Algebra and Discrete Mathematics
Number 2. **(2006).** pp. 127 – 137

RESEARCH ARTICLE

Modules over braces

Wolfgang Rump

Communicated by Yu. A. Drozd

How to solve the QYBE? Construct a cycle set!
How to fix cycle sets? Put them into braces!

To the best of our knowledge, a *brace* can be used to connect different things, to give them stability. In ancient times, *bracelets*, worn round the arm, also have been precious. The mathematical structures mentioned in the title have those two features. Like an incomplete ring, they embrace associativity and left distributivity, refounding both properties into a single equation. It is this equation that makes the unclosed ring precious in turning it into a group under the circle operation.

Precisely, a *brace* is an abelian group A with a right distributive multiplication such that the circle operation $a \circ b := ab + a + b$ makes A into a group, the *adjoint group* A° of A. With respect to a derived operation, every brace is a *cycle set* [4]. Cycle sets arose in connection with set-theoretical solutions of the quantum Yang-Baxter equation (QYBE). Such a solution can be regarded as a map $R\colon X \times X \to X \times X$ satisfying the QYBE property

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

in $X \times X \times X$, where the superscripts refer to the components where R acts upon. Explicitly, R can be written in the form $R(x, y) = (x^y, {}^x y)$. If R is *unitary* and *left non-degenerate*, i. e. $R^{21}R = 1$ and $x \mapsto x^y$ is invertible, the inverse map $x \mapsto y \cdot x$ satisfies

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

2000 Mathematics Subject Classification: *81R50.*
Key words and phrases: *quantum Yang-Baxter equation, radical ring, cycle set, brace.*

for all $x, y, z \in X$. The sets X with such a (left invertible) binary operation are called *cycle sets*. By [4], Proposition 1, cycle sets are in one-to-one correspondence with left non-degenerate unitary solutions R of the QYBE. Unitary solutions R also correspond to symmetric sets in the sense of [1]. We will show (Proposition 2) that a cycle set can be embedded into a brace if and only if the corresponding solution R is also *right non-degenerate* [4]. For the cycle set X, this means that every element admits a unique square root.

Usually, there are many sub-cycle-sets X of a given brace A, hence many solutions of the QYBE. If X generates A as an abelian group, we call X a *cycle base* of A. There is a kind of Galois theory between ideals of A and quotient cycle sets of X [5]. A further instance of this correspondence is proved in Theorem 1.

Basic properties of braces are developed in §1. By an observation of [1], a brace A can be described as a bijective 1-cocycle $A^\circ \to A$ between the group A° and the right A°-module A. Every brace A contains a largest radical subring A_0, and $A_0 = A$ if and only if A is left distributive. We show that modules over a brace form an abelian category and discuss some delicate points in ideal theory. In §3, we consider *square-free* cycle bases X of a brace A, i. e. those whose elements x satisfy $x^2 = 0$. We show that every element $a \in A$ determines a unique element $c(a)$ with $c(a)^2 = 0$, so that the order of $c(a)$ in A° coincides with its order in the abelian group A.

There is a class of Artin-Schelter regular rings of arbitrary global dimension n, also called quantum binomial algebras [3], which give rise to binomial semigroups [2], hence to square-free cycle sets. In [4] we proved the conjecture [2] that the converse is true, i. e. that each finite square-free cycle set arises in this way. Since a square-free cycle set X is non-degenerate, we can regard it as a cycle base of a brace A. Then the mentioned result is equivalent to the statement that the adjoint group A° of A cannot be transitive on X, unless X is a singleton. If A° is a p-group, we will prove that A/A^2 cannot be cyclic if $A^2 \neq 0$.

1. Braces and radical rings

Let A be an abelian group together with a right distributive multiplication, that is,

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

for all $a, b, c \in A$. We call A a *brace* if the *circle operation*

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

makes A into a group. This group will be called the *adjoint group* A° of A. The associativity of A° is easily seen to be equivalent to the equation

$$a(bc+b+c)=(ab)c+ab+ac \tag{3}$$

which looks like a combination of the associative and the left distributive law. In fact, if A is left distributive, then Eq. (3) boils down to the associative law, so that A becomes a *radical ring* (i. e. an associative ring which is a group under the circle operation).

Since the maps $a\mapsto a\circ b$ are bijective, the same is true for $a\mapsto a^b := ab+a$. The inverse of $a\mapsto a^b$ will be denoted by $a\mapsto b\cdot a$, i. e.

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

(To avoid confusion, we use no dot for the ordinary multiplication in A.) If we set $a=b=0$ in (1), we get $0c=0$. Inserting $b=c=0$ in (3) therefore yields $a0=(a0)0+a0+a0$, whence $(a0)^0=0$, and thus $a0=0$. So we have

$$a0=0a=0. \tag{5}$$

In particular, this shows that 0 is the neutral element of the adjoint group A°, like in the theory of radical rings. The inverse of $a\in A$ in A° will be denoted by a'. Thus

$$aa'+a+a'=a'a+a+a'=0. \tag{6}$$

Using (4), the inverse a' can be determined explicitly:

$$a'=-(a\cdot a). \tag{7}$$

In fact, $(-a\cdot a)\circ a = -(a\cdot a)^a + a = 0$.

The similarity between braces and rings can be extended to module theory. We define a *module* over a brace A to be an abelian group M together with a right operation $M\times A\to M$ such that the following hold for $x,y\in M$ and $a,b\in A$.

$$\begin{aligned}(x+y)a &= xa+ya\\ x(a\circ b) &= (xa)b+xa+xb\\ x0 &= 0.\end{aligned} \tag{8}$$

The second equation now states that $a\circ b$ operates on M like $ab+a+b$ in $\mathrm{End}(M)$. This gives a new interpretation of Eq. (3) and its module theoretic generalization. But there is yet another way to look at this fundamental equation. As above, we may abbreviate

$$x^a := xa+x \tag{9}$$

for $x \in M$ and $a \in A$. Then the second equation in (8) takes the simple form

$$(x^a)^b = x^{a \circ b}. \tag{10}$$

This means that the adjoint group A° operates on M, where $x^0 = x$ is granted by the third equation of (8). In particular, it follows that the map $x \mapsto x^a$ is bijective for all $a \in A$. So the axioms (8) just state that M is a right module over the adjoint group A°. By lack of the left distributivity, there are no left modules over braces.

As a special case, a brace A is a module over itself. Using (9), Eq. (2) can be written in the form

$$b - a \circ b + a^b = 0. \tag{11}$$

Therefore, a brace A can be defined to be a group A° together with a right A°-module A and a bijection $A^\circ \to A$ (the identical map) which satisfies the 1-cocycle condition (11). It is natural to ask when this 1-cocycle is a boundary. This happens if and only if there is an element $a \in A$ with $b = a - a^b$, i. e. $b = -ab$, for all $b \in A$. By Eq. (6) with $b := a'$, this implies that $a = 0$, and thus $A = 0$. In other words, homologically trivial braces are trivial.

Most of the basic concepts of ring and module theory carry over to braces without change, but they have to be handled with care. For example, if $f\colon A \to B$ is a *morphism* between braces, i. e. a map which respects addition and multiplication, then $f(A)$ is a *subbrace* of B, i. e. a subset which is closed under addition and multiplication. The kernel of f is an *ideal* of A, that is, an additive subgroup I such that ab and ba belong to I whenever $a \in I$ and $b \in A$. For a given ideal I of A, we can form the *factor brace* $A/I := \{a + I \mid a \in A\}$. To show that multiplication is well-defined for A/I, it suffices to verify that the implication

$$x \in I \;\Rightarrow\; a(x + c) - ac \in I$$

is valid for $a, c \in A$. Since I is A°-invariant, we can write x in the form $x = b^c = bc + b$ for some $b \in I$. Then $a(x + c) - ac = a(b \circ c) - ac = (ab)c + ab \in I$ follows.

For a brace A, morphisms between A-modules, as well as submodules and factor modules, are defined in the obvious way. A submodule of A is called a *right ideal*. Since A-modules can be regarded as A°-modules, they form an abelian category.

Although there are no left modules over non-associative braces, the interaction with associative rings of left operators is of importance. Let R be an associative ring. A module M over a brace A which is a left

R-module will be called an (R, A)-*bimodule* if $(rx)a = r(xa)$ holds for all $x \in M$, $r \in R$, and $a \in A$. The first example arises for any brace A. Define

$$A_0 := \{x \in A \mid \forall\, a, b \in A\colon x(a + b) = xa + xb\}. \tag{12}$$

Proposition 1. A_0 is the largest radical subring of A, and A is an (A_0, A)-bimodule.

Proof. Since radical rings are left distributive, there cannot be a larger radical subring. Eqs. (1) and (5) show that A_0 is an additive subgroup. From Eq. (3) we infer that

$$x(ab) = (xa)b \tag{13}$$

holds for all $x \in A_0$ and $a, b \in A$. For $x, y \in A_0$ and $a, b \in A$, we thus have

$$(xy)(a + b) = x(y(a + b)) = x(ya + yb) = x(ya) + x(yb) = (xy)a + (xy)b,$$

which shows that A_0 is a subbrace of A. Hence A_0 is is a radical ring. The remaining assertion follows by Eq. (13). □

Note that A_0 contains the center of the adjoint group A°. We conclude this section with two simple examples. For more sophisticated examples, we refer to [4, 5].

Example 1. Let B be abelian group and C a right B-module. Define a multiplication in $A := B \oplus C$ by

$$(b_1 + c_1)(b_2 + c_2) := 0 + (c_1^{b_2} - c_1). \tag{14}$$

Then A is a brace with circle operation $(b_1 + c_1) \circ (b_2 + c_2) = (b_1 + b_2) + (c_1^{b_2} + c_2)$.

Example 2. Let A be a brace, and M an A-module. Define $B := M \oplus A$ with

$$(x + a)(y + b) := xb + ab, \tag{15}$$

where $a, b \in A$ and $x, y \in M$. It is easily verified that B is a brace with circle operation

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

2. Cycle bases

Let A be a brace. Eq. (10) can be expressed in terms of the dot product as follows. With $y := x^a$, the equation turns into $(a \circ b) \cdot y^b = a \cdot y$.

Here $a \circ b = a^b + b$. Thus if we set $c := y^b$ and replace a^b by a, we get $(a+b) \cdot c = (b \cdot a) \cdot (b \cdot c)$. By symmetry, this yields

$$(a \cdot b) \cdot (a \cdot c) = (b \cdot a) \cdot (b \cdot c), \tag{16}$$

an equation with just one operation. A set X with a left invertible multiplication satisfying (16) is said to be a *cycle set* [4]. Thus every brace is a cycle set. Left invertibility means that the left multiplication $y \mapsto x \cdot y$ admits an inverse $y \mapsto y^x$. An A°-invariant subset of A which generates A as an abelian group will be called a *cycle base*. By Eq. (16), any cycle base of A is a cycle set. Note that a cycle base generates the adjoint group A°.

A cycle set X is said to be *non-degenerate* [4] if the map $x \mapsto x \cdot x$ is bijective (i. e. every element admits a unique square root).

Proposition 2. A cycle set X is non-degenerate if and only if it arises as a cycle base of a brace.

Proof. Assume first that X is a cycle base of a brace A. For a given $a \in A$, the equation $x \cdot x = a$ can be written as $x = a^x$ or $(-a) \circ x = 0$. Hence it admits a unique solution $x = (-a)'$ By Eq. (7) this shows that

$$x \cdot x = a \Leftrightarrow (-a) \cdot (-a) = -x. \tag{17}$$

Since $-X := \{-x \mid x \in X\}$ is another cycle base of A, it follows that X is non-degenerate. Conversely, let X be a non-degenerate cycle set. By [4], Proposition 6, there is a unique way to make the free abelian group $\mathbb{Z}^{(X)}$ into a cycle set with X as a sub-cycle-set such that

$$a \cdot (b + c) = a \cdot b + a \cdot c \tag{18}$$

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

holds for $a, b, c \in \mathbb{Z}^{(X)}$. Therefore, the deduction of Eq. (16) at the beginning of this section shows that $\mathbb{Z}^{(X)}$ is a brace with X as a cycle base. $\square$

By the absence of left distributivity, ideals of braces are not as easy to handle as in ring theory. We will see below how cycle bases can be used to overcome this difficulty. Let us start with a general criterion for ideals.

Proposition 3. A right ideal I of a brace A is an ideal if and only if I is a normal subgroup of the adjoint group A°.

Proof. Assume first that I is an ideal. The equation

$$a \circ b = a^b + b \tag{20}$$

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 $ba + a = cb + c$ for some $c \in I$. Hence $b \circ a = ba + a + b = cb + c + b = c \circ b$, which shows that I is a normal subgroup of A°. Conversely, let I be normal in A°. For $a, b \in A$, we have $b \circ a \circ b' = (ba+b+a) \circ b' = (ba+b+a)b' + (ba+b+a) + b' = (ba+a)b' + (ba+a)$, which proves the identity

$$ba + a = (b \circ a \circ b')^b. \tag{21}$$

Thus if $a \in I$ and $b \in A$, Eq. (21) implies that $b \circ a \circ b' \in I$. □

Proposition 3 implies that the sum of ideals is again an ideal.

Proposition 4. Let M be a module over a brace A, and let N be a normal subgroup of A°. Then

$$MN := \{\sum_{i=1}^{n} x_i a_i \mid x_i \in M,\ a_i \in N\}$$

is a submodule of M.

Proof. The proof follows from the equation

$$(xa)^b = (x^b)(b' \circ a \circ b) \tag{22}$$

which holds for $x \in M$ and $a, b \in A$. By Eq. (10), we have

$$(xa)^b = (x^a - x)^b = (x^a)^b - x^b = (x^b)^{b' \circ a \circ b} - x^b = (x^b)(b' \circ a \circ b).$$

□

Proposition 4 implies that if I is an ideal of a brace A, then AI is again an ideal of A. However, the product of two ideals need not be an ideal (see Example 2 of [5]). Next we show how ideals can be understood in terms of a cycle base.

For a set X, let $\Pi(X)$ denote the set of *partitions* of X, i. e. sets P of pairwise disjoint non-empty subsets of X with $\bigcup P = X$. If $x, y \in X$ belong to the same $Y \in P$, we write $x \overset{P}{\sim} y$. If $P \in \Pi(X)$ is a *refinement* of $P' \in \Pi(X)$, i. e. $x \overset{P}{\sim} y$ implies $x \overset{P'}{\sim} y$, we write $P \geqslant P'$.

Every morphism $f \colon X \to Y$ of cycle sets gives rise to a partition $P \in \Pi(X)$ with $x \overset{P}{\sim} y$ if and only if $f(x) = f(y)$. Such partitions will be called *ideals* of X. They are characterized by the following properties ($\forall\, x, y, z \in X$):

$$x \overset{P}{\sim} y \;\Leftrightarrow\; z \cdot x \overset{P}{\sim} z \cdot y \tag{23}$$

$$x \overset{P}{\sim} y \;\Rightarrow\; x \cdot z \overset{P}{\sim} y \cdot z. \tag{24}$$

Let A be a brace with a cycle base X. Then every right ideal I of A defines a partition $P(I)$ with $x \overset{P(I)}{\sim} y$ if and only if $y = x^a$ for some $a \in I$. This follows since I is a subgroup of A°.

Theorem 1. Let A be a brace with a cycle base X, and let $P \in \Pi(X)$ be an ideal of X. The additive subgroup I_P of A generated by the differences $x - y$ with $x \overset{P}{\sim} y$ is an ideal with $P(I_P) \geqslant P$. A right ideal I of A with $P(I) = P$ is an ideal if and only if $I_P \subset I$.

Proof. The equivalence (23) implies that I_P is a right ideal of A. To show that I_P is an ideal, we first remark that the conclusion of (24) can be replaced by $z^x \overset{P}{\sim} z^y$. Namely, if we replace z by z^x, we get $z \overset{P}{\sim} y \cdot z^x$. Hence (23) yields $z^y \overset{P}{\sim} z^x$. Assume now that $x \overset{P}{\sim} y$. By Proposition 2, there exists an element $z \in X$ with $y = z \cdot z$. Hence $x^z \overset{P}{\sim} z$. Therefore, the modified version of (24) yields $t^{x^z} \overset{P}{\sim} t^z$ for all $t \in X$, and (23) gives $t^{x^z \circ z'} \overset{P}{\sim} t$. By Eqs. (7) and (20), we have $t(x - y) = t(x + z') = t(x^z \circ z')$, hence

$$t(x - y) = t^{x^z \circ z'} - t \in I_P. \tag{25}$$

Thus $b(x - y) \in I_P$ for all $b \in A$. By Eq. (20), every element of $a \in I_P$ can be written in the form $a = a_1 \circ \cdots \circ a_n$ with $a_i = x_i - y_i$ and $x_i \overset{P}{\sim} y_i$ for all i. Therefore, Eq. (25) shows that $P(I_P) \geqslant P$. To prove that I_P is an ideal, it remains to verify that $ba \in I_P$ holds for all $b \in A$. For $n = 1$, this has been proved above. For arbitrary n, the assertion follows by the formula

$$b(a_1 \circ \cdots \circ a_n) = \sum_{i=0}^{n-1} b^{a_1 \circ \cdots \circ a_i} a_{i+1} \tag{26}$$

which is an immediate consequence of the equation

$$b^{a_1 \circ \cdots \circ a_n} - b = \sum_{i=1}^{n} b^{a_1 \circ \cdots \circ a_i} - \sum_{i=0}^{n-1} b^{a_1 \circ \cdots \circ a_i}.$$

Thus I_P is an ideal with $P(I_P) \geqslant P$.

Finally, let I be a right ideal of A with $P(I) = P$. Then $I_P \subset I$ means that $xa = x^a - x \in I$ holds for all $x \in X$ and $a \in I$, i. e. that I is an ideal. $\square$

To illustrate Theorem 1, let I be an ideal of a brace A. By Proposition 4, we already know that AI is an ideal. By definition, AI is generated, as an abelian group, by the products xa with $x \in X$ and $a \in A$. Since $xa = x^a - x$, we get

$$AI = I_{P(I)}. \tag{27}$$

By induction, this formula yields an explicit representation of the *radical series*

$$A \supset A^2 \supset A^3 \supset \cdots \tag{28}$$

of A, which is defined, inductively, by $A^1 := A$ and $A^{n+1} := A(A^n)$. In contrast to radical rings, the series (28) does not always reach zero, even if A° is a finite p-group [5].

3. Square-free elements

Let A be a brace. We call an element $a \in A$ *square-free* if $a^2 = 0$. The nth power of a in A° will be denoted by $a^{\circ n}$. By definition, we have $a^{\circ 2} = a + a^a$ and $a^{\circ 3} = a + (a + a^a)^a = a + a^a + (a^a)^a$. Similarly, $a^{\circ 4} = a + a^a + (a^a)^a + ((a^a)^a)^a$, and in general, we obtain

$$a^{\circ n} = \sum_{i=0}^{n-1} a^{a^{\circ i}} \tag{29}$$

for $n \in \mathbb{N}$. If the set $C(a)$ of iterates $a, a^a, (a^a)^a, \ldots$ is finite, they form a cycle. Then we call $C(a)$ the *self-cycle* and $s(a) := |C(a)|$ the *self-order* of a. The subgroup of A° generated by a operates transitively on $C(a)$. So if the order $\operatorname{ord}(a)$ of a in A° is finite, it satisfies an equation

$$\operatorname{ord}(a) = s(a) \cdot r(a) \tag{30}$$

with $r(a) \in \mathbb{N}$. We call $r(a)$ the *reduced order* of a. Thus a is square-free if and only if $a^a = a$, i. e. $s(a) = 1$. Define

$$c(a) := \sum C(a) = a^{\circ s(a)}. \tag{31}$$

Proposition 5. Let A be a brace. An element $a \in A$ is square-free if and only if

$$a^{\circ n} = na \tag{32}$$

holds for all $n \in \mathbb{Z}$. If $a \in A$ is of finite self-order in A°, then $c(a)$ is square-free, and $r(a)$ is the order of $c(a)$ in the abelian group A.

Proof. Let $s(a)$ be finite. Then Eq. (29) yields $c(a) \circ c(a) = a^{\circ s(a)} \circ a^{\circ s(a)} = a^{\circ 2s(a)} = 2c(a)$. Hence $c(a)$ is square-free, and a is square-free if and only if $a = c(a)$. The remaining statements follow immediately by Eq. (29). □

A cycle set X is said to be *square-free* if $x \cdot x = x$ holds for all $x \in X$. Since such an X is non-degenerate, it arises, by Proposition 2, as a cycle base of a brace A, and the elements of X are then square-free in A.

A partition P of a cycle set X with $|P| \geqslant 2$ is said to be a *decomposition* of X if $x \overset{P}{\sim} y \cdot x$ holds for all $x, y \in X$. If $X \neq \varnothing$ and X admits no such partition, we call X *indecomposable*. In [4], we proved the following

Theorem 2. Every finite square-free cycle set X with more than one element is decomposable.

If we regard X as a cycle base of a brace A, the theorem becomes more plausible. For $x, y \in X$, we have $x^y = xy - x$, i. e. x and x^y are in the same residue class modulo A^2. If X is indecomposable, this implies that A/A^2 is cyclic, and the generator can be represented by an element in X. Since $x^2 = 0$, it should follow that X must be a singleton. However, this reasoning is not quite correct. A precise statement is given by the following proposition which makes use of a *right radical series*

$$A \supset A^2 \supset A^{(3)} \supset A^{(4)} \supset \cdots \tag{33}$$

with $A^{(n+1)} := (A^{(n)})A$. Note that $A^{(2)}$ is just A^2. The right powers $A^{(n)}$ are right ideals, but not ideals, in general. If $|A|$ is a prime power, it can be shown that $A^{(n)} = 0$ for some n (see [5]).

For a module M over a brace A, and $x \in M$, we abbreviate

$$xA := \left\{ \sum_{i=1}^{n} xa_i \;\middle|\; a_1, \ldots, a_n \in A \right\}. \tag{34}$$

Remark. By Eq. (3), the equation $(xa)b = x(a \circ b) - xa - xb \in xA$ holds for $a, b \in A$. Hence xA is a submodule of M.

Proposition 6. Let A be a finite brace with a square-free cycle base X, such that $A^{(n)} = 0$ for some n. If the abelian group A/A^2 is cyclic, then $A^2 = 0$.

Proof. Since A/A^2 is cyclic, we can assume that $A = \mathbb{Z}x + A^2$ for some $x \in X$. Therefore, $A^2 = (\mathbb{Z}x + A^2)A = xA + A^{(3)}$. Inductively, let us assume that $A^2 = xA + A^{(i)}$ has been shown for some $i \geqslant 3$. Then $A^2 = (\mathbb{Z}x + xA + A^{(i)})A = xA + A^{(i+1)}$. Hence $A^{(n)} = 0$ implies that $A^2 = xA$. Now we set

$$X' := \{x + xa \mid a \in A\}.$$

Since X' is A°-invariant, X' is a cycle set with

$$(x + xa)^{x+xb} = x + x(a \circ (x + xb)). \tag{35}$$

As $A = \mathbb{Z}x + xA$, the additive group of A is generated by X'. By Eq. (20), we have

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

for all $a, b \in A$. Therefore, X' generates the adjoint group A°, i. e. every $a \in A$ can be written in the form $a = 0 \circ x_1 \circ \cdots \circ x_n$ with $x_i \in X'$. Thus (35) yields

$$x + xa = ((x^{x_1})^{x_2} \cdots)^{x_n},$$

which shows that X' is indecomposable. Since $X' \subset X$ is square-free, Theorem 2 implies that $|X'| = 1$. Hence $A^2 = xA = 0$. $\square$

Proposition 6 does not hold without the nilpotency condition $A^{(n)} = 0$ (see Example 3 of [5]). We conclude with the following commutation property of square-free cycle bases.

Proposition 7. Let A be a brace with a square-free cycle base X. If $x \in X$ and $a \in A$ with $x + a \in X$, then $xa \in aA$.

Proof. $x + a \in X$ implies that $a \circ x = (x + a)x + (x + a) \in X$. Hence $0 = (a \circ x)^2 = ((a \circ x)a)x + (a \circ x)a + (a \circ x)x = ((ax + a)a)x + (xa)^x + (ax)a + a^2 + (ax + a)x$. By the above remark (i. e. that xA is a submodule of A), this shows that $xa \in aA$. $\square$

References

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

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

[3] G. Laffaille: Quantum Binomial Algebras, Colloq. Homology and Representation Theory, Vaquerías, 1998, Bol. Acad. Nac. Cienc. (Cordoba) 65 (2000), 177-182

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

[5] W. Rump: Braces, radical rings, and the quantum Yang-Baxter equation, Preprint

Contact information

W. Rump Institut fьr Algebra und Zahlentheorie, Universitдt Stuttgart Pfaffenwaldring 57, D-70550 Stuttgart, Germany
E-Mail: rump@mathematik.uni-stuttgart.de

Received by the editors: 31.10.2005
and in final form 30.06.2006.