*Pacific Journal of Mathematics*

# THE CLASSIFICATION OF NONDEGENERATE UNICONNECTED CYCLE SETS

WOLFGANG RUMP

Volume 323 No. 1 March 2023

PACIFIC JOURNAL OF MATHEMATICS
Vol. 323, No. 1, 2023
https://doi.org/10.2140/pjm.2023.323.205

# THE CLASSIFICATION OF NONDEGENERATE UNICONNECTED CYCLE SETS

WOLFGANG RUMP

*Dedicated to B. V. M.*

**It is known that the set-theoretic solutions to the Yang–Baxter equation studied by Etingof et al. (1999) are equivalent to a class of sets with a binary operation, called nondegenerate cycle sets. There is a covering theory for cycle sets which associates a universal covering to any indecomposable cycle set. The cycle sets arising as universal covers are said to be uniconnected. In this paper, the category of nondegenerate uniconnected cycle sets is determined, and it is proved that up to isomorphism, a nondegenerate uniconnected cycle set is given by a brace $A$ with a transitive cycle base (an adjoint orbit which generates the additive group of $A$). The theorem is applied to braces with cyclic additive or adjoint group, where a more explicit classification is obtained.**

## Introduction

Set-theoretic solutions to the Yang–Baxter equation [2; 30] are self-maps $S : X \times X \to X \times X$ which satisfy the equation

$$(S \times 1_X)(1_X \times S)(S \times 1_X) = (1_X \times S)(S \times 1_X)(1_X \times S)$$

in $X \times X \times X$. A solution $S(x, y) = ({}^x y, x^y)$ is said to be *nondegenerate* if the maps $y \mapsto {}^x y$ and $y \mapsto y^x$ are bijective for all $x \in X$. Suggested by Drinfeld [10], set-theoretic solutions were found on the symplectic leaves of a Poisson Lie group [29] and in connection with semigroups of $I$-type [14; 28]. A systematic study of nondegenerate *involutive* ($S^2 = 1_{X\times X}$) solutions was first given by Etingof, Schedler, and Soloviev [11]. By [18, Propositions 1 and 2], nondegenerate involutive solutions on $X$ are equivalent to *nondegenerate cycle sets* $(X; \cdot)$, that is, sets with a binary operation such that the maps $\sigma(x) : X \to X$ with $\sigma(x)(y) := x \cdot y$ and $x \mapsto x \cdot x$ are bijective, and the equation

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

*MSC2020:* 05E18, 16T25, 81R50.
*Keywords:* braces, coverings, cycle sets, Yang–Baxter equation.

holds in $X$. The correspondence is given as follows. For a nondegenerate involutive solution $S$ on $X$, the inverse maps $y \mapsto x \cdot y$ of $y \mapsto y^x$ make $X$ into a nondegenerate cycle set, and every nondegenerate cycle set $X$ gives rise to a nondegenerate involutive solution $S(x, y) = (x^y \cdot y, x^y)$. If $X$ is finite, the bijectivity of $x \mapsto x \cdot x$ is redundant.

For any cycle set $X$, the $\sigma(x)$ generate a permutation group $G(X) = (G(X); \circ)$ on $X$. If $X$ is nondegenerate, $G(X)$ admits a unique cycle set structure such that

$$\sigma : X \to G(X)$$

is a morphism of cycle sets. In other words, a nondegenerate involutive solution $S$ on $X$ lifts to a solution on $G(X)$. The cycle set structure on $G(X)$ gives rise to a left action of $G(X)$ on the underlying set: $(a \circ b) \cdot c = a \cdot (b \cdot c)$, and the operation

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

is commutative. Such a structure $(G; \circ, +, \cdot)$ is called a *brace* [19]. For any brace $A$, the underlying cycle set is nondegenerate, and $(A; +)$ is an abelian group. The group $A^\circ := (A; \circ)$ is called the *adjoint group* of $A$. Its action on $A$ makes $A$ into a left $A^\circ$-module. Every abelian group $A$ can be regarded as a *trivial brace* with $a \circ b = a + b$ and $a \cdot b = b$ for all $a, b \in A$. For a trivial brace $A$, we write $A^\times$ for the set of its generators as a group.

While cycle sets give rise to solutions to the Yang–Baxter equation, braces form an efficient tool for the study of cycle sets. Besides this, braces arise in affine geometry [3; 4; 5], the theory of solvable groups [6; 7; 23], Hopf–Galois structures [1; 8; 13; 15], and other topics [21].

For a nondegenerate cycle set $X$, let $A(X)$ denote the associated brace with adjoint group $G(X)$. Any surjective morphism $f : X \twoheadrightarrow Y$ of nondegenerate cycle sets lifts along the morphism $\sigma : X \to A(X)$ to a brace morphism $A(f) : A(X) \twoheadrightarrow A(Y)$. If $X$ is *indecomposable* [12], that is, $G(X)$ acts transitively on $X$, then $Y$ is indecomposable. If, in addition, $A(f)$ is invertible, the morphism $f$ is said to be a *covering* [24]. A strategy to classify indecomposable cycle sets was outlined in the latter reference: any indecomposable cycle set $X$ admits a *universal covering* $\widetilde{p} : \widetilde{X} \twoheadrightarrow X$ so that no noninvertible covering of $\widetilde{X}$ is possible. The cycle set $\widetilde{X}$ is indecomposable in a strong sense: the permutation group $G(\widetilde{X})$ acts freely and transitively on $\widetilde{X}$. If $\widetilde{p} : \widetilde{X} \twoheadrightarrow X$ is invertible, $X$ is said to be *uniconnected*. The descent from $\widetilde{X}$ to a cycle set $X$ is given by the *fundamental group* $\pi_1(X)$ of $X$ and is described in [24, Theorem 3.3 and Theorem 4.3].

So the complete classification of indecomposable cycle sets hinges decisively on the determination of the uniconnected cycle sets. By the choice of a base point, the free transitive action of the permutation group allows to identify a uniconnected cycle set $X$ with $G(X)$. If $X$ is nondegenerate, the cycle set structure of $X$ can be determined explicitly in terms of the brace $A(X)$. For cycle sets $X$ with cyclic permutation group $G(X)$, this has been applied in [26, Theorem 1], but ignoring the dependence of a base point, it was falsely assumed that the isomorphism class of $X$ is determined by the brace $A(X)$. The fact that the base point matters was observed recently by Jedlička et al. [17], who give a classification of uniconnected cycle sets with a finite cyclic permutation group. Note that these cycle sets are nondegenerate [18].

In this paper, we determine the category of all nondegenerate uniconnected cycle sets (Theorem 2). Its objects are braces $A$ with a distinguished element $e \in A$ such that the adjoint orbit $X$ of $e$ generates the additive group of $A$. Such a subcycle set $X$ is said to be a *transitive cycle base* [24] of $A$. Morphisms can be viewed as affine extensions of brace morphisms with a translational part in the adjoint group. As a corollary, it follows that a complete set of invariants of a nondegenerate uniconnected cycle set $X$ consists in the brace $A(X)$ together with the transitive cycle base $\sigma(X)$. Conversely, every brace $A$ with a transitive cycle base corresponds to a unique nondegenerate uniconnected cycle set $X$, up to isomorphism. If the permutation group $G(X)$ is cyclic, the result of [17] is obtained in a more conceptional form: the isomorphism classes of nondegenerate uniconnected cycle sets $X$ with $A(X) = A$ correspond bijectively to the set $(A/(\mathrm{Soc}(A) + A^2))^\times$ of generators of the trivial brace $A/(\mathrm{Soc}(A) + A^2)$ (Theorem 17). For finite $A$, the ideals $A^2$ and $\mathrm{Soc}(A)$ — the *socle* [19] — are complementary in the sense that $|A| = |A^2| \cdot |\mathrm{Soc}(A)|$.

For general braces $A$, a certain duality between $A^2$ and $\mathrm{Soc}(A)$ remains true: $A^2$ is the smallest ideal $I$ such that $A/I$ is a trivial brace, and $\mathrm{Soc}(A)$ is the largest ideal $I$ such that the adjoint group $I^\circ$ acts trivially on $A$.

The correspondence between nondegenerate uniconnected cycle sets and braces with a transitive cycle base leads us to the question of which braces $A$ have a nonempty set $\mathscr{T}(A)$ of transitive cycle bases. As a necessary condition, we show that the group $A/A^2$ is cyclic if $\mathscr{T}(A) \neq \varnothing$ (Proposition 7). For *abelian* braces $A$ (i.e., with an abelian adjoint group $A^\circ$) with $\mathscr{T}(A) \neq \varnothing$, we prove that $\mathscr{T}(A) = (A/A^2)^\times$ (Proposition 12). Abelian braces $A$ are equivalent to commutative radical rings, with $a \circ b = ab + a + b$. If $A$ is nilpotent, the necessary condition of Proposition 7 for $\mathscr{T}(A) \neq \varnothing$ is sufficient (Corollary 13).

It is well known that a nontrivial brace $A$ with $A^\circ$ cyclic must be finite. As a commutative radical ring, $A$ is a direct product of its primary components $A_p$. For odd primes $p$, the brace $A_p$ is *cyclic*, which means that its additive group is cyclic, and $A_2$ is cyclic unless $(A_2; +)$ is the Klein four-group. Thus, with a trivial exception, braces $A$ with $A^\circ$ cyclic are contained in the class of cyclic braces, which have been classified in [22]. By [20, Section 7], there are six infinite classes of exceptional cyclic braces of order $2^n$, and all these braces are determined by their adjoint group. We refine this result by showing that up to brace automorphisms, these braces $A$ admit a unique transitive cycle base, hence a unique nondegenerate uniconnected cycle set associated with $A$ (Theorem 19).

## 1. Uniconnected cycle sets

Recall [23] that an *affine structure* on a group $(A;\circ)$ is given by a binary operation $(A;\cdot)$ satisfying the equations

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

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

By [23, Theorem 2.1], a group with an affine structure is equivalent to a *brace* [19], that is,

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

defines an abelian group structure on $A$ with the same unit element as $(A,\circ)$. Equivalently (see [15]), a brace can be described as an abelian group $(A;+)$ with a second group structure $(A,\circ)$ such that

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

holds for $a,b,c\in A$. Equation (4) shows that $a+b=c+d$ implies that $a\circ e+b\circ e=c\circ e+d\circ e$. Thus each $b\in A$ defines an affine map $a\mapsto a\circ b$ on $(A;+)$. The group $A^\circ:=(A;\circ)$ is said to be the *adjoint group* of the brace $A$. For example, any radical ring [16] is a brace with $a\circ b:=ab+a+b$, which explains the terminology. Accordingly, we write 0 for the common unit element of $(A;+)$ and $A^\circ$, and $a'$ for the inverse of $a$ in $A^\circ$.

The adjoint group acts on $(A;+)$ via $b\mapsto a\cdot b$ which makes $A$ into a left $A^\circ$-module:

$$a\cdot(b+c)=(a\cdot b)+(a\cdot c). \tag{5}$$

If $a\mapsto a^b$ denotes the inverse of $a\mapsto b\cdot a$, then (3) can be rewritten as

$$a\circ b=a^b+b. \tag{6}$$

The right action $a\mapsto a^b$ makes $A$ into a right $A^\circ$-module:

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

Equation (6) shows that $a\mapsto a^b$ is the linear part of the affine map $a\mapsto a\circ b$, with translational part $a\mapsto a+b$. Recall that a set $(X;\cdot)$ with a binary operation is said to be a *cycle set* [18] if the left multiplications $\sigma(x):X\to X$ with $\sigma(x)(y):=x\cdot y$ are bijective and the equation

$$(x\cdot y)\cdot(x\cdot z)=(y\cdot x)\cdot(y\cdot z) \tag{7}$$

holds in $X$. A cycle set $X$ is said to be *nondegenerate* [18] if the square map $x \mapsto x \cdot x$ is bijective. Every finite cycle set is nondegenerate [18, Theorem 2]. By [18, Proposition 1], nondegenerate cycle sets are equivalent to nondegenerate involutive set-theoretic solutions to the Yang–Baxter equation [11]. By (1) and (3), every brace $A$ is a cycle set with

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

For $b = -a$, (3) gives $0 = a - a = (a \cdot (-a)) \circ a$. Hence

$$a' = a \cdot (-a) = -(a \cdot a),$$

which shows that every brace is nondegenerate as a cycle set. Equations (6), (5), (3), and (7) show that a brace satisfies $a \cdot (b \circ c) = a \cdot (b^c + c) = (a \cdot b^c) + (a \cdot c) = ((a \cdot c) \cdot (a \cdot b^c)) \circ (a \cdot c) = ((c \cdot a) \cdot (c \cdot b^c)) \circ (a \cdot c)$. Thus

$$a \cdot (b \circ c) = ((c \cdot a) \cdot b) \circ (a \cdot c). \tag{9}$$

A *morphism* of cycle sets $X, Y$ is a map $f : X \to Y$ with $f(x \cdot y) = f(x) \cdot f(y)$ for all $x, y \in X$. A *morphism* of braces is a group homomorphism for the additive and adjoint group:

$$f(a+b) = f(a) + f(b), \quad f(a \circ b) = f(a) \circ f(b).$$

By (3), this implies that $f$ is a morphism of cycle sets. The category of braces will be denoted by **Bra**.

For a cycle set $X$, the group $G(X)$ generated by all $\sigma(x)$, $x \in X$, is called the *permutation group* of $X$. So there is a natural map $\sigma : X \to G(X)$, and $G(X)$ acts from the left on $X$. If this action is transitive, $X$ is said to be *indecomposable*. For a nondegenerate cycle set $X$, the permutation group $G(X)$ is the adjoint group of a brace $A(X)$ such that

$$\sigma : X \to A(X) \tag{10}$$

is a morphism of cycle sets; see [19, Section 1]. Equations (1) and (9) show that the brace $A(X)$ is uniquely determined by these properties. The image $\sigma X$ is of the map (10) together with the cycle set morphism $X \twoheadrightarrow \sigma X$ is called the *retraction* of $X$.

By [24, Section 2], every surjective morphism $f : X \twoheadrightarrow Y$ of cycle sets extends to a unique group homomorphism $G(f)$ so that the diagram

$$\begin{array}{ccc} X & \xrightarrow{\ f\ } & Y \\ \downarrow{\scriptstyle\sigma} & & \downarrow{\scriptstyle\sigma} \\ G(X) & \xrightarrow{G(f)} & G(Y) \end{array}$$

commutes. If $X$ is indecomposable, then $Y = f(X)$ is indecomposable, too. If $X$ is indecomposable and $G(f)$ invertible, $f$ is said to be a *covering* [24]. Then $f$ is equivariant under the action of $G(X)$. By [24, Corollary 3.7], every indecomposable cycle set $X$ has a universal covering $\widetilde{p} : \widetilde{X} \twoheadrightarrow X$ so that every covering of $\widetilde{X}$ is invertible. If $\widetilde{p}$ is invertible, $X$ is said to be *uniconnected*, in analogy to simply connected spaces in topology. By [24, Corollary 3.9], $X$ is uniconnected if and only if $G(X)$ acts freely and transitively on $X$. With the choice of a base point $e \in X$, the group $G(X)$ can then be identified with $X$.

Recall that a subset $X$ of a brace $A$ is said to be a *cycle base* [19] if $X$ is invariant under the action of $A^\circ$ and $X$ generates the additive group of $A$. If $A^\circ$ acts transitively on $X$, then $X$ is said to be a *transitive cycle base* [24]. By $\mathscr{T}(A)$ we denote the set of transitive cycle bases of $A$. Equation (6) shows that a cycle base $X$ of $A$ also generates the adjoint group $A^\circ$.

The following characterization was proved in [27]:

**Theorem 1.** *Let $A$ be a brace with a transitive cycle base $X$ and $e \in X$. Then*

$$a \odot b := b \circ (e^a)' \tag{11}$$

*makes $A$ into a nondegenerate uniconnected cycle set. Every nondegenerate uniconnected cycle set arises in this way.*

**Remark.** Theorem 1 is proved, but not correctly stated, in [27] where the condition $e \in X \in \mathscr{T}(A)$ is replaced by the stronger assumption that $e$ generates $A$. By [25, Theorem 3], both conditions are equivalent if the multipermutation level of $X$ is finite. In general, this is not true even if $X$ is finite; see [25, Example 2].

Equation (11) shows that $e^{a \odot b} = e^{b \circ (e^a)'} = e^a \cdot e^b$. So the map

$$\exp : (A; \odot) \twoheadrightarrow X \tag{12}$$

with $\exp(a) := e^a$ is a cycle set morphism onto $X = e^A := \{e^a \mid a \in A\}$. For $a, b$ in $(A; \odot)$, we have $\sigma(a) = \sigma(b) \iff e^a = e^b$. Thus, up to isomorphism, (12) is the retraction of $(A; \odot)$. Moreover, Equation (11) shows that $A^\circ$ is isomorphic to the permutation group of $(A; \odot)$. Hence $A \cong A(A; \odot)$.

## 2. Coaffine brace morphisms

In this section, we determine the category of nondegenerate uniconnected cycle sets by means of Theorem 1. To this end, we need a weak type of brace morphism.

**Definition.** We define a *coaffine* map $A \to B$ between braces to be a pair $(b, f)$ with a brace morphism $f : A \to B$ and a constant $b \in B$ such that $(b, f)(a) := b \circ f(a)$ for all $a \in A$. We write $\mathrm{Hom}^\sharp(A, B)$ for the set of coaffine maps $f : A \to B$.

The composition of coaffine maps is given by

$$(c, g)(b, f) = (c \circ g(b), gf). \tag{13}$$

It is easily checked that the composition is associative with $(0, 1_A) : A \to A$ as unit morphisms. So **Bra** is a subcategory of the category $\mathbf{Bra}^\sharp$ of braces with coaffine maps as morphisms. A morphism $(b, f)$ in $\mathbf{Bra}^\sharp$ is invertible if and only if $f$ is bijective. Then

$$(b, f)^{-1} = (f^{-1}(b)', f^{-1}).$$

Every coaffine map $(b, f) : A \to B$ has a *translational part* $b = (b, f)(0)$, so that

$$(b, f) = (b, 1_B)(0, f).$$

The translations $(b, 1_B)$ are left translations of the adjoint group $B^\circ$. Therefore, we speak of "coaffine" rather than "affine" maps. The invertible coaffine maps $A \to A$ form a group $\mathrm{Aut}^\sharp(A)$ with the brace automorphisms as a subgroup $\mathrm{Aut}^\flat(A)$. The translations in $\mathrm{Aut}^\sharp(A)$ form a normal subgroup isomorphic to $A^\circ$. Since $A^\circ \cap \mathrm{Aut}^\flat(A) = \{(0, 1_A)\}$, we have a semidirect product

$$\mathrm{Aut}^\sharp(A) = A^\circ \rtimes \mathrm{Aut}^\flat(A).$$

Let $\mathbf{Bra}_\sharp$ be the category of braces with morphisms $[b, f] : A \to B$ given by a brace morphism $f : A \to B$ and an element $b \in B$ such that

$$[b, f](a) := b \cdot f(a).$$

Note that in contrast to $\mathbf{Bra}^\sharp$, the morphisms in $\mathbf{Bra}_\sharp$ are additive maps. The composition is given by $[c, g][b, f](a) = c \cdot g(b \cdot f(a)) = c \cdot (g(b) \cdot gf(a))$. By (1), this gives

$$[c, g][b, f] = [c \circ g(b), gf],$$

similarly to (13). We write $\mathrm{Hom}_\sharp(A, B)$ for the morphisms $A \to B$ in $\mathbf{Bra}_\sharp$. So the maps $(b, f) \mapsto [b, f]$ provide surjections $\mathrm{Hom}^\sharp(A, B) \twoheadrightarrow \mathrm{Hom}_\sharp(A, B)$ which are compatible with compositions.

Theorem 1 shows that every nondegenerate uniconnected cycle set can be represented by a brace $A$ together with an element $e \in X \in \mathscr{T}(A)$. In what follows, we write $(A; e)$ for the uniconnected cycle set $(A; \odot)$ of Theorem 1. By (11),

$$e = (0 \odot 0)'.$$

**Theorem 2.** *Let $(A; e)$ and $(B; u)$ be nondegenerate uniconnected cycle sets. The cycle set morphisms $(A; e) \to (B; u)$ coincide with the coaffine morphisms $(c, f) : A \to B$ with $u = [c, f](e)$.*

*Proof.* Assume first that $(c, f): A \to B$ is a coaffine morphism with $u = [c, f](e) = c \cdot f(e)$. For $a, b \in A$, we have $(c, f)(a \odot b) = c \circ f(b \circ (e^a)') = c \circ f(b) \circ (f(e)^{f(a)})' = c \circ f(b) \circ \big((c \cdot f(e))^{c \circ f(a)}\big)' = (c, f)(b) \circ (u^{(c,f)(a)})' = (c, f)(a) \odot (c, f)(b)$. Thus $(f, c)$ is a morphism $(A; e) \to (B; u)$.

Conversely, let $g : (A; e) \to (B; u)$ be a cycle set morphism. Then $g(b \circ (e^a)') = g(a \odot b) = g(a) \odot g(b) = g(b) \circ (u^{g(a)})'$ for all $a, b \in A$. Replacing $b$ by $b \circ e^a$ gives $g(b) = g(b \circ e^a) \circ (u^{g(a)})'$. So we have

$$g(b \circ e^a) = g(b) \circ u^{g(a)}, \tag{14}$$

$$g(b \circ (e^a)') = g(b) \circ (u^{g(a)})'. \tag{15}$$

Recursively, we define $a^{\circ n}$ by $a^{\circ 1} := a$ and $a^{\circ (n+1)} = a^{\circ n} \circ a$. By induction, (14)–(15) give

$$g(b \circ (e^a)^{\circ n}) = g(b) \circ (u^{g(a)})^{\circ n}$$

for all $n \in \mathbb{Z}$, and a further induction yields

$$g(b \circ (e^{a_1})^{\circ n_1} \circ \cdots \circ (e^{a_r})^{\circ n_r}) = g(b) \circ (u^{g(a_1)})^{\circ n_1} \circ \cdots \circ (u^{g(a_r)})^{\circ n_r}. \tag{16}$$

Since $e^A$ is a cycle base of $A$, each element $a \in A$ is of the form

$$a = (e^{a_1})^{\circ n_1} \circ \cdots \circ (e^{a_r})^{\circ n_r}$$

for some $a_1, \dots, a_r \in A$ and $n_1, \dots, n_r \in \mathbb{Z}$. For $b = 0$, (16) turns into $g(a) = g(0) \circ (u^{g(a_1)})^{\circ n_1} \circ \cdots \circ (u^{g(a_r)})^{\circ n_r}$. Hence

$$g(b \circ a) = g(b) \circ g(0)' \circ g(a) \tag{17}$$

holds for all $a, b \in A$. So the map $f : A \to B$ with $f(a) := g(0)' \circ g(a)$ satisfies

$$f(a \circ b) = f(a) \circ f(b).$$

Now we show that $f$ is a brace morphism. For $b = a'$, (17) gives $g(0) = g(a') \circ g(0)' \circ g(a)$. Hence

$$g(a') = g(0) \circ g(a)' \circ g(0). \tag{18}$$

With $b = 0$, (14) gives $g(e^a) = g(0) \circ u^{g(a)}$. Hence

$$f(e^a) = u^{g(a)}. \tag{19}$$

Thus (3), (19), (17), and (18) yield

$$\begin{aligned}f(a+e^b) &= f((a\cdot e^b)\circ a) = f(e^{b\circ a'}\circ a)\\ &= f(e^{b\circ a'})\circ f(a) = u^{g(b\circ a')}\circ f(a) = u^{g(b)\circ g(0)'\circ g(a')}\circ f(a)\\ &= u^{g(b)\circ g(a)'\circ g(0)}\circ f(a) = ((g(0)'\circ g(a))\cdot u^{g(b)})\circ f(a)\\ &= (f(a)\cdot u^{g(b)})\circ f(a) = f(a)+u^{g(b)} = f(a)+f(e^b).\end{aligned}$$

Since $e^A$ is a cycle base of $A$, we obtain $f(a+b)=f(a)+f(b)$ for all $a,b\in A$, by induction. Hence $f$ is a brace morphism, and $g=(g(0),f)$. For $a=0$, (19) gives $f(e)=u^{g(0)}$. Thus $u=g(0)\cdot f(e)=[g(0),f](e)$. □

**Corollary 3.** *Let $A$ be a brace with $e,u\in X\in\mathscr{T}(A)$. Then $(A;e)\cong(A;u)$.*

*Proof.* There is an element $b\in A$ with $b\cdot e=u$. Hence $[b,1_A](e)=u$, and thus $(A;e)\cong(A;u)$. □

Now let **Uni** be the category of braces $A$ with a distinguished transitive cycle base $X\in\mathscr{T}(A)$. We write $(A;X)$ for the objects of **Uni**. Morphisms $(A;X)\to(B;Y)$ are brace morphisms $f:A\to B$ with $f(X)\subset Y$. Recall that a functor $F$ is said to be *conservative* if it reflects isomorphisms: if $F(g)$ is an isomorphism, then $g$ is an isomorphism. We define a *factor category* of a category $\mathscr{C}$ to be a category $\mathscr{D}$ with a full conservative functor $F:\mathscr{C}\to\mathscr{D}$ such that each object of $\mathscr{D}$ is isomorphic to an object $F(C)$. So the existence of such a functor implies that up to isomorphism, $\mathscr{C}$ and $\mathscr{D}$ have the same objects.

**Corollary 4.** *The object map $(A;e)\mapsto(A;e^A)$ makes* **Uni** *into a factor category of the category of nondegenerate uniconnected cycle sets.*

*Proof.* Every morphism $(A;e)\to(B;u)$ is given by a coaffine morphism $(c,f):A\to B$ with $u=c\cdot f(e)$. Hence $f:(A;e^A)\to(B;u^B)$ is a morphism in **Uni**. Conversely, let $f:(A;e^A)\to(B;u^B)$ be a morphism in **Uni**. Then $f(e)=c\cdot u$ for some $c\in B$. Hence $(c,f)$ is a morphism $(A;e)\to(B;u)$ which is mapped to $f:(A;e^A)\to(B;u^B)$. If $f$ is invertible, $(c,f)$ is invertible, too. □

This implies two characterizations of nondegenerate uniconnected cycle sets:

**Corollary 5.** *Let $A$ be a brace. The automorphism group $\mathrm{Aut}^\flat(A)$ acts on the set $\mathscr{T}(A)$ of transitive cycle bases, and there is a bijection between the isomorphism classes of nondegenerate uniconnected cycle sets $X$ with $A(X)\cong A$, and the set $\overline{\mathscr{T}}(A)$ of $\mathrm{Aut}^\flat(A)$-orbits of $\mathscr{T}(A)$.*

**Corollary 6.** *Two nondegenerate uniconnected cycle sets $X$ and $Y$ are isomorphic if and only if there is a brace isomorphism $f:A(X)\xrightarrow{\sim}A(Y)$ which maps the retraction $\sigma X$ onto $\sigma Y$.*

To analyse $\mathscr{T}(A)$ for a brace $A$, we have to recall the concept of brace ideal. To stress the analogy to ring theory, consider the operation $ab := a^b - a$ in $A$, which satisfies

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

for all $a, b \in A$. An additive subgroup $I$ of a brace $A$ is said to be an *ideal* [19] if $ab \in I$ and $ba \in I$ whenever $a \in I$ and $b \in A$. If only $ab \in I$ is required, $I$ is said to be a *right ideal* of $A$. The residue classes $I + b = \{a + b \mid a \in I\}$ of an ideal form a brace $A/I$ with the induced operations in analogy with ring-theoretic ideals. In particular, $b \mapsto I + b$ is a brace morphism $A \twoheadrightarrow A/I$. For example, the *socle* [19] of any brace $A$ is an ideal

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

such that $A \twoheadrightarrow A/\operatorname{Soc}(A)$ is the retraction of $A$ as a cycle set. Furthermore, the finite sums $a_1 b_1 + \cdots + a_n b_n$ with $a_i, b_i \in A$ form an ideal $A^2$ of $A$. The brace $A/A^2$ is *trivial* in the sense that all products $ab$ are zero, or equivalently, $a \circ b = a + b$ for all $a, b \in A/A^2$. For an abelian group $A$ and its corresponding trivial brace, we write $A^\times$ for the set of its generators. Thus $A^\times$ is empty if the group $(A; +) = A^\circ$ is not cyclic.

**Proposition 7.** *Let $A$ be a brace with a transitive cycle base. Then $A/A^2$ is a cyclic group.*

*Proof.* Two elements $x, y$ of a transitive cycle base satisfy $x = y^a$ for some $a \in A$. Hence $x - y = y^a - y = ya \in A^2$. Thus $A \twoheadrightarrow A/A^2$ maps a transitive cycle base $X$ to a single element $g \in A/A^2$. Since $X$ generates the additive group of $A$, the element $g$ generates $A/A^2$. □

**Proposition 8.** *Let $f : A \twoheadrightarrow B$ be a surjective morphism of braces. Any transitive cycle base $X$ of $A$ is mapped to a transitive cycle base $f(X) \in \mathscr{T}(B)$.*

*Proof.* Since $X$ generates the additive group of $A$, the image $f(X)$ generates $(B; +)$. For any pair $x, y \in X$, there is an element $a \in A$ with $y = a \cdot x$. Hence $f(a) \cdot f(x) = f(a \cdot x) = f(y)$, which shows that $f(X) \in \mathscr{T}(B)$. □

## 3. Abelian braces

Recall that a brace $A$ is said to be *abelian* [20] if its adjoint group $A^\circ$ is commutative. Such braces are radical rings, so that no ambiguity with respect to the powers $A^n$ is possible; see [19, Section 3]. For a finite brace $A$, the additive group is the direct sum of its primary components $A_p := \{a \in A \mid \exists n \in \mathbb{N} : p^n a = 0\}$, which are right ideals of $A$. In what follows, we study the set $\overline{\mathscr{T}}(A)$ of $\operatorname{Aut}^\flat(A)$-orbits of $\mathscr{T}(A)$. By Corollary 5, the elements of $\overline{\mathscr{T}}(A)$ correspond to the isomorphism classes of nondegenerate uniconnected cycle sets $X$ with $A(X) \cong A$.

**Proposition 9.** *Let $A$ be a finite abelian brace. Then $\mathscr{T}(A) \cong \prod_p \mathscr{T}(A_p)$ and $\bar{\mathscr{T}}(A) \cong \prod_p \overline{\mathscr{T}(A_p)}$.*

*Proof.* By [20, Proposition 3], the brace $A$ is a product of its primary components $A_p$. Thus, Proposition 8 implies that the projection $X_p$ of a cycle base $X \in \mathscr{T}(A)$ into $A_p$ is a transitive cycle base, and $X = \prod_p X_p$. Conversely, let $(X_p)$ be a collection of cycle bases $X_p \in \mathscr{T}(A_p)$ for each prime $p$. Then $X := \prod_p X_p$ is a transitive cycle base of $A$. Hence $\mathscr{T}(A) \cong \prod_p \mathscr{T}(A_p)$. The second statement follows since $\mathrm{Aut}^\flat(A) \cong \prod_p \mathrm{Aut}^\flat(A_p)$. □

By Proposition 9, the classification of finite uniconnected cycle sets $X$ with $G(X)$ abelian reduces to the case that $G(X)$ is a finite $p$-group. Since any transitive action of an abelian group on a set is free, we have the following:

**Proposition 10.** *Every indecomposable cycle set with an abelian permutation group is uniconnected.*

The following example shows that uniconnected cycle sets with an abelian permutation group need not be nondegenerate.

**Example 11.** Let $\mathscr{C}(X)$ be the ring of continuous real functions on a nonempty topological space $X$. With respect to the partial order $f \leqslant g$ if and only if $f(x) \leqslant g(x)$ for all $x \in X$, the additive group of $\mathscr{C}(X)$ is an *abelian $\ell$-group* [9], that is, an abelian group with a lattice structure satisfying $(f \vee g) + h = (f + h) \vee (g + h)$. With

$$f \cdot g := g - (f \vee 0),$$

$\mathscr{C}(X)$ satisfies

$$\begin{aligned}(f \cdot g) \cdot (f \cdot h) &= (g - (f \vee 0)) \cdot (h - (f \vee 0)) \\ &= h - (f \vee 0) - ((g - (f \vee 0)) \vee 0) \\ &= h - \big(((g - (f \vee 0)) \vee 0) + (f \vee 0)\big) \\ &= h - (g \vee f \vee 0).\end{aligned}$$

Thus, by symmetry, $\mathscr{C}(X)$ is a cycle set. Since every continuous function is of the form $f - g$ with $f, g \geqslant 0$, the permutation group of $\mathscr{C}(X)$ is the additive group of $\mathscr{C}(X)$. Its action on $\mathscr{C}(X)$ is transitive. Hence $\mathscr{C}(X)$ is uniconnected. However, $f \cdot f = f - (f \vee 0) \leqslant 0$ shows that $\mathscr{C}(X)$ is degenerate.

**Proposition 12.** *Let $A$ be an abelian brace with a transitive cycle base $X$ and $e \in X$. Then $A = \mathbb{Z}e + eA$ and $\mathscr{T}(A) = (A/A^2)^\times$. If $e^n \in A^{n+1}$, then $e^n = 0$.*

*Proof.* By [20, Proposition 3], $A$ is a commutative radical ring. Since $X \in \mathscr{T}(A)$, we have $X = e^A = e + eA$. Hence $A = \mathbb{Z}e + eA$, which yields $A^2 = (\mathbb{Z}e + eA)A = eA$. Thus $\mathscr{T}(A) = (A/A^2)^\times$. Now assume that $e^n \in A^{n+1}$. By induction, we have $A^{n+1} = e^n A$. Indeed, $A^2 = eA$, and if $A^{n+1} = e^n A$ holds for some $n \geqslant 1$, then

$A^{n+2} = (e^n A)A = e^n(eA) = e^{n+1}A$. Hence $e^n \in e^n A \subset A^{n+2} = e^{n+1}A$, and thus $e^n = e^{n+1}a$ for some $a \in A$. So we obtain $e^n = e^n ea = e^{n+2}a^2 = \cdots = e^{2n}a^n$. Hence $i := e^n a^n$ is idempotent. Thus $i^{-i} = i(-i) + i = -i + i = 0$, which yields $i = 0$. Therefore, we get $e^n = e^n i = 0$. □

**Corollary 13.** *A nilpotent abelian brace admits a transitive cycle base if and only if $A/A^2$ is cyclic.*

*Proof.* By Proposition 7, $\mathscr{T} \neq \varnothing$ implies that $A/A^2$ is cyclic. Conversely, let $A/A^2$ be cyclic. Choose $e \in A$ such that $e + A^2$ generates $A/A^2$. Then $A = \mathbb{Z}e + A^2$. Hence $A^2 = eA + A^3$. Assume that $A^n \subset eA + A^{n+1}$ holds for some $n \geqslant 2$. Then $A^{n+1} \subset eA^2 + A^{n+2} \subset eA + A^{n+2}$. By induction, this yields $A^2 = eA$. Thus $A = \mathbb{Z}e + eA$, which shows that $e + eA = \{e^a \mid a \in A\}$ is a transitive cycle base. □

**Corollary 14.** *Let $A$ be an abelian brace with $\mathscr{T}(A) \neq \varnothing$. Then there is an element $e \in A$ such that for all $n \in \mathbb{N}$, we have $A^{n+1} = e^n A$ and*

$$A = \mathbb{Z}e + \mathbb{Z}e^2 + \cdots + \mathbb{Z}e^n + e^n A. \tag{20}$$

*Proof.* By Proposition 12 and its proof, $A = \mathbb{Z}e + eA$ and $A^{n+1} = e^n A$. Assume that (20) holds for some $n \geqslant 1$. Then $A = \mathbb{Z}e + eA = \mathbb{Z}e + \mathbb{Z}e^2 + \cdots + Ze^{n+1} + e^{n+1}A$. By induction, this proves the claim. □

Let $A$ be an abelian brace with $\mathscr{T}(A) \neq \varnothing$. For positive integers $n$, we define

$$I_n := \{m \in \mathbb{Z} \mid mA^n \subset A^{n+1}\}.$$

This gives an increasing chain of ideals $I_1 \subset I_2 \subset \cdots$ in $\mathbb{Z}$. So there are unique integers $r_n \in \mathbb{N}$ with $I_n = \mathbb{Z}r_n$ and divisibility relations

$$\cdots \mid r_4 \mid r_3 \mid r_2 \mid r_1.$$

**Definition.** Let $A$ be an abelian brace with $\mathscr{T}(A) \neq \varnothing$. If $n$ is the smallest integer with $r_n = r_{n+1}$, we call $(r_1, \ldots, r_n)$ the *characteristic sequence* of $A$.

If $e \in X \in \mathscr{T}(A)$, Corollary 14 implies that $A^{n+1} = e^n A$. So the characteristic sequence is given by

$$r_n \mid m \iff me^n \in e^n A.$$

By Proposition 12, $r_n = 1$ implies that $e^n = 0$. Thus $A$ is nilpotent if and only if the last entry of the characteristic sequence is 1.

Let $\hat{A} := \varprojlim A/A^n$ be the inverse limit of the sequence of radical rings

$$\cdots \twoheadrightarrow A/A^4 \twoheadrightarrow A/A^3 \twoheadrightarrow A/A^2.$$

By Corollary 14, each element $a \in A$ can be developed into a power series $a = m_1 e + m_2 e^2 + m_3 e^3 + \cdots$ with unique coefficients $m_i \in \mathbb{Z}$ satisfying $0 \leqslant m_i < r_i$

for $r_i > 0$. So there is an exact sequence

$$\bigcap_{n=1}^{\infty} A^n \hookrightarrow A \twoheadrightarrow \hat{A}.$$

**Example 15.** Let $p$ be a prime and $\mathbb{Z}_p$ the ring of $p$-adic rational numbers. Consider the local ring $\mathbb{Z}_p \oplus \mathbb{Q}$ of pairs $(a, x) \in \mathbb{Z}_p \oplus \mathbb{Q}$ with $(a, x)(b, y) := (ab, ay + bx)$. The Jacobson radical of $\mathbb{Z}_p \oplus \mathbb{Q}$ is $A := p\mathbb{Z}_p \oplus \mathbb{Q}$. Hence $A^n = p^n\mathbb{Z}_p \oplus \mathbb{Q}$ and $\bigcap_{n=1}^{\infty} A^n = \mathbb{Q}$. The cycle bases are $X_r = (rp + p^2\mathbb{Z}_p) \oplus \mathbb{Q}$ with $r \in \{1, \ldots, p-1\}$. As there are no nonzero additive maps $\mathbb{Q} \to p\mathbb{Z}_p$, a brace automorphism $\Phi$ of $A = p\mathbb{Z}_p \oplus \mathbb{Q}$ is given by a matrix

$$\begin{pmatrix} \alpha & 0 \\ \beta & \gamma \end{pmatrix}.$$

Applying $\Phi$ to $(p, 0)(0, 1) = (0, p)$, we get $(\alpha(p), \beta(p))(0, \gamma(1)) = (0, \gamma(p))$. So $\alpha(p)\gamma(1) = \gamma(p) = p\gamma(1)$, which gives $\alpha(p) = p$. Since $\alpha$ is a ring automorphism, this implies that $\alpha = 1$. So the $A^\circ$-orbits of $\mathscr{T}(A)$ are trivial, which shows that $|\bar{\mathscr{T}}(A)| = p - 1$.

**Example 16.** The Jacobson radical of the power series ring $\mathbb{Z}[\![e]\!]$ is $A := e\mathbb{Z}[\![e]\!]$. Its characteristic sequence is $(0)$. There are two cycle bases $e + eA$ and $-e + eA$, and $e \mapsto -e$ induces a brace automorphism. Thus $|\bar{\mathscr{T}}(A)| = 1$.

## 4. Cyclic and cocyclic braces

Recall that a brace $A$ is said to be *cyclic* [20] if its additive group is cyclic. If the adjoint group $A^\circ$ is cyclic, $A$ is said to be *cocyclic* [22]. Note that in contrast to cocyclic braces, cyclic braces need not be abelian. In this section, we apply Corollary 5 to cyclic and cocyclic braces.

**Theorem 17.** *Let $A$ be a cocyclic brace. There is a one-to-one correspondence between the isomorphism classes of nondegenerate uniconnected cycle sets $X$ with $A(X) \cong A$ and the set $(A/(\mathrm{Soc}(A) + A^2))^\times$.*

*Proof.* By Proposition 12, we have $\mathscr{T}(A) = (A/A^2)^\times$. Since $A/A^2$ is cyclic, the epimorphism $A/A^2 \twoheadrightarrow A/(A^2 + \mathrm{Soc}(A))$ restricts to a surjection

$$p : (A/A^2)^\times \twoheadrightarrow (A/(\mathrm{Soc}(A) + A^2))^\times.$$

The embedding $\mathrm{Aut}^\flat(A) \hookrightarrow \mathrm{Aut}(A^\circ) = (A^\circ)^\times$ shows that every brace automorphism of $A$ is given by a map $a \mapsto a^{\circ k}$ for some $k \in \mathbb{Z}$. By [22, Proposition 12], $a \mapsto a^{\circ k}$ is a brace automorphism if and only if $a^{\circ(k-1)} \in \mathrm{Soc}(A)$ for all $a \in A$. So we have a commutative diagram

$$\begin{array}{ccccc} \mathrm{Aut}^\flat(A) & \hookrightarrow & (A^\circ)^\times & \twoheadrightarrow & (A^\circ/\operatorname{Soc}(A)^\circ)^\times \\ & & \downarrow & & \downarrow \\ & & (A/A^2)^\times & \overset{p}{\twoheadrightarrow} & (A/(\operatorname{Soc}(A)+A^2))^\times \end{array}$$

with an exact first row. Now $\mathrm{Aut}^\flat(A)$ acts on $\mathscr{T}(A)=(A/A^2)^\times$, and the orbit of a cycle base $e+A^2=A^2\circ e$ is $A^2\circ e\circ \operatorname{Soc}(A)=(A^2\circ e)+\operatorname{Soc}(A)=e+A^2+\operatorname{Soc}(A)$. So the $\mathrm{Aut}^\flat(A)$-orbits of $\mathscr{T}(A)$ correspond to the elements of $(A/(\operatorname{Soc}(A)+A^2))^\times$. By Corollary 5, this completes the proof. □

**Remark.** Theorem 17 corrects [26, Theorem 1], and its corollary, where it is falsely assumed that $\mathrm{Aut}^\flat(A)$ acts transitively on $\mathscr{T}(A)$ for a cocyclic brace. The inaccuracy was observed recently by Jedlička et al. [17] who gave a correct classification by using different methods.

**Example 18.** Up to isomorphism, there is a single infinite cocyclic brace $A$, and $A$ is trivial; see [22, Section 3]. The brace $A=\langle u\rangle$ has two transitive cycle bases, $\{u\}$ and $\{u^{-1}\}$, and there are two brace automorphisms. So the only uniconnected cycle set $X$ with $A(X)\cong A$ is given by $a\odot b=b\circ u'$, that is, $a\odot u^{\circ n}=u^{\circ(n-1)}$.

We turn our attention to cyclic braces $A$. It is convenient to identify the additive group of $A$ with $\mathbb{Z}/n\mathbb{Z}$ for some $n\in\mathbb{N}$. Assume first that $n=0$. Besides the trivial infinite cyclic brace, there is a nonabelian one, given by $k^\ell:=k(-1)^\ell$; see [20, proof of Proposition 6]. So there is a single transitive cycle base $\{1,-1\}$, which shows that $|\bar{\mathscr{T}}(A)|=1$. The corresponding uniconnected cycle set is given by

$$a\odot b=(-1)^a-b.$$

Now let $A$ be finite. For simplicity, we restrict ourselves to the primary case: $|A|=p^n$ for some prime $p$. (For a classification of all cyclic braces, see [22].) Let $d$ denote the order of the socle $\operatorname{Soc}(A)$. Then $A$ is said to be *exceptional* [20; 22] if $A$ is nontrivial (i.e., $d<p^n$) and either $d=p^{n-1}\neq 1$ or $A/\operatorname{Soc}(A)$ is not cocyclic.

By [20, Theorem 3], a cyclic brace $A$ with $|A|=p^n$ is cocyclic or exceptional. If $A$ is exceptional, then $p=2$, and the adjoint group $A^\circ$ admits a cyclic subgroup of order $2^{n-1}$. Moreover, the isomorphism class of $A$ is uniquely determined by the adjoint group $A^\circ$. The following result refines this fact by showing that there is a single isomorphism class of uniconnected cycle sets $X$ with $G(X)=A^\circ$.

**Theorem 19.** *Let $A$ be an exceptional cyclic brace with $|A|=2^n$. Then $|\bar{\mathscr{T}}(A)|=1$.*

*Proof.* By [20, Section 7], there are six classes of exceptional cyclic braces $A$ with $|A|=2^n$, $n\geqslant 2$, according to their adjoint group; see [20, Proposition 11; 22, Section 6]. Let $C_m$ denote the cyclic group of order $m$. The first two classes contain abelian braces:

(1a) $A^\circ$ is cyclic with $|A| \geqslant 8$ and $\mathrm{Soc}(A) = 2A$. There are $2^{n-2}$ cycle bases with two elements each. By [22, Proposition 1], every automorphism of $(A;+)$ is a brace automorphism. Hence $|\bar{\mathscr{T}}(A)| = 1$.

(1b) $A^\circ = \langle -1 \rangle \times \langle 1 \rangle \cong C_2 \times C_{2^{n-1}}$ is abelian, not cyclic. The socle of $A$ is $\{0, 2^{n-1}\}$. By [22, Proposition 1], the cycle set structure of $A$ is given by

$$a^b = 2ab + a.$$

Hence there is a single cycle base $\{1, 3, 5, \ldots\}$. Thus $|\bar{\mathscr{T}}(A)| = 1$.

For the next three cases, the adjoint group $A^\circ$ is one of the following groups:

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

These groups are 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). For the groups $D_{2^m}$ and $Q_{2^m}$, the brace structure is given by $a = 2$ and $b = 1$, and

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

and $\mathrm{Soc}(A) = \langle a \rangle = 2A$. Hence, as in case (1a), $\mathrm{Aut}^\flat(A) = \mathrm{Aut}(A;+)$, which yields $|\bar{\mathscr{T}}(A)| = 1$.

(3a) $A^\circ = SD_{2^m}$. The brace structure is given by

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

with $a = 2$ and $b = -1$, and $\mathrm{Soc}(A) = 4A$. The transitive cycle bases are

$$\{k, -k + 2^m, k + 2^m, -k\}$$

for $k \equiv 1 \pmod 4$, and the brace automorphisms are $x \mapsto xk$ with $k \equiv 1 \pmod 4$. Hence $|\bar{\mathscr{T}}(A)| = 1$.

(3b) Here $A^\circ$ is the group

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

of order $2^{m+1}$. By [20, Proposition 10], the brace structure is given by $a = 1$ and $b = -1$, and

$$c^1 = c(3 + 2^m), \quad c^{-1} = -c \tag{21}$$

for $c \in A = \mathbb{Z}/2^{m+1}\mathbb{Z}$. We show that

$$2^{m+1} \mid (3 + 2^m)^k - 1 \Longleftrightarrow 2^{m-1} \mid k \tag{22}$$

holds for $m \geqslant 3$ and $k \in \mathbb{N}$. Modulo 8, we have $(3 + 2^m)^k \equiv 3$ for odd $k$, and $(3+2^m)^k \equiv 1$ for even $k$. Thus, to verify (22), we can assume that $k = 2\ell$. Modulo $2^{m+1}$, the binomial formula gives $(3 + 2^m)^k \equiv 3^k \equiv 9^\ell$. By [20, Lemma 4], we have

$$2^{m-2} \mid \tfrac{1}{8}((1 + 8)^\ell - 1) \Longleftrightarrow 2^{m-2} \mid \ell.$$

Hence $2^{m+1} \mid (3+2^m)^k - 1 \Longleftrightarrow 2^{m-2} \mid \frac{1}{8}((1+8)^\ell - 1) \Longleftrightarrow 2^{m-2} \mid \ell \Longleftrightarrow 2^{m-1} \mid k$. This proves (22). Thus $3 + 2^m$ is of order $2^{m-1}$ in the ring $A = \mathbb{Z}/2^{m+1}\mathbb{Z}$, and $(3 + 2^m)^k \equiv 1$ or $\equiv 3 \pmod 8$ for all $k$. By (21), it follows that there is a single cycle base $A \setminus 2A$ of $A$. Whence $|\bar{\mathscr{T}}(A)| = 1$. □

## References


[1] I. Angiono, C. Galindo, and L. Vendramin, "Hopf braces and Yang–Baxter operators", *Proc. Amer. Math. Soc.* **145**:5 (2017), 1981–1995. MR Zbl

[2] R. J. Baxter, "Partition function of the eight-vertex lattice model", *Ann. Physics* **70** (1972), 193–228. MR Zbl

[3] F. Catino and R. Rizzo, "Regular subgroups of the affine group and radical circle algebras", *Bull. Aust. Math. Soc.* **79**:1 (2009), 103–107. MR Zbl

[4] F. Catino, I. Colazzo, and P. Stefanelli, "On regular subgroups of the affine group", *Bull. Aust. Math. Soc.* **91**:1 (2015), 76–85. MR Zbl

[5] F. Catino, I. Colazzo, and P. Stefanelli, "Regular subgroups of the affine group and asymmetric product of radical braces", *J. Algebra* **455** (2016), 164–182. MR Zbl

[6] F. Cedó, E. Jespers, and J. Okniński, "Retractability of set theoretic solutions of the Yang–Baxter equation", *Adv. Math.* **224**:6 (2010), 2472–2484. MR Zbl

[7] F. Cedó, E. Jespers, and A. del Río, "Involutive Yang–Baxter groups", *Trans. Amer. Math. Soc.* **362**:5 (2010), 2541–2558. MR Zbl

[8] L. N. Childs, "Fixed-point free endomorphisms and Hopf Galois structures", *Proc. Amer. Math. Soc.* **141**:4 (2013), 1255–1265. MR Zbl

[9] M. R. Darnel, *Theory of lattice-ordered groups*, Monographs and Textbooks in Pure and Applied Mathematics **187**, Marcel Dekker, New York, 1995. MR Zbl

[10] V. G. Drinfeld, "On some unsolved problems in quantum group theory", pp. 1–8 in *Quantum groups* (Leningrad, 1990), edited by P. P. Kulish, Lecture Notes in Math. **1510**, Springer, Berlin, 1992. MR Zbl

[11] P. Etingof, T. Schedler, and A. Soloviev, "Set-theoretical solutions to the quantum Yang–Baxter equation", *Duke Math. J.* **100**:2 (1999), 169–209. MR Zbl

[12] P. Etingof, A. Soloviev, and R. Guralnick, "Indecomposable set-theoretical solutions to the quantum Yang–Baxter equation on a set with a prime number of elements", *J. Algebra* **242**:2 (2001), 709–719. MR Zbl

[13] S. C. Featherstonhaugh, A. Caranti, and L. N. Childs, "Abelian Hopf Galois structures on prime-power Galois field extensions", *Trans. Amer. Math. Soc.* **364**:7 (2012), 3675–3684. MR Zbl

[14] T. Gateva-Ivanova and M. Van den Bergh, "Semigroups of $I$-type", *J. Algebra* **206**:1 (1998), 97–112. MR Zbl

[15] L. Guarnieri and L. Vendramin, "Skew braces and the Yang–Baxter equation", *Math. Comp.* **86**:307 (2017), 2519–2534. MR Zbl

[16] N. Jacobson, *Structure of rings*, Amer. Math. Soc. Colloq. Publ. **37**, Providence, RI, 1964. MR

[17] P. Jedlička, A. Pilitowska, and A. Zamojska-Dzienio, "Cocyclic braces and indecomposable cocyclic solutions of the Yang–Baxter equation", *Proc. Amer. Math. Soc.* **150**:10 (2022), 4223–4239. MR Zbl

[18] W. Rump, "A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation", *Adv. Math.* **193**:1 (2005), 40–55. MR Zbl

[19] W. Rump, "Braces, radical rings, and the quantum Yang–Baxter equation", *J. Algebra* **307**:1 (2007), 153–170. MR Zbl

[20] W. Rump, "Classification of cyclic braces", *J. Pure Appl. Algebra* **209**:3 (2007), 671–685. MR Zbl

[21] W. Rump, "The brace of a classical group", *Note Mat.* **34**:1 (2014), 115–144. MR Zbl

[22] W. Rump, "Classification of cyclic braces, II", *Trans. Amer. Math. Soc.* **372**:1 (2019), 305–328. MR Zbl

[23] W. Rump, "Construction of finite braces", *Ann. Comb.* **23**:2 (2019), 391–416. MR Zbl

[24] W. Rump, "Classification of indecomposable involutive set-theoretic solutions to the Yang–Baxter equation", *Forum Math.* **32**:4 (2020), 891–903. MR Zbl

[25] W. Rump, "One-generator braces and indecomposable set-theoretic solutions to the Yang–Baxter equation", *Proc. Edinb. Math. Soc.* (2) **63**:3 (2020), 676–696. MR Zbl

[26] W. Rump, "Cocyclic solutions to the Yang–Baxter equation", *Proc. Amer. Math. Soc.* **149**:2 (2021), 471–479. MR Zbl

[27] W. Rump, "Uniconnected solutions to the Yang–Baxter equation arising from self-maps of groups", *Canad. Math. Bull.* **65**:1 (2022), 225–233. MR Zbl

[28] J. Tate and M. van den Bergh, "Homological properties of Sklyanin algebras", *Invent. Math.* **124**:1-3 (1996), 619–647. MR Zbl

[29] A. Weinstein and P. Xu, "Classical solutions of the quantum Yang–Baxter equation", *Comm. Math. Phys.* **148**:2 (1992), 309–343. MR Zbl

[30] C. N. Yang, "Some exact results for the many-body problem in one dimension with repulsive delta-function interaction", *Phys. Rev. Lett.* **19** (1967), 1312–1315. MR Zbl

Received March 23, 2022. Revised October 8, 2022.

WOLFGANG RUMP
INSTITUTE FOR ALGEBRA AND NUMBER THEORY
UNIVERSITY OF STUTTGART
STUTTGART
GERMANY
rump@mathematik.uni-stuttgart.de

# PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm





See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2023 is US $605/year for the electronic version, and $820/year for print and electronic.
Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

# PACIFIC JOURNAL OF MATHEMATICS

Volume 323 No. 1 March 2023