mathrm{Aut}(G)) = \{1, \alpha_{1,2^{n-1}}\}. \tag{25}$$

The additive group $\mathbb{Z}/2^{n+1}\mathbb{Z} = \langle 1\rangle$ of the brace A with $A^\circ = G$ is given by $a = 2$ and $b = 1$, so that $a^k = 2k$ and $ba^k = 1 + 2k$. Since $\mathrm{Soc}(A) = 2A$, the brace automorphisms are multiplications by odd elements $1 + 2j$. Thus

$$\mathrm{Aut}^\flat(A) = \{\alpha_{1+2j,j} \mid j \in \mathbb{Z}/2^n\mathbb{Z}\}.$$

Since $a^{-1}ba = bb^{-1}a^{-1}ba = ba^2$, the group of inner automorphisms is

$$\mathrm{Inn}(G) = \langle \alpha_{-1,0}\rangle \times \langle \alpha_{1,2}\rangle \cong C_2 \times C_{2^{n-1}}.$$

Hence $\mathrm{Aut}^\flat(A) \cap \mathrm{Inn}(G) = Z(\mathrm{Aut}(G))$. Since $|\mathrm{Aut}^\flat(A)| = |\mathrm{Inn}(G)| = 2^n$, Eq. (24) follows.

Next, we consider the case $G = SD_{2^m}$. Then $\mathrm{Aut}(G)$ consists of the elements $\alpha_{i,j}$ with $\alpha_{i,j}(a) = a^i$ and $\alpha_{i,j}(b) = ba^j$, with i odd and j even in $\mathbb{Z}/2^m\mathbb{Z}$. Thus $|\mathrm{Aut}(G)| = 2^{2m-2}$. Equation (25) follows by the same argument as before. With $a = 2$ and $b = -1$ in $\mathbb{Z}/2^{m+1}\mathbb{Z}$, we have $a^i = 2i$ and $a^j b = -1 - 2j$. Since $\mathrm{Soc}(A) = 4A$, the brace automorphisms are multiplications by elements of the form $1 + 4i$. So we obtain

$$\mathrm{Aut}^\flat(A) = \{\alpha_{1+4i,-2i} \mid i \in \mathbb{Z}/2^{m-1}\mathbb{Z}\}.$$

Since $a^{-1}ba = b(ba^{-1}b)a = ba^{2+2^{m-1}}$, we have

$$\mathrm{Inn}(G) = \langle \alpha_{-1+2^{m-1},0}\rangle \times \langle \alpha_{1,2+2^{m-1}}\rangle \cong C_2 \times C_{2^{m-1}}.$$

Hence $\mathrm{Aut}^\flat(A) \cap \mathrm{Inn}(G) = Z(\mathrm{Aut}(G))$. Together with $|\mathrm{Aut}^\flat(A)| = 2^{m-1}$ and $|\mathrm{Inn}(G)| = 2^m$, this proves Eq. (24). □

Using Proposition 16, we can calculate $\beta_2^H(G)$ simultaneously for all three cases.

Corollary. *Let A be an exceptional cyclic brace with a dihedral, generalized quaternion, or semidihedral adjoint group G. For every subgroup H of G with an abelian factor group, the number $\beta_2^H(G)$ of double cosets $\mathrm{Aut}^H(G)\,\alpha\,\mathrm{Aut}^\flat(A)$ in $\mathrm{Aut}(G)$ is 1.*

Proof. Since $\langle a^2\rangle = G' \subset H$, we have $\mathrm{Inn}(G) \subset \mathrm{Aut}^H(G)$. Thus $\mathrm{Aut}^H(G)\,\alpha\,\mathrm{Aut}^\flat(G) = \mathrm{Aut}(G)$ for all $\alpha \in \mathrm{Aut}(G) = \mathrm{Inn}(G)\,\mathrm{Aut}^\flat(G)$. □

It remains to consider the braces A of type (3b) with adjoint group

$$M_{2^m} := \{a, b \mid a^{2^m} = b^2 = 1,\ bab^{-1} = a^{1+2^{m-1}}\} \qquad (m \geqslant 3)$$

of order 2^{m+1}. By [25], Proposition 10, the brace structure is given by $a = 1$ and $b = -1$, and

$$\mu(1) = \frac{1 + 2^m + 2^{m+1} - (-2)^{m+1}}{3}, \qquad \mu(-1) = -1.$$

To compare with [25], note that $\mu(1)$ is the inverse of $3 + 2^m$ modulo 2^{m+1}. For this "almost commutative" group $G = M_{2^m}$, the subgroup $G' = \langle a^{2^{m-1}} \rangle = \operatorname{Soc}(A)$ is of order 2, and G/G' is of type (1b). The center of G is $\langle a^2 \rangle = 4A$, a brace ideal. The subgroups between G and $\langle a^2 \rangle$ are the cyclic groups $\langle a \rangle$ and $\langle ba \rangle$, and $\langle b, a^2 \rangle \cong C_2 \times C_{2^{m-1}}$. By induction, we find that $b(ba)b^{-1} = ab = ba^{1+2^{m-1}} = (ba)^{1+2^{m-1}}$. Therefore, the replacement of a by ba induces an automorphism of G which maps $\langle a \rangle$ to $\langle ba \rangle$. The following proposition reduces type (3b) to type (1b).

Proposition 17. *Let A be an exceptional cyclic brace with adjoint group $G = M_{2^m}$, and let H be a proper subgroup of G with an abelian factor group. Then $\beta_2^H(G) = \beta_2^{H/G'}(G/G')$.*

Proof. The automorphism group $\operatorname{Aut}(G)$ consists of the elements α_i and β_i with $i \in \{1, \dots, 2^m\}$ which satisfy Eqs. (23) for odd i. Every automorphism of G induces an automorphism of G/G'. So there is a group homomorphism $\operatorname{Aut}(G) \to \operatorname{Aut}(G/G')$. The nontrivial brace automorphism of G/G' does not belong to the image. So the image is the subgroup $\operatorname{Aut}_{\langle b \rangle}(G/G')$ of automorphisms which fix b. This gives a short exact sequence

$$\langle \alpha_{1+2^{m-1}}, \beta_1 \rangle \hookrightarrow \operatorname{Aut}(G) \twoheadrightarrow \operatorname{Aut}_{\langle b \rangle}(G/G').$$

The socle of A is generated by $a^{2^{m-1}} = 2^m$. Therefore, the only nontrivial brace automorphism of A is a multiplication by $1+2^m$. Hence $a = 1$ is mapped to $1+2^m = 1 \circ 2^m = a^{1+2^{m-1}}$, and $b = -1$ is mapped to $-1 - 2^m = -1 + 2^m = (-1) \circ 2^m = ba^{2^{m-1}}$. Thus $\operatorname{Aut}^\flat(A) = \{1, \beta_{1+2^{m-1}}\} \subset \langle \alpha_{1+2^{m-1}}, \beta_1 \rangle = \operatorname{Aut}^{G'}(G) \subset \operatorname{Aut}^H(G)$, which yields $\operatorname{Aut}^H(G)\, \alpha\, \langle \alpha_{1+2^{m-1}}, \beta_1 \rangle = \operatorname{Aut}^H(G)\, \langle \alpha_{1+2^{m-1}}, \beta_1 \rangle\, \alpha = \operatorname{Aut}^H(G)\alpha$ for all $\alpha \in \operatorname{Aut}(G)$. So $\beta_2^H(G) = 2^{m+1} : |\operatorname{Aut}^H(G)|$. Furthermore,

$$\tfrac{1}{4} \cdot \big|\operatorname{Aut}^H(G)\big| = \big|\operatorname{Aut}^{H/G'}(G/G') \cap \operatorname{Aut}_{\langle b \rangle}(G/G')\big|. \tag{26}$$

If $\operatorname{Aut}^{H/G'}(G/G') \subset \operatorname{Aut}_{\langle b \rangle}(G/G')$, the right-hand side of Eq. (26) is equal to

$$\big|\operatorname{Aut}^{H/G'}(G/G')\big| = \tfrac{1}{2} \cdot \big|\operatorname{Aut}^{H/G'}(G/G')\operatorname{Aut}^\flat\big(A/\operatorname{Soc}(A)\big)\big|.$$

Otherwise, it is equal to $\frac{1}{2} \cdot \big|\operatorname{Aut}^{H/G'}(G/G')\big|$, and $a^{2^{m-2}} \in H$, which yields $|\operatorname{Aut}^{H/G'}(G/G')| = |\operatorname{Aut}^{H/G'}(G/G')\operatorname{Aut}^\flat(A/\operatorname{Soc}(A))|$. Thus, in any case,

$$\tfrac{1}{4} \cdot \big|\operatorname{Aut}^H(G)\big| = \tfrac{1}{2} \cdot \big|\operatorname{Aut}^{H/G'}(G/G')\operatorname{Aut}^\flat(A/\operatorname{Soc}(A))\big|.$$

Whence $\beta_2^{H/G'}(G/G') = 2^m : |\operatorname{Aut}^{H/G'}(G/G')\operatorname{Aut}^\flat(A/\operatorname{Soc}(A))| = 2^{m+1} : |\operatorname{Aut}^H(G)|$. □

7. Enumeration of cyclic braces and T-structures

The results of Section 6 enable us to give a complete enumeration of cyclic braces with a given adjoint group. Together with Corollary 2 of Theorem 3, we obtain the following theorem.

Theorem 4. *Let G be a solvable, 2-nilpotent, almost Sylow-cyclic group, with a Sylow p-subgroup P_p for $p \in \pi(G)$. The number of isomorphism classes of cyclic braces with adjoint group G is $\beta(G) = \prod_{p\in\pi(G)} \beta_p(G)$, where $\beta_p(G)$ is given by Eq. (22) for cyclic P_p of length $\geqslant 2$ with $p \notin \pi(G')$. If P_p is cyclic and $p \in \pi(G')$ or $\lambda_p(G) < 2$, then $\beta_p(G) = 1$. If P_p is not cyclic, then $p = 2$, and*

$$\beta_2(G)=\begin{cases} 1 & \text{for } c_2(G) = 0, \\ 1 & \text{for } P_2 \text{ of type } (2a) \text{ or } (2b) \text{ or } (3a), \\ 2 & \text{for } P_2 \text{ of type } (1b) \text{ or } (3b) \text{ with } c_2(G) = 1 \text{ and } (P_2)_G \text{ cyclic,} \\ 2^{c_2(G)-1} & \text{for } P_2 \text{ of type } (1b) \text{ or } (3b) \text{ with } c_2(G) > 1 \text{ or } (P_2)_G \text{ noncyclic.} \end{cases}$$

Example 4. As an illustration, let us consider the braces or order 80, where all possible Sylow 2-subgroups arise. There are 52 groups of order 80, 5 abelian, and 75 non-abelian. Among the 52 groups, 23 admit an affine structure according to Corollary 1 of Theorem 2. Two of them are abelian, and three are Sylow-cyclic. Five of the 23 admissible groups have Sylow 2-subgroups isomorphic to $C_2 \times C_8$, and five of them M_8. The dihedral group D_8 arises 3 times, the generalized quaternion group Q_4 3 times, and the semidihedral group SD_8 4 times.

Let us first consider the three Sylow-cyclic groups. By Corollary 2 of Theorem 3, $C_{80} = C_{16} \times C_5$ admits three nonisomorphic affine structures, while the two semidirect products $C_{16} \ltimes C_5$ give rise to seven braces, four if C_{16} maps onto $\mathrm{Aut}(C_5)$, and three otherwise.

So we are left with the groups G which are not Sylow-cyclic. The products $G = P \times C_5$ with a 2-group P give just one brace [24]. So we get five braces with P of all types except (1a). There are three other decomposable groups, namely, $G = C_8 \times D_5$ and $G = C_2 \times H$, with two semidirect products $H = C_8 \ltimes C_5$. In all three cases, the Sylow 2-subgroup is $C_8 \times C_2$. By Proposition 15, the first case gives two braces. For the semidirect product $H = C_8 \ltimes C_5$ where C_8 maps onto $\mathrm{Aut}(C_5)$, we get two braces, and the other one gives a single brace.

Now let us assume that G is indecomposable. There is another group G with Sylow 2-subgroup of type (1b), a semidirect product $G = C_8 \ltimes D_5$ where C_8 maps to $\mathrm{Aut}(C_5)$. By Proposition 15, this gives two braces.

There are two remaining groups with Sylow 2-subgroup P isomorphic to D_8, namely, the dihedral group D_{40} and a semidirect product $G = D_5 \ltimes D_4$. Furthermore, there are two indecomposable groups with $P \cong Q_4$, and three further groups with $P \cong SD_8$. By the corollary of Proposition 16, each of these groups gives a single brace.

Finally, we have four indecomposable groups G with Sylow 2-subgroup isomorphic to M_8. There are two cases where the image of $M_8 \to \mathrm{Aut}(C_5)$ has order two. The induced map $C_8 \times C_2 \to \mathrm{Aut}(C_5)$ has a cyclic kernel in one case, which yields two braces, and a noncyclic kernel in the other case, which gives a single brace by Proposition 17 (with Proposition 15). For the other two groups, M_8 maps onto $\mathrm{Aut}(C_5)$, each giving two braces. To distinguish the latter two cases, we give an explicit representation of their groups.

In the first case, the group G is

$$G = \langle a, b, c \mid a^8 = b^2 = c^5 = 1, bab^{-1} = a^5, aca^{-1} = c^3, bc = cb \rangle.$$

Thus, $\langle a, b \rangle \cong M_8$, and $\langle c \rangle \cong C_5$. For the action of M_8/M_8' on C_5, the presentation shows that b acts trivially, while a maps to a generator of C_5. The other group is given by

$$G = \langle a, b, c \mid a^4 = d^2, c^5 = d^4 = 1, ada^{-1} = d^{-1}, aca^{-1} = c^3, cd = dc \rangle.$$

Here $\langle a, d | a^4 = d^2, d^4 = 1, ada^{-1} = d^{-1} \rangle$ is isomorphic to M_8, using the substitution $b := da^6$. Again, $\langle c \rangle$ is our normal subgroup C_5. Via $M_8 \to \mathrm{Aut}(C_5)$, the element a is mapped to a generator of C_5, which yields two braces for G.

In total, the above discussion shows that there are 36 cyclic braces of order 80.

Classification of T-structures. It remains to recall the connection between T-structures in the sense of Etingof *et al.* [12] and cyclic braces. A *T-structure* [12] is defined to be an abelian group A with a bijection $T\colon A \to A$ satisfying

$$T(ka) = kT^k(a)$$

for all $a \in A$ and $k \in \mathbb{Z}$. By [12], Theorem A.7, it follows that T-structures on a cyclic group A are equivalent to braces with additive group A. Indeed, if A is a brace, then

$$T(a) := a \cdot a$$

gives a T-structure, and conversely, every T-structure on a cyclic group $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$ defines a brace with

$$k \cdot \ell := \ell\, T^k(1).$$

At the end of the paper [12], the classification of T-structures on a cyclic group is stated as an open question. By Theorem 4, this problem is now solved.

Acknowledgments

We owe thanks to Leandro Vendramin for computer calculations which helped to cross-check the results of this paper.

References

[1] Louis Auslander, *The structure of complete locally affine manifolds*, Topology **3** (1964), no. suppl. 1, 131–139, DOI 10.1016/0040-9383(64)90012-6. MR0161255

[2] Louis Auslander, *Simply transitive groups of affine motions*, Amer. J. Math. **99** (1977), no. 4, 809–826, DOI 10.2307/2373867. MR0447470

[3] L. Auslander and L. Markus, *Holonomy of flat affinely connected manifolds*, Ann. of Math. (2) **62** (1955), 139–151, DOI 10.2307/2007104. MR0072518

[4] David Bachiller, *Classification of braces of order p^3*, J. Pure Appl. Algebra **219** (2015), no. 8, 3568–3603, DOI 10.1016/j.jpaa.2014.12.013. MR3320237

[5] David Bachiller, *Counterexample to a conjecture about braces*, J. Algebra **453** (2016), 160–176, DOI 10.1016/j.jalgebra.2016.01.011. MR3465351

[6] David Bachiller, Ferran Cedó, and Eric Jespers, *Solutions of the Yang-Baxter equation associated with a left brace*, J. Algebra **463** (2016), 80–102, DOI 10.1016/j.jalgebra.2016.05.024. MR3527540

[7] Yves Benoist, *Une nilvariété non affine* (French, with English summary), J. Differential Geom. **41** (1995), no. 1, 21–52. MR1316552

[8] W. Burnside, On finite groups in which all the Sylow subgroups are cyclical, Messenger Math. 35 (1905), 46–50.

[9] Ferran Cedó, Eric Jespers, and Ángel del Río, *Involutive Yang-Baxter groups*, Trans. Amer. Math. Soc. **362** (2010), no. 5, 2541–2558, DOI 10.1090/S0002-9947-09-04927-7. MR2584610

[10] Marston Conder, Primož Potočnik, and Jozef Širáň, *Regular maps with almost Sylow-cyclic automorphism groups, and classification of regular maps with Euler characteristic* $-p^2$, J. Algebra **324** (2010), no. 10, 2620–2635, DOI 10.1016/j.jalgebra.2010.07.047. MR2725192
[11] Xian Kun Du, *The centers of a radical ring*, Canad. Math. Bull. **35** (1992), no. 2, 174–179, DOI 10.4153/CMB-1992-025-0. MR1165165
[12] Pavel Etingof, Travis Schedler, and Alexandre Soloviev, *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Math. J. **100** (1999), no. 2, 169–209, DOI 10.1215/S0012-7094-99-10007-X. MR1722951
[13] P. Hall, *A Note on Soluble Groups*, J. London Math. Soc. **3** (1928), no. 2, 98–105, DOI 10.1112/jlms/s1-3.2.98. MR1574393
[14] P. Hall, *On the Sylow Systems of a Soluble Group*, Proc. London Math. Soc. (2) **43** (1937), no. 4, 316–323, DOI 10.1112/plms/s2-43.4.316. MR1575218
[15] P. Hall, *A Characteristic Property of Soluble Groups*, J. London Math. Soc. **12** (1937), no. 3, 198–200, DOI 10.1112/jlms/s1-12.2.198. MR1575073
[16] I. Martin Isaacs, *Finite group theory*, Graduate Studies in Mathematics, vol. 92, American Mathematical Society, Providence, RI, 2008. MR2426855
[17] Nathan Jacobson, *Structure of rings*, American Mathematical Society Colloquium Publications, Vol. 37. Revised edition, American Mathematical Society, Providence, R.I., 1964. MR0222106
[18] Jiang-Hua Lu, Min Yan, and Yong-Chang Zhu, *On the set-theoretical Yang-Baxter equation*, Duke Math. J. **104** (2000), no. 1, 1–18, DOI 10.1215/S0012-7094-00-10411-5. MR1769723
[19] John Milnor, *On fundamental groups of complete affinely flat manifolds*, Advances in Math. **25** (1977), no. 2, 178–187, DOI 10.1016/0001-8708(77)90004-4. MR0454886
[20] W. Keith Nicholson, *Semiperfect rings with abelian adjoint group*, Pacific J. Math. **54** (1974), 201–207. MR0369430
[21] Derek John Scott Robinson, *A course in the theory of groups*, Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York-Berlin, 1982. MR648604
[22] Wolfgang Rump, *A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation*, Adv. Math. **193** (2005), no. 1, 40–55, DOI 10.1016/j.aim.2004.03.019. MR2132760
[23] Wolfgang Rump, *Modules over braces*, Algebra Discrete Math. **2** (2006), 127–137. MR2320986
[24] Wolfgang Rump, *Braces, radical rings, and the quantum Yang-Baxter equation*, J. Algebra **307** (2007), no. 1, 153–170, DOI 10.1016/j.jalgebra.2006.03.040. MR2278047
[25] Wolfgang Rump, *Classification of cyclic braces*, J. Pure Appl. Algebra **209** (2007), no. 3, 671–685, DOI 10.1016/j.jpaa.2006.07.001. MR2298848
[26] Wolfgang Rump, *Semidirect products in algebraic logic and solutions of the quantum Yang-Baxter equation*, J. Algebra Appl. **7** (2008), no. 4, 471–490, DOI 10.1142/S0219498808002904. MR2442072
[27] Wolfgang Rump, *The brace of a classical group*, Note Mat. **34** (2014), no. 1, 115–144. MR3291816
[28] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York-Heidelberg, 1973. Translated from the French; Graduate Texts in Mathematics, No. 7. MR0344216
[29] Michio Suzuki, *On finite groups with cyclic Sylow subgroups for all odd primes*, Amer. J. Math. **77** (1955), 657–691, DOI 10.2307/2372591. MR0074411
[30] J. F. Watters, *On the adjoint group of a radical ring*, J. London Math. Soc. **43** (1968), 725–729, DOI 10.1112/jlms/s1-43.1.725. MR0229677
[31] W. J. Wong, *On finite groups with semi-dihedral Sylow* 2*-subgroups*, J. Algebra **4** (1966), 52–63, DOI 10.1016/0021-8693(66)90050-0. MR0210779
[32] Hans Zassenhaus, *Über endliche Fastkörper* (German), Abh. Math. Sem. Univ. Hamburg **11** (1935), no. 1, 187–220, DOI 10.1007/BF02940723. MR3069653

Institute for Algebra and Number Theory, University of Stuttgart, Pfaffenwaldring 57, D-70550 Stuttgart, Germany
Email address: rump@mathematik.uni-stuttgart.de