BRACES AND SYMMETRIC GROUPS WITH SPECIAL CONDITIONS

FERRAN CEDÓ, TATIANA GATEVA-IVANOVA, AGATA SMOKTUNOWICZ

ABSTRACT. We study symmetric groups and left braces satisfying special conditions, or identities. We are particularly interested in the impact of conditions like **Raut** and **lri** on the properties of the symmetric group and its associated brace. We show that the symmetric group $G = G(X, r)$ associated to a nontrivial solution (X, r) has multipermutation level 2 if and only if G satisfies **lri**. In the special case of a two-sided brace we express each of the conditions **lri** and **Raut** as identities on the associated radical ring G_*. We apply these to construct examples of two-sided braces satisfying some prescribed conditions. In particular we construct a finite two-sided brace with condition **Raut** which does not satisfy **lri**. (It is known that condition **lri** always implies **Raut**). We show that a finitely generated two-sided brace which satisfies **lri** has a finite multipermutation level which is bounded by the number of its generators.

CONTENTS

Date: September 10, 2018.

2010 *Mathematics Subject Classification.* Primary 16T25, 16W22, 16N20, 16N40, 20F16, 81R50.

Key words and phrases. Yang–Baxter Equation, set-theoretic solutions, brace, braided group, Jacobson radical.

* The first author was partially supported by the grant MINECO MTM2014-53644-P

** The second author was partially supported by Grant I 02/18 of the Bulgarian National Science Fund, by ICTP, Trieste, and by Max-Planck Institute for Mathematics, Bonn

*** The third author was supported by ERC Advanced grant 320974.

1. Preliminaries

A quadratic set is a pair (X, r), where X is a non-empty set and $r\colon X \times X \to X \times X$ is a bijective map. Recall that (X, r) is involutive if $r^2 = \mathrm{id}_{X^2}$. The image of (x, y) under r is presented as $r(x, y) = ({}^x y, x^y)$. Consider the maps $\mathcal{L}_x, \mathcal{R}_x\colon X \to X$ defined by

$$\mathcal{L}_x(y) = {}^x y \quad \text{and} \quad \mathcal{R}_x(y) = y^x,$$

for all $x, y \in X$. The quadratic set (X, r) is non-degenerate if $\mathcal{L}_x$ and $\mathcal{R}_x$ are bijective for all $x \in X$. The map r is *a set-theoretic solution of the Yang–Baxter equation* (YBE) if the braid relation

$$r^{12} r^{23} r^{12} = r^{23} r^{12} r^{23}$$

holds in $X \times X \times X$, where $r^{12} = r \times \mathrm{id}_X$, and $r^{23} = \mathrm{id}_X \times r$. In this case (X, r) is called *a braided set.* A braided set (X, r) with r involutive is called *a symmetric set.*

Convention 1.1. In this paper "*a solution*" means "*an involutive non-degenerate set-theoretic solution of the YBE* ", or equivalently, "*a non-degenerate symmetric set*" (X, r).

A left brace is a triple $(G, +, \cdot)$, where G is a set, $+$ and $\cdot$ are two binary operations, such that $(G, +)$ is an abelian group, $(G, \cdot)$ is a group and

$$a \cdot (b + c) + a = a \cdot b + a \cdot c, \tag{1.1}$$

for all $a, b, c \in G$. The group $(G, +)$ is the additive group of the left brace and $(G, \cdot)$ is its multiplicative group. *A right brace* is defined similarly, but replacing property (1.1) by $(b + c) \cdot a + a = b \cdot a + c \cdot a$. If $(G, +, \cdot)$ is both a left and a right brace (for the same operations), then it is called *a two-sided brace.*

It is known that if $(G, +, \cdot)$ is a left brace, and 0 and e, respectively, denote the neutral elements with respect to the two operations "$+$" and "$\cdot$" in G, then $0 = e$.

In any left brace $(G, +, \cdot)$ one defines the operation $*$ by the rule:

$$a * b = a \cdot b - a - b, \ a, b \in G. \tag{1.2}$$

It is known and easy to check that $*$ is left distributive with respect to the sum $+$. In general $*$ is not right distributive, nor associative, but it satisfies the following condition

$$(a * b + a + b) * c = a * (b * c) + a * c + b * c, \ \forall a, b, c \in G, \tag{1.3}$$

see the original definition of right brace of Rump [Ru, Definition 2]. It is also known that $(G, +, \cdot)$ is a two-sided brace if and only if $(G, +, *)$ is a Jacobson radical ring.

Takeuchi introduced the notions of a braided group and a symmetric group as the group versions of a braided set and a symmetric set, respectively, [Ta]. We recall the definitions.

A braided group is a pair (G, r), where G is a group and $r : G \times G \longrightarrow G \times G, \quad r(a, b) = ({}^a b, a^b)$ is a bijective map satisfying the following conditions

$$\begin{array}{llll}
\mathbf{ML0}: & {}^a 1 = 1,\ {}^1 u = u, & \mathbf{MR0}: & 1^u = 1,\ a^1 = a, \\
\mathbf{ML1}: & {}^{ab} u = {}^a({}^b u), & \mathbf{MR1}: & a^{uv} = (a^u)^v, \\
\mathbf{ML2}: & {}^a(u.v) = ({}^a u)({}^{a^u} v), & \mathbf{MR2}: & (a.b)^u = (a^{{}^b u})(b^u),
\end{array}$$

and the compatibility condition

$$\mathbf{M3}: \quad uv = ({}^u v).(u^v),$$

for all $a, b, u, v \in G$. For each braided group (G, r) the map r is *a braiding operator*, so (G, r) is a braided set, see [LYZ], see also [Ta].

A symmetric group is a braided group (G, r) with an involutive braiding operator r. Each symmetric group (G, r) is a nondegenerate symmetric set, that is (G, r) is a solution.

It was proven by the second author that symmetric groups and left braces are equivalent structures, see [GI] Theorem 3.6. More precisely, the following hold.

(i) Every symmetric group (G, r) has a canonically associated structure of a left brace $(G, +, \cdot)$, where the operation "$+$" on G is defined via

$$a + b := a \cdot ({}^{a^{-1}} b), \text{ or equivalently, } a + {}^a b = a \cdot b,\ a, b \in G. \tag{1.4}$$

(ii) Conversely, every left brace $(G, +, \cdot)$ has a canonically associated structure of a symmetric group (G, r), that is a group with a braiding operator $r : G \times G \longrightarrow G \times G$, $r(a, b) := ({}^a b, a^b)$, with left and right actions of G upon itself given by the formulae

$${}^a b := a \cdot b - a = a * b + b, \qquad a^b := {}^{({}^a b)^{-1}} a,\ \ \forall\, a, b \in G. \tag{1.5}$$

Moreover, the following condition holds in G

$$\mathbf{Laut}: \quad {}^a(b + c) = {}^a b + {}^a c, \quad \forall a, b, c \in G.$$

By convention a symmetric groups (G, r) is always considered together with the associated left brace $(G, +, \cdot)$ and vice versa.

For each solution (X, r) of the YBE Etingof, Schedler and Soloviev introduced in [ESS] two groups: the structure group $G = G(X, r)$ and the permutation group $\mathcal{G} = \mathcal{G}(X, r)$. The structure group G is generated by X and has quadratic defining relations $xy = {}^x y x^y$, for all $x, y \in X$. (The group $G(X, r)$ is also called the YB-group of (X, r)). The set X is embedded in G. The group G acts on the left (and on the right) on the set X, so the assignment $x \mapsto \mathcal{L}_x$ extends to a group homomorphism $\mathcal{L} : G(X, r) \longrightarrow \mathrm{Sym}(X),\ a \mapsto \mathcal{L}_a \in Sym(X)$, where $\mathcal{L}_a(x) = {}^a x$. By definition the permutation group $\mathcal{G} = \mathcal{G}(X, r)$ is the image $\mathcal{L}(G(X, r))$ of G. The group $\mathcal{G}$ is generated by the set $\{\mathcal{L}_x \mid x \in X\}$. It is known, see [LYZ], that there is unique braiding operator $r_G : G \times G \longrightarrow G \times G$, such that the restriction of r_G on $X \times X$ is exactly the map r. We call (G, r_G) *the symmetric group associated to* (X, r). Moreover, the epimorphism $\mathcal{L} : G(X, r) \longrightarrow \mathcal{G}(X, r)$ is a braiding preserving map which induces a canonical structure of a symmetric group $(\mathcal{G}, r_{\mathcal{G}})$, see [GI] (or [CJO] for the equivalent version in the language of left braces).

An ideal of a left brace $(G, +, \cdot)$ is a normal subgroup I of its multiplicative group which is invariant with respect to the left action of G upon itself, i.e. ${}^{a}b \in I$ for all $a \in G$ and all $b \in I$. It is known that every ideal I of $(G, +, \cdot)$ is a subgroup of its additive group, and is invariant with respect to the right action of G.

Each left brace $(G, +, \cdot)$ has several invariant decreasing chains of subsets.

The series $G^{(n)}$, introduced by Rump, [Ru], consists of ideals of G:

$$G = G^{(1)} \supseteq G^{(2)} \supseteq G^{(3)} \supseteq \cdots, \text{ where } G^{(n+1)} = G^{(n)} * G, n \geq 1. \tag{1.6}$$

The second series, G^n, [Ru], is defined as

$$G = G^1 \supseteq G^2 \supseteq G^3 \supseteq \cdots, \text{ where } G^{n+1} = G * G^n, \ n \geq 1. \tag{1.7}$$

Recall the following definition.

Definition 1.2. [GIM] Let (X, r) be a quadratic set.

(1) The following are called *cyclic conditions on* X.

cl1 :	${}^{({}^{y}x)}x = {}^{y}x$, for all $x, y \in X$;	**cr1** :	$x^{({}^{x}y)} = x^{y}$, for all $x, y \in X$;
cl2 :	${}^{({}^{x}y)}x = {}^{y}x$, for all $x, y \in X$;	**cr2** :	$x^{(y^{x})} = x^{y}$, for all $x, y \in X$.

(X, r) is called *cyclic* if it satisfies all cyclic conditions.

(2) Condition **lri** is defined as

$$\textbf{lri:} \qquad ({}^{x}y)^{x} = y = {}^{x}(y^{x}), \text{ for all } \quad x, y \in X.$$

In other words **lri** holds if and only if (X, r) is non-degenerate and $\mathcal{R}_x = \mathcal{L}_{x^{-1}}$ and $\mathcal{L}_x = \mathcal{R}_{x^{-1}}$.

Symmetric groups and their braces with special conditions on the actions like **lri** or **Raut** were studied first in [GI]. Here we continue this study (i) for general symmetric groups (G, r), and (ii) under the additional assumption that the associated left brace $(G, +, \cdot)$ is a two-sided brace.

Definition 1.3. [GI] A left brace $(G, +, \cdot)$ satisfies condition **Raut** if

$$\textbf{Raut}: \quad (a + b)^{c} = a^{c} + b^{c}, \ \forall a, b, c \in G.$$

Note that condition **lri** on the symmetric group (G, r) implies that the left and the right actions of the group G upon itself are mutually inverse, while condition **Raut** links the two parallel structures- the symmetric group structure and the brace structure of G.

Notation 1.4. We shall use notation as in [GI]. As usual, given a solution (X, r), $G = G(X, r)$ denotes its structure group, and $\mathcal{G} = \mathcal{G}(X, r)$ denotes its permutation group. The canonically associated symmetric groups will be denoted by (G, r_G) and $(\mathcal{G}, r_{\mathcal{G}})$, respectively. In the case when (X, r) is a multipermutation solution of level

m we shall write $\mathrm{mpl}(X, r) = m$. Given a two-sided brace $(G, +, \cdot)$, the associated Jacobson radical ring is denoted by $G_* = (G, +, *)$

2. Left braces $(G, +, \cdot)$, the operation $*$ and some identities

We study symmetric groups (G, r) and left braces $(G, +, \cdot)$ satisfying the identity $(a * b) * c = a * (b * c)$, for all $a, b, c \in G$, or equivalently, $(G, *)$ is a semigroup with zero ($e = 0$ is a zero element in $(G, *)$). Clearly, if $(G, +, \cdot)$ is a two-sided brace, then $(G, *)$ is a semigroup. In particular, we are interested in the following questions.

Questions 2.1. (1) *What can be said about symmetric sets (X, r) for which some of the symmetric groups $G = G(X, r)$, or $\mathcal{G} = \mathcal{G}(X, r)$ has associative law for the operation $*$?*

(2) *Does it exist a left brace $(G, +, \cdot)$, such that $(G, *)$ is a semigroup, but $(G, +, \cdot)$ is not a two-sided brace?*

It is known that if (X, r) is a solution, then $G(X, r)$ is a two-sided brace *iff* (X, r) is a trivial solution, [GI, Theorem 6.3]. We shall prove that in the special case when $G = G(X, r)$ is the symmetric group of a solution (X, r), $(G, *)$ is a semigroup if and only if G is a two-sided brace, and therefore (X, r) is a trivial solution, see Corollary 2.3.

Proposition 2.2. *Let (G, r) be a symmetric group and let $(G, +, \cdot)$ be the corresponding left brace. Suppose $(G, *)$ is a semigroup and the additive group $(G, +)$ has no elements of order two. Then $(G, +, \cdot)$ is a two-sided brace, or equivalently, $(G, +, *)$ is a Jacobson radical ring.*

Proof. We shall prove that

$$(-a) * b = -(a * b), \ \forall a, b \in G. \tag{2.1}$$

By (1.3), we have

$$[a + (-a) + a * (-a)] * b = a * b + (-a) * b + a * [(-a) * b], \quad \forall a, b \in G.$$

This together with the obvious equality $[a + (-a) + a * (-a)] * b = [a * (-a)] * b$, and the associative law in $(G, *)$ imply

$$a * [(-a) * b] = [a * (-a)] * b = a * b + (-a) * b + a * [(-a) * b], \quad \forall a, b \in G.$$

It follows that $a * b + (-a) * b = 0$, so the identity (2.1) holds in G. Note that $(G, +, *)$ satisfies the hypothesis of [Smok1, Theorem 13], and therefore $(G, +, *)$ is a Jacobson radical ring. □

An easy consequence of Proposition 2.2 and [GI, Corollari 5.16] is the following result.

Corollary 2.3. *Let (X, r) be a solution, (G, r_G), $(\mathcal{G}, r_{\mathcal{G}})$, $(G, +, \cdot)$, $(\mathcal{G}, +, \cdot)$ in usual notation.*

(1) *$(G,*)$ is a semigroup if and only if $(G,+,\cdot)$ is a two-sided brace, so in this case (X,r) is the trivial solution.*
(2) *Suppose the additive group $(\mathcal{G},+)$ has no elements of order two ($a+a\neq e, \forall a\in\mathcal{G}$). Then $(\mathcal{G},*)$ is a semigroup if and only if it is a two-sided brace. Moreover, if X is a finite set, then (X,r), is a multipermutation solution, and*

$$0\leq \operatorname{mpl}(\mathcal{G},r_{\mathcal{G}})=m-1\leq \operatorname{mpl}(X,r)\leq \operatorname{mpl}(G,r_G)=m<\infty.$$

Recall that the series G^n and $G^{(n)}$ of a left brace are defined by (1.6), and (1.7).

Lemma 2.4. *Let $(G,+,\cdot)$ be a left brace. Suppose that $(G,*)$ is a semigroup. Then $G^n\subseteq G^{(n)}$ for all positive integers n.*

Proof. We shall use induction on n to prove the equality of sets

$$G^n=\{\sum_{i=1}^{k} g_{i,1}*\cdots *g_{i,n}\mid k \text{ is a positive integer, and } g_{i,j}\in G\}. \tag{2.2}$$

For $n=2$, one has $G^2=G*G=G^{(2)}$ by definition, thus

$$G^2=\{\sum_{i=1}^{k} g_i*h_i\mid k \text{ is a positive integer, } g_i,h_i\in G\}.$$

Let $n>2$ and assume (2.2) is true for all $m<n$. By (1.7) one has

$$G^n=G*G^{n-1}=\{\sum_{i=1}^{k} g_i*h_i\mid k \text{ is a positive integer, } g_i\in G,\ h_i\in G^{n-1}\}. \tag{2.3}$$

By the induction hypothesis every pair $g\in G, h\in G^{n-1}$ satisfies

$$\begin{aligned} g*h &= g*\sum_{i=1}^{k} g_{i,1}*\cdots *g_{i,n-1}\\ &= \sum_{i=1}^{k} g*g_{i,1}*\cdots *g_{i,n-1}, \end{aligned}$$

where $g_{i,j}\in G$. This together with (2.3) implies the desired equality of sets (2.2).

It is clear that $g_1*\cdots *g_n=(\dots(g_1*g_2)*\cdots)*g_n\in G^{(n)}$, whenever $g_i\in G, 1\leq i\leq n$. Therefore $G^n\subseteq G^{(n)}$. ∎

Remark 2.5. Let G be a set with two operations "$\cdot$" and "$+$" such that $(G,\cdot)$ is a group, and $(G,+)$ is an abelian group. (We do not assume $(G,+,\cdot)$ is a brace). Let $*$ be a new operation on G defined by (1.2).

(1) $(G,+,\cdot)$ is a left brace if and only if $(G,+,*)$ satisfies a left distributive law: $a*(b+c)=a*b+a*c, \quad \forall\, a,b,c\in G$.
(2) $(G,+,\cdot)$ is a right brace if and only if $(G,+,*)$ satisfies a right distributive law: $(a+b)*c=a*c+b*c, \quad \forall\, a,b,c\in G$.

Lemma 2.6. *Let $(G,+,\cdot)$ be a left brace, such that $(G,*)$ is semigroup. If $G^n=0$ for some positive integer n then $(G,+,\cdot)$ is a two-sided brace.*

Proof. It follows from [Smok2, Lemma 15] that for every $a, b, c \in G$ there are $d_i, d'_i \in G$ such that

$$(a+b)*c = a*c + b*c + \sum_{i=0}^{2n}(-1)^{i+1}((d_i * d'_i)*c - d_i*(d'_i*c)). \tag{2.4}$$

By hypothesis $(G,*)$ is a semigroup, so $(d_i * d'_i)*c - d_i*(d'_i*c) = 0,\ 0 \leq i \leq 2n$, which together with (2.4) imply $(a+b)*c = a*b + a*c$, for all $a, b, c \in G$. Therefore, by Remark 2.5 $(G, +, \cdot)$ is a two-sided brace. □

Proposition 2.7. *Let (G, r) be a symmetric group of a finite multipermutation level,* $\mathrm{mpl}(G, r) = m$. *Suppose $(G,*)$ is a semigroup. Then the following two conditions hold.*

(1) *The left brace $(G, +, \cdot)$ is a two-sided brace, and hence $(G, +, *)$ is a Jacobson radical ring.*
(2) *The group $(G, \cdot)$ is nilpotent.*

Proof. By hypothesis (G, r) has a finite multipermutation level, $\mathrm{mpl}(G, r) = m$, so [CGIS, Proposition 6] implies that $G^{(m+1)} = 0$ and $G^{(m)} \neq 0$. It follows from Lemma 2.4 that $G^{m+1} \subseteq G^{(m+1)} = 0$. Clearly, the hypothesis of Lemma 2.6 is satisfied, so $(G, +, \cdot)$ is a two-sided brace. This proves part (1) of the proposition. The nilpotency of the the group $(G, \cdot)$ follows from [Smok2, Proposition 8]. □

Question 2.8. *Under the hypothesis of Proposition 2.7, can we find an upper bound $B(m)$, depending on m, so that G has nilpotency class $\leq B(m)$?*

Proposition 2.9. *Let (G, r) be a finite symmetric group such that $(G,*)$ is a semigroup. The following conditions are equivalent.*

(1) *(G, r) has a finite multipermutation level,* $\mathrm{mpl}(G, r) = m$.
(2) *$(G, \cdot)$ is a nilpotent group.*
(3) *$(G, +, \cdot)$ is a two-sided brace.*

Proof. The implications (1) $\Longrightarrow$ (2) and (1) $\Longrightarrow$ (3) follow from Proposition 2.7. The implication (3) $\Longrightarrow$ (1) is well known, [Ru], [GI]. (2) $\Longrightarrow$ (3). Assume the group G is nilpotent. Then [Smok2, Theorem 1] implies $G^n = 0$ for some positive integer n. It follows from Lemma 2.6 that $(G, +, \cdot)$ is a two-sided brace. □

Recall that (X, r) is a multipermutation solution if and only if the corresponding symmetric group $(\mathcal{G}, r_{\mathcal{G}})$ has a finite multipermutation level, [GI, Theorem 5.15].

Corollary 2.10. *Let (X, r) be a multipermutation solution, $\mathcal{G} = \mathcal{G}(X, r)$. Then $(\mathcal{G}, *)$ is a semigroup if and only if the left brace $(\mathcal{G}, +, \cdot)$ is a two-sided brace.*

Remark 2.11. Let (G, r) be a symmetric group, and let $(G, +, \cdot)$ be the corresponding left brace. Suppose that $(G, +, *)$ is a Jacobson radical ring generated by a finite set $X = \{x_1, \cdots, x_n\} \subseteq G$. If $(G,*)$ satisfies the identity

$$x*u*x = 0, \forall x \in X, \quad u \in G, (u = e \text{ is possible})$$

then the left brace G is nilpotent of nilpotency class $\leq n+1$. Moreover, (G,r) has finite multipermutation level, $\operatorname{mpl}(G,r) \leq n$.

Proof. By assumption $(G,+,*)$ is a Jacobson radical ring. Therefore any element from $G^{(k)}, k \geq 1$, can be written as a sum of elements w of the form $w = y_1 * y_2 * \cdots * y_s,\ \ y_j \in X \bigcup \{e\},\ 1 \leq j \leq s,\ s \geq k$. But $|X| = n$, hence every such element $w \in G^{(n+1)}$ has a subword $x * a * x$, where $x \in X, a \in G$, or has the shape $w = u * e * v,\ u, v \in G$, so in each case $w = 0$. Hence $G^{(n+1)} = 0$, and therefore, by [CGIS, Proposition 6], $\operatorname{mpl}(G,r) \leq n$. □

3. Symmetric sets (X,r) whose associated groups and braces have special properties

It was proven in [GI, Theorem 8.2], that for a nontrivial square-free solution (X,r), with $G = G(X,r)$ one has $\operatorname{mpl}(X,r) = \operatorname{mpl}(G,r_G) = 2$ if and only if (G,r_G) satisfies condition **lri**. We generalize this result for arbitrary solutions (X,r).

Theorem 3.1. *Let (X,r) be a solution of arbitrary cardinality, $G = G(X,r)$, (G,r_G), $(G,+,\cdot)$ in usual notation. The following conditions are equivalent.*

1. *(G,r_G) is a non-trivial solution with condition **lri**.*
2. *(G,r_G) is a multipermutation solution of level 2.*
3. *G acts (nontrivially) upon itself as automorphisms that is*

$$\mathcal{L}_{(a^b)} = \mathcal{L}_a, \quad \forall\, a,b \in G,\ \text{and}\ \mathcal{L}_a \neq id_G,\ \text{for some}\ a \in G.$$

4. *(X,r) is a non-trivial solution with **lri** and the brace $(G,+,\cdot)$ satisfies **Raut**.*

Each of these conditions imply $\operatorname{mpl}(X,r) \leq 2$.

Proof. [GI, Proposition 7.13] gives the implications (2) $\Longleftrightarrow$ (3) $\Longrightarrow$ (1). The equivalence (1) $\Longleftrightarrow$ (4) follows from [GI, Corollary 7.11].

(1) $\Longrightarrow$ (2). Assume that (G,r_G) is a nontrivial solution which satisfies **lri**. We shall show that $\mathcal{L}_{({}^a z)} = \mathcal{L}_z$ for all $z \in X, a \in G$.

By [GIM, Proposition 2.25], G satisfies the cyclic conditions. We use successively **ML0**, **ML2**, **lri** and **cl2** to obtain

$$1 = {}^a(b^{-1}b) = {}^a(b^{-1})^{(a^{b^{-1}})}b = {}^a(b^{-1})^{({}^b a)}b = {}^a(b^{-1}){}^a b,$$

for all $a,b \in G$. Thus

$$ {}^a(b^{-1}) = ({}^a b)^{-1},\ \forall a,b \in G. \tag{3.1}$$

Let $x,y,z \in X$. Then condition **lri** implies

$$ (xy^{-1})^{z^{-1}} = {}^z(xy^{-1}). \tag{3.2}$$

Note that $y^{-1} = -\left({}^{y^{-1}}y\right) = -\left(y^y\right)$. We now compute each side of (3.2). For the left-hand side we obtain

$$\begin{aligned}(xy^{-1})^{z^{-1}} &= x^{((y^{-1})(z^{-1}))}(y^{-1})^{z^{-1}} \quad \text{(by } \mathbf{MR2}\text{)}\\ &= {}^{(z^y)}x(y^{-1})^{z^{-1}} \quad \text{(by } \mathbf{lri} \text{ and (3.1))}\\ &= \left({}^{(z^y)}x\right)\left({}^{z}(-(y^y))\right)\\ &= \left({}^{(z^y)}x\right) + {}^{\left({}^{(z^y)}x\right)}\left({}^{z}(-(y^y))\right) \quad \text{(by (1.4))}\\ &= \left({}^{(z^y)}x\right) - {}^{\left({}^{(z^y)}x\right)}\left({}^{z}(y^y)\right).\end{aligned}$$

Our computation of the right-hand side gives

$$\begin{aligned}{}^{z}(xy^{-1}) &= ({}^{z}x)\cdot\left({}^{({}^{z}x)}(y^{-1})\right) \quad \text{(by } \mathbf{ML2}\text{)}\\ &= ({}^{z}x) + {}^{({}^{z}x)}\left({}^{({}^{z}x)}(-(y^y))\right) \quad \text{(by (1.4))}\\ &= ({}^{z}x) - {}^{({}^{z}x)\cdot({}^{z}x)}(y^y)\\ &= ({}^{z}x) - {}^{(z\cdot x)}(y^y).\end{aligned}$$

Therefore the following equality holds in G

$$\left({}^{(z^y)}x\right) - {}^{\left({}^{(z^y)}x\right)}\left({}^{z}(y^y)\right) = ({}^{z}x) - {}^{(z\cdot x)}(y^y). \tag{3.3}$$

Note that $(G, +)$ is a free abelian group with a basis X, and $\left({}^{(z^y)}x\right)$, ${}^{\left({}^{(z^y)}x\right)}\left({}^{z}(y^y)\right)$, $({}^{z}x)$, ${}^{(z\cdot x)}(y^y) \in X$. Hence the equality (3.3) implies that either

$${}^{(z^y)}x = {}^{z}x, \tag{3.4}$$

or

$${}^{(z^y)}x \neq {}^{z}x, \quad \text{and} \quad ({}^{z}x) - {}^{(z\cdot x)}(y^y) = 0. \tag{3.5}$$

We claim that (3.5) is impossible. Indeed, $0 = 1$ in G, hence ${}^{z}(xy^{-1}) = ({}^{z}x) - {}^{(z\cdot x)}(y^y) = 0$ implies ${}^{z}(xy^{-1}) = 1$, which by **ML0** gives $xy^{-1} = 1$, and therefore $x = y$. Now the cyclic condition implies $\left({}^{(z^y)}x\right) = \left({}^{(z^x)}x\right) = ({}^{z}x)$, which contradicts (3.5). It follows then that ${}^{({}^{y}z)}x = {}^{z}x$, for all $x, y, z \in X$. This, together with **lri** and (3.1), imply "enforced" cyclic conditions

$$\begin{aligned}{}^{(z^y)}x &= {}^{z}x, \qquad {}^{({}^{y}z)}x = {}^{z}x\\ x^{({}^{y}z)} &= x^z, \qquad x^{(z^y)} = x^z,\end{aligned} \tag{3.6}$$

for all $x, y, z \in X^\star = X \cup X^{-1}$, where $X^{-1} = \{x^{-1} \mid x \in X\}$.

We use induction on the length $|a|$ of $a \in G$ to show that

$${}^{({}^{y}z)}a = {}^{z}a, \quad {}^{(z^y)}a = {}^{z}a, \quad \forall a \in G,\ \forall y, z \in X^\star. \tag{3.7}$$

The base for induction follows from (3.6). Assume (3.7) is in force for all $a \in G$ with $1 \leq |a| \leq k$. Suppose $a \in G, 2 \leq |a| = k+1$, then $a = tb, t \in X^\star, b \in G, |b| = k$. We use **ML2** and the inductive hypothesis (IH) to yield:

$$\begin{array}{rcll} {}^{({}^yz)}a & = & {}^{({}^yz)}(tb) = ({}^{({}^yz)}(t))({}^{(({}^yz)^t)}(b)) & \\ & = & ({}^{({}^yz)}(t))({}^{(({}^yz))}(b)) & \text{by IH} \\ & = & ({}^zt)({}^zb) & \text{by IH} \\ {}^za & = & {}^z(tb) = ({}^z(t))({}^{(z^t)}(b)) & \\ & = & ({}^zt)({}^zb) & \text{by IH.} \end{array}$$

This implies the first equality in (3.7) for all $a \in G, y, z \in X^\star$. Using **lri** one deduces that the second equality in (3.7) is also in force. Similar technique "extends" (3.7) on the whole group G, so that the following equalities hold:

$$^{({}^bc)}a = {}^ca, \quad ^{(b^c)}a = {}^ca \quad \forall a, b, c \in G.$$

It follows from [GI, Lemma 7.12] that the symmetric group (G, r_G) satisfies the four equivalent conditions.

$$(3.8) \quad \begin{array}{llll} \textbf{(i)} & \mathcal{L}_{({}^ba)} = \mathcal{L}_a, \ \forall\, a, b \in G; & \textbf{(ii)} & \mathcal{L}_{(a^b)} = \mathcal{L}_a, \ \forall\, a, b \in G; \\ \textbf{(iii)} & \mathcal{R}_{({}^ba)} = \mathcal{R}_a, \ \forall\, a, b \in G; & \textbf{(iv)} & \mathcal{R}_{(a^b)} = \mathcal{R}_a, \ \forall\, a, b \in G. \end{array}$$

By [GI, Proposition 7.13] each of the conditions (i) through (iv) is equivalent to (2). We have shown the implication (1) $\Longrightarrow$ (2), so $\mathrm{mpl}(G, r_G) = 2$. By [GI, Theorem 5.15], one has $\mathrm{mpl}(G, r_G) - 1 \leq \mathrm{mpl}(X, r) \leq \mathrm{mpl}(G, r_G)$, and therefore $\mathrm{mpl}(X, r) \leq 2$. □

Suppose (X, r) is a solution with **lri**, and (G, r_G) is its associated symmetric group. Let $(\overline{G}, r_{\overline{G}})$ be a symmetric group, and assume there is a braiding-preserving map (homomorphism of solutions)

$$\mu : X \longrightarrow \overline{G} \quad x \mapsto \overline{x} \in \overline{G}$$

Then by [LYZ, Theorem 9], the map μ extends canonically to a braiding preserving group homomorphism (that is a homomorphism of symmetric groups)

$$\mu : (G, r_G) \longrightarrow (\overline{G}, r_{\overline{G}}) \quad a \mapsto \overline{a} \in \overline{G}.$$

Moreover, if $\overline{X} = \mu(X)$ is a set of (multiplicative) generators of $\overline{G}$ then $\mu : G \longrightarrow \overline{G}$ is an epimorphism of symmetric groups.

The following result is a generalization of [GI, Theorem 7.10(2)].

Theorem 3.2. *Let (X, r) be a symmetric set with **lri** (not necessarily finite), let $(\overline{G}, \overline{r})$ be a symmetric group, and let $(\overline{G}, +, .)$ be the associated left brace. Assume there is a braiding-preserving map (homomorphism of solutions)*

$$\mu : X \longrightarrow \overline{G}, \quad x \mapsto \overline{x} \in \overline{G},$$

such hat the image $\mu(X) = \overline{X}$, is an $\overline{r}$-invariant subset of $(\overline{G}, \overline{r})$ and generates the (multiplicative) group $\overline{G}$. The following conditions are equivalent on $\overline{G}$.

(1) *The left brace $(\overline{G}, +, \cdot)$ satisfies condition **Raut**.*
(2) *$(\overline{G}, r_{\overline{G}})$ satisfies condition **lri**.*

Proof. (1) $\Longrightarrow$ (2). Suppose (X,r) satisfies **lri** and $\overline{G}$ satisfies condition **Raut**.

Recall that $X^\star = \{x \mid x \in X \text{ or } x^{-1} \in X\}$. By [GI, Proposition 7.6], condition **lri** on (X,r) extends to

$$\textbf{lri}\star: \quad {}^a(x^a) = x = ({}^a x)^a, \quad \forall\, x \in X^\star,\ a \in G. \tag{3.9}$$

Denote by $\overline{X^\star} = \mu(X^\star)$ the image of $X^\star$ in $\overline{G}$. (It is possible that $\overline{X^\star}$ contains the unit $1 = 1_{\overline{G}}$ of the group $\overline{G}$).

We shall extend **lri** on the symmetric group $(\overline{G}, r_{\overline{G}})$ in two steps. **1.** We show that

$$^{(\overline{a})^{-1}}\overline{u} = \overline{u}^{\overline{a}} \quad \text{for all } \overline{a} \in \overline{X^\star},\ \overline{u} \in \overline{G}. \tag{3.10}$$

For $\overline{u} \in \overline{G}$ we consider $u \in G$ of minimal length, such that $\mu(u) = \overline{u}$. Without loss of generality we may assume that $\overline{u} \neq 1$ (this follows from **ML0** and **MR0**). We use induction on the minimal length $|u|$ of u, with $\mu(u) = \overline{u}$. Condition **lri**$\star$, (3.9) gives the base for induction. Assume (3.10) holds for all $\overline{a} \in \overline{X^\star}$ and all $\overline{u} \in \overline{G}$, where $\overline{u} = \mu(u), |u| \leq n$. Let $\overline{a} \in \overline{X^\star}$ and suppose $\overline{w} \in \overline{G}$, where $\overline{w} = \mu(w), |w| = n+1$. A reduced form of w can be written as $w = xu$, where $x \in X^\star,\ u \in G,\ |u| = n$. We present $\overline{w}^{\overline{a}}$ as

$$\overline{w}^{\overline{a}} = (\overline{xu})^{\overline{a}} = ((\overline{x})(\overline{u}))^{\overline{a}} = (\overline{x} + {}^{\overline{x}}(\overline{u}))^{\overline{a}},$$

and consider the following equalities in G:

$$\begin{array}{rcll} \overline{w}^{\overline{a}} & = & (\overline{x} + {}^{\overline{x}}(\overline{u}))^{\overline{a}} & \\ & = & (\overline{x})^{\overline{a}} + ({}^{\overline{x}}(\overline{u}))^{\overline{a}} & \text{by } \textbf{Raut} \\ & = & {}^{(\overline{a})^{-1}}(\overline{x}) + {}^{(\overline{a})^{-1}}({}^{\overline{x}}(\overline{u})) & \text{by IH} \\ & = & {}^{(\overline{a})^{-1}}(\overline{x} + {}^{\overline{x}}(\overline{u})) & \text{by } \textbf{Laut} \\ & = & {}^{(\overline{a})^{-1}}(\overline{x} \cdot \overline{u}) & \\ & = & {}^{(\overline{a})^{-1}}(\overline{w}), & \end{array} \tag{3.11}$$

where IH is the inductive assumption. This verifies (3.10) for all $\overline{a} \in \overline{X^\star}$, and all $\overline{u} \in \overline{G}$. Clearly, (3.10) is equivalent to

$$^{\overline{a}}(\overline{u}^{\overline{a}}) = \overline{u} \quad \forall\, \overline{a}, \overline{u}, \text{ where } \overline{a} \in \overline{X^\star},\ \overline{u} \in \overline{G}. \tag{3.12}$$

2. We shall extend (3.12) for all $\overline{a} \in \overline{G}$. We use induction again, this time on the minimal length of the elements $a \in G$ with $\mu(a) = \overline{a}$. The base of the induction is given by (3.12). Assume ${}^{\overline{a}}(\overline{u}^{\overline{a}}) = \overline{u}$ for all $\overline{a}, \overline{u} \in \overline{G}$, where there is an $a \in G$, such that $\mu(a) = \overline{a}$, and $|a| \leq n$. Let $\overline{a}, \overline{u} \in \overline{G}$, and assume the minimal length of the a's with $\mu(a) = \overline{a}$ is $|a| = n+1$. Then $a = bx,\ x \in X^\star, b \in G, |b| = n$. The following equalities hold:

$$\begin{array}{rcll} {}^{\overline{a}}(\overline{u}^{\overline{a}}) & = & {}^{\overline{bx}}(\overline{u}^{\overline{bx}}) & \\ & = & {}^{\overline{b}}({}^{\overline{x}}((\overline{u}^{\overline{b}})^{\overline{x}})) & \\ & = & {}^{\overline{b}}(\overline{u}^{\overline{b}}) & \text{by IH} \\ & = & \overline{u} & \text{by IH.} \end{array} \tag{3.13}$$

This verifies

$$^{\overline{a}}(\overline{u}^{\overline{a}}) = \overline{u}, \quad \forall\, \overline{a},\ \overline{u}, \in \overline{G}.$$

The remaining identity

$$({}^{\overline{a}}\overline{u})^{\overline{a}} = \overline{u}, \quad \forall\, \overline{a},\ \overline{u}, \in \overline{G}$$

is straightforward. We have shown that the symmetric group $(\overline{G}, \overline{r})$ satisfies condition **lri**.

(2) $\Longrightarrow$ (1). It follows from [GI, Theorem 7.10] that condition **lri** on an arbitrary symmetric group implies **Raut** on the corresponding left brace. □

Corollary 3.3. *Let (X, r) be a symmetric set with **lri** (not necessarily finite), notation as usual. The symmetric group $(\mathcal{G}, r_{\mathcal{G}})$ satisfies condition **lri** if and only if the associated left brace $(\mathcal{G}, +, \cdot)$ satisfies condition **Raut**.*

Proof. The map

$$\mathcal{L} : (G, r_G) \longrightarrow (\mathcal{G}, r_{\mathcal{G}}), \quad x \mapsto \mathcal{L}_x,$$

is a braiding preserving homomorphisms of symmetric groups, the image $\mathcal{L}(X)$ generates the permutation group $\mathcal{G}$. So the hypothesis of Theorem 3.2 is satisfied for $\mu = \mathcal{L}$, which implies the equivalence of **lri** and **Raut** on $(\mathcal{G}, r_{\mathcal{G}})$. □

The next corollary follows from Corollary 3.3, and [GI, Theorems 8.5 and 5.15].

Corollary 3.4. *Suppose (X, r) is a finite square-free solution, notation as usual. If the symmetric group $(\mathcal{G}, r_{\mathcal{G}})$ satisfies condition **Raut**, then (X, r) is a multipermutation solution of level $m < |X|$, and*

$$\operatorname{mpl}(X, r) = \operatorname{mpl}(G, r_G) = m, \ \ \operatorname{mpl}(\mathcal{G}, r_{\mathcal{G}}) = m - 1.$$

4. Conditions **lri** and **Raut** on symmetric groups with two-sided braces

In this section we study symmetric groups (G, r) whose associated braces $(G, +, .)$ are two-sided, or equivalently $G_* = (G, +, *)$ are Jacobson radical rings. We present each of the conditions **lri** and **Raut** in terms of identities on the radical ring G_*.

We start with some useful results interpreting various conditions on a symmetric group (G, r) in terms of the operation $*$

Lemma 4.1. *Let (G, r) be a symmetric group. The the following conditions hold.*

(1) *G satisfies the identity*

$$(a * c + c) * a^c + a^c = a, \quad \forall a, c \in G. \tag{4.1}$$

(2) *Suppose the associated brace $(G, +, \cdot)$ is two-sided. Then the Jacobson radical ring $G_* = (G, +, *)$ satisfies the identities*

$$a * c * a^c + c * a^c + a^c = a, \quad \forall a, c \in G. \tag{4.2}$$

$$^{({}^a c)}a = a * c * a + {}^c a, \quad \forall a, c \in G. \tag{4.3}$$

Proof. (1) The map r is involutive, which is equivalent to the following conditions on the actions

$$ {}^{{}^a c}(a^c) = a, \quad ({}^a c)^{a^c} = c, \;\; \forall\, a, c \in G. \tag{4.4} $$

We use (1.5) to present the first equality in terms of the the operations $+, *$ and yield

$$ \begin{array}{rcl} a & = & {}^{{}^a c}(a^c) \\ & = & ({}^a c) * (a^c) + a^c \\ & = & (a * c + c) * (a^c) + a^c. \end{array}, $$

so (4.1) holds.

(2) Suppose the associated brace is two-sided, let $G_* = (G, +, *)$. Clearly, the identities (4.1) and (4.2) are equivalent. Let $a, c \in G$ then

$$ {}^{({}^a c)}a = ({}^a c) * a + a = (a * c + c) * a + a = a * c * a + c * a + a = a * c * a + {}^c a, $$

which proves (4.3) □

Proposition 4.2. *Suppose (G, r) is a symmetric group. The following conditions are equivalent*

(1) *G satisfies the identity*

$$ (c^a) * a = c * a, \;\; \forall\, a, c \in G. \tag{4.5} $$

(2) *(G, r) satisfy the cyclic condition* ***cl1**:*

$$ \textbf{\textit{cl1}}: \quad {}^{c^a}a = {}^c a \;\; \forall\, a, c \in G. \tag{4.6} $$

(3) *(G, r) satisfies* ***lri**.*

(4) *G satisfies all cyclic conditions, see Definition 1.2.*

Proof. The equivalence (1) $\Longleftrightarrow$ (2) follows straightforwardly from the equalities

$$ {}^{c^a}a = (c^a) * a + a, \quad {}^c a = c * a + a, \; a, c \in G \tag{4.7} $$

(2) $\Longrightarrow$ (3). Assume **cl1** is in force. We shall verify the first and the second **lri** equalities

$$ \textbf{lri1}: \quad ({}^c a)^c = a, \; \forall a, c \in G, \qquad \textbf{lri2}: \quad {}^c(a^c) = a \;\; \forall a, c \in G. $$

Let $a, c \in G$. By the non-degeneracy there exists $b \in G$, with $c = b^a$. We use (4.4) and **cl1** to obtain $a = ({}^b a)^{b^a} = ({}^{b^a} a)^{b^a} = ({}^c a)^c$. This proves **lri1**. It follows from the non-degeneracy again that there exists $d \in G$, such that $a = {}^c d$. One has ${}^c(a^c) = {}^c(({}^c d)^c) = {}^c d = a$, so the equality **lri2** is also in force.

(3) $\Longrightarrow$ (2). Let $a, c \in G$. Then **lri1** and (4.4) imply $({}^{c^a} a)^{c^a} = a = ({}^c a)^{c^a}$. By the non-degeneracy ${}^{c^a} a = {}^c a$, which proves **cl1**. We have shown the equivalence of conditions (1), (2), and (3). The equivalence of (3) and (4) follows from [GIM, Lemma 2.24]. □

Theorem 4.3. *Let (G, r) be a symmetric group with a two-sided associated brace $(G, +, .)$, and let $G_* = (G, +, *)$ be the corresponding Jacobson radical ring. The following conditions are equivalent.*

(1) *G_* satisfies the identity*

$$a * c * a = 0, \quad \forall a, c \in G. \tag{4.8}$$

(2) *G_* satisfies the identity (4.5).*
(3) *The symmetric group (G, r) satisfies conditions **lri**.*
(4) *The symmetric group (G, r) satisfies all cyclic conditions.*

Proof. The equivalence of conditions (2), (3), and (4) follows from Proposition 4.2. By Lemma 4.1 G satisfies the identity (4.3) which implies the equivalence

$$[{}^{({}^a c)}a = {}^c a, \ \forall\ a, c \in G] \Longleftrightarrow [a * c * a = 0, \ \forall\ a, c \in G].$$

Now the implication (4) $\Longrightarrow$ (1) is straightforward. We shall prove (1) $\Longrightarrow$ (2). Assume (4.8) holds. By Lemma 4.1 G satisfies the identity

$$a = a * c * a^c + c * a^c + a^c, \quad \forall\ a, c \in G.$$

Hence

$$\begin{aligned} a * c &= (a * c * a^c + c * a^c + a^c) * c \\ &= a * (c * a^c * c) + c * a^c * c + a^c * c \\ &= a^c * c \qquad\qquad \text{by (4.8)}, \end{aligned}$$

which proves (2). We have verified the equivalence of conditions (1), (2), (3) and (4). □

Corollary 4.4. *Suppose (G, r) is a symmetric group of arbitrary cardinality, such that*

(i) *$(G, +, \cdot)$ is a two-sided brace, so $G_* = (G, +, *)$ is the corresponding Jacobson radical ring;*
(ii) *G_* is finitely generated (as a ring) by a set X of N generators (equivalently, the group $(G, \cdot)$ is finitely generated);*
(iii) *(G, r) satisfies **lri**.*

Then the following conditions hold.

(1) *$a * G * a = 0$, for every $a \in G$.*
(2) *The ring G_* is nilpotent with level of nilpotency $\leq N + 1$.*
(3) *(G, r) has multipermutation level $\mathrm{mpl}(G, r) \leq N$.*

Proof. By Theorem 4.3 condition **lri** on (G, r) implies the identity $a * b * a = 0$, for all $a, b \in G$, so (1) is in force. Conditions (2) and (3) follow straightforwardly from Remark 2.11. □

Theorem 4.5. *Let $G = (G, r)$ be a symmetric group. Assume its associated left brace $(G, +, .)$ is a two-sided brace, and let $G_* = (G, +, *)$ be the corresponding Jacobson radical ring.*

(1) *Let* $a, b, c \in G,\ u = u(a,b,c) = (a+b)c,\ w = w(a,b,c) = ({}^{(a+b)}c)(a^c + b^c)$. *Then there is an equality*

$$w = a * c * b^c + b * c * a^c + u. \tag{4.9}$$

(2) *G satisfies condition* ***Raut*** *if and only if the following identity is in force*

$$a * c * b^c + b * c * a^c = 0, \quad \forall a, b, c \in G. \tag{4.10}$$

Proof. (1). We compute u and w as elements of the radical ring G_*. One has $u = (a+b)c = (a+b) * c + a + b + c$, hence

$$u = a * c + b * c + a + b + c. \tag{4.11}$$

Now we compute w:

$$\begin{array}{rcl} w & = & ({}^{(a+b)}c)(a^c + b^c) \\ & = & ({}^{(a+b)}c) * (a^c + b^c) + {}^{(a+b)}c + a^c + b^c \\ & = & ((a+b) * c + c) * (a^c + b^c) + ((a+b) * c + c) + a^c + b^c \\ & = & (a * c + b * c + c) * (a^c + b^c) + ((a+b) * c + c) + a^c + b^c \\ & = & a * c * a^c + a * c * b^c + b * c * a^c + b * c * b^c + c * a^c + c * b^c \\ & & + a * c + b * c + c + a^c + b^c \\ & = & [a * c * a^c + c * a^c + a^c] + [b * c * b^c + c * b^c + b^c] \\ & & + a * c * b^c + b * c * a^c + a * c + b * c + c \\ & = & a + b + a * c * b^c + b * c * a^c + a * c + b * c + c \quad \text{(we have applied (4.2) twice)} \\ & = & (a * c * b^c) + (b * c * a^c) + (a * c + b * c + a + b + c) \\ & = & (a * c * b^c) + (b * c * a^c) + u \qquad \text{(by (4.11))}, \end{array}$$

which proves (1).

(2). Note that condition **Raut** holds in G *iff*

$$(a+b)c = ({}^{(a+b)}c)((a+b)^c) = ({}^{(a+b)}c)(a^c + b^c),\ \forall a, b, c \in G. \tag{4.12}$$

In other words (in notation as above) condition **Raut** in G is equivalent to

$$u(a,b,c) = w(a,b,c),\ \forall a, b, c \in G.$$

This together with (4.9) implies that G satisfies **Raut** if and only if the identity (4.10) is in force. □

5. Graded Jacobson radical rings $(G, +, *)$, their braces and symmetric groups

In this section we consider graded Jacobson radical rings $R = (R, +, *)$.

Convention 5.1. To each Jacobson radical ring $R = (R, +, *)$, by convention we associate canonically a symmetric group (R, r) and a two-sided brace $(R, +, \cdot)$ with operations and actions satisfying

$$\begin{array}{l} a \cdot b = a * b + a + b, \\ {}^a b = a * b + b = a \cdot b - a, \quad a^b = {}^{({}^a b)^{-1}} a, \\ \qquad \forall\ a, b \in R. \end{array} \tag{5.1}$$

Conversely, if (G, r) is a symmetric group whose left brace $(G, +, \cdot)$ is a two-sided brace, by convention we associate to G the corresponding Jacobson radical ring $G_* = (G, +, *)$.

By a graded ring we shall mean a ring graded by the additive semigroup of positive integers. Thus a graded Jacobson radical ring $R = (R, +, *)$ is presented as

$$R = \oplus_{i=1}^{\infty} R_i, \text{ where } R_i * R_j \subseteq R_{i+j},\ 0 \in R_j,\ i, j \geq 1.$$

As usual, each element $a \in R_j, a \neq 0$, is called *a homogeneous element of degree* j, by convention the zero element 0 has degree 0.

For consistency with our notation the operation multiplication in R is denoted by $*$ (the ring R does not have unit element with respect to the operation $*$).

Proposition 5.2. *Let (G, r) be a symmetric group, such that the associated left brace $(G, +, \cdot)$ is two-sided. Suppose the associated Jacobson radical ring $G_* = (G, +, *)$ is graded: $G_* = \oplus_{i=1}^{\infty} G_i$, and is generated as a ring by the set $V \subseteq G_1$. Then* $\operatorname{mpl}(G, r) = m$ *if and only if* $G_m \neq 0$ *and* $G_i = 0$, $\forall\, i \geq m + 1$.

Proof. Consider the chain of ideals $G^{(1)} = G,\ G^{(n+1)} = G^{(n)} * G, n \geq 1$, see (1.6). One has $G_i \subseteq G^{(k)}$, for all $i \geq k$, moreover

$$G^{(k)} = \oplus_{i \geq k} G_i,\ \forall\, k \geq 1. \tag{5.2}$$

By [CGIS, Proposition 6], the symmetric group (G, r) has finite multipermutation level $\operatorname{mpl}(G, r) = m < \infty$ if and only if $G^{(m+1)} = 0$ and $G^{(m)} \neq 0$. This together with (5.2) imply that $\operatorname{mpl}(G, r) = m$ if and only if $G_m \neq 0$, and $G_i = 0$, for all $i \geq m + 1$. □

Remark 5.3. Let R be a graded Jacobson radical ring. Suppose $a, b, c \in R$ are nonzero elements, and a is a homogeneous element of degree i, that is $a \in R_i$. Then it is clear that

$$\begin{array}{ll} (i) & {}^{b}a = a + \tilde{a}, \quad \text{where } \widetilde{a} = b * a \in \oplus_{j > i} R_j; \\ (ii) & a^{c} = a + \tilde{a}, \quad \text{where } \tilde{a} = (({}^{a}c)^{-1}) * a \in \oplus_{j > i} R_j \end{array} \tag{5.3}$$

Lemma 5.4. *Let $R_* = (R, +, *)$ be a graded Jacobson radical ring, $R_* = \oplus_{i=1}^{\infty} R_i$. Let $(R, +, \cdot)$ be the associated two-sided brace, and let (R, r) be the associated symmetric group. Suppose the brace R satisfies condition* ***Raut***.

(1) *The following equality holds for homogeneous elements of R:*

$$a_i * c_j * b_k + b_k * c_j * a_i = 0, \quad \forall\, a_i \in R_i,\ c_j \in R_j,\ b_k \in R_k,\ i, j, k \geq 1. \tag{5.4}$$

(2) *Moreover, if the additive group $(R, +)$ has no elements of order two, then*

$$a_i * c_j * a_i = 0, \quad \forall\, a_i \in R_i,\ c_j \in R_j, i, j \geq 1. \tag{5.5}$$

Proof. (1) Let $a \in R_i, c \in R_j, b \in R_k,\ i,j,k \geq 1$ be non-zero elements (we omit the indices of a, b, c for simplicity of notation). Consider he equalities

$$\begin{array}{rcll} 0 & = & a * c * (b^c) + b * c * (a^c) & \text{by Theorem 4.5} \\ & = & a * c * [b + \tilde{b}] + b * c * [a + \tilde{a}] & \text{see Remark 5.3} \\ & = & [a * c * b + b * c * a] + [a * c * \tilde{b} + b * c * \tilde{a}] = f + g, & \end{array}$$

where $f = a * c * b + b * c * a$, and $g = a * c * \tilde{b} + b * c * \tilde{a}$. Clearly, $f \in R_{i+j+k}$, and $g \in \oplus_{m \geq i+j+k+1} R_m$, see Remark 5.3. But R is a graded ring, hence the equality $f + g = 0$ holds *iff* $f = 0$ and $g = 0$. This proves (5.4).

(2) Assume now that $(R, +)$ has no elements of order two, and let $a = a_i \in R_i, c = c_j \in R_j, i, j \geq 1$. Then we set $k = i$, $b_k = a$ in (5.4) and obtain

$$a_i * c_j * a_i + a_i * c_j * a_i = 0,$$

which implies the desired equality $a_i * c_j * a_i = 0$, $\forall i, j \geq 1$. □

Theorem 5.5. *Let $R_* = (R, +, *)$ be a graded Jacobson radical ring, $R_* = \oplus_{i=1}^{\infty} R_i$. Let $(R, +, \cdot)$, and (R, r), respectively, be the associated two-sided brace and the corresponding symmetric group. Suppose the additive group $(R, +)$ has no elements of order two. The following two conditions are equivalent.*

(1) *The brace $(R, +, \cdot)$ satisfies condition **Raut**.*
(2) *The symmetric group (R, r) satisfies condition **lri**.*

Proof. (1) $\Longrightarrow$ (2). Assume the brace $(R, +, \cdot)$ satisfies **Raut**. We shall prove that $a * c * a = 0, \forall a, c \in R$. Suppose $a, c \in R$ and present each of them as a finite sums of homogeneous components. So $a = \sum_{i=1}^{N} a_i$, $c = \sum_{j=1}^{N} c_j$, where $a_i, c_i \in R_i, i \geq 1$, and there are natural numbers N_a, N_c, such that $a_i = 0$ for all $i \geq N_a$, $c_j = 0$ for all $j \geq N_c$. Set $N = \max(N_a, N_c)$.

Lemma 5.4 implies the following equalities

$$(5.6) \qquad a_i * c_j * a_k + a_k * c_j * a_i = 0 \quad \text{and} \quad a_i * c_j * a_i = 0,$$

for all i, j, k with $1 \leq i, j, k \leq N$. Then, by (5.6), one has

$$\begin{array}{rcl} a * c * a & = & (\sum_{i=1}^{N} a_i) * (\sum_{j=1}^{N} c_j) * (\sum_{k=1}^{N} a_k) \\ & = & \sum_{j=1}^{N} \sum_{1 \leq i < k \leq N} (a_i * c_j * a_k + a_k * c_j * a_i) + \sum_{j=1}^{N} \sum_{i=1}^{N} (a_i * c_j * a_i) \\ & = & 0 \end{array}$$

We have shown that $a * c * a = 0, \forall a, c \in R$, which by Theorem 4.3 implies condition **lri**.

The implication (2) $\Longrightarrow$ (1) follows from [GI, Theorem 7.10]. □

6. Constructions and examples

It is not difficult to construct a Jacobson radical ring $R = (R, +, *)$ with $y*x*y \neq 0$, for some $x, y \in R$, for example one can use Golod-Shafarevich theorem. Another way to find such radical rings is to fix a field F, to consider the free noncommutative F-algebra S (without unit) generated by a finite set X, and let I be the two-sided ideal

$$I = S^4 = \{\sum_{i=1}^{n} s_{1,i} * s_{2,i} * s_{3,i} * s_{4,i} \mid s_{1,i}, s_{2,i}, s_{3,i}, s_{4,i} \in S\}.$$

Then the quotient $R = S/I$ is a nil-algebra ($a^4 = 0, \forall a \in R$), hence R is a Jacobson radical ring. Moreover $x*y*x \neq 0$, for any $x, y \in X$, and therefore the corresponding brace $(R, +, \cdot)$ does not satisfy **lri**.

Note that Theorem 3.1 provides us with a class of symmetric groups (G, r) and their left braces $(G, +, \cdot)$ each of which is not two-sided, but satisfies **lri** and **Raut**, e.g. $G = G(X, r)$, where (X, r) is a square-free solution of arbitrary cardinality and $\mathrm{mpl}(X, r) = 2$.

Theorem 6.1. *Let F be a field of characteristic two, and let A be the free F-algebra (without identity element) generated by the elements x, y. Let I be the two-sided ideal of A generated by the set*

$$W = \{x*y*y+y*y*x, x*x*y+y*x*x\} \bigcup \{x_1*x_2*x_3*x_4 \mid x_1, x_2, x_3, x_4 \in \{x, y\}\},$$

*and let R be the quotient ring $R = A/I$. Then $(R, +, *)$ is a graded Jacobson radical ring and the associated brace $(R, +, \cdot)$ satisfies condition **Raut** but the symmetric group (R, r_R) does not satisfy **lri**. Moreover,* $\mathrm{mpl}(R, r_R) = 3$

Proof. Let $X = \{x, y\}$. Observe that, $R = (R, +, *)$ is a graded radical ring $R = \oplus_{i=1}^{\infty} R_i$ with $R_i = 0$ for every $i > 3$, and $R_1 = \mathrm{Span}_F X$. By Proposition 5.2, $\mathrm{mpl}(R, r_R) = 3$, since $R_3 \neq 0$. It is easy to show that W is a Groebner basis of the ideal I w.r.t. the degree-lexicographic order on the free semigroup $\langle x, y\rangle$. (Here the semigroup multiplication is denoted by $*$, and we assume $x > y$). Hence the set

$$x,\ y,\ x*x,\ x*y,\ y*x,\ y*y,\ y*y*y,\ y*y*x,\ y*x*y,\ y*x*x,\ x*y*x,\ x*x*x$$

project to an F- basis of R, considered as an F- vector space. In particular, $x*y*x \neq 0, y*x*y \neq 0$ in R, hence by Theorem 4.3, R doesn't satisfy **lri**. We shall show that R satisfies **Raut**. By Theorem 4.5 it will be enough to show

$$a*b*c+c*b*a = 0, \ \ \forall a, b, c \in X.$$

Clearly, at least two of the elements a, b, c coincide. If $a = c$ ($a = b = c$ is also possible) then $a*b*c+c*b*a = a*b*a+a*b*a = 0$, since the field F has characteristic 2. If $a = b \neq c$, then $a*b*c+c*b*a = a*a*c+c*a*a = 0$ holds in R, since by construction the element $a*a*c+c*a*a \in A$ is contained in the ideal I. Similarly, if $b = c \neq a$ one has $a*b*c+c*b*a = a*b*b+b*b*a = 0$. We have shown that $a * b * c + c * b * a = 0$ for all $a, b, c \in X$, therefore R satisfies condition **Raut**. □

Theorem 6.2. *Let F be a field of arbitrary characteristic, and let A be the free F-algebra (without identity element) generated by the elements x, y. Let I be the two-sided ideal of A generated by the set of monomials*

$$W = \{x_1 * x_2 * x_3 * x_4 \mid x_1, x_2, x_3, x_4 \in \{x, y\}\},$$

*and let $(R, +, *)$ be the monomial algebra $R = A/I$. Then $(R, +, *)$ is a graded Jacobson radical ring and the associated brace $(R, +, \cdot)$ does not satisfy condition **Raut**. Moreover,* $\mathrm{mpl}(R, r_R) = 3$.

Proof. Note first that I is a monomial ideal, generated by the set W of all monomials of length 4 in A, so $R = (R, +, *)$ is a graded algebra, moreover as a nil-algebra, R is a graded Jacobson radical ring $R = \oplus_{i=1}^{\infty} R_i$ with $R_i = 0$ for every $i > 3$, and $R_1 = \mathrm{Span}_F\{x, y\}$. By Proposition 5.2, this implies $\mathrm{mpl}(R, r_R) = 3$ (since $R_3 \neq 0$). The set W is a Groebner basis of I, so the set of all words in x, y of length ≤ 3 projects to an F- basis of R. In particular, $x * x * y + y * x * x$ is a nonzero element of R, and setting $a = b = x, c = y$ we see that $a * b * c + c * b * a = x * x * y + y * x * x \neq 0$ in R. It follows from Theorem 5.5 that the two-sided brace $(R, +, \cdot)$ does not satisfy **Raut**. □

References

[CGIS] Cedó, F., Gateva–Ivanova, T, Smoktunowicz, A, *On the Yang-Baxter equation and left nilpotent left braces*, Journal of Pure and Applied Algebra, **221** (2017), 751–756. doi:10.1016/j.jpaa.2016.07.014

[CJO] Cedó, F., Jespers, E. , Okniński J., *Braces and the Yang–Baxter equation*, Commun. Math. Phys. **327**, (2014) 101–116.

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

[GI] Gateva-Ivanova, T., *Set-theoretic solutions of YBE, Braces and Symmetric groups*, arXiv:1507.02602v4 [math.QA]

[GIM] Gateva-Ivanova, T. and Majid, S., *Matched pairs approach to set theoretic solutions of the Yang–Baxter equation*, J. Algebra **319** (2008), 1462–1529.

[LYZ] Lu, J., Yan, M., and Zhu, Y., *On the set-theoretical Yang–Baxter equation*, Duke Math. J. **104** (2000), 1–18.

[Ru] Rump,W., *Braces, radical rings, and the quantum Yang-Baxter equation*, J. Algebra **307** (2007), 153–170

[Smok1] Smoktunowicz, A., *A note on set-theoretic solutions of the Yang-Baxter equation*, J. Algebra,article in press, DOI: 10.1016/j.jalgebra.2016.04.015.

[Smok2] Smoktunowicz, A., *On Engel groups, nilpotent groups, rings, braces and the Yang-Baxter equation*, to appear in Trans. Amer. Math. Soc.

[Ta] Takeuchi, M., *Survey on matched pairs of groups. An elementary approach to the ESS-LYZ theory*, Banach Center Publ. **61** (2003), 305–331.

Ferran Cedó, Departament de Matemàtiques, Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona), Spain

Tatiana Gateva-Ivanova, American University in Bulgaria, 2700 Blagoevgrad, and Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria

Agata Smoktunowicz, School of Mathematics, The University of Edinburgh, James Clerk Maxwell Building, The Kings Buildings, Mayfield Road EH9 3JZ, Edinburgh
E-mail: cedo@mat.uab.cat, Tatyana@aubg.edu, A.Smoktunowicz@ed.ac.uk