Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra 307 (2007) 153–170
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Braces, radical rings, and the quantum Yang–Baxter equation

Wolfgang Rump

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

Received 15 December 2005

Available online 30 May 2006

Communicated by Michel Van den Bergh

Abstract

Non-degenerate cycle sets are equivalent to non-degenerate unitary set-theoretical solutions of the quantum Yang–Baxter equation. We embed such cycle sets into generalized radical rings (braces) and study their interaction in this context. We establish a Galois theory between ideals of braces and quotient cycle sets. Our main result determines the relationship between two square-free cycle sets operating transitively on each other.

Keywords: Quantum Yang–Baxter equation; Set-theoretical solution; Radical ring; Cycle set; Brace; Square-free

0. Introduction

The study of set-theoretical solutions of the quantum Yang–Baxter equation was initiated by Drinfeld [2] and pursued by several authors [3–6,10–13]. In [12] we showed that left non-degenerate unitary solutions are equivalent to *cycle sets*, i.e. sets X with a left invertible binary operation satisfying the equation

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

We showed that finite cycle sets X give rise to (left and right) non-degenerate solutions and can be naturally extended to the free abelian group $\mathbb{Z}^{(X)}$. The above equation is then replaced by

$$(a + b) \cdot c = (a \cdot b) \cdot (a \cdot c).$$

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

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2006.03.040

An abelian group A with a left distributive multiplication which makes A into a cycle set satisfying the preceding equation is called a *linear* cycle set [12].

In this article, we show that linear cycle sets are closely related to radical rings. More precisely, we prove that a linear cycle set A can be regarded as an abelian group 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°. Though A is neither left distributive nor associative, it satisfies an equation (B2) which generalizes both conditions (see Definition 2). There is a natural largest radical subring of A which coincides with A if A is left distributive. Another equivalent description, due to [4], represents A as a module over the group A° such that A and A° are related via a bijective 1-cocycle $\tau : A^\circ \to A$. With regard to the property that A combines two different equations or groups to a new entity, we call A a *brace*.

There is a module theory over braces, which will be developed, to some extent, in Sections 3 and 4. A sub-cycle-set X of a brace A which generates A as an abelian group will be called a *cycle base* of A. For the analysis of X and A, ideals of A play an important part (see below). We establish a kind of Galois theory for ideals of A in terms of partitions of X (Theorem 1).

Our main reason for introducing braces was to apply them to cycle sets and their corresponding solutions of the quantum Yang–Baxter equation. A cycle set X is said to be *square-free* if $x \cdot x = x$ holds for all $x \in X$. In [12] we proved that every finite square-free cycle set X with more than one element admits a *decomposition*, i.e. a non-trivial partition into left invariant sub-cycle-sets. This result substantiated the conjecture [4,6] that the solutions of the quantum Yang–Baxter equation corresponding to finite square-free cycle sets arise from *binomial semigroups* [5,6], hence from *quantum binomial algebras* [6,9]. A new and much more general conjecture [5] claims that every finite square-free cycle set X with more than one element has two different elements x, y with equal left multiplication on X. The truth of this conjecture would imply that every finite square-free unitary solution of the quantum Yang–Baxter equation is a multipermutation solution in the sense of [4].

The use of braces leads to the following strategy to attack problems of that type. We start with a non-degenerate cycle set X and embed it into a brace A so that X becomes a cycle base of A. Then the inverse of the map $x \mapsto y \cdot x$ in X can be expressed by $x \mapsto x + xy$ in A. So the left multiplication of an element $x \in X$ by y in X does not change x modulo A^2. Hence X decomposes unless A/A^2 is cyclic. Moreover, X is square-free if and only if the elements $x \in X$ satisfy $x^2 = 0$ in A. This sheds new light upon the decomposition theorem [12]. On the other hand, the more general conjecture claims that a brace A with a finite square-free cycle base admits a non-trivial *socle*

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

This would be trivial if A is a radical ring. In general, however, the question is rather delicate. It can be regarded as a nilpotency problem. However, there are at least two kinds of radical series of A. To distinguish them, we set $A^{n+1} := A(A^n)$ and $A^{(n+1)} := (A^{(n)})A$ for $n \in \mathbb{N}$. It is fairly easy to prove that the second series consists of right ideals, and that $A^{(n)} = 0$ for some n if $|A|$ is a prime power. Nevertheless, this does not imply that $\operatorname{Soc}(A)$ is not zero. The latter would follow if we could show that the first radical series ends up with 0. We will prove that A^n is an ideal for all n, but it is indeed possible that the A^n stabilize at a non-zero ideal (see Example 2). The

conjecture thus states that this cannot happen if A has a finite square-free cycle base X. By the decomposition theorem [12], we can assume that A is a sum of two proper right ideals B and C with cycle bases Y and Z forming a partition of X. By induction, we can further assume that $B^n = C^n = 0$ for some n. So we are led to the question whether the powers $((BC)C\cdots)C$ and $((CB)B\cdots)B$ might stabilize at non-zero right ideals. By Theorem 1, this can be expressed in terms of the sub-cycle-sets Y and Z of X.

Our main theorem (Theorem 2) deals with the case where Y and Z operate transitively on each other. It states that the elements of Y and Z can be arranged as cycles, i.e. $Y = \{y_i\}_{i\in\mathbb{Z}/m\mathbb{Z}}$ and $Z = \{z_j\}_{j\in\mathbb{Z}/n\mathbb{Z}}$ such that $y_i \cdot z_j = z_{j+1}$ and $z_j \cdot y_i = y_{i+1}$ for all $i \in \mathbb{Z}/m\mathbb{Z}$ and $j \in \mathbb{Z}/n\mathbb{Z}$. In the special case $Y = Z$, the square-free property implies that $|Y| = |Z| = 1$, which yields the decomposition theorem [12]. Note that Theorem 2 does not give any information about the internal structure of Y and Z. By induction, however, we can assume that Y contains two elements y and y' with equal left multiplication on Y. Hence y and y' operate in the same way on $Y \cup Z$. This proves the general conjecture for unions of two mutually transitive cycle sets.

1. Fully retractible cycle sets

A set X with a binary operation $X^2 \xrightarrow{\cdot} X$ is called a *cycle set* [12] if the left multiplication $\sigma(x) : y \mapsto x \cdot y$ is invertible, and the equation

$$(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z) \tag{1}$$

holds for all $x, y, z \in X$. Thus σ defines a map

$$\sigma : X \to \mathrm{S}(X) \tag{2}$$

into the group $\mathrm{S}(X)$ of permutations on X. If we introduce

$$y^x := \sigma(x)^{-1}(y), \tag{3}$$

a cycle set X can be defined in terms of equations, namely, Eq. (1) together with

$$x \cdot y^x = (x \cdot y)^x = y. \tag{4}$$

A *morphism* between cycle sets X, Y is defined to be a map $f : X \to Y$ which satisfies

$$f(x \cdot y) = f(x) \cdot f(y) \tag{5}$$

for all $x, y \in X$. We call a cycle set X *non-degenerate* if the map $x \mapsto x \cdot x$ is bijective. For example, this condition is satisfied when X is *square-free*, i.e. $x \cdot x = x$ for all $x \in X$. The category of non-degenerate cycle sets will be denoted by **Cyc**.

In [12] we have shown that non-degenerate cycle sets X are in one-to-one correspondence with set-theoretical solutions R of the quantum Yang–Baxter equation which are non-degenerate and unitary. Let us briefly recall this correspondence. If X is given, we define $R : X^2 \to X^2$ by

$$R(x, y) := \left(x^y, x^y \cdot y\right). \tag{6}$$

Then R satisfies the *quantum Yang–Baxter equation*

$$R^{12}R^{13}R^{23} = R^{23}R^{13}R^{12} \tag{7}$$

and the *unitarity condition*

$$R^{21}R = 1. \tag{8}$$

Moreover R is *non-degenerate*, i.e. the component maps $x \mapsto x^y$ and $y \mapsto x^y \cdot y$ are bijective. If we apply a twist $(x, y) \mapsto (y, x)$ to R, we get a map S which satisfies the braid relation

$$S^{12}S^{23}S^{12} = S^{23}S^{12}S^{23}. \tag{9}$$

In this way, the unitary solutions R of (7) correspond to the symmetric sets (X, S) in the sense of [4].

Definition 1. A cycle set A with an abelian group structure will be called *linear* [12] if it satisfies the following equations ($\forall a, b, c \in A$):

$$a \cdot (b + c) = a \cdot b + a \cdot c, \tag{10}$$

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

Remark. Equation (10) immediately gives $a \cdot 0 = 0$. Hence, if we set $a = b = 0$, Eq. (11) turns into $0 \cdot c = 0 \cdot (0 \cdot c)$. Since every element can be written in the form $0 \cdot c$, we thus get

$$a \cdot 0 = 0; \quad 0 \cdot a = a \tag{12}$$

for all $a \in A$. Therefore, Definition 1 is equivalent to that of [12].

Note that Eq. (11) implies (1). The category of linear cycle sets with the obvious morphisms will be denoted by **LCyc**. By [12, Proposition 9], every linear cycle set is non-degenerate.

Proposition 1. *The forgetful functor* **LCyc** $\to$ **Cyc** *admits a left adjoint.*

Proof. Let X be a non-degenerate cycle set. Consider the free abelian group $\mathbb{Z}^{(X)}$ generated by X. The left multiplication (2) in X admits a unique extension to a map $X \times \mathbb{Z}^{(X)} \xrightarrow{\cdot} \mathbb{Z}^{(X)}$ such that Eq. (10) is satisfied for all $a \in X$ and $b, c \in \mathbb{Z}^{(X)}$. By [12, Proposition 6], there is a further extension $\mathbb{Z}^{(X)} \times \mathbb{Z}^{(X)} \xrightarrow{\cdot} \mathbb{Z}^{(X)}$ which makes $\mathbb{Z}^{(X)}$ into a linear cycle set. Moreover, the embedding $X \hookrightarrow \mathbb{Z}^{(X)}$ is a morphism in **Cyc**, and every morphism $X \to A$ into a linear cycle set A has a unique extension $\mathbb{Z}^{(X)} \to A$ in **LCyc**. This proves the proposition. □

For any cycle set X, the image $\sigma(X)$ in $\mathrm{S}(X)$ admits an induced binary operation

$$\sigma(x) \cdot \sigma(y) := \sigma(x \cdot y), \tag{13}$$

and $\sigma(X)$ is called the *retraction* of X (cf. [4, 3.2], [12, §6]). By [12, Proposition 10], the retraction $\sigma(X)$ is non-degenerate if and only if X is non-degenerate. Thus any $X \in \mathbf{Cyc}$ gives rise to a natural morphism

$$X \twoheadrightarrow \sigma(X) \tag{14}$$

in **Cyc**. If (14) is injective, we call X *irretractible*, otherwise *retractible*. If X is linear, then Eq. (11) implies that (14) makes $\sigma(X)$ into a linear cycle set such that (14) becomes a morphism in **LCyc**. For any $X \in \mathbf{Cyc}$, the retraction of $\mathbb{Z}^{(X)}$ will be denoted by $\mathrm{A}(X)$. So the retraction of X can be identified with the image of the cycle set morphism

$$X \to \mathrm{A}(X). \tag{15}$$

In general, the retraction of $X \in \mathbf{Cyc}$ may be retractible. Therefore, we call X *fully retractible* if some iterated retraction $\sigma^n(X)$ is a singleton. Such cycle sets correspond to *multipermutation solutions* [4] of Eq. (9).

2. Rings and braces

In this section, we turn our attention to linear cycle sets. We will show that they are closely related to radical rings. First, let us rewrite the axioms (10)–(11) of a linear cycle set in terms of the inverse operation a^b. For this purpose, we introduce the binary operation

$$a \circ b := a^b + b. \tag{16}$$

Proposition 2. *Let A be an abelian group with a binary operation $A \times A \xrightarrow{\cdot} A$, such that the left multiplication admits an inverse* (3)*. Then A is a linear cycle set if and only if the following are satisfied*:

$$(a+b)^c = a^c + b^c, \tag{17}$$

$$\left(a^b\right)^c = a^{b \circ c}. \tag{18}$$

Proof. Equation (10) is equivalent to $b + c = (a \cdot b + a \cdot c)^a$. Replacing b by b^a and c by c^a, the latter equation turns into (17). To convert (11) into (18), replace b by b^a and then c by $(c^a)^b$. This gives $(a + b^a) \cdot (c^b)^a = c$, which is equivalent to (18). □

Remark 1. The abbreviation (16) does not only make Eq. (18) more appealing. If (17) is assumed, Eq. (18) is equivalent to the associativity

$$(a \circ b) \circ c = a \circ (b \circ c). \tag{19}$$

Proposition 3. *For a linear cycle set A, the operation* (16) *defines a group structure on A.*

Proof. While Eq. (17) trivially implies that $0^c = 0$, Eq. (12) yields $a^0 = a$. Hence

$$0 \circ a = a \circ 0 = a. \tag{20}$$

By Eq. (16), we have $(a \cdot (-a)) \circ a = (a \cdot (-a))^a + a = -a + a = 0$. Hence

$$\big(-(a \cdot a)\big) \circ a = 0, \tag{21}$$

which gives $a = a^0 = a^{(-a \cdot a) \circ a}$. Therefore, Eq. (18) implies that $a \cdot a = a^{-(a \cdot a)}$, which yields $a \circ (-(a \cdot a)) = a^{-(a \cdot a)} - a \cdot a = 0$. □

Remark 2. Equation (16) can be interpreted as a bijective 1-cocycle from $(A, \circ)$ to A (see [4, 2.4]).

Now we proceed one step further and replace a^b by a multiplication.

Definition 2. Let A be an abelian group with a multiplication $A \times A \to A$. We call A a *brace* if the following are satisfied for all $a, b, c \in A$.

(B1) $(a + b)c = ac + bc$.
(B2) $a(bc + b + c) = (ab)c + ab + ac$.
(B3) The map $x \mapsto xa + x$ is bijective.

At first glance, (B2) looks like a cross between associativity and left distributivity. In fact, together with

(B4) $a(b + c) = ab + ac$,

the axioms (B1) and (B2) just state that A is an associative ring (without 1).

There is another, less obvious, interpretation of (B2). As for an ordinary ring, let us introduce the *circle operation*

$$a \circ b := ab + a + b. \tag{22}$$

Proposition 4. *Let A be an abelian group with a right distributive multiplication. A is a brace if and only if A is a group with respect to the circle operation* (22).

Proof. Using (B1), a direct calculation shows that the associativity of (22) is equivalent to (B2). Moreover, (B1) implies that $0c = 0$ for all $c \in A$. Assume now that A is a brace. Inserting $b = c = 0$ in (B2) yields $(a0)0 + a0 = 0$. Hence $a0 = 0$ by virtue of (B3). Thus every brace satisfies

$$0a = a0 = 0, \tag{23}$$

which is equivalent to $0 \circ a = a \circ 0 = a$. Now (B3) implies that every $a \in A$ has a unique left inverse a' with respect to (22). Hence $a' \circ a \circ a' = 0 \circ a' = a' \circ 0$, which gives $a \circ a' = 0$. Thus we have shown that A is a group with respect to (22), when A is a brace. Now the converse is trivial. □

Recall that an associative ring is said to be a *radical ring* if it is a group with respect to the circle operation (22). So we get

Corollary. *A brace A is left distributive if and only if it is a radical ring.*

Next we show that braces are equivalent to linear cycle sets via

$$a^b = ab + a. \tag{24}$$

Proposition 5. *Equation* (24) *establishes a one-to-one correspondence between braces and linear cycle sets.*

Proof. This follows from Proposition 2 and Remark 1. □

Note, in particular, that by virtue of (24), the circle operation (22) of a brace coincides with the operation (16) of the corresponding linear cycle set. Therefore, all operations and concepts for linear cycle sets apply to braces as well. For example, it makes sense to speak of a retractible brace. In the sequel, the transfer of terminology between linear cycle sets and braces will be assumed without further notice.

For an associative ring R, the circle operation (22) gives rise to a semigroup with neutral element 0, the *adjoint monoid* of R.

Definition 3. Let A be a brace. The group $A^\circ := (A, \circ)$ will be called the *adjoint group* of A. An abelian group M together with a monoid morphism from A° to the adjoint monoid of $\mathrm{End}(M)^{\mathrm{op}}$ will be called an *A-module*.

Explicitly, this means that there is a right operation

$$M \times A \to M \tag{25}$$

such that

$$(x + y)a = xa + ya, \tag{26}$$

$$x(a \circ b) = (xa)b + xa + xb, \tag{27}$$

$$x0 = 0 \tag{28}$$

holds for $x, y \in M$ and $a, b \in A$. In particular, Definition 2 together with Eq. (23) shows that A itself is an A-module. The category of A-modules, with additive maps respecting the operation (25) as morphisms, will be denoted by $\mathbf{Mod}(A)$.

Remark 1, and Eq. (27) as a consequence of Definition 3, give two rather different interpretations of (B2). A third interpretation comes from the fact that every A-module M can be regarded as a right A°-module via

$$M \times A^\circ \to M; \quad (x, a) \mapsto xa + x, \tag{29}$$

and vice versa. This follows by a straightforward calculation. Therefore, the analogue of (B3) holds for modules over braces, too. Hence we have an equivalence of categories

$$\mathbf{Mod}(A) \approx \mathbf{Mod}\text{-}A^\circ \tag{30}$$

which shows that **Mod**(A) is an abelian category. In particular, the endomorphisms of any module M over a brace A form an associative ring with 1, denoted by $\mathrm{End}_A(M)$. The concepts of submodule, factor module, sum and intersection of submodules, carry over to **Mod**(A) without change. As usual, the submodules of A will be called *right ideals*. (Since A need not be left distributive, there is no similar concept of left ideal.) By Eq. (27), every element x of an A-module M *generates* a submodule $xA + \mathbb{Z}x$, consisting of the finite sums $xa_1 + \cdots + xa_r + nx$ with $a_1, \ldots, a_r \in A$ and $n \in \mathbb{Z}$. By lack of the left distributivity (B4), this description cannot be simplified, in general.

A map $f : A \to B$ between braces will be called a *morphism* if f respects addition and multiplication. The image $f(A)$ of a morphism f is always a *subbrace* of B, that is, a subset which is closed under addition and multiplication. A subbrace I of A will be called an *ideal* if ab and ba belong to I whenever $a \in I$ and $b \in A$. The kernel of any morphism between braces is an ideal, and each ideal arises in this way. In fact, every ideal I of a brace A gives rise to a morphism $A \to A/I$ onto the *factor brace* $A/I := \{a + I \mid a \in A\}$. To see that A/I is well-defined, we have to verify that $a(x + c) - ac \in I$ whenever $x \in I$ and $a, c \in A$. Since I is an A°-submodule of A, we can write x in the form $x = bc + b$ with a unique $b \in I$. Now the assertion follows immediately by (B2).

3. Radical series and socle series of a brace

Let A be a brace. For an A-module M, define

$$MA := \left\{ \sum_{i=1}^{n} x_i a_i \;\middle|\; x_i \in M,\ a_i \in A \right\}. \tag{31}$$

By virtue of (26) and (27), this is a submodule of M. In particular, we set $A^{(1)} := A$, and $A^{(n+1)} := (A^{(n)})A$. This gives a descending sequence of right ideals

$$A \supset A^{(2)} \supset A^{(3)} \supset \cdots, \tag{32}$$

which need not be ideals, in general (see Example 2 below).

If A is an associative ring, and $M \in$ **Mod**(A), then MI is a submodule for any ideal I. For an arbitrary brace A, this is also true, but not at all obvious.

Proposition 6. *Let A be a brace, and $M \in$* **Mod**(A). *For any ideal I of A,*

$$MI := \left\{ \sum_{i=1}^{n} x_i a_i \;\middle|\; x_i \in M,\ a_i \in I \right\}$$

is a submodule of M.

Proof. Let $x \in M$, $a \in I$, and $b \in A$ be given. It suffices to show that $(xa)b \in MI$. By Eq. (27), we have $(xa)b = x(a \circ b) - xa - xb$. Thus we have to show that $x(a \circ b) - xb \in MI$. Let b' be the inverse of b in A°. Then $b'b + b' + b = 0$. Hence

$$c := b' \circ a \circ b = (b'a + b' + a) \circ b = (b'a + b' + a)b + (b'a + b' + a) + b$$
$$= (b'a + a)b + (b'a + a) \in I.$$

So we get $x(a \circ b) - xb = x(b \circ c) - xb = (xb)c + xc \in MI$. □

Proposition 6 shows, in particular, that the product JI of a right ideal J with an ideal I is a right ideal. In contrast to ordinary module theory, JI need not be an ideal when I and J are ideals (see Example 2 below). However, Proposition 6 implies the following

Corollary. *Let I be an ideal of a brace A. Then AI is an ideal.*

Therefore, we define the *radical series*

$$A \supset A^2 \supset A^3 \supset \cdots \tag{33}$$

of a brace A by $A^1 := A$, and $A^{n+1} := A(A^n)$. By the preceding corollary, the radical series consists of ideals. Note that $A^2 = A^{(2)}$.

Dually, we define the *socle series* of A by $\operatorname{Soc}_0(A) = 0$ and

$$\operatorname{Soc}_{n+1}(A) := \big\{x \in A \mid \forall a \in A\colon\ ax \in \operatorname{Soc}_n(A)\big\}, \tag{34}$$

for all $n \in \mathbb{N}$. Instead of $\operatorname{Soc}_1(A)$, we also write $\operatorname{Soc}(A)$.

Proposition 7. *The socle series of a brace A consists if ideals. The factor brace $A/\operatorname{Soc}(A)$ is isomorphic to the retraction of A.*

Proof. Let us first prove the equivalence

$$c \in \operatorname{Soc}(A) \quad \Leftrightarrow \quad \forall a \in A\colon\ a(b + c) = ab \tag{35}$$

for any $b \in A$. Assume that $c \in \operatorname{Soc}(A)$. Then (B2) yields $a(b + c) = a(bc + b + c) = (ab)c + ab + ac = ab$. Conversely, let the right-hand condition of (35) be satisfied. Then $c = db + d$ for a unique $d \in A$. Hence $ab = a(b + db + d) = (ad)b + ad + ab$, which gives $(ad)b + ad = 0$ for all $a \in A$. Thus $ad = 0$ for all $a \in A$, i.e. $d \in \operatorname{Soc}(A)$. So we have proved the implication $c \in \operatorname{Soc}(A) \Rightarrow d \in \operatorname{Soc}(A)$ for any $b \in A$. Therefore, $\operatorname{Soc}(A)$ is invariant under the adjoint group A°. In particular, this shows that $\operatorname{Soc}(A)$ is invariant under right multiplication. Hence $d \in \operatorname{Soc}(A)$ implies that $c \in \operatorname{Soc}(A)$, which completes the proof of (35). Now (35) also shows that $\operatorname{Soc}(A)$ is an additive subgroup of A. Hence $\operatorname{Soc}(A)$ is an ideal. By induction, it follows that the socle series consists of ideals.

To prove the remaining assertion, we note that two elements $a, b \in A$ are mapped to the same element in the retraction $\sigma(A)$ if and only if $a \cdot x = b \cdot x$ holds for all $x \in A$. Since left multiplication is invertible, the latter equation is equivalent to $x^a = x^b$. By Eq. (24), this can be written as $xa = xb$. Therefore, Eq. (35) implies that $A/\operatorname{Soc}(A)$ is isomorphic to the retraction of A. □

Table 1

	111	100	011	010	101	001	110
111	0	0	0	0	0	0	0
100	110	0	001	111	110	111	001
011	110	0	001	111	110	111	001
010	110	111	110	0	001	111	001
101	110	111	110	0	001	111	001
001	0	111	111	111	111	0	0
110	0	111	111	111	111	0	0

Example 1. Let R be an associative ring with 1, and let A be a right (unital) R-module. Assume that $\mu : A \to R^\times$ is a homomorphism from the additive group of A into the unit group of R such that

$$\mu\big(a\mu(b)\big) = \mu(a) \tag{36}$$

holds for all $a, b \in A$. Then it is readily verified that the multiplication

$$ab := a\big(\mu(b) - 1\big) \tag{37}$$

makes A into a brace. For example, consider the group ring $A = (\mathbb{Z}/n\mathbb{Z})[C_n]$ of a cyclic group $C_n = \langle c \rangle$ of order n, where $n = 0$ stands for the infinite cyclic group, and put $R := A$. Then

$$\mu\left(\sum n_i c^i\right) := c^{\sum n_i} \tag{38}$$

defines a morphism μ which satisfies (36). Hence A becomes a brace with

$$A^2 = \operatorname{Soc}(A) = \operatorname{Ker}\mu. \tag{39}$$

Example 2. Let A be a three-dimensional vector space over the prime field $\mathbb{F}_2$. The elements of A can thus be represented as $\{0,1\}$-words of length 3. We introduce a multiplication on the abelian group A by Table 1 (the line and column of 000 are omitted).

Then A is a brace with $A^2 = \{0, 111, 001, 110\} = A^3$, $A^{(3)} = \{0, 111\}$, $A^{(4)} = 0$, and trivial socle. Hence A cannot be a ring. Note that, while $A^{(2)}$ is always an ideal, $A^{(3)}$ is not an ideal in this example. Since $A^{(3)} = (A^2)A$, this also shows that the product of two ideals need not be an ideal. The adjoint group A° is of dihedral type. It can be generated, e.g., by $c = 011$ (order 4) and $s = 100$ (order 2) with $s \circ c \circ s \circ c = 0$.

Next we will give a combinatorial description of brace ideals.

Definition 4. Let A be a brace. A subset X of A will be called a *cycle base* if X is invariant under A° and X generates A as an abelian group.

Since X generates A°, the invariance under A° can be replaced by the condition that X is a sub-cycle-set of A. For example, A itself is a cycle base of A. On the other hand, every non-degenerate cycle set X is a cycle base of $\mathbb{Z}^{(X)}$. By Definition 4, the adjoint group A° of a brace A operates on each cycle base of A, and by Proposition 7, the kernel of this operation is $\operatorname{Soc}(A)$.

Definition 5. Let X be a set. By $\Pi(X)$ we denote the set of *partitions* of X, i.e. collections P of pairwise disjoint non-empty subsets of X such that $\bigcup P = X$. If $x, y \in X$ belong to the same $Y \in P$, we also write $x \overset{P}{\sim} y$. For $P, P' \in \Pi(X)$, we call P a *refinement* of P' and write $P \geqslant P'$ if $x \overset{P}{\sim} y$ implies $x \overset{P'}{\sim} y$. Note that $\Pi(X)$ is a complete lattice with join

$$\bigvee_{i\in I} P_i = \left\{ \bigcap_{i\in I} Y_i \;\middle|\; Y_i \in P_i,\ \bigcap_{i\in I} Y_i \neq \emptyset \right\}. \tag{40}$$

Let A be a brace with cycle base X. Every subgroup H of A° gives rise to a partition $P(H)$ such that $x, y \in X$ belong to the same $Y \in P(H)$ if and only if $y = xa + x$ for some $a \in H$. By Eq. (18), it follows that $P(H)$ is a partition. Conversely, every $P \in \Pi(X)$ defines a subgroup

$$I(P) := \left\{ a \in A \mid \forall Y \in P\colon\ Y^a = Y \right\} \tag{41}$$

of A°, where $Y^a := \{ya + y \mid y \in Y\}$.

Every partition $P \in \Pi(X)$ satisfies $\operatorname{Soc}(A) \subset I(P)$, and

$$P\big(I(P)\big) = \bigvee \left\{ P' \in \Pi(X) \mid I(P') = I(P) \right\}. \tag{42}$$

Similarly, if H is a subgroup of A°, then $I(P(H))$ is the largest subgroup H' of A° which satisfies $P(H') = P(H)$.

Definition 6. Let X be a cycle set, and let $P \in \Pi(X)$ be a partition. We define P to be *normal* if the equivalence

$$x \overset{P}{\sim} y \quad \Leftrightarrow \quad z \cdot x \overset{P}{\sim} z \cdot y \tag{43}$$

holds for all $x, y, z \in X$. If, in addition,

$$x \overset{P}{\sim} y \quad \Rightarrow \quad x \cdot z \overset{P}{\sim} y \cdot z \tag{44}$$

holds in X, we call P an *ideal* of X.

Remark. If $P \in \Pi(X)$ is normal, the implication (44) is equivalent to

$$x \overset{P}{\sim} y \quad \Rightarrow \quad z^x \overset{P}{\sim} z^y. \tag{45}$$

In fact, by virtue of (43), the conclusion of (44) is equivalent to $z \overset{P}{\sim} (y \cdot z)^x$. Now (45) follows if we substitute z by z^y.

Note that any morphism $f : X \to Y$ of cycle sets defines an ideal P of X such that $x \overset{P}{\sim} y \Leftrightarrow f(x) = f(y)$. Conversely, every ideal P of a cycle set X gives rise to a cycle set X/P with underlying set P and the induced operation. Thus if $Y, Z \in P$ with $y \in Y$ and $z \in Z$ are given, then $Y \cdot Z$ is the unique element of P that contains $y \cdot z$.

Theorem 1. *Let A be a brace with a cycle base X.*

(a) *A subgroup $N \supset \mathrm{Soc}(A)$ of A° is normal if and only if $P(N)$ is normal.*
(b) *A subgroup $I \supset \mathrm{Soc}(A)$ of A° is an ideal of A if and only if $P(I)$ is an ideal of X such that the cycle set $X/P(I)$ is non-degenerate.*
(c) *If $P \in \Pi(X)$ is an ideal with X/P non-degenerate, then $I(P)$ is an ideal of A.*

Proof. In what follows, let b' denote the inverse of an element $b \in A^\circ$. We show first that an ideal I of A is a normal subgroup of A°. The equation

$$a \circ b = a^b + b \tag{46}$$

shows that I is a subgroup of A°. If $a \in I$ and $b \in A^\circ$, then $ba + a \in I$ can be written in the form $ba + a = cb + c$ with a unique $c \in I$. Hence $b \circ a = ba + a + b = cb + c + b = c \circ b$. This shows that I is a normal subgroup of A°.

(a) The condition that $P(N)$ is normal states that $x^b \overset{P(N)}{\sim} (x^a)^b$ holds for all $x \in X$ and $a \in N$, i.e. there is an element $c \in N$ with $(x^a)^b = (x^b)^c$. By Eq. (18), the latter equation is equivalent to $x(a \circ b) = x(b \circ c)$. Since X generates A as an abelian group, this means that $a \circ b$ and $b \circ c$ belong to the same residue class modulo $\mathrm{Soc}(A)$. Hence $\mathrm{Soc}(A) \subset N$ implies that the condition reduces to $b' \circ a \circ b \in N$ for all $a \in N$ and $b \in A^\circ$.

(b) By virtue of (a), we can assume that I is a normal subgroup of A°, so that $P := P(I)$ is a normal partition. Let us show first that I is an ideal of A if and only if I is invariant under A°. The necessity is trivial. Conversely, let I be A°-invariant. By Eq. (46), we infer that I is an additive subgroup of A. The invariance of I under left multiplication follows by the equation

$$b \circ a \circ b' = (ba + a)^{b'} \tag{47}$$

obtained in the proof of Proposition 6.

Next we analyse (45) under the assumption that P is normal. With $y := x^a$ for some $a \in I$, the implication (45) says that for $x, z \in X$ and $a \in I$, there exists an element $c \in I$ with $(z^x)^c = z^{x^a}$. This means that for $x \in X$ and $a \in I$, there are $c \in I$ and $s \in \mathrm{Soc}(A)$ with $x \circ c = s + x^a$. The latter equation says that $(s + x^a) \circ x' \in I$, i.e. $t \circ x^a \circ x' \in I$ for some $t \in \mathrm{Soc}(A)$. As $\mathrm{Soc}(A) \subset I$, this is equivalent to $x^a \circ x' \in I$. Since $x^a \circ x' = (xa + x)x' + xa + x + x' = (xa)^{x'}$, we have shown that P is an ideal if and only if $(xa)^{x'} \in I$ holds for $x \in X$ and $a \in I$. Here it makes no difference if we replace a by a'. Now Eq. (46) yields $(xa')^{x'} \circ x \circ a = (xa' + x) \circ a = x^{a'} \circ a = x + a = a^{x'} \circ x$, whence $(xa')^{x'} = a^{x'} \circ x \circ a' \circ x'$. Therefore, P is an ideal if and only if $a^{x'} \in I$ for all $a \in I$ and $x \in X$.

Now we assume that P is an ideal. Consider the cycle base $-X := \{-x \mid x \in X\}$. Since $(-x)^a = -(x^a)$, the partition of I with respect to $-X$ is $-P := \{-Y \mid Y \in P\}$. Moreover, the equation $-x = (x')^x$ implies that $x' \in -X$ for all $x \in X$. Let us show that $-P$ is an ideal of $-X$ if and only if X/P is non-degenerate. By Definition 6, $-P$ is an ideal if and only if

$$\forall x, y, z \in X\colon \quad x \overset{P}{\sim} y \quad \Rightarrow \quad z^{(-x)'} \overset{P}{\sim} z^{(-y)'}. \tag{48}$$

Let us show that (48) is equivalent to

$$\forall x, y, z \in X\colon \quad x \overset{P}{\sim} y \quad \Rightarrow \quad (-x)' \overset{P}{\sim} (-y)'. \tag{49}$$

Assume that $x \overset{P}{\sim} y$. If (48) holds, then $(-x)' = x^{(-x)'} \overset{P}{\sim} x^{(-y)'} \overset{P}{\sim} y^{(-y)'} = (-y)'$. The converse follows by Definition 6. If we replace x by $-x'$ and y by $-y'$, then (49) becomes

$$\forall x, y, z \in X: \quad x \cdot x \overset{P}{\sim} y \cdot y \quad \Rightarrow \quad x \overset{P}{\sim} y$$

since $-x' = x \cdot x$. So we have shown that $-P$ is an ideal if and only if X/P is non-degenerate. Therefore, the preceding paragraph implies that P is an ideal with X/P non-degenerate if and only if $a^{x'} \in I$ and $a^{(-x)'} \in I$ for all $a \in I$ and $x \in X$. Since X generates the adjoint group A°, the latter condition exactly states that I is invariant under A°, i.e. an ideal of A.

(c) Let $P \in \Pi(X)$ be an ideal of X. Assume that $a \in I(P)$. For $x \in X$ and $b \in A$, this implies that $(x^b)^a \overset{P}{\sim} x^b$. Hence $x^{b \circ a \circ b'} \overset{P}{\sim} x$, which shows that $I(P)$ is a normal subgroup of A°. So it remains to prove that $I(P)$ is A°-invariant. This means that $x^{a^b} \overset{P}{\sim} x$ holds for $a \in I(P)$, $x \in X$, and $b \in A$. By Eq. (46), $a^b \circ b' = a + b'$. Therefore, we have to show that $x^{a+b'} \overset{P}{\sim} x^{b'}$ holds for $a \in I(P)$, $x \in X$, $b \in A$. By induction, it suffices to prove the equivalence

$$\forall x \in X: \quad x^{a'} \overset{P}{\sim} x^{b'} \quad \Leftrightarrow \quad \forall x \in X: \quad x^{a'+y} \overset{P}{\sim} x^{b'+y} \tag{50}$$

for $a, b \in A$ and $y \in X$. Note that the left-hand side of (50) is equivalent to $\forall x \in X$: $x^a \overset{P}{\sim} x^b$. Assume that this condition is satisfied. By (44), this yields $x^{y^a} \overset{P}{\sim} x^{y^b}$ for all $x \in X$. Since $a' + y = y^a \circ a'$, we infer that

$$x^{a'+y} = x^{y^a \circ a'} \overset{P}{\sim} x^{y^b \circ a'} \overset{P}{\sim} x^{y^b \circ b'} = x^{b'+y}$$

holds for all $x \in X$. The reverse implication follows by a similar argument as in (b), replacing X by $-X$. □

Let us apply Theorem 1 to a brace A with a finite square-free cycle base X. Then the main result of [12] can be expressed by the implication

$$\big|P(A)\big| = 1 \quad \Rightarrow \quad |X| = 1. \tag{51}$$

For any ideal I of A, the ideal AI is generated, as an abelian group, by the differences $x - y$ with $x \overset{P(I)}{\sim} y$. Thus AI merely depends on the partition $P(I)$.

As mentioned in the introduction, there is a new conjecture [5] which claims that every finite square-free cycle set X is fully retractible. In terms of braces, this means that the socle series of any brace A with a finite square-free cycle base reaches A. Equivalently, the conjecture claims that the radical series of A reaches 0, i.e. there is no ideal $I \neq 0$ of A with $AI = I$. If we express this again in terms of X, we arrive at a new version of the conjecture which states that there is no non-trivial partition P of X which satisfies (43) and (44) such that any pair $x, x' \in X$ with $x \overset{P}{\sim} x'$ is connected by a sequence $x = x_0, x_1, \ldots, x_n = x'$ in X with $y_i \cdot x_{i-1} = z_i \cdot x_i$ for some $y_1, \ldots, y_n, z_1, \ldots, z_n \in X$ with $y_i \overset{P}{\sim} z_i$.

Our main result (Theorem 2) implies that such a partition P must be trivial if $|P| \leqslant 2$.

4. Simple modules

Let A be a brace, and let R be an associative ring with 1. Assume that $M \in \mathbf{Mod}(A)$ admits a left operation $R \times M \to M$ which makes M into a left R-module. Then we call M an (R, A)-*bimodule* if

$$(rx)a = r(xa) \tag{52}$$

holds for $x \in M$, $r \in R$, and $a \in A$. We call $S \in \mathbf{Mod}(A)$ *simple* if S has exactly two submodules. The analogue of Schur's lemma holds for simple A-modules, that is, $D := \mathrm{End}_A(S)$ is a skew-field. So S becomes a (D, A)-bimodule. Since SA is a submodule of S, we have either $SA = S$ or $SA = 0$. In the latter case, we call S *trivial*. If A is a radical ring, all simple A-modules are trivial since $A = \mathrm{Rad}\, A$ (see [8, p. 9, Theorem 2]).

Let S be a simple A-module. Then pS is a submodule for any rational prime p. If $pS = S$ for all p, then S is torsion-free and divisible as an abelian group. Hence S can be regarded as a $(\mathbb{Q}, A)$-bimodule. Otherwise, there is exactly one p with $pS = 0$, and S is an $(\mathbb{F}_p, A)$-bimodule. Thus any simple A-module S is a vector space over some prime field F. We call $\mathrm{char}\, S := \mathrm{char}\, F$ the *characteristic* of S.

Proposition 8. *Let A be a brace with $|A| = p^n$ for a rational prime p. Then every simple A-module S of characteristic p is trivial.*

Proof. By (29), S can be regarded as a module over the group algebra $\mathbb{F}_p A^\circ$. Since A° is a p-group, S is trivial as an A°-module (see [1, Lemma 3.14.1]). This means that $xa + x = x$ for all $x \in S$ and $a \in A$. Hence S is trivial as a module over the brace A. □

Corollary. *Let A be a brace with $|A| = p^n$ for a rational prime p. Then $A^{(n+1)} = 0$.*

Proof. For any $i \in \{1, \dots, n\}$, there is a submodule M of $A^{(i)}$ such that $A^{(i)}/M$ is simple. Hence $A^{(i+1)} \subset M$. By induction, this yields $A^{(n+1)} = 0$. □

The following example shows that Proposition 8 does not hold for arbitrary finite braces.

Example 3. Let $A := \{0, 1, 2, 3, 4, 5\}$ be the additive group of the ring $\mathbb{Z}/6\mathbb{Z}$. Consider the group homomorphism $\mu : A \to (\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\}$ which maps $\{0, 2, 4\}$ to 1 and $\{1, 3, 5\}$ to 5. Then A becomes a brace by Example 1, with multiplication (37) depicted by Table 2. Table 3 displays the circle operation of A. Here A° is isomorphic to the symmetric group S_3, generated by $c := 2$ and $s := 3$, such that $c \circ c \circ c = s \circ s = s \circ c \circ s \circ c = 0$. Moreover, $A^2 = \{0, 2, 4\} = A^{(3)}$ is a non-trivial simple A-module of characteristic 3. Note also that $\{2, 3, 4\}$ is a square-free cycle base of A.

Table 2

	1	2	3	4	5
1	4	0	4	0	4
2	2	0	2	0	2
3	0	0	0	0	0
4	4	0	4	0	4
5	2	0	2	0	2

Table 3

$\circ$	1	2	3	4	5
1	0	3	2	5	4
2	5	4	1	0	3
3	4	5	0	1	2
4	3	0	5	2	1
5	2	1	4	3	0

5. Square-free cycle sets

We have seen in Section 1 (15) that every non-degenerate cycle set X admits a natural morphism

$$\rho : X \to \mathrm{A}(X) \tag{53}$$

into a brace $\mathrm{A}(X)$, such that the retraction $\rho(X)$ of X is a cycle base of $\mathrm{A}(X)$. The subgroup of $\mathrm{S}(X)$ generated by $\sigma(X)$ can be identified with the adjoint group $\mathrm{A}(X)^\circ$. Thus if X is finite, $\mathrm{A}(X)$ is finite, too. The square-free property (see Section 1) of $\rho(X)$ means that $x^2 = 0$ holds for all $x \in \rho(X)$. So the term "square-free" translates well into the language of braces. Note that a cycle set is square-free if and only if its one-element subsets are sub-cycle-sets.

Let A be a brace. The torsion part $\mathrm{t}\,A$ of A as an abelian group is a right ideal, and $\mathrm{t}\,A$ admits a primary decomposition

$$\mathrm{t}\,A = \coprod_{p\,\text{prime}} A_p \tag{54}$$

into right ideals A_p. Assume that A is finite. Then the p-components A_p are Sylow subgroups of A°, and $A = A_2 \circ A_3 \circ A_5 \circ \cdots$. By Hall's theorem [7], this implies that A° is solvable. Note that the natural projection $\mathrm{pr} : A \twoheadrightarrow A_p$ need not be a morphism of cycle sets.

For an element $a \in A$, and $n \in \mathbb{N}$, we denote the n-fold product $a \circ \cdots \circ a$ by $a^{\circ n}$ and extend this notation to $n \in \mathbb{Z}$ such that $a^{\circ(-n)} \circ a^{\circ n} = 0$.

We say that a cycle set X *operates* on a set Z via a map $X \times Z \to Z$ given by $(x, z) \mapsto x \cdot z$ if the maps $z \mapsto x \cdot z$ are bijective and Eq. (1) holds for $x, y \in X$ and $z \in Z$. The maps $z \mapsto x \cdot z$ generate a subgroup of $\mathrm{S}(Z)$. If this permutation group is transitive, the operation of X on Z will also be called *transitive*. A non-empty cycle set X is said to be *decomposable* [12] if it admits a non-trivial partition $X = Y \sqcup Z$ with $x \cdot y \in Y$ and $x \cdot z \in Z$ for all $x \in X$, $y \in Y$, $z \in Z$, otherwise *indecomposable*. We agree that the empty cycle set is decomposable. Note that for any decomposition $X = Y \sqcup Z$ of cycle sets, Y and Z operate on each other.

Definition 7. We call a cycle set X with a decomposition $X = Y \sqcup Z$ a *bi-cycle* if $Y = \{y_i\}_{i \in \mathbb{Z}/m\mathbb{Z}}$ and $Z = \{z_j\}_{j \in \mathbb{Z}/n\mathbb{Z}}$ such that $y_i \cdot z_j = z_{j+1}$ and $z_j \cdot y_i = y_{i+1}$ for all $i \in \mathbb{Z}/m\mathbb{Z}$ and $j \in \mathbb{Z}/n\mathbb{Z}$.

For example, every element x of a square-free cycle set X gives rise to a permutation $\sigma(x)$ of X which yields a decomposition of X into (finite or infinite) cycles. Let $\mathrm{C}_x(y)$ denote the cycle which contains y. Then [12, Proposition 3], implies that for every pair of different elements $x, y \in X$, the cycles $\mathrm{C}_y(x)$ and $\mathrm{C}_x(y)$ are disjoint, and that $\mathrm{C}_y(x) \sqcup \mathrm{C}_x(y)$ is a bi-cycle.

Now we are ready to state our main result which generalizes Theorem 1 of [12].

Theorem 2. *Let X be a square-free cycle set with two finite sub-cycle-sets Y and Z such that Y and Z operate transitively on each other. Then $y \cdot z = y' \cdot z$ holds for all $y, y' \in Y$ and $z \in Z$.*

We need the following lemmata.

Lemma 1. *Let A be a brace, and let $a \in A$ be an element with $a^2 = 0$. Then*

$$a^{\circ n} = na \tag{55}$$

holds for all $n \in \mathbb{Z}$.

Proof. This follows immediately from the equation $(na) \circ a = (na)a + na + a = n(a^2) + na + a = (n+1)a$. □

To state the next lemma, we use the following abbreviation. Let G be a group which operates on a set X. We write $g \sim h$ for two elements $g, h \in G$ if there is some $x \in X$ such that $g^n x = h^n x$ holds for all $n \in \mathbb{Z}$.

Lemma 2. *Let G be a finite p-group acting transitively on a set X. Assume that G admits a generating subset S such that for any pair $s, t \in S$, there exists a sequence $s = s_0 \sim s_1 \sim \cdots \sim s_n = t$ in S. Then $sx = tx$ holds for all $s, t \in S$ and $x \in X$.*

Proof. There is nothing to prove if $|X| \leqslant 1$. Therefore, assume that $|X| > 1$. Then there is a normal subgroup N of G with $|N| = p$. Hence G/N acts transitively on the set X/N of N-orbits. By induction, we can assume that the residue classes $s + N$ with $s \in S$ all act in the same way on X/N. Since this action is transitive, X/N is a cycle, i.e. $X/N = \{X_i \mid i \in \mathbb{Z}/m\mathbb{Z}\}$ with $sX_i = X_{i+1}$. In particular, this implies that $|X_1| = \cdots = |X_m|$. If $|X_1| = 1$, we are done. Otherwise, $|N| = p$ implies that $|X_i| = p$ for all i. Consider two elements $s, t \in S$. If $s \sim t$, there is some $x \in X$ with $s^n x = t^n x$ for all $n \in \mathbb{Z}$. Therefore, $s^{-1}t$ acts trivially on X/N. Since G is a p-group, the action of $s^{-1}t$ on X_i is either trivial or a p-cycle. Assume that $x \in X_i$. Then $s^{-1}tx = x$, which shows that $s^{-1}t$ is trivial on X_i. Furthermore, we get $s(s^{j-i}x) = t(t^{j-i}x)$ with $s^{j-i}x = t^{j-i}x \in X_j$, for any $j \in \mathbb{Z}/m\mathbb{Z}$. Hence $s^{-1}t$ acts trivially on all of X. Since every pair $s, t \in S$ is related by a chain $s \sim s_1 \sim \cdots \sim t$ in S, the proof is complete. □

Lemma 3. *Let A be a finite brace with a square-free cycle base X. Assume that A° operates transitively on a set Z, such that each pair $x, x' \in X$ is connected by a sequence $x = x_0 \sim x_1 \sim \cdots \sim x_n = x'$ in X. Then $xz = x'z$ holds for all $x, x' \in X$ and $z \in Z$.*

Proof. For $A = 0$, the lemma is trivial. Otherwise, we choose a minimal normal subgroup $N \neq \{1\}$ of A°. Since A° is solvable, N is an elementary abelian p-group for some rational prime p. Hence $N \subset A_p$. By assumption, A°/N operates transitively on the set Z/N of N-orbits in Z, and the connectivity condition of the lemma holds for A°/N and Z/N instead of A° and Z. Therefore, by induction, we can assume that $Z/N = \{Z_i\}_{i \in \mathbb{Z}/m\mathbb{Z}}$ and $xZ_i = Z_{i+1}$ for all $x \in X$ and $i \in \mathbb{Z}/m\mathbb{Z}$. If $|A| = q \cdot |A_p|$, then $p \nmid q$, and $A_p = qA$. Hence qX is a cycle base of A_p. Since $N \subset A_p$, the orbits of the adjoint group A_p° define a partition of Z/N. As a cycle base, qX generates the group A_p°, and by Lemma 1, we have $qX = X^{\circ q}$. Therefore, A_p° divides Z into $d := \gcd(n, q)$ equally distributed parts $Z'_1, \ldots, Z'_d$, where

$$Z'_i := \bigcup_{j=1}^{n/d} Z_{i+jd}.$$

Thus A_p° operates transitively on each Z'_i, and Lemma 1 shows that any sequence $x_0 \sim x_1 \sim \cdots \sim x_n$ in X gives rise to a sequence $qx_0 \sim qx_1 \sim \cdots \sim qx_n$ in qX with respect to a fixed Z'_i. So Lemma 2 implies that $(qx)z = (qx')z$ for all $x, x' \in X$ and $z \in Z$. In particular, this shows that each element of qX operates transitively on Z'_i, for any $i \in \{1, \ldots, d\}$. Consequently, each $x \in X$

operates transitively on Z. Therefore, two elements $x, x' \in X$ with $x \sim x'$ satisfy $xz = x'z$ for all $z \in Z$. Since each pair $x, x' \in X$ is connected by a chain $x \sim \cdots \sim x'$, the lemma is proved. □

Proof of Theorem 2. Consider the cycle set morphism $\rho' : Y \hookrightarrow X \to \mathrm{A}(X)$. Then $\rho'(Y)$ is a cycle base of some right ideal A of $\mathrm{A}(X)$. By assumption, A° operates transitively on Z. Let $y, y' \in Y$ be given. Since Z operates transitively on Y, there are finite sequences $y = y_0, y_1, \ldots, y_n = y'$ in Y and $z_1, \ldots, z_n \in Z$ such that $z_i \cdot y_{i-1} = y_i$ for all $i \in \{1, \ldots, n\}$. By [12, Proposition 3], this implies that $\rho'(y_0) \sim \rho'(y_1) \sim \cdots \sim \rho'(y_n)$. Thus Lemma 3 applies, which completes the proof. □

As a first consequence, we get

Corollary 1. *Let X be a finite square-free cycle set with a decomposition $X = Y \sqcup Z$ such that Y and Z operate transitively on each other. Then X is a bi-cycle.*

Proof. Theorem 2 implies that $Z = \{z_i\}_{i \in \mathbb{Z}/m\mathbb{Z}}$ with $y \cdot z_i = z_{i+1}$ for all $y \in Y$ and $i \in \mathbb{Z}/m\mathbb{Z}$. By symmetry, this shows that X is a bi-cycle. □

As a second special case of Theorem 2, we get the main result of [12].

Corollary 2. *Let $X \neq \emptyset$ be a finite square-free cycle set which operates transitively on itself. Then X is a singleton.*

Proof. By Theorem 2, the retraction of X is trivial, and every element $x \in X$ operates transitively on X. Hence $X = \mathrm{C}_x(x) = \{x\}$. □

References

[1] D.J. Benson, Representations and Cohomology, I, Cambridge Stud. Adv. Math., vol. 30, Cambridge Univ. Press, Cambridge, 1991.

[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, Geometric crystals and set-theoretical solutions to the quantum Yang–Baxter equation, Comm. Algebra 31 (2003) 1961–1973.

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

[5] T. Gateva-Ivanova, A combinatorial approach to the set-theoretic solutions of the Yang–Baxter equation, J. Math. Phys. 45 (2004) 3828–3858.

[6] T. Gateva-Ivanova, M. Van den Bergh, Semigroups of I-type, J. Algebra 206 (1998) 97–112.

[7] P. Hall, A characteristic property of soluble groups, J. London Math. Soc. 12 (1937) 188–200.

[8] N. Jacobson, Structure of Rings, Amer. Math. Soc. Colloq. Publ., vol. 37, 1964.

[9] G. Laffaille, Quantum binomial algebras, in: Colloq. Homology and Representation Theory, Vaquerías, 1998, in: Bol. Acad. Nac. Cienc. (Cordoba), vol. 65, 2000, pp. 177–182.

[10] J.-H. Lu, M. Yan, Y.-C. Zhu, On the set-theoretical Yang–Baxter equation, Duke Math. J. 104 (2000) 1–18.
[11] M. Takeuchi, Survey on matched pairs of groups—An elementary approach to the ESS-LYZ theory, in: Noncommutative Geometry and Quantum Groups, Warsaw, 2001, in: Banach Center Publ., vol. 61, Polish Acad. Sci., Warsaw, 2003, pp. 305–331.
[12] W. Rump, A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation, Adv. Math. 193 (2005) 40–55.
[13] A.P. Veselov, Yang–Baxter maps and integrable dynamics, Phys. Lett. A 314 (2003) 214–221.