Available online at www.sciencedirect.com
ScienceDirect

Journal of Pure and Applied Algebra 209 (2007) 671–685

JOURNAL OF
PURE AND
APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Classification of cyclic braces

Wolfgang Rump

Institut für Algebra und Zahlentheorie, Universität Stuttgart, Pfaffenwaldring 57, D-70550 Stuttgart, Germany

Received 13 December 2005; received in revised form 17 May 2006
Available online 21 August 2006
Communicated by T. Hibi

Abstract

Etingof, Schedler, and Soloviev have shown [P. Etingof, T. Schedler, A. Soloviev, Set-theoretical solutions to the quantum Yang–Baxter equation, Duke Math. J. 100 (1999) 169–209] that T-structures on cyclic groups come from bijective 1-cocycles and thus give rise to solutions of the quantum Yang–Baxter equation. At the end of their paper, they ask for a classification of T-structures on cyclic groups, especially p-groups. We solve the latter problem by means of generalized radical rings (=braces).

MSC: Primary: 81R50

0. Introduction

Let A be a right module over a group G. Etingof, Schedler, and Soloviev [3] have shown that every bijective 1-cocycle $\pi: G \to A$ (see Section 1) gives rise to a set-theoretical solution of the quantum Yang–Baxter equation (QYBE)

$$R^{12}R^{13}R^{23} = R^{23}R^{13}R^{12}$$

in the sense of Drinfeld [2]. The solutions arising in this way play a key rôle for the study of more general set-theoretical solutions of the QYBE (see [3,7], and the literature cited there). On the other hand, bijective 1-cocycles $\pi: G \to A$ are equivalent to *braces* (see Section 1), i.e. abelian groups A with a right distributive multiplication such that the circle operation

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

makes A into a group, the *adjoint group* A°. Thus every radical ring [5] is a brace, and every commutative brace is a radical ring.

There is some interest in classifying bijective 1-cocycles $\pi: G \to A$, due to their relationship to the QYBE and other mathematical structures. Of course, a general classification is out of reach, even if A is finite. For cyclic A, it is shown in [3] that a bijective 1-cocycle $\pi: G \to A$ is equivalent to a *T-structure*, that is, a bijection $T: A \to A$ such

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

0022-4049/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2006.07.001

that

$$T(ma) = mT^m(a)$$

holds for all $a \in A$ and $m \in \mathbb{Z}$. For $A = \mathbb{Z}$, it is easily seen that there are just two T-structures, namely, $T(n) = n$ and $T(n) = (-1)^n n$. So it is natural to ask for a classification of T-structures on arbitrary cyclic groups. Roughly speaking, this amounts to an analysis of (not necessarily abelian) "deformations" G of A. Note that the 1-cocycle connection with A forces G to be solvable [3]. The question to classify T-structures on cyclic groups, and in particular, cyclic p-groups, was raised at the end of [3] and remained to be open.

In this paper, we provide a complete classification in the p-group case, and give a partial one in the general case, using properties of braces. In terms of braces, the general problem consists in a classification of *cyclic* braces, i.e. braces with a cyclic additive group. Our main result states that for a cyclic brace A with $|A| = p^m$ for some prime p, the adjoint group A° admits a cyclic subgroup of index ≤ 2. Hence A° must be cyclic if $p > 2$. For arbitrary $n = |A|$, we classify the braces with cyclic A° and call them *bicyclic*. Being commutative, every bicyclic brace is a radical ring. Moreover, bicyclic braces are equivalent to linear congruential generators with maximum period, which are well-known in the theory of random numbers [6].

More generally, we classify cyclic braces A with A° abelian (Theorem 1). In Theorem 2, we show that every cyclic brace A is bicyclic or *exceptional* (see Section 5). Thus if $|A| = p^m$ with p prime, we infer that A is bicyclic unless $p = 2$. For $|A| = 2^m$, we classify the exceptional braces A and show that they form an infinite tree (Section 7). Up to isomorphism, the braces of this tree are determined by their adjoint group. Conversely, apart from the cyclic groups of order ≤ 4, every 2-group with a cyclic subgroup of index 2 occurs as the adjoint group of an exceptional cyclic brace.

1. Braces

Let A be an abelian group with a multiplication $A \times A \to A$. We call A a *brace* [8] if A is *right distributive*, i.e.

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

and A is a group with respect to the *circle operation*

$$a \circ b := ab + a + b. \tag{2}$$

Like in the theory of radical rings (see, e.g., [5,10,1]), this group A° is called the *adjoint group* of A. The inverse of an element $a \in A^\circ$ will be denoted by a'. Thus

$$a \circ a' = a' \circ a = 0 \tag{3}$$

holds for all $a \in A$.

A *morphism* between braces is defined to be an additive group homomorphism that respects multiplication. Thus braces form a category **Bra**, and the passage from A to its adjoint group A° is a functor **Bra** → **Grp** into the category of groups. The image of a morphism $f\colon A \to B$ in **Bra** is a *subbrace* of B, i.e. an additive subgroup which is closed under multiplication. The kernel $\operatorname{Ker} f := \{a \in A \mid f(a) = 0\}$ is an *ideal* of A, i.e. an additive subgroup I with $ab \in I$ and $ba \in I$ for all $a \in I$ and $b \in A$. Any ideal I of A gives rise to a morphism $A \to A/I$ onto the *factor brace* $A/I = \{a + I \mid a \in A\}$ with the induced multiplication [8]. In [8] we showed that the *socle*

$$\operatorname{Soc}(A) := \{a \in A \mid \forall b \in A\colon ba = 0\} \tag{4}$$

of a brace A is an ideal.

The associativity of (2) is equivalent to the equation

$$a(b \circ c) = (ab)c + ab + ac. \tag{5}$$

If $R_a \in \operatorname{End}(A)^{\mathrm{op}}$ denotes the right multiplication $x \mapsto xa$ in A, this equation can be written in the form

$$R_{b\circ c} = R_b \circ R_c, \tag{6}$$

where $R_b \circ R_c := R_b R_c + R_b + R_c$.

With the abbreviation

$$a^b := ab + a, \tag{7}$$

using right distributivity, Eq. (5) can also be written as

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

Therefore, every brace A can be regarded as a right A°-module. In fact, Eqs. (1) and (5) also imply that $a^0 = a$ for all $a \in A$. Thus if we replace the multiplication of A by the operation (7) and regard the identical map of A as a bijection $\pi\colon A^\circ \to A$, it follows that the structure of a brace is equivalent to a right module A over a group A° together with a bijection $\pi\colon A^\circ \to A$ satisfying the 1-cocycle condition

$$\pi(a \circ b) = \pi(a)^b + \pi(b). \tag{9}$$

In other words, a brace A is tantamount to a *bijective cocycle datum* in the sense of [3], Definition 2.3. If we regard π as an identification, Eq. (9) reads as

$$a \circ b := a^b + b, \tag{10}$$

which is equivalent to Eq. (2).

Note that $\mathrm{Soc}(A)$ is the kernel of the group homomorphism $\rho\colon A^\circ \to \mathrm{Aut}(A)^{\mathrm{op}}$ which defines the right A°-module structure of A. The factor brace $A/\mathrm{Soc}(A)$ is called the *retraction* of A (cf. [3], 3.2).

By [8], Proposition 5, there is a one-to-one correspondence between braces and linear cycle sets. Recall [7,8] that a *linear cycle set* is defined to be an abelian group A with a multiplication $A \times A \xrightarrow{\cdot} A$ such that the maps $b \mapsto a \cdot b$ are bijective, and

$$a \cdot (b + c) = a \cdot b + a \cdot c \tag{11}$$

$$(a + b) \cdot c = (a \cdot b) \cdot (a \cdot c) \tag{12}$$

holds for all $a, b, c \in A$. The relationship is given by

$$a \cdot b := ba' + b. \tag{13}$$

In what follows, we make no difference between braces and linear cycle sets.

In [3], a *T-structure* is defined to be an abelian group A together with a bijection $T\colon A \to A$ which satisfies

$$T(ma) = mT^m(a) \tag{14}$$

for all $a \in A$ and $m \in \mathbb{Z}$. It is easy to see that every brace A gives rise to a T-structure

$$T(a) := a \cdot a. \tag{15}$$

In fact, $(m + 1)a \cdot a = (ma + a) \cdot a = (ma \cdot a) \cdot (ma \cdot a)$, which gives

$$(m + 1)a \cdot a = T(ma \cdot a). \tag{16}$$

Since $0 \cdot a = a$, this yields $ma \cdot a = T^m(a)$, i.e. (14), by two-fold induction.

We call a brace *cyclic* if its additive group is cyclic. By [3], Theorem A.7, every cyclic brace can be recovered by its T-structure, so that cyclic braces are equivalent to T-structures on cyclic groups C_n. By [3], Proposition 3.7, such T-structures correspond to multipermutation solutions of the quantum Yang–Baxter equation. The problem to classify T-structures on C_n, raised at the end of [3], remained open, even in the case where n is a prime power. A solution of the latter problem will be given in Section 7.

2. The retraction of a cyclic brace

Let A be a cyclic brace. We identify the additive group of A with that of $\mathbb{Z}/n\mathbb{Z}$, where $n = |A|$ if A is finite, and $n = 0$ otherwise. So there is a natural ring multiplication in $A = \mathbb{Z}/n\mathbb{Z}$, which will be indicated by juxtaposition. To avoid confusion, we express the brace multiplication by means of the operation (7). Since every automorphism of the additive group of A is of the form $a \mapsto ac$ with $c \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, the operation (7) is given by a map

$$\mu \colon \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^{\times} \tag{17}$$

such that

$$a^b = a\mu(b). \tag{18}$$

In the following, the residue class $1 + n\mathbb{Z}$, being the unit element of the ring $\mathbb{Z}/n\mathbb{Z}$, will be denoted by 1.

Proposition 1. *Let A be an associative ring with unity. A map $\mu \colon A \to A^{\times}$ makes A into a brace via Eq.* (18) *if and only if*

$$\mu(a\mu(b) + b) = \mu(a)\mu(b) \tag{19}$$

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

Proof. Eq. (19) is equivalent to $\mu(a\mu(b)+b)^{-1} = \mu(b)^{-1}\mu(a)^{-1}$. If we replace a by $a\mu(b)^{-1}$, we get $\mu(a+b)^{-1} = \mu(b)^{-1}\mu(a\mu(b)^{-1})^{-1}$. As A is a unital ring, this means that

$$c\mu(a + b)^{-1} = c\mu(b)^{-1}\mu(a\mu(b)^{-1})^{-1} \tag{20}$$

holds for $a, b, c \in A$. By (18), the product (13) is given by

$$b \cdot a = a\mu(b)^{-1}. \tag{21}$$

Therefore, Eq. (20) is equivalent to (12), while Eq. (11) is a trivial consequence of (21). Thus Eq. (19) states that (21) makes A into a linear cycle set. □

Applying Proposition 1 to $A = \mathbb{Z}/n\mathbb{Z}$, we infer that a map (17) makes A into a cyclic brace via (18) if and only if Eq. (19) holds for $a, b \in A$. Assume this from now on. Then (18) yields

$$\mu(b) = 1^b. \tag{22}$$

We call $\mu \colon A \to A^{\times}$ the *structure map* of A. By Eq. (18), we have

$$\mathrm{Soc}(A) = \mathrm{Ker}\,\mu := \{a \in A \mid \mu(a) = 1\}. \tag{23}$$

Note that by virtue of (10) and (18), Eq. (19) states that $\mu \colon A^{\circ} \to A^{\times}$ is a group homomorphism. As $\mathrm{Soc}(A)$ is an ideal of A, the equivalence $a \in \mathrm{Soc}(A) \Leftrightarrow a^b \in \mathrm{Soc}(A)$ holds for all $b \in A$. Therefore, Eq. (10) implies that the fibers of μ are of the form

$$\mathrm{Soc}(A) \circ b = \mathrm{Soc}(A) + b. \tag{24}$$

Since $|A^{\times}| < |A^{\circ}| = n$ if A is finite, we infer that $\mathrm{Soc}(A) \neq 0$. So there is a non-zero $s \in \mathbb{N}$ with $s \mid n$ such that

$$\mathrm{Ker}\,\mu = s\mathbb{Z}/n\mathbb{Z} \neq 0. \tag{25}$$

Hence μ is determined by the induced injection

$$\nu \colon A/\mathrm{Soc}(A) \cong \mathbb{Z}/s\mathbb{Z} \rightarrowtail (\mathbb{Z}/n\mathbb{Z})^{\times}. \tag{26}$$

In particular, this shows that the adjoint group of $A/\mathrm{Soc}(A)$ is abelian. Since $|(\mathbb{Z}/n\mathbb{Z})^{\times}| = \varphi(n)$, we have $s \mid \varphi(n)$. To include the case $n = 0$, we set

$$\varphi(0) := |\mathbb{Z}^{\times}| = 2. \tag{27}$$

So we get a commutative diagram

$$\begin{tikzcd}
A \arrow[r, "\mu"] \arrow[d, two heads, "q"] & A^{\times} \arrow[d, two heads, "q^{\times}"] \\
A/\mathrm{Soc}(A) \arrow[r, "\overline{\mu}"] \arrow[ur, tail, "\nu"] & (A/\mathrm{Soc}(A))^{\times}
\end{tikzcd} \tag{28}$$

where $\overline{\mu}$ is the structure map of $A/\mathrm{Soc}(A)$, ν embeds $(A/\mathrm{Soc}(A))^{\circ}$ into $A^{\times}$, and $q^{\times}$ is induced by the natural projection q. The following lemma shows that $q^{\times}$ is surjective.

Lemma 1. *Let n, s be positive integers with $s \mid n$. Every surjective ring homomorphism $q\colon \mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/s\mathbb{Z}$ induces a surjection $q^{\times}\colon (\mathbb{Z}/n\mathbb{Z})^{\times} \twoheadrightarrow (\mathbb{Z}/s\mathbb{Z})^{\times}$ between the unit groups.*

Proof. By induction, we can assume that $n = sp$ for a prime p, and that q is the natural ring homomorphism. Thus let $k + s\mathbb{Z}$ be a unit in $\mathbb{Z}/s\mathbb{Z}$. If $p \nmid k$, we can lift $k + s\mathbb{Z}$ to the unit $k + n\mathbb{Z}$. Otherwise, the unit $(k + s) + n\mathbb{Z}$ will do. In fact, if $p \mid k$ and $p \mid k + s$, then $p \mid s$. So k and s would not be relatively prime, in contrast to the assumption. □

Note that Lemma 1 does not hold for $n = 0$. In this case, however, the map $q^{\times}$ in (28) is surjective, too, since $|(A/\mathrm{Soc}(A))^{\times}| = 1$.

Proposition 2. *Let A be a cyclic brace with structure map $\mu\colon A \to A^{\times}$. A map $\mu'\colon A \to A^{\times}$ defines an isomorphic brace if and only if there exists a unit $e \in A^{\times}$ such that $\mu'(a) = \mu(ea)$ for all $a \in A$.*

Proof. The map μ' defines an isomorphic brace if and only if there is an automorphism $f\colon A \to A$ of the additive group which defines an isomorphism $(A, \mu') \to (A, \mu)$ of braces, i.e.

$$f(a\mu'(b)) = f(a^b) = f(a)^{f(b)} = f(a)\mu(f(b))$$

for all $a, b \in A$. This means that there exists a unit $e \in A^{\times}$ with $ea\mu'(b) = ea\mu(eb)$ for $a, b \in A$, i.e. $\mu'(b) = \mu(eb)$ for $b \in A$. □

3. Abelian braces

We call a brace A *abelian* if its adjoint group A° is abelian. The embedding (26) shows that the retraction of a cyclic brace is abelian.

Proposition 3. *Let A be an abelian brace. Then A is a commutative radical ring. If A is finite, it has a natural ring decomposition*

$$A = \prod_{p \text{ prime}} A_p \tag{29}$$

into its primary components $A_p := \{a \in A \mid \exists m \in \mathbb{N}\colon p^m a = 0\}$.

Proof. Eq. (2) shows that A is commutative. Hence A is left distributive. Therefore, Eq. (5) implies that A is associative, and thus a radical ring. If A is finite, its additive group is a torsion group. Then (29) follows since the A_p are ideals of A. □

Using Proposition 1, we get a very simple and explicit characterization of abelian cyclic braces.

Theorem 1. *Let $n, d \in \mathbb{N}$ be given such that $p \mid d \mid n$ for each prime divisor p of n. Then*

$$\mu(a) := 1 + ad \tag{30}$$

is the structure map of an abelian cyclic brace $A = \mathbb{Z}/n\mathbb{Z}$, where $d = |\mathrm{Soc}(A)|$ if A is finite, and $d = 0$ otherwise. Up to isomorphism, every abelian cyclic brace arises in this way.

Proof. We have $\mu(a\mu(b)+b) = 1+(a(1+bd)+b)d = (1+ad)(1+bd) = \mu(a)\mu(b)$ for $a, b \in A$, which proves Eq. (19). The condition that every prime divisor of n divides d implies that $1 + Ad \subset A^\times$. Hence μ makes A into a cyclic brace by Proposition 1. Furthermore, Eq. (30) yields $a \circ b = a\mu(b)+b = a+abd+b = b\circ a$ for all $a, b \in A$. By Eq. (30), we have $\operatorname{Ker}\mu = \{a \in A \mid ad = 0\}$. Therefore, Eq. (23) implies that $d = |\mathrm{Soc}(A)|$ if A is finite. If $n = 0$, the condition $p \mid d \mid n$ for all p gives $d = 0$.

Conversely, let $A = \mathbb{Z}/n\mathbb{Z}$ be an abelian cyclic brace with structure map $\mu\colon A \to A^\times$. Assume that $\mu(1) = (d+1)+n\mathbb{Z}$. Then $a(d+1)+1 = a\circ 1 = 1\circ a = \mu(a)+a$ for all $a \in A$, whence (30) holds. By Lemma 1 and Proposition 2, we can modify μ such that $d \mid n$. Since $\mu(A) \subset A^\times$, we have $1 + Ad \subset A^\times$. Suppose that there is a prime divisor p of n which does not divide d. Then we find an integer k such that $p \mid 1 - kd$, a contradiction. Hence A is of the desired form. □

Corollary. *There is a one-to-one correspondence between abelian cyclic braces $A = \mathbb{Z}/n\mathbb{Z}$ and divisors $d \in \mathbb{N}$ of n such that $p \mid d$ for each prime divisor p of n.*

We call d the *socle order* of A. Let $\alpha(n)$ denote the number of isomorphism classes of abelian cyclic braces A with $|A| = n$. Theorem 1 shows that the number-theoretic function α is *multiplicative*, i.e.

$$\alpha(mn) = \alpha(m)\alpha(n) \tag{31}$$

for relatively prime positive integers m, n.

Remark. By Proposition 3, an abelian cyclic brace is tantamount to a commutative radical ring A with a cyclic additive group. In terms of the socle order d, the brace multiplication $a * b := a^b - a$ in A has a very simple description. By Eq. (30), we have $a^b = a\mu(b) = a(1+bd)$. Hence

$$a * b = abd. \tag{32}$$

In particular, if $d = 0$ or $d = |A| < \infty$, then (32) yields $a * b = 0$ for all $a, b \in A$. More generally, every abelian group A gives rise to a radical ring A with zero multiplication. Thus A is an abelian brace where A° coincides with the additive group. We call such a brace *trivial*.

Lemma 2. *The equivalence*

$$2^{m+1} \mid k \;\Leftrightarrow\; 2^{m+3} \mid 3^k - 1 \tag{33}$$

holds for $m, k \in \mathbb{N}$.

Proof. We use the abbreviation $2^m \parallel k$ to state that $2^m \mid k$ but $2^{m+1} \nmid k$. If k is odd, then $3^k \equiv (-1)^k \equiv -1 \pmod 4$, which implies that $8 \nmid 3^k - 1$. Therefore, the reverse implication "$\Leftarrow$" in (33) is valid for $m = 0$. So it suffices to prove the implication

$$2^m \parallel k \;\Rightarrow\; 2^{m+2} \parallel 3^k - 1$$

for $k, m \in \mathbb{N}$ with $m \geq 1$. We proceed by induction on m.

Assume that $2^m \parallel k$. Then $k = 2l$ for some $l \in \mathbb{N}$. Hence $3^k - 1 = (3^l+1)(3^l-1)$. If $m = 1$, then l is odd. Therefore, $3^2 \equiv 1 \pmod 8$ implies that $3^l \equiv 3 \pmod 8$. This gives $4 \parallel 3^l + 1$ and $2 \parallel 3^l - 1$, whence $2^3 \parallel 3^k - 1$. Thus let $m > 1$. Then l is even, which yields $2 \parallel 3^l + 1$. Furthermore, the inductive hypothesis gives $2^{m+1} \parallel 3^l - 1$. Whence $2^{m+2} \parallel 3^k - 1$. □

For an element a of a brace A, and $k \in \mathbb{N}$, let $a^{\circ k}$ denote the k-fold product $a \circ \cdots \circ a$.

Proposition 4. *Let $A = \mathbb{Z}/2^m\mathbb{Z}$ be an abelian cyclic brace with $m \geq 2$ and $|\mathrm{Soc}(A)| = 2$. Then A° is a product $\langle 1\rangle \times \langle -1\rangle$ of cyclic subgroups of order 2^{m-1} and 2, respectively. Furthermore, the elements of the subgroup $\langle 1\rangle$ belong to the residue classes $4\mathbb{Z}$ and $1 + 4\mathbb{Z}$.*

Proof. By Theorem 1, we can assume that the structure map $\mu\colon A \to A^\times$ satisfies Eq. (30). Then $a\circ 1 = a\mu(1)+1 = 3a+1$. Hence $1^{\circ k} = \frac{1}{2}(3^k - 1) + 2^m\mathbb{Z}$ for all $k \in \mathbb{N}$. By Lemma 2, this shows that 1 is of order 2^{m-1} in A°. Since $\mu(-1) = -1$, we get $(-1)\circ(-1) = (-1)(-1) - 1 = 0$, whence $-1 \in A^\circ$ is of order 2. Modulo 4, the elements $1^{\circ k} = (1 + 3 + \cdots + 3^{k-1}) + 2^m\mathbb{Z}$ cover the residue classes $4\mathbb{Z}$ and $1 + 4\mathbb{Z}$. Since $a \circ (-1) = a(-1) - 1 = -a - 1$, this shows that 1 and -1 generate the whole group A°. □

Remark. By Theorem 1 and Eq. (32), the successive retractions of an abelian cyclic brace A_m with $|A_m| = 2^m$ and $|\mathrm{Soc}(A_m)| = 2$ form a sequence

$$A_m \twoheadrightarrow A_{m-1} \twoheadrightarrow A_{m-2} \twoheadrightarrow \cdots \twoheadrightarrow A_2 \twoheadrightarrow A_1 \twoheadrightarrow A_0$$

with $|A_k| = 2^k$ for $k \in \{0, \ldots, m\}$. In this sequence, only A_0° and A_1° are cyclic.

4. Cocyclic residue classes

In this section, we classify cyclic braces A with cyclic adjoint group A°. We call such braces A *bicyclic*.

Lemma 3. *Let $A = \mathbb{Z}/n\mathbb{Z}$ be a cyclic brace with structure map $\mu\colon A \to A^\times$. Then*

$$e^{\circ k} = e(1 + \mu(e) + \mu(e)^2 + \cdots + \mu(e)^{k-1}) \tag{34}$$

holds for all $e \in A$ and $k \in \mathbb{N}$.

Proof. This follows easily by induction on k. □

Definition 1. Let n be a positive integer. We call a residue class $c \in \mathbb{Z}/n\mathbb{Z}$ *cocyclic* if

$$1 + c + c^2 + \cdots + c^{n-1} = 0 \tag{35}$$

and the map

$$\pi_c\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \tag{36}$$

given by

$$\pi_c(k + n\mathbb{Z}) := 1 + c + c^2 + \cdots + c^{k-1} \tag{37}$$

for positive integers k is bijective.

Note that Eq. (35) implies that

$$1 + c + c^2 + \cdots + c^{k+n-1} = 1 + c + c^2 + \cdots + c^{k-1}$$

holds for all $k \in \mathbb{N}$. Hence π_c is well-defined. Furthermore, Definition 1 yields $c \in (\mathbb{Z}/n\mathbb{Z})^\times$. For example, $c = 1$ is always cocyclic and leads to the trivial permutation π_1.

The following table shows that $5 + 16\mathbb{Z}$ is cocyclic. (The residue class $k + 16\mathbb{Z}$ is abbreviated by k.)

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
5^k	5	9	13	1	5	9	13	1	5	9	13	1	5	9	13	1
$\pi_5(k)$	1	6	15	12	13	2	11	8	9	14	7	4	5	10	3	0

Here 5 is of order 4 modulo 16. Similarly, $9 + 16\mathbb{Z}$ is cocyclic of order 2, and $13 + 16\mathbb{Z}$ is cocyclic of order 4. These are the only cocyclic residue classes in $\mathbb{Z}/16\mathbb{Z}$.

Remark. For $a, b \in \mathbb{Z}/n\mathbb{Z}$ with $b = k + n\mathbb{Z}$, the map (37) satisfies an equation

$$\pi_c(a + b) = \pi_c(a)c^k + \pi_c(b) \tag{38}$$

which shows that π_c is a bijective 1-cocycle. Conversely, it is easy to verify that every bijective 1-cocycle $\pi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is of the form $\pi = e\pi_c$ for some cocyclic $c \in \mathbb{Z}/n\mathbb{Z}$ and $e \in (\mathbb{Z}/n\mathbb{Z})^\times$.

The identity

$$(1 + c + c^2 + \cdots + c^{n-1})(c - 1) = c^n - 1 \tag{39}$$

shows that a cocyclic $c \in \mathbb{Z}/n\mathbb{Z}$ satisfies $c^n = 1$. Therefore, the order of c divides n and $\varphi(n)$.

Lemma 4. *Let p be a rational prime and $0 \neq d \in \mathbb{Z}$ such that $p \mid d$ if $p > 2$ and $4 \mid d$ if $p = 2$. Then the equivalence*

$$p^m \,\Bigg|\, \frac{(1+d)^k - 1}{d} \iff p^m \mid k \tag{40}$$

holds for all $m, k \in \mathbb{N}$.

Proof. We embed $\mathbb{Z}$ into the ring $\mathbb{Z}_p$ of p-adic integers. Let $v\colon \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ denote the exponential valuation with $v(p) = 1$. Then it suffices to prove the equation

$$v\left(\frac{(1+d)^k - 1}{d}\right) = v(k).$$

Now [9] II, Lemma 3.2, implies that $(1+d)^k = 1 + a$ with $v(a) = v(d) + v(k)$. This proves the claim. □

Let $A = \mathbb{Z}/n\mathbb{Z}$ be a bicyclic brace with structure map μ and $0 < n \in \mathbb{N}$. Then A° is generated by some $e \in A$, i.e. $A = \{e, e^{\circ 2}, \dots, e^{\circ n}\}$. Therefore, Lemma 3 implies that $e \in (\mathbb{Z}/n\mathbb{Z})^\times$, and that $c := \mu(e)$ is cocyclic. Furthermore, $\mu(e^{\circ k}) = \mu(e)^k = c^k$ for all k. By Eq. (34) and Proposition 2, the isomorphism class of A does not change if we modify the structure map μ by the constant e, which yields

$$\mu(1 + c + c^2 + \dots + c^{k-1}) = c^k \tag{41}$$

for $k \in \{1, \dots, n\}$. Note that Eq. (41) defines the structure map of a bicyclic brace with $\mu(1) = c$ whenever c is cocyclic. Thus we obtain the first statement (a) of the following

Proposition 5. *Let n be a positive integer.*

(a) *Every cocyclic residue class $c \in \mathbb{Z}/n\mathbb{Z}$ defines a bicyclic brace $A = \mathbb{Z}/n\mathbb{Z}$ via (41). Up to isomorphism, every finite bicyclic brace arises in this way.*

(b) *Let $A = \mathbb{Z}/n\mathbb{Z}$ be a finite bicyclic brace with socle order d. Then $1 + A^\times d$ is the set of cocyclic residue classes which define A via (41).*

(c) *Two cocyclic residue classes $c, c' \in \mathbb{Z}/n\mathbb{Z}$ define isomorphic bicyclic braces if and only if they generate the same subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. (b) Let $c \in A$ be a cocyclic residue class which defines A. Then Eqs. (39) and (41) show that $\mu(a) = 1 + a(c-1)$ for all $a \in A$. Hence Theorem 1 and Proposition 2 imply that $c \in 1 + A^\times d$. Conversely, every $c' \in 1 + A^\times d$ is of the form $c' = 1 + e(c-1)$ with $e \in A^\times$. Since $c = r + n\mathbb{Z}$ is cocyclic, we have

$$e = 1 + c + \dots + c^{l-1} = \frac{r^l - 1}{r - 1} + n\mathbb{Z}$$

for some $l \in \mathbb{N}$. Therefore, we get $c' = c^l$. We show that l is relatively prime to n. By Theorem 1, every prime divisor p of n divides $r - 1$. If $p > 2$, then Lemma 4 implies that $p \nmid l$. In case $p = 2$, suppose that $l = 2m$ with $m \in \mathbb{N}$. Then $e = (c^m + 1)(1 + c + \dots + c^{m-1})$, where $c^m + 1 \in 2A$, a contradiction. Hence l is relatively prime to n. Thus

$$\frac{r^{lk} - 1}{r^l - 1} + n\mathbb{Z} = \frac{r^{lk} - 1}{r - 1} e^{-1} + n\mathbb{Z}$$

runs through $\mathbb{Z}/n\mathbb{Z}$ for $k \in \{1, \dots, n\}$, i.e. c^l is cocyclic.

(c) We have shown that every cocyclic residue class that defines A is of the form c^l with l coprime to n, i.e. c and c^l generate the same subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. We also have proved that such c^l are cocyclic. □

Proposition 5 shows that for a finite bicyclic brace A with socle order d, there is a canonical choice $c := (d+1) + n\mathbb{Z}$ of a cocyclic residue class which defines A. Therefore, the determination of all cocyclic residue classes is equivalent to the classification of the finite bicyclic braces.

Proposition 6. *An abelian cyclic brace $A = \mathbb{Z}/n\mathbb{Z}$ with $n \in \mathbb{N}$ is bicyclic if and only if its socle order d satisfies $4 \mid d$ whenever $4 \mid n$.*

Proof. Let $\mu: A \to A^\times$ be the structure map. Assume first that A is infinite. By Eqs. (23) and (24), there are only two cases to consider.

Case 1. $\operatorname{Ker}\mu = \mathbb{Z}$. Then $k \circ l = k + l$ for all $k, l \in \mathbb{Z}$. This brace is bicyclic with $d = 0$.

Case 2. $\operatorname{Ker}\mu = 2\mathbb{Z}$. Then

$$\mu(l) := (-1)^l \tag{42}$$

for all $l \in \mathbb{Z}$. In fact, this gives a brace since Eq. (19) is satisfied. Here

$$k \circ l = k(-1)^l + l, \tag{43}$$

which shows that this cyclic brace is non-abelian.

Now let n be finite. By Proposition 3, we can assume that $n = p^m$ with p prime. If the implication $4 \mid n \Rightarrow 4 \mid d$ is not satisfied, then $p = d = 2$ and $m \geq 2$. Thus A is not bicyclic by Proposition 4. Conversely, assume that $n > 2$, and $4 \mid d$ in case $p = 2$. With $c := (d + 1) + n\mathbb{Z}$, Lemma 4 implies that $\pi_c(a) = 0 \Leftrightarrow a = 0$ for all $a \in A$. Hence if $\pi_c(a + b) = \pi_c(b)$, then (38) yields $\pi_c(a) = 0$, and thus $a = 0$. This shows that c is cocyclic, whence A is bicyclic by Proposition 5. □

The following corollary is an immediate consequence of Propositions 5 and 6.

Corollary. *Let n be a positive integer. A residue class $c = r + n\mathbb{Z}$ is cocyclic if and only if the implications*

$$p \mid n \Rightarrow p \mid r - 1, \qquad 4 \mid n \Rightarrow 4 \mid r - 1 \tag{44}$$

hold for all rational primes p.

Remark. Stefan Kohl brought to our attention that cocyclic residue classes arise in the theory of random numbers. Let n be a positive integer and $c = r + n\mathbb{Z}$. A recursive formula

$$x_0 = 0, \qquad x_{k+1} = cx_k + 1 \tag{45}$$

in $\mathbb{Z}/n\mathbb{Z}$ is known as a *linear congruential generator*. Knuth has shown [6] that the sequence (x_k) has full period n if and only if the implications (44) hold for all primes p. In fact, if we regard $\mathbb{Z}/n\mathbb{Z}$ as a bicyclic brace given by the cocyclic residue class c, then (43) just says that $x_{k+1} = x_k \circ 1$, whence $x_k = 1^{\circ k}$ for all k.

Cocyclic residue classes have nice arithmetical properties, accordant with the properties of braces. For a positive integer n, we denote the set of cocyclic residue classes in $\mathbb{Z}/n\mathbb{Z}$ by $B(n)$.

Proposition 7. *Let n be a positive integer.*

(a) *Every surjective ring homomorphism $\mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}$ maps $B(n)$ into $B(m)$.*
(b) *If $c \in \mathbb{Z}/n\mathbb{Z}$ is cocyclic and $a \in \mathbb{Z}/n\mathbb{Z}$, then a and $\pi_c(a)$ generate the same subgroup of $\mathbb{Z}/n\mathbb{Z}$.*
(c) *$B(n)$ is a cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.*
(d) *If $n = n_1 n_2$ with $n_1, n_2 \in \mathbb{N}$ relatively prime, then $B(n) \cong B(n_1) \times B(n_2)$.*

Proof. (a) follows by the corollary of Proposition 6, and (b) is a consequence of the same corollary together with Lemma 4. Now let $n = n_1 n_2$ be a factorization of n into relatively prime integers $n_i \in \mathbb{N}$. Then (a) implies that the natural isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times$$

induces an embedding

$$\varepsilon: B(n) \hookrightarrow B(n_1) \times B(n_2)$$

which is bijective by the corollary of Proposition 6. Furthermore, the same corollary implies that $B(p^m)$ is a cyclic subgroup of $(\mathbb{Z}/p^m\mathbb{Z})^\times$ for any prime p, and the order of $B(p^m)$ is a power of p. Hence (c) and (d) follow. □

Remark. Proposition 7 shows that the number-theoretic function $\beta(n) := |B(n)|$ is multiplicative. For a rational prime p, the implication (44) yields

$$\beta(p^m) = \begin{cases} p^{m-1} & \text{for } p > 2 \\ 2^{m-2} & \text{for } p = 2 \end{cases}$$

whenever $p^m > 2$.

Corollary 1. *Let n be a positive integer. Then*

$$B(n) = \{c \in \mathbb{Z}/n\mathbb{Z} \mid \beta(n)(c-1) = 0\}. \tag{46}$$

Proof. Since β is multiplicative, we can assume, without loss of generality, that $n = p^m$ for some prime p. If $c = r + p^m\mathbb{Z}$, then Eq. (46) states that $c \in B(p^m) \Leftrightarrow r \equiv 1 \pmod{d}$, where $d := p^m/\beta(p^m)$. Therefore, Eq. (46) follows immediately by (44). □

Corollary 2. *Let $A = \mathbb{Z}/n\mathbb{Z}$ with $n \in \mathbb{N}$ be a finite cyclic brace with structure map $\mu\colon A \to A^\times$. Then A is bicyclic if and only if $\mu(1) \in B(n)$. If A is bicyclic with socle order d, then $\mu(A^\times)$ is the set of cocyclic residue classes which define A.*

Proof. If A is bicyclic, then Theorem 1 and Proposition 5(b) imply that $\mu(A^\times) = 1 + A^\times d$, the set of cocyclic residue classes which define A. Conversely, assume that $c := \mu(1) \in B(n)$. Then every element $a \in A$ is of the form $a = 1 + c + \cdots + c^{k-1}$ for some $k \in \{1, \dots, n\}$. By Lemma 3, we have $a = 1^{\circ k}$. Hence A is bicyclic. □

5. The non-exceptional case

Let $A = \mathbb{Z}/n\mathbb{Z}$ be a finite cyclic brace with $|A/\mathrm{Soc}(A)| = s$. We call A *exceptional* if A is non-trivial, i.e. $s \neq 1$, and $(s+1) + n\mathbb{Z} \notin B(n)$ when $A/\mathrm{Soc}(A)$ is bicyclic. Otherwise, we call A *non-exceptional*. Proposition 6 yields the following

Theorem 2. *Every non-exceptional finite cyclic brace is bicyclic.*

Proof. Assume that $A = \mathbb{Z}/n\mathbb{Z}$ is non-exceptional with $n \in \mathbb{N}$ positive and $|A/\mathrm{Soc}(A)| = s$. If A is trivial, then A is bicyclic. Thus let A be non-trivial. Then $A/\mathrm{Soc}(A)$ is bicyclic, $s \mid n$, and $(s+1) + n\mathbb{Z} \in B(n)$. Let d be the socle order of $A/\mathrm{Soc}(A)$, and $\bar{c} := (d+1) + s\mathbb{Z}$. Consider the commutative diagram (28). Then $\overline{\mu}$ can be modified to a map $\bar{\bar{\mu}}$ which satisfies Eq. (37), i.e.

$$\bar{\bar{\mu}}(1 + \bar{c} + \bar{c}^2 + \cdots + \bar{c}^{k-1}) = \bar{c}^k \tag{47}$$

for $k \in \{1, \dots, s\}$. So there is a unit $\bar{e} \in (A/\mathrm{Soc}(A))^\times$ with $\bar{\bar{\mu}}(a) = \bar{\mu}(ea)$ for all $a \in A/\mathrm{Soc}(A)$. By Lemma 1, the unit $\bar{e}$ can be lifted to a unit $e \in A^\times$, i.e. $q(e) = \bar{e}$. Therefore, diagram (28) remains valid if we replace μ by $a \mapsto \mu(ea)$ and $\overline{\mu}$ by $\bar{\bar{\mu}}$, i.e. we can assume without loss of generality that $\overline{\mu}(1) = \bar{c}$. If we set $c := \mu(1) = r + n\mathbb{Z}$, we thus get $q^\times(c) = \overline{\mu}q(1) = \overline{\mu}(1) = \bar{c}$. Since $A/\mathrm{Soc}(A)$ is bicyclic, Proposition 5 implies that $\bar{c} \in B(s)$.

Furthermore, as $(s+1) + n\mathbb{Z}$ is cocyclic, the corollary of Proposition 6 yields $p \mid n \Rightarrow p \mid s \Rightarrow p \mid r - 1$ for p prime or $p = 4$. Therefore, we get $c \in B(n)$. Hence A is bicyclic by Corollary 2 of Proposition 7. □

Corollary. *For an odd prime p, every cyclic brace A with $|A| = p^m$ is bicyclic.*

Proof. By Proposition 6, the retraction of A is bicyclic. Therefore, the corollary of Proposition 6 implies that A is non-exceptional. Hence A is bicyclic by Theorem 2. □

Example. Let $\nu\colon \mathbb{Z}/3\mathbb{Z} \rightarrowtail (\mathbb{Z}/21\mathbb{Z})^\times$ be the injective group homomorphism with $\nu(1) := 16 + 21\mathbb{Z}$, and let $q\colon \mathbb{Z}/21\mathbb{Z} \twoheadrightarrow \mathbb{Z}/3\mathbb{Z}$ denote the natural ring epimorphism. Then $\mu := \nu q$ is the structure map of a cyclic brace $A = \mathbb{Z}/21\mathbb{Z}$ with $|\mathrm{Soc}(A)| = 7$. So the retraction of A is bicyclic, but $4 + 21\mathbb{Z}$ is not cocyclic. Thus A is exceptional, and Theorem 2 does not apply. Since $3 \mid 21$, but $3 \nmid 7$, Theorem 1 shows that A is not abelian.

6. Primary cyclic braces

From now on, we consider cyclic braces A with $|A| = p^m$ for some prime p. We call them *primary cyclic*. By the corollary of Theorem 2, such braces are bicyclic for $p > 2$. Therefore, we focus our attention upon the case $p = 2$. If A is not bicyclic, it is exceptional by Theorem 2. So the retraction $A/\mathrm{Soc}(A)$ is either not bicyclic or $|A/\mathrm{Soc}(A)| = 2$. The following definition comprises the latter case.

Definition 2. Let $A = \mathbb{Z}/n\mathbb{Z}$ be a cyclic brace with structure map $\mu\colon A \to A^\times$. We call A *involutive* if there exists an element $c \in A^\times$ of order 2 such that

$$\mu(k + n\mathbb{Z}) = c^k \tag{48}$$

for all $k \in \mathbb{Z}$. We call c the *characteristic class* of A.

For example, the non-abelian infinite cyclic brace is involutive. By Proposition 2, the characteristic class c is an invariant of the isomorphism class of A. Furthermore, Eq. (48) implies that $\mathrm{Soc}(A) = \mathrm{Ker}\,\mu$ is of index 2 in A. Hence n must be even.

Proposition 8. *For a given $n \in \mathbb{N}$ with $2 \mid n$, any $c \in (\mathbb{Z}/n\mathbb{Z})^\times$ of order 2 defines an involutive brace $A = \mathbb{Z}/n\mathbb{Z}$ via (48). A is abelian if and only if $c = (1 + \frac{n}{2}) + n\mathbb{Z}$.*

Proof. Assume that $c = r + n\mathbb{Z}$. Since n is even, r must be odd. This implies that $c^r = c$, whence Eq. (19) is satisfied. Thus Eq. (48) defines an involutive brace $A = \mathbb{Z}/n\mathbb{Z}$. For even residue classes $a, b \in A$, we have $a \circ b = a + b = b \circ a$.

Thus let a be even and b odd. Then $a \circ b = ac + b$ and $b \circ a = b + a$. Hence $a \circ b = b \circ a$ is equivalent to $ac = a$. If a and b are both odd, the same equation yields $(a - b)c = a - b$. Therefore, A is abelian if and only if $2(c - 1) = 0$, i.e. $\frac{n}{2} \mid r - 1$. Since c is of order 2, this means that $c = (1 + \frac{n}{2}) + n\mathbb{Z}$. □

Remark. Note that the residue class $c = (1 + \frac{n}{2}) + n\mathbb{Z}$ is of order 2 in $(\mathbb{Z}/n\mathbb{Z})^\times$ if and only if $4 \mid n \neq 0$.

Corollary. *Every abelian involutive brace A with $|A|$ divisible by 8 is bicyclic.*

Proof. Assume that $n = 2^m n'$ with $m \geq 3$ and n' odd. Since $A = \mathbb{Z}/n\mathbb{Z}$ is abelian, Proposition 8 implies that $c = r + n\mathbb{Z}$ with $r = 1 + 2^{m-1}n'$. By Corollary 2 of Proposition 7, we have to verify that c is cocyclic. By Proposition 7, this means that $r + 2^m\mathbb{Z}$ and $r + n'\mathbb{Z}$ are cocyclic. Since $m \geq 3$, this follows by the corollary of Proposition 6. □

Remark. The corollary does not hold without the condition $8 \mid n$. In fact, the involutive brace with characteristic class $3 + 4\mathbb{Z}$ is abelian, but its adjoint group is the Klein Four group.

Next we consider exceptional primary cyclic braces A for which the retraction is not bicyclic.

Definition 3. Let $A = \mathbb{Z}/n\mathbb{Z}$ be a cyclic brace with structure map $\mu\colon A \to A^\times$. We call A *semi-involutive* if there exists an element $c \in A^\times$ of order 2 such that $c \neq -1$ and

$$\mu(k + n\mathbb{Z}) = \begin{cases} 1 & \text{if } k \equiv 0 \pmod 4 \\ c & \text{if } k \equiv 1 \pmod 4 \\ -c & \text{if } k \equiv 2 \pmod 4 \\ -1 & \text{if } k \equiv 3 \pmod 4. \end{cases} \tag{49}$$

We call c the *characteristic class* of A.

Since $c \neq -1$, we have $-1 \neq 1$, which shows that $\mathrm{Soc}(A)$ is of index 4 in A. Hence $4 \mid n$. If $c = r + n\mathbb{Z}$, then $r \equiv \pm 1 \pmod 4$. By diagram (28) and Proposition 1, the structure map $\overline{\mu}\colon B \to B^\times$ of the retraction $B := A/\mathrm{Soc}(A) \cong \mathbb{Z}/4\mathbb{Z}$ satisfies $\overline{\mu}(1\overline{\mu}(1) + 1) = \overline{\mu}(1)^2$, which gives $\overline{\mu}((r + 1) + 4\mathbb{Z}) = r^2 + 4\mathbb{Z} = 1$. Hence $r + 1 \equiv 0 \pmod 4$, i.e.

$$r \equiv 3 \pmod 4. \tag{50}$$

Therefore, Definition 3 implies that $A/\mathrm{Soc}(A)$ is involutive but not bicyclic.

The characteristic class c is an invariant of the isomorphism class of A. In fact, if μ is replaced by $a \mapsto \mu(ea)$ for a unit e, then e belongs to $1 + 4\mathbb{Z}$ or $3 + 4\mathbb{Z}$. In the first case, c remains the same, while in the second case, $\mu(1) = -1$, which cannot be a characteristic class. In analogy to Proposition 8, we have

Proposition 9. *For a given $n \in \mathbb{N}$ with $4 \mid n$, any $c = r + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ of order 2 with $c \neq -1$ and $r \equiv 3$ (mod 4) defines a semi-involutive brace A via (49). Up to isomorphism, the semi-involutive brace with characteristic class $3 + 8\mathbb{Z}$ is the only one which is abelian.*

Proof. By (49), $\mu: A \to A^{\times}$ induces a map $\nu: \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^{\times}$. Thus according to Proposition 1, we have to verify the equation

$$\nu(a(-1)^b + b) = \nu(a)\nu(b), \tag{51}$$

where $a, b \in \mathbb{Z}/4\mathbb{Z}$, and $(-1)^{k+4\mathbb{Z}} := (-1)^k$. If we regard $\mathbb{Z}/4\mathbb{Z}$ as an involutive brace B with characteristic class $3 + 4\mathbb{Z}$, then $a \circ b = a(-1)^b + b$, and Eq. (51) just says that ν defines a group homomorphism $B^{\circ} \to (\mathbb{Z}/n\mathbb{Z})^{\times}$. Therefore, Eq. (51) holds since B° is the Klein Four group. So we have shown that μ makes $\mathbb{Z}/n\mathbb{Z}$ into a semi-involutive brace.

Now assume that $A = \mathbb{Z}/n\mathbb{Z}$ is abelian. Then $1 \circ (-1) = 1(-1) - 1$ and $(-1) \circ 1 = -c + 1$. Hence $c = 3 + n\mathbb{Z}$. Therefore, $c^2 = 1$ implies that $n = 8$. By Theorem 1, this brace is abelian, as it satisfies Eq. (30) with $d = 2$. □

Now we turn our attention to the case $|A/\mathrm{Soc}(A)| \geq 8$.

Proposition 10. *Let $m \geq 4$ be an integer. Up to isomorphism, there is exactly one non-abelian cyclic brace $A = \mathbb{Z}/2^m\mathbb{Z}$ such that $A/\mathrm{Soc}(A)$ is not bicyclic and $|A/\mathrm{Soc}(A)| \geq 8$. It satisfies $|\mathrm{Soc}(A)| = 2$, and its structure map is given by*

$$\mu(1) = (3 + 2^{m-1}) + 2^m\mathbb{Z}, \qquad \mu(-1) = -1 + 2^m\mathbb{Z}. \tag{52}$$

Proof. Assume that $A = \mathbb{Z}/2^m\mathbb{Z}$ is cyclic, such that $A/\mathrm{Soc}(A)$ is not bicyclic, and $|A/\mathrm{Soc}(A)| = 2^s \geq 8$. By diagram (28), μ induces a group monomorphism $\nu: (A/\mathrm{Soc}(A))^{\circ} \rightarrowtail (\mathbb{Z}/2^m\mathbb{Z})^{\times}$, and $\mu = \nu q$. By Propositions 4 and 6, $A/\mathrm{Soc}(A)$ is a product $\langle 1 \rangle \times \langle -1 \rangle$ of cyclic subgroups, where $\langle -1 \rangle$ is of order 2. On the other hand, $(\mathbb{Z}/2^m\mathbb{Z})^{\times} = \{\pm 1\} \times \langle 5 + 2^m\mathbb{Z} \rangle$. Since $5 + 2^m\mathbb{Z}$ is of order 2^{m-2}, the element

$$u := 5^{2^{m-s-1}} + 2^m\mathbb{Z} \in (\mathbb{Z}/2^m\mathbb{Z})^{\times} \tag{53}$$

is of order 2^{s-1}. Therefore,

$$\{\pm u, \pm u^3, \pm u^5, \ldots, \pm u^{2^{s-1}-1}\} \subset (\mathbb{Z}/2^m\mathbb{Z})^{\times} \tag{54}$$

is a complete list of elements of order 2^{s-1}, and the elements of order 2 are -1 and $\pm u^{2^{s-2}}$. Thus $\nu(1)$ belongs to the list (54), while $\nu(-1)$ is of order 2. By Lemma 1, we can modify μ by a unit according to Proposition 2 such that $\overline{\mu}: A/\mathrm{Soc}(A) \to (A/\mathrm{Soc}(A))^{\times}$ satisfies Eq. (30). Since $A/\mathrm{Soc}(A)$ is not bicyclic, Proposition 6 implies that

$$\overline{\mu}(a) = 1 + 2a \tag{55}$$

for all $a \in A/\mathrm{Soc}(A)$. In particular, $\overline{\mu}(-1) = -1$. Since u belongs to the residue class 1 modulo 4, we get $\nu(-1) \in \{-1, -u^{2^{s-2}}\}$. Now Eq. (55) does not change if we replace μ by $a \mapsto \mu(ae)$ with a unit $e \in A^{\times}$ such that $2(q(e) - 1) = 0$. So we can choose $e := (1 + 2^{s-1}) + 2^m\mathbb{Z}$. Thus $\overline{\mu}(-q(e)) = 1 - 2q(e) = -1$, which shows that $-q(e)$ is of order 2 in $(A/\mathrm{Soc}(A))^{\circ}$. Therefore, if $\nu(-1) = -u^{2^{s-2}}$, then $\nu(-q(e)) = -1$. Consequently, the modification of μ by e can be used to get

$$\mu(-1) = -1. \tag{56}$$

On the other hand, Eq. (55) shows that $\overline{\mu}(1) = 3 + 2^s\mathbb{Z}$. For $m > s + 1$, the element u belongs to the residue class 1 modulo 8. Then the list (54) contains no element of the residue class 3 modulo 8, i.e. $\mu(1)$ cannot belong to that list. Hence $m = s+1$, i.e. $|\mathrm{Soc}(A)| = 2$. Since $\overline{\mu}(1) = 3+2^s\mathbb{Z}$, there remain only two possibilities, either $\mu(1) = 3+2^m\mathbb{Z}$ or $\mu(1) = (3 + 2^{m-1}) + 2^m\mathbb{Z}$.

To show that these elements belong to the list (54), note first that $u = 5 + 2^m\mathbb{Z}$. Therefore, the elements $-u^{2k+1}$ of (54) cover the whole residue class 3 modulo 8. This shows that both values of $\mu(1)$ are realizable as cyclic braces. Let us first consider the case $\mu(1) = 3 + 2^m\mathbb{Z} =: c$. Lemma 3 implies that

$$1^{\circ k} = 1 + c + c^2 + \cdots + c^{k-1} = \frac{3^k - 1}{2} + 2^m\mathbb{Z}$$

holds for all $k \in \mathbb{N}$. By Lemma 2, it follows that 1 is of order 2^{m-1} in A°. Therefore, the elements of $\langle 1 \rangle$ cover the residue classes 0 and 1 modulo 4. By Eq. (56), $-1 \in A^\circ$ is of order 2, and $1 \circ (-1) = (-1) \circ 1 = -2 + 2^m\mathbb{Z}$. Hence A is abelian. In the second case, we have $1 \circ (-1) = -2 + 2^m\mathbb{Z}$, but $(-1) \circ 1 = (-2 + 2^{m-1}) + 2^m\mathbb{Z}$, i.e. A is non-abelian. □

7. The exceptional hierarchy

In this section, we give a complete classification of primary cyclic braces. To this end, we reconsider first the families of exceptional braces obtained in the last section. It will turn out that their adjoint group admits a cyclic subgroup of index 2. The following classification of such groups is well-known ([4], Theorem 12.5.1; [11], IV.3.7).

Proposition 11 (*Hall, Zassenhaus*). *Let G be a group of order 2^m with a cyclic subgroup of index 2. Then G belongs to exactly one of the following types.*

(1a) *G is cyclic*
(1b) *$G \cong C_2 \times C_{2^{m-1}}$ with $m \geq 2$ (abelian, non-cyclic)*
(2a) *$G \cong \langle a, b \mid a^{2^{m-1}} = 1, b^2 = 1, bab^{-1} = a^{-1} \rangle$ with $m \geq 3$ (dihedral)*
(2b) *$G \cong \langle a, b \mid a^{2^{m-1}} = 1, b^2 = a^{2^{m-2}}, bab^{-1} = a^{-1} \rangle$ with $m \geq 3$ (generalized quaternion)*
(3a) *$G \cong \langle a, b \mid a^{2^{m-1}} = 1, b^2 = 1, bab^{-1} = a^{-1+2^{m-2}} \rangle$ with $m \geq 4$*
(3b) *$G \cong \langle a, b \mid a^{2^{m-1}} = 1, b^2 = 1, bab^{-1} = a^{1+2^{m-2}} \rangle$ with $m \geq 4$.*

The adjoint groups of the non-abelian cyclic braces considered above are given in the following

Proposition 12. *Let $A = \mathbb{Z}/2^m\mathbb{Z}$ be a non-abelian cyclic brace.*

(a) *If A is involutive with characteristic class c, then either $c = -1$ and A° is dihedral (type 2a), or $c = (-1 + 2^{m-1}) + 2^m\mathbb{Z}$ and A° is a generalized quaternion group (type 2b).*
(b) *If A is semi-involutive, then its characteristic class is $c = (-1 + 2^{m-1}) + 2^m\mathbb{Z}$, and A° is of type (3a).*
(c) *If $A/\mathrm{Soc}(A)$ is not bicyclic and $|A/\mathrm{Soc}(A)| \geq 8$, then A° is of type (3b).*

Proof. In the following, we abbreviate the residue class $k + 2^m\mathbb{Z}$ by $\overline{k}$. As before, we write 1 instead of $\overline{1}$. The elements of order 2 in $A^\times$ are -1 and $\pm 1 + \overline{2^{m-1}}$.

(a) Let A be involutive. Then $m \geq 3$ since A is non-abelian. Therefore, the corollary of Proposition 6 implies that $1 + \overline{2^{m-1}} \in B(2^m)$. Thus Corollary 2 of Proposition 7 shows that either $c = -1$ or $c = -1 + \overline{2^{m-1}}$. In both cases, $\mu(\overline{2}) = c^2 = 1$. Hence $\overline{2}^{\circ k} = \overline{2k}$ for all $k \in \mathbb{N}$, and thus $\overline{2}$ is of order 2^{m-1}. In the first case, $1 \circ 1 = 0$, and $1 \circ \overline{2} \circ 1 = \overline{3} \circ 1 = -\overline{2} = \overline{2}^{\circ(-1)}$. Thus A° is dihedral. In the second case, $1 \circ 1 = \overline{2^{m-1}} = \overline{2}^{\circ 2^{m-2}}$, and $1 \circ \overline{2} = \overline{3}$. Since $\overline{2}^{\circ(-1)} \circ 1 = (-\overline{2}) \circ 1 = -\overline{2}(-1 + \overline{2^{m-1}}) + 1 = \overline{3}$, we infer that A° is a generalized quaternion group.

(b) Next let A be semi-involutive. Since A is non-abelian, Proposition 9 yields $m \geq 4$ and $c = -1 + \overline{2^{m-1}}$. Here $\mu(\overline{2}) = -c = 1 + \overline{2^{m-1}}$. Hence $\overline{k} \circ \overline{2} = \overline{k} + \overline{2}$ if k is even. By induction, this gives $\overline{2}^{\circ k} = \overline{2k}$ for all $k \in \mathbb{N}$, and $\overline{2}$ is of order 2^{m-1} in A°. Furthermore, Eq. (49) yields $(-1) \circ (-1) = 0$, and $(-1) \circ \overline{2} \circ (-1) = (1 + \overline{2^{m-1}}) \circ (-1) = \overline{2^{m-1}} - \overline{2} = \overline{2}^{\circ(2^{m-2}-1)}$, which shows that A° is of type (3a).

(c) Finally, let $A/\mathrm{Soc}(A)$ be not bicyclic and $|A/\mathrm{Soc}(A)| \geq 8$. Then $m \geq 4$. With $c := \overline{3} + \overline{2^{m-1}}$, we have $c^k = \sum_{l=0}^{k} \binom{k}{l} \overline{3}^l (\overline{2^{m-1}})^{k-l} = \overline{3}^k + \binom{k}{1} \overline{3}^{k-1} \overline{2^{m-1}} = \overline{3}^k$ for $k \in \mathbb{N}$ even. By Proposition 10, we have $|\mathrm{Soc}(A)| = 2$ and $\mu(1) = c$. Hence

$$1^{\circ k} = 1 + c + c^2 + \cdots + c^{k-1} = \frac{(3 + 2^{m-1})^k - 1}{2 + 2^{m-1}} + 2^m\mathbb{Z} = \frac{3^k - 1}{2 + 2^{m-1}} + 2^m\mathbb{Z}$$

for even k. As the order of 1 in A° must be even, Lemma 2 shows that the order of 1 is 2^{m-1}. Therefore, since $A/\mathrm{Soc}(A)$ is not bicyclic, Proposition 4 implies that the order of 1 in the adjoint group of $A/\mathrm{Soc}(A)$ is 2^{m-2}. Hence

$$1^{\circ 2^{m-2}} = \overline{2}^{m-1}. \tag{57}$$

Furthermore, Eq. (52) yields $(-1) \circ (-1) = 0$ and $(-1) \circ 1 \circ (-1) = (-\overline{2} - \overline{2}^{m-1}) \circ (-1) = 1 + \overline{2}^{m-1}$. Also, Eq. (57) gives $1^{\circ(2^{m-2}+1)} = \overline{2}^{m-1} \circ 1 = \overline{2}^{m-1} + 1$, whence A° is of type (3b). □

Now we are ready to prove our main theorem.

Theorem 3. *A primary cyclic brace A is bicyclic or exceptional. If A is exceptional, then $|A| = 2^m$ with $m \geq 2$, and A° has a cyclic subgroup of index 2. Up to isomorphism, an exceptional primary cyclic brace A is uniquely determined by its adjoint group A°. Conversely, all the groups of Proposition 11, except the cyclic groups of order ≤ 4, arise in this way.*

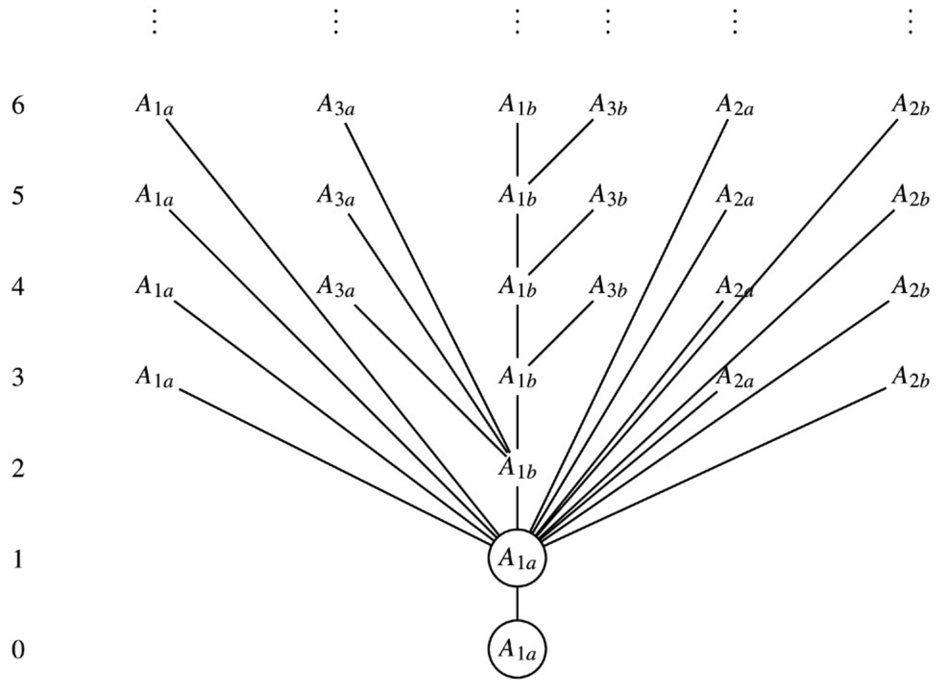
Proof. The first statement follows by Theorem 2. Thus let A be an exceptional primary cyclic brace with structure map $\mu\colon A \to A^\times$. Then $|A| = 2^m$ with $m \geq 2$. If A is bicyclic, then $|\mathrm{Soc}(A)| \geq 4$ and $|A/\mathrm{Soc}(A)| = 2$. Hence $m \geq 3$, the isomorphism class of A is uniquely determined by m, and A° is of type (1a).

If A is abelian, but not bicyclic, then $|\mathrm{Soc}(A)| = 2$. This gives an exceptional brace A for each $m \geq 2$. By Proposition 4, the adjoint group A° is of type (1b).

Now let A be non-abelian. If $|A/\mathrm{Soc}(A)| = 2$, then $\mu(A) = \{1, c\}$ with an element $c \in A^\times$ of order 2. Therefore, Eq. (48) holds, and A is involutive. By Proposition 12, this gives two series of braces A with A° of type (2a) and (2b), respectively.

Next we consider the case where A is non-abelian with $|A/\mathrm{Soc}(A)| = 4$. Since A is exceptional, this means that $A/\mathrm{Soc}(A)$ is not bicyclic. By Proposition 4, we have $A/\mathrm{Soc}(A) = \langle 1 \rangle \times \langle -1 \rangle$. Hence $\mu(1)$ and $\mu(-1)$ are different elements of order 2 in $A^\times$. The structure map $\overline{\mu}$ of $A/\mathrm{Soc}(A)$ satisfies $\overline{\mu}(1) = \overline{\mu}(-1) = -1$. Hence $\mu(1)$ and $\mu(-1)$ belong to the residue class 3 modulo 4. Thus $\{\mu(1), \mu(-1)\} = \{-1, c\}$ with $c := (-1 + 2^{m-1}) + 2^m\mathbb{Z}$. By Proposition 2, we can assume that $\mu(-1) = -1$. According to Definition 3, A is semi-involutive, and Proposition 12 shows that A° is of type (3a). The remaining case $|A/\mathrm{Soc}(A)| \geq 8$ is also covered by Proposition 12. □

The tree of exceptional cyclic braces can be visualized as follows.



The numbers m on the left-hand side refer to the size of each brace A, i.e. $|A| = 2^m$, while the subscript of A indicates the type of A°. The vertical axis consists of the abelian, non-bicyclic braces. In downward direction, each brace is connected to its retraction. Therefore, the whole tree is rooted in the zero brace. The two braces with $m \leq 1$ are encircled since they are non-exceptional.

References

[1] B. Amberg, O. Dickenschied, On the adjoint group of a radical ring, Canad. Math. Bull. 38 (1995) 262–270.

[2] 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.

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

[4] M. Hall Jr., The Theory of Groups, 12th printing, Macmillan, New York, 1973.

[5] N. Jacobson, Structure of rings, Amer. Math. Soc. Colloq. Publ. 37 (1974).

[6] D.E. Knuth, The art of computer programming, in: Seminumerical Algorithms, vol. 2, Addison-Wesley, Reading, Mass., 1969.

[7] W. Rump, A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation, Adv. Math. 193 (2005) 40–55.

[8] W. Rump, Braces, radical rings, and the quantum Yang–Baxter equation (Preprint).

[9] J.-P. Serre, A Course in Arithmetic, Springer-Verlag (GTM 7), New York, 1973.

[10] J.F. Watters, On the adjoint group of a radical ring, J. London Math. Soc. 43 (1968) 725–729.

[11] H.J. Zassenhaus, The Theory of Groups, 2nd ed., Chelsea, New York, 1958.