TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 370, Number 9, September 2018, Pages 6535–6564
http://dx.doi.org/10.1090/tran/7179
Article electronically published on March 20, 2018

ON ENGEL GROUPS, NILPOTENT GROUPS, RINGS, BRACES AND THE YANG-BAXTER EQUATION

AGATA SMOKTUNOWICZ

Abstract. It is shown that over an arbitrary field there exists a nil algebra R whose adjoint group R^o is not an Engel group. This answers a question by Amberg and Sysak from 1997. The case of an uncountable field also answers a recent question by Zelmanov.

In 2007, Rump introduced braces and radical chains $A^{n+1} = A \cdot A^n$ and $A^{(n+1)} = A^{(n)} \cdot A$ of a brace A. We show that the adjoint group A^o of a finite right brace is a nilpotent group if and only if $A^{(n)} = 0$ for some n. We also show that the adjoint group A^o of a finite left brace A is a nilpotent group if and only if $A^n = 0$ for some n. Moreover, if A is a finite brace whose adjoint group A^o is nilpotent, then A is the direct sum of braces whose cardinalities are powers of prime numbers. Notice that A^o is sometimes called the multiplicative group of a brace A. We also introduce a chain of ideals $A^{[n]}$ of a left brace A and then use it to investigate braces which satisfy $A^n = 0$ and $A^{(m)} = 0$ for some m, n.

We also describe connections between our results and braided groups and the non-degenerate involutive set-theoretic solutions of the Yang-Baxter equation. It is worth noticing that by a result of Gateva-Ivanova braces are in one-to-one correspondence with braided groups with involutive braiding operators.

1. Introduction

In [44], Rump introduced braces as a generalisation of Jacobson radical rings and as a tool for describing solutions of the Yang-Baxter equation. In the same paper, he introduced the following two series of subsets A^n and $A^{(n)}$ of a right brace A, defined inductively as $A^{n+1} = A \cdot A^n$ and $A^{(n+1)} = A^{(n)} \cdot A$, where $A = A^1 = A^{(1)}$. We will also use the notation $A^{n+1} = A \cdot A^n$ and $A^{(n+1)} = A^{(n)} \cdot A$ where $A = A^1 = A^{(1)}$ for a left brace A.

Let A be a finitely generated Jacobson radical ring. It is known that the adjoint group A^o of A is a nilpotent group if and only if A is a nilpotent ring, i.e., $A^n = 0$ for some n [3]. In this paper, we show that a similar result holds for finite braces.

Theorem 1.1. *Let A be a finite left brace. Then the adjoint group of A is nilpotent if and only if $A^n = 0$ for some n. Moreover, such a brace is the direct sum of braces whose cardinalities are powers of prime numbers.*

Received by the editors November 27, 2015, and in revised form, November 21, 2016 and December 16, 2016.

2010 *Mathematics Subject Classification.* Primary 16N80, 16N40, 16P90, 16T25, 16T20, 20F45, 81R50.

Key words and phrases. Engel group, nilpotent group, adjoint group of a ring, braces, nil rings, nil algebras, the Yang-Baxter equation.

This research was supported with ERC advanced grant 320974.

Recall that the direct sum $A = \bigoplus_{i=0}^{n} A_i$ of braces is defined in the same way as for rings; namely, if $a = (a_1, \ldots, a_n) \in A$ and $b = (b_1, \ldots, b_n) \in A$, then $a + b = (a_1 + b_1, \ldots, a_n + b_n)$ and $a \cdot b = (a_1 \cdot b_1, \ldots, a_n \cdot b_n)$. Recall that a result of Rump shows that if A is a left brace whose adjoint group A^o is a finite p-group, then $A^n = 0$ for some n (Corollary after Proposition 8 [44]). Notice that if A is a left brace, then by using the opposite multiplication we get a right brace; therefore if A is a right brace, then the group A^o is nilpotent if and only if $A^{(n)} = 0$.

Observe that by writing Example 3 of Rump [44] in the language of left braces, we see that there is a left brace A of cardinality 6 such that $A^{(3)} = 0$ and $A^n \neq 0$ for every n, the adjoint group A^o is not a nilpotent group, and hence A° is not an Engel group. This shows that the adjoint group of a finite brace need not be a nilpotent group and that the assumption of Theorem 1.1 that $A^n = 0$ for some n is necessary. Notice that by writing Example 2 of Rump [44] in the language of left braces we get that there is a finite left brace A such that $A^4 = 0$ and $A^{(n)} \neq 0$ for every n, whose adjoint group A^o is a nilpotent group ([44], Example 2).

Recall that in [44] Rump introduced the following two series of subsets A^n and $A^{(n)}$ of a right brace A, defined inductively as $A^{n+1} = A \cdot A^n$ and $A^{(n+1)} = A^{(n)} \cdot A$, where $A = A^1 = A^{(1)}$. We introduce the following chain $A^{[n]}$ of ideals of any left or right brace A:

$$A^{[n+1]} = \sum_{i=1}^{n} A^{[i]} \cdot A^{[n+1-i]},$$

where $A^{[1]} = A$. It is clear that $A^{[n]} \subseteq A^{[n-1]} \subseteq \ldots \subseteq A^{[1]} = A$ and that for every i, $A^{[i]}$ is a two-sided ideal of A. Recall that for subsets $C, D \subseteq A$ we use notation $C \cdot D = \sum_{i=1}^{\infty} c_i d_i$ with $c_i \in C, d_i \in D$ where almost all c_i, d_i are zero (so the sums $\sum_{i=1}^{\infty} c_i d_i$ are finite). Our next results follow.

Theorem 1.2. *Let A be a left brace (finite or infinite) such that $A^{[s]} = 0$ for some s. If $a \in A^{[i]}$, $b \in A^{[j]}$, $c \in A^{[k]}$, then*

$$(a + b)c - ac - bc \in A^{[i+j+k]}.$$

Let $P \subseteq A$ and let S be the set of all products of elements from P. If R is the additive subgroup of A generated by elements from S, then R is a left brace (with the addition and the multiplication inherited from A). Moreover, if P is a finite set, then R is a finite left brace.

We obtain that the following result holds for both finite and infinite braces.

Theorem 1.3. *Let A be a left brace and let n be a natural number. Then the following assertions are equivalent:*

1. *$A^{(n)} = 0$ and $A^m = 0$ for some natural numbers m, n.*
2. *$A^{[n]} = 0$ for some natural number n.*
3. *$A^{(n)} = 0$ for some n, and the group A^o is nilpotent.*
4. *The adjoint group A^o is nilpotent, and the solution of the Yang-Baxter equation associated to A is a multipermutation solution (A^o is also called the multiplicative group of the brace A in* [18]*).*

Recall that in [22], Etingof, Shedler, and Soloviev introduced a retraction of a solution of the Yang-Baxter equation. A solution (X, r) is called a multipermutation solution of level m if m is the smallest non-negative integer that, after applying the operation of retraction m times, the obtained solution has cardinality 1. If such m

exists the solution is also called retractable (see [22] or [19, page 2474] for a more detailed definition). Such a solution is also called a *multipermutation solution*, that is, a solution which has a finite multipermutation level (for a detailed definition see [23], [18]). There are many interesting results in this area [10–13, 18–20, 22, 27, 29, 44, 55]. Proposition 5.16 from [23], Proposition 7 from [44], and the above Theorem 1.3 motivated the following related result:

Remark 1.4 ([17]). Let A be a left brace, and let (A, r) be the solution to the Yang-Baxter equation associated to A (as at the beginning of Section 2). Then (A, r) is a solution of multipermutation level $m < \infty$ if and only if $A^{(m+1)} = 0$ and $A^{(m)} \neq 0$.

The proof of Remark 1.4 is very similar to the proof of Proposition 5.16 of [23] and can be found in [17]; it is also possible to prove it by applying Proposition 7 of [44] several times translated to left braces.

Our next result concerns adjoint groups of radical rings and nil rings. Recall that nil rings have been used by many authors to construct examples of groups; for example triply factorized groups, SN-groups, torsion groups, Engel groups, and p-groups. Therefore, it might be useful to describe new methods for constructing and investigating such rings. This is one of the aims which motivated our next result.

Recall that if R is any ring, then the adjoint semigroup of R is constructed according to the following rule: $a \circ b = ab + a + b$. It is also denoted $1 + R$, and it is a group if and only if R is a Jacobson radical ring. Amberg, Catino, Dickenschied, Kazarin, Plotkin, Shalev, Sysak, and others proved many interesting results on the adjoint group of a radical ring [4, 6–8, 14, 18, 30, 38, 46, 51]. Amongst many other interesting results, Amberg, Dickenschied, and Sysak showed that the adjoint group R^o of any Jacobson radical ring is an SN-group in which every finite subgroup is nilpotent [3] (recall that a group G is an SN-group if it has a series with abelian factors; see [40], Vol. 1, pp. 9ff. and 25). As mentioned in their paper, by using Zelmanov's theorem on the restricted Burnside problem (see [57–59]), properties of SN-groups and their new ingenious ideas, they were able to deduce the following: If R is a finitely generated Jacobson radical ring, then the following are equivalent: (a) R is an n-Engel ring for some $n \geq 1$, (b) R is a nilpotent ring, (c) R^o is an n-Engel group for some $n \geq 1$. Recall that the aforementioned result of Zelmanov asserts that an n-Engel Lie algebra over an arbitrary field is locally nilpotent and that any torsion free n-Engel Lie ring is nilpotent [57–59]. A surprisingly short proof by Shalev assures that if a radical ring R is an n-Engel algebra over a field of prime characteristic, then the adjoint group R^o of R is m-Engel for some m [46]. A natural question arises then whether an analogy of any of these results would hold for Engel groups and Engel Lie rings. Notice that every nil ring is an Engel Lie ring (for some interesting related results see [2, 37, 47, 48, 53, 54]). Golod has constructed a nil and not locally nilpotent ring whose adjoint group is an Engel group. In 1997 in [3], Amberg and Sysak asked the following question: *If R is a nil ring, is the adjoint group R^o an Engel group?* Similar questions were also asked in [3, 51]. At the conference in Porto Cesareo in July 2015, after one of the talks Zelmanov asked the following question: *If R is a nil algebra over an uncountable field, is the adjoint group R^o an Engel group?* Our result answers these questions in the negative.

Theorem 1.5. *There is a nil ring R such that the adjoint group of R^o is not an Engel group. Moreover, R can be taken to be an algebra over an arbitrary field.*

The paper is organized as follows: in Section 2 we mention connections with the Yang-Baxter equation and braided groups. In Sections 6–12 we prove Theorem 1.5. In Sections 3–5 we prove Theorems 1.1, 1.2, and 1.3. Sections 6–12 and Sections 3–5 can be read independently.

2. Notation and applications for the Yang-Baxter equations and for braided groups

Around 2005, Rump introduced braces as a generalisation of Jacobson radical rings. He also showed that braces correspond to solutions of the Yang-Baxter equation [44]. In [35] Lu, Yan, and Zhu proposed a general way of constructing set-theoretical solutions of the Yang-Baxter equation using braiding operators on groups. In this paper, by a solution of the Yang-Baxter equation we will mean a non-degenerate involutive set-theoretic solution of the Yang-Baxter equation, as in [18].

Let R be a Jacobson radical ring; then R yields a solution $r : R \times R \to R \times R$ to the Yang-Baxter equation with the Yang-Baxter operator $r(x, y) = (u, v)$, where $u = x \cdot y + y$, $v = z \cdot x + x$, and z is the inverse of $u = x \cdot y + y$ in the adjoint group R^o of R (so $z \cdot (x \cdot y + y) + z + (x \cdot y + y) = 0$). The same holds when $(R, +, \cdot)$ is a left brace, and this solution is called the solution *associated to left brace* R and will be denoted as (R, r) (for a reference see [18, 21, 44]).

In [42, p. 128], Rump gave the following definition of a right brace: "Let A be an abelian group together with a right distributive multiplication, that is,

$$(a + b)c = ac + bc$$

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

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

makes A into a group. This group A^o will be called the *adjoint group* of a brace A." In [18] Cedó, Jespers, and Okninski wrote the definition of a brace in terms of operation o; in their paper the adjoint group A^o is called the multiplicative group of brace A.

Similarly, a left brace is an abelian group $(A, +)$ together with a left distributive multiplication, that is, $a(b+c) = ab+ac$ such that the circle operation $a\circ b = ab+a+b$ makes A into group. For a left brace A, the associativity of A^o is easily seen to be equivalent to the equation $(ab + a + b)c = a(bc) + ac + bc$. A right brace which is also a left brace is called a two-sided brace; Rump has shown that two-sided braces are exactly Jacobson radical rings.

In [22] Etingof, Shedler, and Soloviev introduced a retraction of a solution of the Yang-Baxter equation and described some classes of the solutions. They also introduced retractable solutions, which are now also called multipermutation solutions (see [18, 22, 23]). Theorem 2 of [18] by Cedó, Jespers, and Okninski assures that: *If G is a left brace, then there exists a solution (X, r') of the Yang-Baxter equation such that the solution $Ret(X, r')$ is isomorphic to the solution associated to the left brace G, and, moreover, $\mathcal{G}(X, r)$ is isomorphic to the multiplicative group of the left brace G. Furthermore, if G is finite, then X can be taken as a finite set.*

By writing Example 3 of Rump [44] in the language of left braces, we get that there is a finite left brace A whose adjoint group A^o is the symmetric group S_3 which is not a nilpotent group ([44], Example 3); moreover $A^{(3)} = 0$ and $A^n \neq 0$ for every n. By Remark 1.4 the solution to the Yang-Baxter equation associated to A is a multipermutation solution. Observe that by applying the aforementioned Theorem 2 from [18] to this example we obtain the following remark.

Remark 2.1 (Related to Example 3 [44]). There is a finite multipermutation solution (X, r) of the Yang-Baxter solution whose permutation group $\mathcal{G}(X, r)$ of left actions associated with (X, r) is not a nilpotent group.

Recall that permutation group $\mathcal{G}(X, r)$ of left actions associated with (X, r) was introduced by Gateva-Ivanova in [24] (see also [23]). By writing Example 2 from [44] in the language of a left brace we get that there is a finite left brace A such that $A^4 = 0$, $A^{(n)} \neq 0$ for every n, whose multiplicative group is a nilpotent group ([44, Example 2]). By Remark 1.4 the solution associated to A is not a multipermutation solution. This implies, together with Theorem 2 from [18], the following remark.

Remark 2.2 (Related to Example 2 [44]). There is a finite solution (X, r) to the Yang-Baxter equation which is not a multipermutation solution and whose permutation group $\mathcal{G}(X, r)$ of left actions associated with (X, r) is a nilpotent group.

We get the following related result for (possibly infinite) braces.

Proposition 2.3. *Let A be a left brace such that the solution of the Yang-Baxter equation associated to A is a multipermutation solution. Then the adjoint group A^o of A is nilpotent if and only if $A^n = 0$ for some natural number n.*

Gateva-Ivanova and Van den Bergh [28] and independently Etingof, Schedler, and Soloviev [22] gave a group theoretical interpretation of the set-theoretic involutive non-degenerate solutions of the Yang-Baxter equation. Cedó, Jespers, and Okninski [16, 18] asked which groups are multiplicative groups of braces. A similar question in the language of ring theory was asked in [4, 5]. In this paper we obtain the following corollary of Theorem 1.5, which is related to this question.

Corollary 2.4. *There is a finitely generated, two-sided brace whose multiplicative group is a torsion group but not an Engel group.*

By a result of Gateva-Ivanova (see Theorem 3.7 of [23]), every brace G can be considered as a braided group with the involutive braided operator. Moreover, by Proposition 6.2 of [23], G is a two-sided brace if and only if the corresponding braided group satisfies the following identity:

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

for every $a, b, c \in G$. By combining the Gateva-Ivanova result with Corollary 2.4, we obtain that:

Corollary 2.5. *There is a countable, braided group (G, σ) with an involutive braided operator σ which is a torsion-group and not an Engel group. Moreover, G satisfies a non-trivial identity*

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

for all $a, b, c \in G$. We use notation $\sigma(a, b) = ({}^a b, a^b)$.

This shows that infinite braided groups satisfying non-trivial identities can be quite complicated.

We also get the following result for finite braided groups.

Proposition 2.6. *Let G be a finite nilpotent group and let (G, σ) be a symmetric group (in the sense of Takeuchi). Let $(G, +, o)$ be a left brace associated to (G, σ) as in Theorem 3.8 in [23]. Then $(G, +, o)$ is a direct sum of left braces whose cardinalities are powers of prime numbers. These braces correspond to Sylow subgroups of G.*

3. Braces with $A^n = 0$ and $A^{(m)} = 0$

In [44] Rump introduced the following two series of subsets of any right brace A. One of the series introduced by Rump is $\ldots \subseteq A^{(2)} \subseteq A^{(1)} = A$, where $A^{(n+1)} = A^{(n)} \cdot A$ and $A^{(1)} = A$. The other series introduced by Rump is $\ldots \subseteq A^2 \subseteq A^1 = A$, where $A^{n+1} = A \cdot A^n$ and $A^1 = A$. Following Rump, we will also use the notation $A^{n+1} = A \cdot A^n$ and $A^{(n+1)} = A^{(n)} \cdot A$ where $A = A^1 = A^{(1)}$ for a left brace A.

Rump has proved that the series A^n of every right brace consists of two-sided ideals [44]. Similarly, for a left brace A, the series $A^{(n)}$ consists of two-sided ideals. Recall that I is an ideal in a brace A if for $i, j \in I$ and $a \in A$ we have $i + j \in I$ and $a \cdot i \in I, i \cdot a \in I$; see [44].

We propose another series, defined for any left or right brace. This series consists of two-sided ideals in any left or right brace A. We define the series $\ldots \subseteq A^{[2]} \subseteq A^{[1]} = A$, where

$$A^{[n+1]} = \sum_{i=1}^{n} A^{[i]} \cdot A^{[n+1-i]}.$$

Then it is clear that $A^{[n]}$ is an ideal in A for every n, and $A^{[n+1]} \subseteq A^{[n]}$.

Recall that for subsets $C, D \subseteq A$ we use notation

$$C \cdot D = \sum_{i=1}^{\infty} c_i d_i$$

with $c_i \in C, d_i \in D$, and almost all c_i, d_i equal zero (so the sums $\sum_{i=1}^{\infty} c_i d_i$ are finite).

Theorem 3.1. *Let $(A, \cdot, +)$ be a left or right brace. If m, n are natural numbers and $A^n = A^{(m)} = 0$, then $A^{[s]} = 0$ for some number s.*

Proof. We will prove the result in the case when A is a right brace; the case when A is a left brace is done by considering the brace with the opposite multiplication. We will proceed by induction on n. If $n = 2$, then $0 = A^2 = A \cdot A = A^{(2)} = A^{[2]}$, so the result holds. Suppose that there is a natural number $s_{n,m}$ such that any right brace satisfying $A^n = 0$ and $A^{(m)} = 0$ satisfies $A^{[s_{n,m}]} = 0$.

Assume now that our brace satisfies $A^{n+1} = 0$ and $A^{(m)} = 0$. Let $p > s_{n,m} \cdot m$, and suppose that $a \in A^{[p]}$. Then $a = \sum_i a_i b_i$ for some $a_i, b_i \in A$ with $a_i \in A^{[p-q_i]}$, $b_i \in A^{[q_i]}$, for some numbers q_i. Observe that if $q_i > s_{n,m}$, then $b_i \in A^n$ (by the inductive assumption applied to the brace A/A^n; this brace is well defined as A^n is an ideal in A). In this case we get $a_i b_i \in A \cdot A^n = A^{n+1} = 0$. Therefore $q_i \leq s_{n,m}$, as otherwise $a_i b_i = 0$. Consequently we can assume that all $q_i \leq s_{n,m}$. For each i, we can now write $a_i = \sum_i a_{i,j} b_{i,j}$, and by the same argument as before, we get that each $b_{i,j} \in A^{[r_i]}$ for some $r_i \leq s_{n,m}$ (as otherwise $b_{i,j} \in A^n$ by the inductive assumption applied to A/A^n, and so $a_{i,j}b_{i,j} \in A^{n+1} = 0$). Observe now that since A is a right brace then

$$\sum_i a_i b_i = \sum_i (\sum_j a_{i,j} b_{i,j}) b_i = \sum_{i,j} (a_{i,j} b_{i,j}) b_i.$$

Continuing in this way we get that $a \in \sum_{c_1,\dots,c_m \in A}((((A \cdot c_1) \cdot c_2) \dots \cdot c_{m-1}) \cdot c_m)$, and since $A^{(m)} = 0$ we get that each $a = 0$, so $A^{[p]} = 0$. □

Theorem 3.2. *Let $(A, \cdot, +)$ be either a left brace or a right brace. If $A^n = A^{(m)} = 0$ for some natural numbers m, n, then the multiplicative group of A is a nilpotent group.*

Proof. Let $a, b \in A$; then $[a, b] = a \circ b \circ a^{-1} \circ b^{-1}$ where a^{-1} and b^{-1} are inverses of a and b respectively in the adjoint group A^o. We will construct a finite lower central series of A^o. By Theorem 3.1 there is s such that $A^{[s]} = 0$. We proceed by induction on s. If $A^{[2]} = 0$, then A is commutative so the result holds. Suppose that the result holds for all numbers smaller than s; by the inductive assumption applied to $A' = A/A^{[s-1]}$ we get $[[[[A, A]A] \dots]A] \in A^{[s-1]}$ (m brackets for some m). Since $A^{[s-1]}$ is in the center of A we get that $[[[[A, A]A] \dots]A] = 0$ ($m + 1$ brackets); hence A has a finite lower central series. □

Theorem 3.3. *Let A be a left brace such that $A^{(n)} = 0$ for some n. If the multiplicative group of A is nilpotent, then $A^m = 0$ for some m, and hence $A^{[s]} = 0$ for some s.*

Proof. By assumption $A^{(n)} = 0$ for some n. We can assume that n is minimal possible. Let $b \in A^{(n-1)}$, $a \in A$, and let a^{-1} and b^{-1} be the inverses of respectively a and b in the adjoint group A^o. Recall that A^o is the group under the circle operation $a \circ b = ab + a + b$. We will show that

$$a \circ b \circ a^{-1} \circ b^{-1} = ab.$$

Note that $A^{(n-1)} \subseteq Soc(A) = \{x \in A \mid x \circ a = x + a\}$. By [38, Corollary after Proposition 6], $A^{(n-1)}$ is an ideal. Hence $A^{(n-1)}$ is a normal subgroup of the multiplicative group of the left brace A. Let $b \in A^{(n-1)}$ and $a \in A$. Since $0 = b \circ b^{-1} = b + b^{-1}$, we have that $b^{-1} = -b$:

$$\begin{aligned}
[a, b] &= a \circ b \circ a^{-1} \circ b^{-1} \\
&= a \circ b \circ a^{-1} + b^{-1} \quad (\text{since } a \circ b \circ a^{-1} \in A^{(n-1)}) \\
&= a \circ (b + a^{-1}) - b \\
&= a \circ b + a \circ a^{-1} - a - b \\
&= a \circ b - a - b \\
&= ab.
\end{aligned}$$

Therefore $[a, b] = a \circ b \circ a^{-1} \circ b^{-1} = ab$.

Since the multiplicative group A^o of A is nilpotent we get

$$[a_m[\dots[a_2[a_1, b_1]]]] = 0$$

for some m. Therefore $[a_m[\dots[a_2[a_1, b_1]]]] = a_m(a_{m-1}(\dots(a_2(a_1b))))$. Consequently $A(A(\dots A(A^{(n-1)}))) = 0$ (m brackets).

We will now apply this result to prove our theorem; we will use induction on n (recall that n is such that $A^{(n)} = 0$). For $n = 2$ the result holds since $A^{(2)} = A^2 = A^{[2]}$. Suppose now that the result holds for all numbers smaller than n, so if B is a left brace and $B^{(n-1)} = 0$ and the adjoint group of B^o is nilpotent, then $B^{(n')} = 0 = B^{[n']}$ for some n'.

Recall that $A^{(n-1)}$ is an ideal in A, and hence a normal subgroup of A^o [18, 44]; hence the adjoint group of brace $A/A^{(n-1)}$ is nilpotent. We can apply the inductive assumption for the brace $B' = A/A^{(n-1)}$ and we get that $B^{n'} = 0$; hence $A^{n'} = A(A(\dots A)) \subseteq A^{(n-1)}$. Therefore $A^{m+n'} \subseteq A(A(\dots A(A^{(n-1)}))) = 0$. By Theorem 3.1 we get that $A^{[s]} = 0$ for some s. □

Let us remark that the first part of the above proof was provided by Ferran Cedó after reading the original proof in the first version in this manuscript.

4. Structure of left braces with $A^n = 0$

In this section we observe some connections between nilpotent braces and nilpotent rings. We start with the following lemma.

Lemma 4.1. *Let s be a natural number and let A be a left brace such that $A^s = 0$ for some s. Let $a, b \in A$. Define inductively elements $d_i = d_i(a,b), d'_i = d'_i(a,b)$ as follows: $d_0 = a$, $d'_0 = b$, and for $i \leq 1$ define $d_{i+1} = d_i + d'_i$ and $d'_{i+1} = d_i d'_i$. Then for every $c \in A$ we have*

$$(a+b)c = ac + bc + \sum_{i=0}^{2s} (-1)^{i+1}((d_i d'_i)c - d_i(d'_i c)).$$

Proof. Observe first that by an inductive argument $d'_i \in A^i$ for each i. Observe that for $i \geq 1$ we have

$$d_{i+1} \cdot c = (d_i + d'_i) \cdot c = ((d_{i-1} + d'_{i-1}) + d_{i-1}d'_{i-1}) \cdot c.$$

Recall that since A is a left brace then

$$d_{i+1}c = (d_{i-1} + d'_{i-1} + d_{i-1}d'_{i-1}) \cdot c = d_{i-1}c + d'_{i-1}c + d_{i-1}(d'_{i-1}c).$$

The same holds when we increase i by 1; hence $d_{i+2}c = d_i c + d'_i c + d_i(d'_i c)$. Subtracting the above equation from the previous one we get

$$d_{i+1}c - d_{i+2}c = (d_{i-1}c - d_i c) + e_i,$$

where $e_i = d'_{i-1}c - d'_i c + d_{i-1}(d'_{i-1}c) - d_i(d'_i c)$. Observe that

$$e_i = (d_{i-2}d'_{i-2})c - (d_{i-1}d'_{i-1})c + d_{i-1}(d'_{i-1}c) - d_i(d'_i c).$$

Therefore,

$$\sum_{i=1}^{s} e_{2i} = \sum_{i=1}^{s} (d_{2i-2}d'_{2i-2})c - (d_{2i-1}d'_{2i-1})c + d_{2i-1}(d'_{2i-1}c) - d_{2i}(d'_{2i}c).$$

Notice that if $i \geq s$, then $d'_i \in A^s = 0$. Therefore $\sum_{i=1}^{s} e_{2i} = (d_0 d'_0)c + q$ where

$$q = \sum_{i=1}^{s} d_{2i-1}(d'_{2i-1}c) - (d_{2i-1}d'_{2i-1})c - \sum_{i=1}^{s} d_{2i}(d'_{2i}c) - (d_{2i}d'_{2i})c.$$

Observe now that $d_{i+1}c - d_{i+2}c = (d_{i-1}c - d_ic) + e_i$ implies that

$$\sum_{i=1}^{s}(d_{2i+1}c - d_{2i+2}c) = \sum_{i=1}^{s}(d_{2i-1}c - d_{2i}c) + \sum_{i=1}^{s} e_{2i};$$

therefore

$$d_{2s+1}c - d_{2s+2}c = d_1c - d_2c + \sum_{i=1}^{s} e_{2i}.$$

Observe that $d_{2s+2} = d_{2s+1} + d'_{2s+1} = d_{2s+1}$ since $d'_{2s+1} \in A^s = 0$. Consequently $d_2c - d_1c = \sum_{i=1}^{s} e_{2i} = (d_0d'_0)c + q$. Recall that $d_0 = a$, $d'_0 = b$, $d_1 = a+b$, $d'_1 = ab$, and $d_2 = a+b+ab$. Therefore $d_1c = (a+b)c$ and $d_2c = (a+b+ab)c = ac + bc + a(bc)$. Consequently $d_1c = d_2c - (d_0d'_0)c - q$. It follows that $(a+b)c = ac + bc + a(bc) - (d_0d'_0)c - q = ac + bc + d_0(d'_0c) - (d_0d'_0)c - q$. Notice that $d_0(d'_0c) - (d_0d'_0)c - q = \sum_{i=0}^{2s}(-1)^{i+1}((d_id'_i)c - d_i(d'_ic))$, which finishes the proof. ☐

For an element $a \in A$ and a natural number i, by

$$i \cdot a$$

we will denote the sum of i copies of element a (hence $0 \cdot a = 0$).

Lemma 4.2. *Let the assumptions and notation be as in Lemma* 4.1*. Suppose that there is a natural number m such that $m \cdot a = m \cdot b = 0$. Let d_i, d'_i be as in Lemma* 4.1*; then $m \cdot d_i = m \cdot d'_i = 0$ for every $i \geq 1$.*

Proof. We will first show that $m \cdot d'_t = 0$ for every $t \geq 0$. For $t = 0$ we have $m' \cdot d'_o = m \cdot b = 0$. Suppose the result holds for some $t \geq 0$. Then $m \cdot d'_{t+1} = m \cdot (d_td'_t) = d_t(m \cdot d'_t) = 0$.

We will now show that $m \cdot d_t = 0$ for all $t \geq 0$. For $t = 0$ we have $m \cdot d_0 = m \cdot a = 0$. Suppose the result holds for some $t \geq 0$. Then $m \cdot d_{t+1} = m \cdot d_t + m \cdot d'_t = 0$ by the inductive assumption. ☐

Let A be a left brace and let $S, Q \subseteq A$ be additive subgroups of A. Then we denote $S + Q = \{s + q : s \in S, q \in Q\}$.

Lemma 4.3. *Let $(A, +, \cdot)$ be a finite left brace of cardinality $p_1^{\alpha_1} \dots p_k^{\alpha_k}$ for some prime pairwise distinct numbers $p_1, \dots, p_k$ and natural numbers $\alpha_1, \dots, \alpha_k$. Then*

$$A = A_1 + A_2 + \dots + A_k,$$

where A_i is the additive subgroup of the additive group $(A, +)$ of cardinality $p_i^{\alpha_i}$ for every $i \leq k$. Moreover, $(A_i, +, \cdot)$ is a brace for each $i \leq k$.

Proof. Since the additive group of A is a finite abelian group, then by using the primary decomposition theorem we can decompose the additive group $(A, +)$ into a sum of additive subgroups of A; we can call them $A_1, \dots, A_k$, where A_i is an additive subgroup of A of cardinality $p_i^{\alpha_i}$ and $A_i \cap A_j = 0$. Observe that if $x, y \in A$ and $p \cdot y = 0$ for some natural number p, then $p \cdot (xy) = x \cdot (py) = 0$. Therefore if $a, a' \in A_i$, then $a \cdot a' \in A_i$; hence A_i is closed under the multiplication. We know that A_i is closed under the addition; hence it is also closed under the operation $\circ$, where $a \circ b = a \cdot b + a + b$ for $a, b \in A$. Observe that since A is a finite group, then the inverse of $a \in A$ in the adjoint group A^o is of the form $a \circ a \circ \dots \circ a$; hence it belongs to A_i. It follows that A_i is a left brace. ☐

Theorem 4.4. *Let A be a finite left brace such that $A^n = 0$ for some n. Then A is the direct sum of braces whose cardinalities are powers of prime numbers. In particular, the adjoint group A^o of A is a nilpotent group.*

Proof. Let notation be as in Lemma 4.3. We will first show that if $a, b \in A$ and $m \cdot a = m' \cdot c = 0$ for some coprime natural numbers m, m', then $a \cdot c = 0$. Let $a \in A$. By $\deg(a)$ we will denote the largest number $i \leq n$ such that $a \in A^i$. We will proceed by induction on $i = 2n - \deg(a) - \deg(c)$. If $2n - \deg(a) - \deg(c) = 0$, then $a, c \in A^n = 0$, so the result holds. Suppose now that $i > 0$ and that result holds when $2n - \deg(a) - \deg(c) < i$. We will show that the result also holds for $2n - \deg(a) - \deg(c) = i$.

Let j be a natural number. Let $c, d_1, d_1', \ldots, d_n, d_{n'}$ be as in Lemma 4.1, applied for a and for $b = ja$ and for $s = n$. Denote $q_j = \sum_{i=0}^{2s}(d_i d_i')c - d_i(d_i'c)$; then by Lemma 4.1 we have

$$(a + ja)c = ac + (ja)c + q_j.$$

By Lemma 4.2, $m \cdot d_i = m \cdot d_i' = 0$ for all $i \geq 0$. Observe now that for any i, the order of element $d_i'c$ is a divisor of m' and hence is coprime with m. This follows because, by the assumption at the beginning of the proof, the order of c is m' and m' is coprime with m. Observe that $m' \cdot (d_i'c) = d_i'c + \ldots + d_i'c = d_i' \cdot (m' \cdot c) = 0$.

Observe that $d_i(d_i'c) = 0$ by the inductive assumption, as $2n - \deg(d_i) - \deg(d_i'c) \leq 2n - \deg(d_i) - (\deg(c) + 1) < 2n - \deg(a) - \deg(c)$. Similarly $(d_i d_i')c = 0$ by the inductive assumption since $2n - \deg(d_i d_i') - \deg(c) \leq 2n - (\deg(d_i') + 1) - \deg(c) < 2n - \deg(a) - \deg(c)$. Therefore $q_j = 0$. Consequently for every natural number j,

$$(a + ja)c = ac + (ja)c.$$

Recall that m, m' are coprime numbers; therefore there are natural numbers ξ, β such that $\beta m' - \xi \cdot m = 1$. Denote $e = \xi \cdot m + 1 = \beta \cdot m'$. Observe now that by the above $ac = (ea)c = ((e-1)a)c + ac = ((e-2)a)c + ac + ac = \ldots = e(ac) = a(ec) = 0$. We have proved that $ac = 0$. Therefore if $a \in A_i$ and $c \in A_j$, then $ac = 0$, provided that $i \neq j$ (where A_i is as in Lemma 4.3).

Let $a_i \in A_i$ for $i = 1, \ldots, k$ and let $b \in A$. By the property of a left brace

$$b \cdot (\sum_{i=1}^{k} a_i) = \sum_{i=1}^{k} b a_i.$$

Let $c_i \in A_i$. To show that A is the direct sum of braces A_i it remains to show that $(\sum_{j=1}^{k} a_j)c_i = a_i c_i$. We will show that for every $l \leq k$, $(\sum_{j=1}^{l} a_j)c_i = a_i c_i$ if $i \leq l$ and $(\sum_{j=1}^{l} a_j)c_i = 0$ if $i > l$. We will proceed by induction on l. The result is true for $l = 1$. Let $l > 1$ and suppose that the result holds for $l - 1$.

Observe first that $a_l \cdot (\sum_{j=1}^{l-1} a_j) = \sum_{j=1}^{l-1} a_l a_j = 0$ by the first part of the proof. Hence $(\sum_{j=1}^{l} a_j)c_i = (a_l + (\sum_{j=1}^{l-1} a_j) + a_l(\sum_{j=1}^{l-1} a_j))c_i = a_l c_i + (\sum_{j=1}^{l-1} a_j)c_i + a_l((\sum_{j=1}^{l-1} a_j)c_i)$. By the inductive assumption $(\sum_{j=1}^{l-1} a_j)c_i = a_i c_i$ if $i \leq l - 1$ and $(\sum_{j=1}^{l-1} a_j)c_i = 0$ otherwise. Suppose that $i > l$. Then $(\sum_{j=1}^{l-1} a_j)c_i = 0$ and $a_l c_i = 0$; hence $(\sum_{j=1}^{l} a_j)c_i = 0$, as required. If $i = l$, then $(\sum_{j=1}^{l-1} a_j)c_i = 0$ so $(\sum_{j=1}^{l} a_j)c_i = a_l c_i = a_i c_i$, as required. If $i < l$, then $(\sum_{j=1}^{l-1} a_j)c_i = a_i c_i$, $a_l c_i = 0$, and $(a_l(\sum_{j=1}^{l-1} a_j)c_i) = a_l(a_i c_i) = 0$ as $a_l \in A_l$ and $a_i c_i \in A_i$ and $l \neq i$. Hence $(\sum_{j=1}^{l} a_j)c_i = a_l c_i = a_i c_i$, as required. Therefore, A is the direct sum of braces A_i.

We will now show the nilpotency of A. Observe first that for every i, A_i is a p-group and hence is nilpotent. Observe then that if $a \in A_i$ and $b \in A_j$ for $i \neq j$, then $a \circ b = b \circ a$ since $a \circ b = a + b + ab = a + b$ and $b \circ a = b + a + ba = b + a$ by the above. Therefore, A^o is the direct product of groups A_i for $i = 1, \ldots, k$, and hence it is a nilpotent group. □

5. Braces whose adjoint group is nilpotent

In this section we will investigate the structure of braces whose adjoint groups are nilpotent. For the following result we use a short proof which was provided by Ferran Cedó after reading the original proof in the first version in this manuscript.

Theorem 5.1. *Let A be a finite left brace such that the adjoint group A^o is a nilpotent group. Then A is a direct sum of braces whose cardinalities are powers of prime numbers. Assume that A has cardinality $p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, for some prime pairwise distinct numbers $p_1, \ldots, p_k$ and some natural numbers $\alpha_1, \ldots, \alpha_k$. Then $A^n = 0$ where n is the largest number from among $\alpha_1 + 1$, $\alpha_2 + 1, \ldots, \alpha_k + 1$.*

Proof (Provided by Ferran Cedó). The first part is easier to prove using the equivalent definition of left brace [18, Definition 1]: A left brace is a set B with two binary operations: a sum $+$ and a multiplication $\circ$, such that $(B, +)$ is an abelian group, $(B, \circ)$ is a group, and $a \circ (b + c) + a = a \circ b + a \circ c$ for all $a, b, c \in B$.

Suppose that B is a finite left brace such that its multiplicative group is nilpotent. Let P be a Sylow p-subgroup of the additive group of the left brace B. By [18, Lemma 1], $\lambda_a(P) = P$ for all $a \in B$, where $\lambda_a(b) = a \circ b - a$. In particular P is closed by the multiplication, and hence it is a subgroup of the multiplicative group of the left brace B. Thus P is a Sylow p-subgroup of the multiplicative group of B. Since the multiplicative group of B is nilpotent, P is a normal subgroup in $(B, \circ)$. Hence P is an ideal of the left brace B (see [18, Definition 3]). Therefore, if $P_1, \ldots, P_r$ are the Sylow subgroups of the additive group of B, then they are also the Sylow subgroups of the multiplicative group of B; in fact they are ideals of B and $B = P_1 \circ \ldots \circ P_r = P_1 + \ldots + P_r$ is the inner direct product of the subbraces $P_1, \ldots, P_r$.

The second part of Theorem 5.1 is a consequence of [44, Corollary after Proposition 8]. □

Proof of Theorem 1.1. If $A^n = 0$ for some n, then by Theorem 4.4 the group A^o is nilpotent, and A is the direct sum of braces whose cardinalities are prime numbers. On the other hand, if A is a left brace and A^o is nilpotent, then $A^n = 0$ for some n, by Theorem 5.1. □

Proof of Theorem 1.2. This follows from Lemma 4.1 applied several times, taking into account that $A^{[s]} = 0$. □

Proof of Theorem 1.3. Notice that (1) and (2) are equivalent by Theorem 3.1. Notice that by Remark 1.4, (3) and (4) are equivalent. By Theorems 3.2 and 3.3 properties (3) and (1) are equivalent. □

Proof of Proposition 2.3. This follows from Remark 1.4 and Theorems 3.2 and 3.3. □

6. Jacobson radical

In this section we give some preliminary results on Jacobson radical rings.

Lemma 6.1. *Let F be a field. Let n be a natural number. Let R be an F-algebra generated by elements a, b (without an identity element), and suppose that $a^2 = 0$ and $b^n = 0$ for some n. Let S be the F-linear space spanned by elements $a \cdot b^i$ for $0 < i < n$. If all finite matrices with entries from S are nilpotent, then R is a Jacobson radical ring.*

Proof. We will use the well-known fact that a one-sided ideal in which every element is quasi-regular generates a two-sided ideal which is Jacobson radical [34]. Let R' be a subring of R generated by elements from S. Since all matrices with entries from S are nilpotent, then by Theorem 1.2 from [50] R' is a Jacobson radical ring. Consider ring S' generated by elements from S and from Sa and by element a. Recall that $a^2 = 0$, and so $SaS = 0$. Therefore Sa is a two-sided ideal in S' which is nilpotent; also S'/Sa is Jacobson radical, since R' is Jacobson radical. It follows that S' is Jacobson radical.

Observe that $S'R \subseteq S' + S'a = S'$; hence S' is a right ideal in R. Therefore the two-sided ideal generated by S' in R is Jacobson radical; we will call this ideal I. Observe now that the ring R/I is nilpotent, as it is generated by powers of b. It follows that R is Jacobson radical. □

Lemma 6.2. *Let F be a field. Let n be a natural number. Let R be an F-algebra generated by elements a, b (without an identity element), and suppose that $a^2 = 0$ and $b^n = 0$ for some n. Let $R[x]$ be the polynomial ring in one variable x over R. Let Q be the F-linear space spanned by elements $a \cdot b^i x^j$ for $0 < i < n$, $0 \leq j$. If all finite matrices with entries from Q are nilpotent, then $R[x]$ is a Jacobson radical ring, and hence R is a nil ring.*

Proof. Amitsur's theorem assures that if R is a ring such that $R[x]$ is Jacobson radical, then R is a nil ring (Theorem 15A.5 of [41]). Therefore it suffices to show that $R[x]$ is Jacobson radical. Observe that by Theorem 1.2 from [50], if R' is a subring of $R[x]$ generated by elements from Q, then R' is Jacobson radical. Let $S' = R' + R'a + F[a][x]$ (where $F[a]$ denotes the subalgebra of R generated by a); then similarly as in Lemma 6.1 we get that S' is Jacobson radical. It then follows that the two-sided ideal I generated by S' in R is Jacobson radical, and moreover that $R[x]/I$ is nil. Therefore $R[x]$ is Jacobson radical. □

By R^1 we denote the usual extension of a ring R by the identity element.

Lemma 6.3. *Let F be a field, and let $R = F[a, b]$ be the free algebra (without an identity element) generated by elements a, b. Given $c \in R$, by $F[c]$ we will denote the subalgebra of R generated by c. Let S be the linear F-subspace of $F[a, b]$ spanned by elements ab and $a \cdot b^2$. Let I be the ideal of $F[a, b]$ generated by a^2, b^3, and by elements from sets $F_1, F_2, \dots$ such that $F_i \subseteq S^i$ for every i.*

1. *If $p + q + t + t' + t'' \in I$ and $p \in abR^1, q \in bR^1aR^1$, $t \in F[a]$, $t' \in F[b]$, $t'' \in a^2R^1bR^1$, then $p, q, t, t', t'' \in I$.*
2. *If $p + q \in I$ and $p \in R^1ba, q \in Rb$, then $p, q \in I$.*
3. *If $p = e_1 + e_2 + \ldots + e_n$ with $e_i \in F \cdot S^i$ and $p \in I$, then $e_i \in I$ for all $i \leq n$.*

Proof. (1) By specialising at $b = 0$ we get that $t \in F[a^2] \subseteq I$, and by specialising at $a = 0$ we get $t' \subseteq F[b^3] \in I$; notice that $t'' \in I$, hence $p + q \in I$. Denote

$Z = \bigcup_{i=1}^{\infty} F_i$. Notice that $I \subseteq ZR^1 + b^3R^1 + a^2R^1 + bI + aI$. It follows that $p + q \in (ZR^1 + aI + a^2R^1) + (bI + b^3R^1)$. Observe that $Z \subseteq aR$. Therefore, $p \in (ZR^1 + aI + a^2R^1) \subseteq I$ and $q \in (bI + b^3R^1) \subseteq I$, as required.

(2) Observe now that $I \subseteq Ia + Ib + R^1 \cdot Z + R^1a^2 + R^1b^3$; hence $p + q \in (Ia \cap R^1ba) + Rb + R^1a^2$. Notice that $p \in R^1ba$ and $q \in Rb$. It follows that $p \in Ia \cap R^1ba$, and hence $p \in I$ and so $q = (p + q) - p \in I$.

(3) Let J be the ideal of R generated by elements from sets F_i, and let $\langle a^2 \rangle$, $\langle b^3 \rangle$ denote ideals generated by a^2 and b^3 respectively; then $p - j \in \langle a^2 \rangle + \langle b^3 \rangle$ for some $j \in J$. Notice that p has no terms from $\langle a^2 \rangle + \langle b^3 \rangle$. Consequently $p \in I' + bI' + b^2I' + I'a + bI'a + b^2I'a$, where I' is the ideal of E generated by elements from sets F_i and F_i', where E is the F-algebra generated by elements from S, and where $F_i' = (F_ib + F_ib^2 + Rb^3) \cap E$. Hence $p - i \in bI' + b^2I' + I'a + bI'a + b^2I'a$ for some $i \in I'$. Since the left hand side belongs to aR^1b and the right hand side to $Ra + bR$ it follows that $p - i = 0$, so $p \in I' \subseteq E$. Therefore in the factor ring E/I' we have that $p + I'$ is the zero element.

Observe that I' is a homogeneous ideal in E when we assign gradation of elements from S to have gradation 1, from S^2 gradation 2, etc. Now $p + I' = 0$ in E/I', so $\sum_{j=1}^{n}(e_j + I') = 0$ in E/I', and since E/I' is a graded ring and each $e_j + I'$ has gradation j it follows that $e_i + I' = 0$; hence $e_i \in I$, for every I. $\square$

7. Ideals generated by powers of matrices are "small"

Let R be a ring and let $R[x]$ be the polynomial ring over R. Given a matrix M with entries from $R[x]$, let $P(M)$ denote the linear space spanned by coefficients of polynomials which are entries of matrix M.

We will say that a ring R and a linear space S satisfy assumption (1) when

1. R is the free algebra (without identity) generated by two elements a, b over a field F.
2. S is the linear F-subspace of $F[a, b]$ spanned by elements ab and $a \cdot b^2$.

Lemma 7.1. *Let R, S satisfy assumption* (1)*, and let $R[x]$ be the polynomial ring over R in one variable x. Let m be a natural number and let M be a matrix with entries from $S^m \cdot F[x]$. Let $C = \{c_1, c_2, \dots, c_j\}$, where $c_1, \dots, c_j$ are non-zero elements from $F \cdot S^m$. Let $r = r_1r_2r_3$ where r_i is a product of n_i elements from set C, for $i = 1, 2, 3$, with $n_i \geq 0$.*

If $r \in P(M^{n_1+n_2+n_3})$, then $r_i \in P(M^{n_i})$ for $i = 1, 2, 3$.

Proof. We can write $M^n = M^{n_1} \cdot M^{n_2} \cdot M^{n_3}$. Therefore $P(M^n) \subseteq P(M^{n_1}) \cdot P(M^{n_2}) \cdot P(M^{n_3})$. Hence

$$r = r_1 \cdot r_2 \cdot r_3 \in P(M^{n_1})P(M^{n_2})P(M^{n_3})$$

and $r_i \in F \cdot S^{m \cdot n_i}, P(M^{n_i}) \subseteq F \cdot S^{m \cdot n_i}$. It follows that $r_i \in P(M^{n_i})$ for $i = 1, 2, 3$.

Indeed, if $r_j \notin P(M^{n_j})$ for some j, then we would find a linear mapping $f : F \cdot S^{m \cdot n_j} \to F \cdot S^{m \cdot n_j}$ such that $f(P(M^{n_j})) = 0$ and $f(r_j) \neq 0$, and we can apply this mapping to the above inclusion at appropriate places, obtaining a contradiction. $\square$

Definition 7.2. Let F be an infinite field. Let R, S satisfy assumption (1). Let $f : F \cdot S^m \to F$ be an F-linear mapping. For every i we can extend the mapping f to the mapping $f : F \cdot S^{m \cdot i} \to F$ by defining $f(w_1 \dots w_i) = f(w_1) \dots f(w_i)$ for $w_1, \dots, w_i \in S^m$ and then extending it by linearity to all elements from $F \cdot S^{m \cdot i}$.

Let $t(x) = \sum_{i=0}^{n} t_i x^i$ for some $t_i \in R$; then we denote $f(t(x)) = \sum_{i=0}^{n} f(t_i)x^i$. Let M be a matrix with entries $m_{i,j}$; by $f(M)$ we will denote the matrix with corresponding entries equal to $f(m_{i,j})$.

Similarly, if $g : F \cdot S^m \to F \cdot S^m$ is a linear mapping, then for every i we can extend the mapping g to the mapping $g : F \cdot S^{m\cdot i} \to F \cdot S^{m\cdot i}$ by defining $g(w_1 \dots w_i) = g(w_1) \dots g(w_i)$ for $w_1, \dots, w_i \in S^m$ and then extending it by linearity to all elements from $F \cdot S^{m\cdot i}$.

Lemma 7.3. *Let notation be as in Lemma* 7.1. *Assume that $f(c_i) \neq 0$ for all $i \leq j$, where $c_i \in S^m$ are as in Lemma* 7.1. *Let $f : F \cdot S^m \to F$ be a linear mapping, and let $f : F \cdot S^{m\cdot n_2} \to F$ be as in Definition* 7.2. *Let F be an infinite field, and let $n = n_1 + n_2 + n_3$ be natural numbers. If $r = r_1 r_2 r_3 \in P(M^n)$, then*

$$r_1 f(r_2) r_3 \in P(M^{n_1} f(M^{n_2}) M^{n_3}).$$

Proof. Let M be a d-by-d matrix and let $a_{i,j}(x)$ be the polynomial which is at the i,j entry of M^n. Notice that $a_{i,j}(x) = \sum_{k,l\leq d} b_{i,k}(x)c_{k,l}(x)d_{l,j}(x)$, where $b_{i,k}$ is the i,k entry of matrix M^{n_1}, $c_{k,l}(x)$ is the k,l entry of M^{n_2}, and $d_{l,j}$ is the l,j entry of matrix M^{n_3}. Similarly $n_{i,j}(x) = \sum_{k,l\leq d} b_{i,k}(x)f(c_{k,l}(x))d_{l,j}(x)$ is the i,j-th entry of matrix $M^{n_1} f(M^{n_2}) M^{n_3}$.

Notice that since F is infinite, by a Vandermonde matrix argument we get that $P(M^n) = \sum_{i,j\leq d, p\in F} F \cdot a_{i,j}(p)$ and

$$P(M^{n_1} f(M^{n_2}) M^{n_3}) = \sum_{i,j\leq d, p\in F} F \cdot n_{i,j}(p).$$

If $r = r_1 r_2 r_3 \in P(M^n)$, then $r \in \sum_{i,j\leq D, p\in F} F \cdot a_{i,j}(p)$; hence

$$r_1 r_2 r_3 \in span_{p\in F, i,j\leq d} \sum_{k,l\leq d} b_{i,k}(p)c_{k,l}(p)d_{l,j}(p).$$

If we apply the mapping f as in Definition 7.2 at appropriate places we get that

$$r_1 f(r_2) r_3 \in span_{p\in F, i,j\leq d} \sum_{k,l\leq d} b_{i,k}(p)f(c_{k,l}(p))d_{l,j}(p).$$

Recall that $n_{i,j}(x) = \sum_{k,l\leq d} b_{i,k}(x)f(c_{k,l}(x))d_{l,j}(x)$ is the i,j-th entry of matrix $M^{n_1} f(M^{n_2}) M^{n_3}$. Therefore the linear space spanned by elements

$$\sum_{k,l\leq d} b_{i,k}(p)f(c_{k,l}(p))d_{l,j}(p)$$

for $p \in F$ equals the space spanned by $n_{i,j}(p)$ for $p \in P$. We have shown at the beginning of this proof that the latter space equals $P(M^{n_1} f(M^{n_2}) M^{n_3})$. Therefore $r_1 f(r_2) r_3 \in span_{i,j\leq d, p\in F} n_{i,j}(p) \subseteq P(M^{n_1} f(M^{n_2}) M^{n_3})$. $\square$

Lemma 7.4. *Let R be an F-algebra. Let P be a linear space spanned by the coefficients of polynomials $h_i(x) \in R[x]$ for $i = 1, 2, \dots$. Then for arbitrary non-zero polynomial $g(x)$ from $F[x]$ the linear space Q spanned by the coefficients of polynomials $g(x)h_i(x)$ equals P.*

Proof. Clearly $P \subseteq Q$. Let P_i denote the space spanned by the coefficients of x^i of polynomials $h_1(x), h_2(x), \dots$.

By calculating the coefficient by the smallest power of x in polynomials $g(x)h_i(x)$ we get that $P_0 \subseteq Q$. By then calculating the coefficient by the second-smallest power of x in $g(x)h_i(x)$ we get that $P_1 \in Q + P_0 \subseteq Q$. Continuing in this way we get $P_i \subseteq Q + P_0 + \ldots + P_{i-1}$, so $P_i \subseteq Q$ for every i. It follows that $P \subseteq Q$. ☐

Lemma 7.5. *Let notation be as in Definition* 7.2 *and Lemma* 7.3. *Let t be a natural number and let M be a d-by-d matrix. Let $n_1, n_2, n_3 \geq 0$. Then for all $d \geq 1$ we have*

$$P(M^{n_1} f(M^{n_2}) M^{n_3}) \subseteq \sum_{i=1}^{d+1} P(M^{n_1} f(M)^i M^{n_3}).$$

Proof. Let $b_{i,k}$ denote the i,k entry of matrix M^{n_1}, let $c_{k,l}(x)$ denote the k,l entry of M^{n_2}, and let $d_{l,j}$ denote the l,j entry of matrix M^{n_3}.

Let $n_{i,j}(x)$ be the i,j-th entry of matrix $M^{n_1} f(M^{n_2}) M^{n_3}$; then

$$n_{i,j}(x) = \sum_{k,l \leq d} b_{i,k}(x) f(c_{k,l}(x)) d_{l,j}(x).$$

Notice that $f(M)$ is a matrix with coefficients from $F[x]$. Every matrix with entries from the field of rational functions $F\{x\}$ in variable x satisfies its characteristic polynomial. It follows that there are polynomials $f_i(x)$ such that

$$\sum_{i=1}^{d+1} f_i(x) f(M)^i = 0$$

with $f_{d+1}(x)$ non-zero.

Therefore for every n there is a polynomial $g_n(x) \in F[x]$ such that $g_n(x) f(M)^n \in \sum_{i=1}^{d+1} F[x] \cdot f(M)^i$. By Lemma 7.4,

$$P(M^{n_1} f(M^{n_2}) M^{n_3}) = P(g(x) M^{n_1} f(M^{n_2}) M^{n_3}) = P(M^{n_1} g(x) f(M^{n_2}) M^{n_3}).$$

We know that $g_n(x) f(M^{n_2}) \subseteq \sum_{i=1}^{d+1} F[x] f(M)^i$; hence

$$P(M^{n_1} g(x) f(M^{n_2}) M^{n_3}) \subseteq \sum_{i=1}^{d+1} P(F[x] \cdot M^{n_1} f(M)^i M^{n_3}).$$

By Lemma 7.4 we get $P(M^{n_1} f(M^{n_2}) M^{n_3}) \subseteq \sum_{i=1}^{d+1} P(M^{n_1} f(M)^i M^{n_3})$. ☐

We will say that M, R, S, m, d, α satisfy assumption (2) if

1. R, S satisfy assumption (1) and m, d, α are natural numbers.
2. M is a d-by-d matrix with entries from $S^m \cdot F[x]$. Moreover,

$$M \subseteq R + Rx + Rx^2 + \ldots + Rx^\alpha.$$

Let $c_1, \ldots, c_j$ be linearly independent elements from $F \cdot S^m$ and denote $C = \{c_1, \ldots, c_j\}$. Let $v = c_{i_1} \ldots c_{i_j}$ and $v' = c_{k_1} \ldots c_{k_j}$ for some $i_1, \ldots, i_j$, and some $k_1, \ldots, k_j$. We will say that words v and v' are distinct if $i_l \neq j_l$ for some $l \leq j$.

Let r be a product of elements from the set C. We say that w is a subword of degree n in r if w is a product of n elements from C and $r = vwv'$ for some v, v' which are also products of elements from C.

Lemma 7.6. *Let F be an infinite field. M, R, S, m, d, α satisfy assumption (2). Let q be a natural number. Let $c_1, \ldots, c_j$ be linearly independent elements from $F \cdot S^m$, and let r, r' be products of q elements from the set $C = \{c_1, \ldots, c_j\}$. If $n \geq 8d^3 \cdot (\alpha + 1)$ and r has at least n pairwise distinct subwords of length n, and r' has at least n pairwise distinct subwords of length n, then $r \cdot r' \notin P(M^t)$, for any t.*

Proof. Suppose on the contrary that $rr' \in P(M^t)$. Let $p_1, \ldots, p_n$ be subwords of r of degree n, and let $q_1, q_2, \ldots, q_n$ be subwords of r' of length n. Then there are $s_{i,k}$ such that $p_i s_{i,k} q_k$ is a subword of $r \cdot r'$ for all $i, k \leq n$. By Lemma 7.1, $r \cdot r' \in P(M^t)$ implies that $p_i s_{i,k} q_k \in P(M^{m_{i,k}})$ for some $m_{i,k}$. Let $f : F \cdot S^m \to F$ be a linear mapping, and let $f : F \cdot S^{m \cdot n_2} \to F$ be as in Definition 7.2. We can choose f such that $f(c_i) \neq 0$ for $i = 1, 2, \ldots, j$, and hence $f(s_{i,k}) \neq 0$ for every $i, k \leq n$. By Lemma 7.3,

$$p_i f(s_{i,k}) q_k \in P(M^n f(M^{m_{i,k}-2n}) M^n).$$

By Lemma 7.5, $p_i q_k \in \sum_{l=1}^{d+1} P(M^n f(M^l) M^n)$. Notice that the linear space $\sum_{l=1}^{d+1} P(M^n f(M^l) M^n)$ has dimension smaller than $d^2(d+1) \cdot (2n\alpha + 2)$.

Observe now that since p_i and q_i are products of n elements c_i and $c_i's$ and are linearly independent over F, then elements $p_i q_k$ are linearly independent over F. Therefore elements $p_i q_k$ span a linear space over field F of dimension at least n^2. Hence $n^2 \leq d^2(d+1) \cdot (2n\alpha + 2) < 8d^3 \cdot (\alpha + 1) \cdot n$, a contradiction. □

8. Subspaces E_i and E_i'

Let F be a countable field and let R, S satisfy assumption (1). Since F is countable, we can enumerate finite matrices with entries in $S \cdot F[x]$ as $X_1, X_2, \ldots$. We can assume that the matrix X_i is a d_i-by-d_i matrix where $d_i \leq i$ and X_i has entries in $F \cdot (S + Sx + S \cdot x^2 + \ldots + S \cdot x^i)$ for every i, if necessary taking $X_i = 0$ for some i.

The following is similar to Theorem 5 from [49].

Theorem 8.1. *Let F be a countable field, let R, S satisfy assumption* (1) *and let matrices $X_1, X_2, \ldots$ be as above. Let $0 < m_1 < m_2 < \ldots$ be a sequence of natural numbers such that m_i is a power of two and $2^{2^{m_i}}$ divides m_{i+1} for all $i \geq 1$. Denote $R(m) = F \cdot S^m$ for every m. Let E_i' be the linear space spanned by all coefficients of polynomials which are entries of the matrix $X_i^{2^{2^{m_i}}}$ and let*

$$E_i = \sum_{j=0}^{\infty} R(j \cdot m_{i+1}) E_i' S R.$$

Then there is an ideal I in R contained in $\sum_{i=1}^{\infty} E_i + bE_i + b^2 E_i + \langle a^2 \rangle + \langle b^3 \rangle$ and such that R/I is a nil ring, where $\langle a^2 \rangle, \langle b^3 \rangle$ denote ideals in R generated by elements a^2 and b^3.

Proof. Observe first that the ideal I_k of R generated by coefficients of polynomials which are entries of the matrices $X_k^{2m_{k+1}+2}$ is contained in the subspace $E_k + bE_k + b^2 E_k + \langle a^2 \rangle + \langle b^3 \rangle$. It follows because entries of every matrix X_k have degree one in the subring generated by S with elements of S of degree one. In general if $n > m_{k+1} + 2^{2^{m_k}} + 1$, then coefficients of polynomials which are entries of matrix X_k^n belong to $R(i) E_k' R(1) R$ for every $0 \leq i < n - m_{k+1} - 1$.

Define $I = \sum_{i=1}^{\infty} I_k + \langle a^2 \rangle + \langle b^3 \rangle$; then $I \subseteq \sum_{i=1}^{\infty} E_i + bE_i + b^2 E_i + \langle a^2 \rangle + \langle b^3 \rangle$. Observe also that, by Lemma 6.2, R/I is a nil ring. □

Lemma 8.2. *Let F be an infinite field and let $T \subseteq L$ be finitely dimensional F-linear spaces. Let $c_1, c_2, \ldots, c_j \in L$, and let $c_1, c_2, \ldots, c_j, \notin T$. Then there is a linear mapping $f : L \to F$ such that T is contained in the kernel of f and $c_1, c_2, \ldots, c_j$ are not contained in the kernel of f.*

Moreover there is a linear mapping $g : L \to L$ such that T is contained in the kernel of g and $c_1, c_2, \dots, c_j$ are not contained in the kernel of g and the image of g has co-dimension 1 in L.

Proof. Let Q be a maximal linear space such that $c_1, c_2, \dots, c_m, \notin Q$ and $T \subseteq Q$. We will show that L/Q is a one dimensional linear space. Suppose on the contrary, that there are two elements $x+Q, y+Q$ in L/Q which are linearly independent over F. By maximality of Q, we get that there are $\alpha \neq \beta$ such that linear spaces $Q + F \cdot (x + \alpha \cdot y)$ and $Q + F \cdot (x + \beta \cdot y)$ both contain some element c_i. Then $c_i - t_1 \cdot (x + \alpha \cdot y) \in Q$ and $c_i - t_2 \cdot (x + \beta \cdot y) \in Q$ for some $t_1, t_2 \in F$. It follows that $t_1 \cdot (x+\alpha \cdot y) - t_2 \cdot (x + \beta \cdot y) \in Q$, a contradiction since $x+Q$ and $y+Q$ are linearly independent in L/Q. We can now take $g : L \to L$ to be such that $f(q) = 0$ for every $q \in Q$, and the image of g has co-dimension 1 in L. Observe that the natural linear mapping $f : L \to L/Q$; then L/Q has dimension 1, so L/Q is isomorphic as a linear space to F. In this way we can define the mapping f. □

9. Words w_i

In this section we give some supporting results on some monomials related to Engel elements.

Definition 9.1. Let M be the free monoid generated by elements A, B, A', B'. Define inductively a sequence of infinite monomials W_i as follows:

$$W_1 = A, \quad W_2 = ABA', \quad W_3 = W_2 B \bar{W}_2,$$

and

$$W_{n+1} = W_n B \bar{W}_n,$$

where $\bar{W} = (\sigma(W))^{op}$ where $\sigma : M \to M$ is a homomorphism of monoids such that $\sigma(A) = A'$, $\sigma(A') = A$, $\sigma(B) = B'$, and $\sigma(B') = B$. Recall that if $x_i \in \{A, A', B, B'\}$, then $(x_1 x_2 \dots x_n)^{op} = x_n x_{n-1} \dots x_1$. We will sometimes refer to monomials from M as words. Observe also that for every $n > 0$,

$$\bar{W}_{n+1} = W_n B' \bar{W}_n.$$

Lemma 9.2. *For every i, W_i has length $2^i - 1$.*

Proof. By induction on i. □

Lemma 9.3. *Let notation be as in Lemma 9.2. Let $\alpha(c, v)$ denote the number of occurrences of c in a word $v \in M$. Then for every $n \geq 1$ $\alpha(A, W_{n+1}) = \alpha(A', W_{n+1}) = \alpha(B, W_{n+1}) = 2^{n-1}$ and $\alpha(B', W_{n+1}) = 2^{n-1} - 1$. Moreover in the word W_{n+1} after elements A, A' appears either B or B', and after elements B, B' appears either A or A'.*

Proof. Observe that for $v = W_n B'$ we have $\alpha(A, v) + \alpha(A', v) = \alpha(B, v) + \alpha(B', v)$, as in v after A and A' always appears after either B or B' and vice-versa. We will now proceed with the proof of our theorem by induction on n. For $n = 1$ we have $W_2 = ABA'$, so the result holds in this case. Suppose that the result holds for some $n \geq 1$; we will show that it holds for $n + 1$.

Observe that for every word v, we have $\alpha(A, v) = \alpha(A', \bar{v})$ and $\alpha(B, v) = \alpha(B', \bar{v})$. Recall that $W_{n+1} = W_n B \bar{W}_n$; consequently $\alpha(A, W_{n+1}) = \alpha(A', W_{n+1})$, $\alpha(B, W_{n+1}) = \alpha(B', W_{n+1}) + 1$. Let $v = W_{n+1} B'$; then by the above $\alpha(A, v) = \alpha(A', v)$ and $\alpha(B, v) = \alpha(B', v)$.

By Lemma 9.2, $\alpha(A,v)+\alpha(A',v)+\alpha(B,v)+\alpha(B',v)=2^{n+1}$. Hence $\alpha(A,v)=\alpha(A',v)=\alpha(B,v)=\alpha(B',v)=2^{n-1}$. The result follows. □

Definition 9.4. Let M be a free monoid generated by elements A, A', B, B'. Let $v \in M$. Let R be a ring, and let $x, y, z, t \in R$. By $v(x, y, z, t)$ we will denote the element of R obtained by substituting $A = x$, $B = y$, $A' = z$, and $B' = t$ in the word v.

Definition 9.5. Let F be a field, and let R be a ring generated by elements a, b, such that $a^2 = 0, b^3 = 0$. Then $1+a$ and $1+b$ are invertible elements in R^1. Denote

$$v_1 = [1+a, 1+b] = (1+a)(1+b)(1+a)^{-1}(1+b)^{-1},$$

$$v_2 = [v_1, 1+b] = v_1(1+b)v_1^{-1}(1+b)^{-1},$$

$$v_{n+1} = [v_n, 1+b] = v_n(1+b)v_n^{-1}(1+b)^{-1}.$$

Lemma 9.6. *Let notation be as in Definition* 9.5. *Denote* $z_{n+1} = v_n \cdot (1+b)$. *Then* $z_2 = (1+a)(1+b)(1+a)^{-1} = (1+a)(1+b)(1-a)$ *and*

$$z_{n+1} = z_n \cdot (1+b) \cdot z_n^{-1}$$

for $n = 2, 3, \ldots$. *Moreover,*

$$(z_{n+1})^{-1} = z_n \cdot (1 - b + b^2) \cdot z_n^{-1}.$$

Proof. It is clear that $z_2 = v_1(1+a) = (1+a)(1+b)(1+a)^{-1} = (1+a)(1+b)(1-a)$. By the definition of v_{n+1} we get

$$\begin{aligned} z_{n+1} &= v_n(1+b) = v_{n-1}\cdot(1+b)\cdot v_{n-1}^{-1} = [v_{n-1}(1+b)]\cdot(1+b)\cdot[(1+b)^{-1}v_{n-1}^{-1}] \\ &= z_n \cdot (1+b)\cdot z_n^{-1}. \end{aligned}$$

This implies $z_{n+1}^{-1} = z_n(1-b+b^2)z_n^{-1}$. □

Notation. Let notation be as in Definition 9.1. Let R be a ring generated by elements a, b such that $a^2 = 0$ and $b^3 = 0$. In what follows we will use the following notation:

$$w_n = W_n(a, b, -a, b^2 - b), \bar{w}_n = \bar{W}_n(a, b, -a, b^2 - b).$$

Lemma 9.7. *Let notation be as above and as in Definition* 9.1. *Then* $w_1 = a$, $w_2 = -aba$, $\bar{w}_1 = -a$, *and* $\bar{w}_2 = -a(b^2 - b)a$. *Moreover, for every* n, $w_{n+1} = w_n \cdot b \cdot \bar{w}_n$ *and* $\bar{w}_{n+1} = w_n \cdot (b^2 - b) \cdot \bar{w}_n$.

Proof. It follows from Definition 9.1 by induction on n. □

Lemma 9.8. *Let F be a field and let R, S satisfy assumption* (1). *Let notation be as in Lemmas* 9.7 *and* 9.6. *Let $T(j)$ be the linear space spanned by all monomials $x_1x_2\ldots x_n$ such that $x_i \in \{a, b\}$ and the cardinality of the set $\{1 \le i \le n-1 : x_ix_{i+1} \in \{ab, ba\}\}$ is at most j (n is arbitrary).*

Then for every $n \ge 2$,

$$z_n - w_n - 1, z_n^{-1} - \bar{w}_n - 1 \in T(2^n - 3)$$

and

$$w_n, \bar{w}_n \in F \cdot S^{2^{n-1}-1}a \subseteq T(2^n - 2).$$

Recall that S is the linear space over F spanned by elements ab and $a \cdot b^2$.

Proof. We will proceed by induction. We will use Lemmas 9.7 and 9.6.

For $n = 2$ we have $w_2 = -aba \subseteq F \cdot Sa \subseteq T(2) = T(2^2 - 2)$, and $z_2 = (1+a)(1+b)(1-a) = -aba + (ab + b - a^2 - ba) + 1$. Therefore, $z_2 - w_2 - 1 = ab + b - a^2 - ba \in T(1) = T(2^2 - 3)$, as required.

Recall that $\bar{w}_2 = -a(b^2 - b)a \in F \cdot Sa \subseteq T(2)$. Observe also that $z_2^{-1} = (1+a)(1-b+b^2)(1-a) = -a(b^2-b)a + a(b^2-b) + (b^2-b) - a^2 - (b^2-b)a + 1$; hence $z_2^{-1} - \bar{w}_2 - 1 \in T(1)$, as required.

Suppose now that the result holds for some number $n \geq 2$; we will prove it for $n+1$. Observe that for all i, j, we have $T(i)T(j) \subseteq T(i+j+1)$, as we have only one more place when the words from $T(i)$ and $T(j)$ meet where a change from a to b or from b to a can appear.

Observe that $w_{n+1} = w_n b \bar{w}_n$; hence by the inductive assumption

$$w_{n+1} \in T(2^n - 2)T(0)T(2^n - 2) \subseteq T(2^n - 2 + 0 + 2^n - 2 + 2) = T(2^{n+1} - 2).$$

We have $z_{n+1} = z_n(1+b)z_n^{-1}$; hence for some $q, q' \in T(2^n - 3) + F$,

$$z_{n+1} = (w_n + q)(1+b)(\bar{w}_n + q').$$

By the inductive assumption

$$q(1+b)q' \subseteq T(2^n - 3)T(0)T(2^n - 3) \subseteq T(2^n - 3 + 0 + 2^n - 3 + 2) = T(2^{n+1} - 4).$$

Similarly $q(1+b)\bar{w}_n \subseteq T(2^n - 3)T(0)T(2^n - 2) \subseteq T(2^{n+1} - 3)$ and $w_n(1+b)q' \subseteq T(2^{n+1} - 3)$. Consequently, $z_{n+1} - w_{n+1} - 1 \in T(2^{n+1} - 3)$. The proof that $\bar{w}_{n+1} \in T(2^{n+1} - 2)$ and $z_{n+1}^{-1} - \bar{w}_{n+1} \in T(2^{n+1} - 3)$ is analogous.

Notice also that by Lemma 9.3 and by Notation before Lemma 9.7

$$w_n, \bar{w}_n \in S^{2^{n-1}-1}a \subseteq T(2^n - 2).$$

□

Lemma 9.9. *Let F be an infinite field. Let R, S satisfy assumption* (1). *Let I be the ideal of R generated by elements from sets $F_1, F_2, \ldots$, where $F_i \subseteq F \cdot S^i$ for every i and by elements a^2 and b^3. Denote $w'_{n+1} = W_{n+1}(a, b, -a, b^2 - b) \in R$, $w'_{n+2} = W_{n+2}(a, b, -a, b^2 - b) \in R$. Let v_n, z_{n+1} be as in Definition* 9.5 *and Lemma* 9.6 *applied for ring $\bar{R} = R/\langle a^2, b^3 \rangle$. Let I' be the ideal of $\bar{R}$ which is generated by images in $R/\langle a^2, b^3\rangle$ of elements from sets $F_1, F_2, \ldots$.*

If $v_n - 1 \in I'$ for some $n > 1$, then $w'_{n+1}b \in I$, and hence $w'_{n+2} \in I$.

Proof. Let $z'_{n+1} \in R$ be such that the image of z'_{n+1} in $R/\langle a^2, b^3\rangle$ is z_{n+1}. Recall that $z_{n+1} = v_n \cdot (1+b)$ (as in Lemma 9.6). Observe that $v_n - 1 \in I'$ is equivalent to $z_{n+1} \cdot (1+b)^{-1} - 1 \in I'$. This implies that $z_{n+1} - (1+b) \in I'$ and hence $z'_{n+1} - (b+1) \in I$ (since $a^2, b^3 \in I$). Observe that $R/I = \bar{R}/I'$. We can write $z'_{n+1} - (b+1) = p + q + t + t' + t'' \in I$ for some $p \in ab \cdot R^1$, $q \in bR^1aR^1$, $t \in F[a], t' \in F[b]$, $t'' \in a^2R^1bR^1$, as in Lemma 6.3. By Lemma 6.3 of [1] we get $p, q, t, t', t'' \in I$. By Lemma 9.8 we get $p = w'_{n+1} + v + i$ for some $v \in T(2^{n+1} - 3) \cap abR^1$ and $i \in \langle a^2, b^3\rangle$. We can write $v = v' + v'' + v'''$ where $v' \in Rba$, $v'' \in Rb$, and $v''' \in Ra^2$ (we can assume that $v, v', v'' \in abR^1$ since $v \in abR^1$). Notice that $v''' \in I$ and $i \in I$; hence $w'_{n+1} + v' + v'' \in I$. By Lemma 6.3 of [2] we get that $w'_{n+1} + v' \in I$. Therefore, $w'_{n+1}b + v'b \in I$ and $v'b \in T(2^{n+1} - 2)$. Notice that $v'b \in ab \cdot R^1 \cap R^1 \cdot ab$. It follows that $v'b \in F + F \cdot S + F \cdot S^2 + \ldots + F \cdot S^{2^n - 1} + i'$ for some $i' \in \langle a^2, b^3 \rangle$. By Lemma 9.3, $w'_{n+1}b \subseteq F \cdot S^{2^n}$. By Lemma 6.3 of [3] $w'_{n+1}b \in I$. Observe also that $w'_{n+1}b \in I$ implies that $w'_{n+2} = w'_{n+1}b\bar{w}'_{n+1} \in I$. □

10. Combinatorics of words

The following lemma immediately follows from the proof of Theorem 1.3.13, p. 22, of [36]. We repeat a slightly modified proof.

Lemma 10.1. *Let n be a natural number. Let w be an infinite word which has less than n subwords of degree n; then $u = cddd\dots$ for some words c, d such that c has length smaller than $n!$ and d has length $n!$.*

Moreover if u is a finite word which has less than n subwords of degree n, then $u = cddd\dots d$ for some words c, d such that c has length smaller than $n! + n!$ and d has length $n!$.

Proof. Notice that for some $m \leq n$, w has the same number of words of length m and $m+1$. Hence for every subword v_1 in w of length m we have exactly one possibility of a subword u_1 of w which has length $m+1$ and which contains v as the beginning. Let v_2 be the ending of length m in u_1. We can apply the same reasoning to v_2 instead of v_1 and find word u_2 containing v_2 as at the beginning. After at most n steps we get $v_i = v_j$ for some $i \neq j$, and then from the step j, $v_{k+j} = v_k$ for each k. Therefore $w = v_1 \dots v_{i-1}vvvvvvv...$ where v is some word of length $t < n+1$. Because t divides $n!$ we get the result for w.

If u is a finite word, then we can apply similar reasoning. □

We can then get the following.

Lemma 10.2. *Let R, S satisfy assumption (1). Let $v' = c_1 \dots c_m$ with each $c_i \in F \cdot S^m$ for some m. We say that w is a subword of v' of length n if $v' = uwu'$ where for some k, $u = c_1 \dots c_k$, $w = c_{k+1}c_{k+2}\dots c_{k+n}$, $u' = c_{k+n+1}\dots c_m$ (u and u' may be trivial words). Let n be a natural number. Assume that v' has less than n subwords of degree n; then $u = cddd\dots d$ for some subwords c, d such that c has length smaller than $n! + n!$ and d has length $n!$.*

Proof. It follows from Lemma 10.1. □

Theorem 10.3. *Let $0 < m_1 < m_2 < \dots$ be such that each m_i is a power of two, $2^{2^{m_i}} < m_{i+1}$ and $2^{2^{m_i}}$ divides m_{i+1} for every i. Let $R(i), S, E_1$ be as in Theorem 8.1. Assume that $2^{m_1} > 17! \cdot 10$. Then $w_n b \notin E_1$ for any n, where $w_n = W_n(a, b, -a, b^2 - b)$.*

Proof. Suppose, on the contrary, that $w_n = W_n(a, b, -a, b^2 - b)b \in E_1$. We can assume that $n > m_2$, since $w_i b \in E_1$ implies that $w_{i+1}b \in E_1$, by the definition of W_i and E_1. Recall that $R(2^{n-1}) = F \cdot S^{2^{n-1}}$. Since $w_n b \in R(2^{n-1})$, by Lemma 9.2 and the fact that m_2 is a power of two, we can assume that 2^{n-1} is divisible by m_2 (because we can take larger n if needed by the argument from the first lines of this proof).

Denote $w = w_n b$. We can write $w = w'_1 \dots w'_t$ with each $w'_i \in R(m_2)$. Since $w \in E_1$ it follows that some $w'_j \in E_1 \cap R(m_2)$ (it can be proved using linear mappings similarly as in the proof of Lemma 7.1). Then $w'_j = v_1 \dots v_{m_2/m_1}$ for $v_i \in R(m_1)$. Denote $\alpha = 2^{2^{m_1}}/m_1$; then $v_1 \dots v_\alpha \in E'_1$, where E'_1 is the linear space spanned by all coefficients which are entries of the matrix $X_1^{2^{2^{m_1}}}$, by Theorem 8.1.

Write $v_1 \dots v_\alpha = vv'$, where $v, v' \in R(\alpha/2)$. Recall that $vv' \in P({X_1}^j)$ for $j = 2^{2^{m_1}}$. By Lemma 7.6 we get that for every $n > 8d^3 \cdot (\alpha + 1)$ either v or v' has less than n subwords of length n. Without restraining generality we can assume that it happens for v' (by a subword we mean a product $v_i v_{i+1} \dots v_j$ for some $i \leq j$).

In our case $\alpha = 1$, $d = 1$ because of assumptions on matrix $M = X_1$ (before Theorem 8.1), so we can take $n = 17$. By Lemma 10.2 $v' = cddd \dots d$ for some words c, d such that c has length smaller than $17! + 17!$ and d has length $17!$.

By assumption $2^{2^{m_1}} = 2^k$ for some k. By the definition of words W_i we get that $vv' = w_{k+1}b$ and $vv' = w_k b \bar{w}_k b$. It follows that $v = w_k b$ and $v' = \bar{w}_k b$.

Observe now that $v' = \bar{w}_k b$ implies that $v' = w_{k-1}(b^2 - b)\bar{w}_{k-1}b$.

By Lemma 9.3 we can write $w_{k-1} = ab_{2^{k-2}-1} \cdot b_{2^{k-2}-1}a \dots ab_2 \cdot ab_1 a$ where $b_i \in \{b, b^2 - b\}$. Then $v' = w_{k-1}(b^2 - b)\bar{w}_{k-1}b$ yields

$$v' = (ab_{2^{k-2}-1} \cdot ab_{2^{k-2}-2} \dots ab_2 \cdot ab_1 \cdot a(b^2 - b))(a\bar{b}_1 \cdot a\bar{b}_2 \dots a\bar{b}_{2^{k-2}-1} \cdot ab),$$

where $\bar{b} = b^2 - b$ and $\overline{b^2 - b} = b$. By Lemma 10.2 applied to v' and to $m = 1$ we get that $v' = cddd \dots d$ for some words $c \in R(\alpha \cdot m_1), d \in R(17! \cdot m_1)$, where c has length smaller than $17! + 17!$, so $\alpha < 17! + 17!$.

By the assumptions of our theorem $k > 17! \cdot 10$. We can write

$$v' = w_{k-1}(b^2 - b)\bar{w}_{k-1}b = s \cdot p \cdot q \cdot r \cdot t$$

for some $s, t \in R$ and some $p, r, q \in R(17! \cdot m_1)$ with $spq = w_{k-1}(b^2 - b)$. Notice then that $s \in R(q \cdot m_1)$ for some $q > 17! \cdot 2$. Then because $v' = cddd \dots$ and d has length $17!$ we get $p = q = r$. Recall that $spq = w_{k-1}(b^2 - b)$, and by the above

$$s \cdot p \cdot q = (ab_{2^{k-2}-1} \cdot ab_{2^{k-2}-2} \dots ab_2 \cdot ab_1 \cdot a(b^2 - b)).$$

Consequently, $q = ab_{17! \cdot m_1 - 1}a \dots b_2 ab_1 a(b^2 - b)$, $r = a\bar{b}_1 a\bar{b}_2 a \dots a\bar{b}_{17! \cdot m_1}$, and $p = p' ab_{17! \cdot m_1}$, for some p'. Recall that $p = r$; it follows that $b_{17! \cdot m_1} = \bar{b}_{17! \cdot m_1}$, which is impossible, as $b_{17! \cdot m_1} \in \{b, b^2 - b\}$ and $\bar{b} = b^2 - b$ and $\overline{b^2 - b} = b$. We have obtained a contradiction. □

11. Mapping T

In this section we will use the following notation:

$$w_t = W_t(a, b, -a, b^2 - b), \quad \bar{w}_t = \bar{W}_t(a, b, -a, b^2 - b).$$

Recall that by Lemma 9.2 we have

$$w_k b, w_k(b^2 - b) \in R(2^{k-1}).$$

Recall that, given matrix M with entries in $R[x]$, by $P(M)$ we denote the linear space spanned by coefficients of polynomials which are entries of matrix M. The linear spaces E_i and E'_i are as in Theorem 8.1.

Let R, S satisfy assumption (1). By S-monomial we will mean a product of elements from the set $\{ab, a(b^2 - b)\}$.

Lemma 11.1. *Let F be a field and let R, S satisfy assumption (1). Let n, j be natural numbers. Let $d_1, \dots, d_j$ be S-monomials from $R(m_{n+1})$ such that $v_1, \dots, v_\beta \notin \sum_{k=1}^{n} E_k$. Then there is a linear mapping $T' : R(m_{n+1}) \to R(m_{n+1})$ such that*

$$T'(\sum_{k=1}^{n} E_n \cap R(m_{n+1})) = 0.$$

Moreover there are non-zero S-monomials $d'_1 \dots d'_j \in \{ab, a(b^2 - b)\}$ and non-zero $\alpha_1, \dots, \alpha_j \in F$ and non-zero $d \in R(m_{n+1} - 1)$ such that $T'(v_k) = \alpha_k \cdot dd'_k$ for all

$k \le \beta$. Moreover, there is a linear mapping $f : R(m_{n+1}-1) \to R(m_{n+1}-1)$ such that $T'(uv) = f(u)v$ for all S-monomials u, v with $v \in R(1)$ and $u \in R(m_{n+1}-1)$.

Proof. By the definition of sets E_k, $R(m_{i+1}) \cap \sum_{k=1}^{i} E_k = P' \cdot R(1)$ for some linear space P'. Each v_k can be written as $v_k = c_k e_k$ where c_k, e_k are S-monomials and where $e_k \in R(1)$. It follows that $c_k \notin P'$ for each k. We apply Lemma 8.2 for $L = R(m_{i+1}-1)$ and $T = P'$ to get linear mapping $f : R(m_{i+1}-1) \to R(m_{i+1}-1)$ such that $f(c_k) \neq 0$ for every k, and the image of f has co-dimension 1 in $R(m_{i+1}-1)$. There is $d \neq 0$ such that $d \in Im(f)$, and since f has co-dimension 1, the image of f is $F \cdot d$. Hence $f(c_k)$ is a non-zero multiple of d for every k. Moreover by Lemma 8.2 we have $f(P') = 0$. Therefore mapping $T'(uv) = f(u)v$ defined for S-monomials u, v with $v \in R(1)$, $u \in R(m_{i+1}-1)$, and extended by linearity to all elements of $R(m_{i+1})$ satisfies the thesis of our theorem. □

Definition 11.2. Let $T' : R(m_{n+1}) \to R(m_{n+1})$ be a mapping as in Lemma 11.1. For every j, we can extend the mapping T' to the mapping $T : R(j \cdot m_{n+1}) \to R(j \cdot m_{n+1})$ by defining $T(w_1 \dots w_j) = T'(w_1) \dots T'(w_j)$ for $w_1, \dots, w_j \in R(m_{n+1})$ and then extending it by linearity to all elements from $R(j \cdot m_{n+1})$.

Let M be a matrix with entries $m_{i,j}$. By $T(M)$ we will denote the matrix with corresponding entries equal to $T(m_{i,j})$.

Lemma 11.3. *Let $n \ge 1$ be a natural number. Let $0 < m_1 < m_2 < \dots$ be such that each m_i is a power of two, $2^{2^{m_i}} < m_{i+1}$, and $2^{2^{m_i}}$ divides m_{i+1} for every i. Suppose that $w_j b \notin \sum_{i=1}^{n} E_i$ for every j and $w_t b \in \sum_{i=1}^{n+1} E_i$ for some t. Denote $\beta = 2^{2^{m_{n+1}}}/m_{n+1}$ and $k = 2^{m_{n+1}}$. Then the following hold:*

- *Then $w_{k+1} b = v_1 \dots v_\beta$ for some S-monomials $v_1, \dots, v_\beta \in R(m_{n+1})$.*
- *Moreover, there is a mapping $T' : R(m_{n+1}) \to R(m_{n+1})$ satisfying assumptions of Lemma 11.1 and such that $T'(v_i) \neq 0$ for all $i \le m_{n+2}/m_{n+1}$ and $T'(\sum_{i=1}^{n} E_i \cap R(m_{n+1})) = 0$.*
- *Let $T : R(m_{n+2}) \to R(m_{n+1})$ be defined as in Definition 11.2 using our mapping T', and let*
$$M = T(X_{n+1}^{m_{n+1}}),$$
where X_{n+1} is as in Theorem 8.1. Then $T(w_{k+1} b) \in P(M^\beta)$.

Proof. Observe that we can assume that t is arbitrarily large, since $w_i b \in \sum_{i=1}^{\infty} E_i$ implies $w_{i+1} b \in \sum_{i=1}^{\infty} E_i$ by the definition of words w_i. Therefore we can assume that $t > m_{n+2}$. By the definition of words $w_i b = W_i(a, b, -a, b^2 - b)b$ and by Lemma 9.2 we see that $w_t b = u_1 \dots u_l$ with each $u_i \in R(m_{n+2})$ (since length of $w_t b$ is 2^t we can do it since $2^t \ge m_{n+2}$). Observe that since $w_t b \in \sum_{i=1}^{n+1} E_i$ it follows that for some ξ we have
$$u_\xi \in \sum_{i=1}^{n+1} E_i \cap R_{m_{n+2}}$$
(it can be proved using linear mappings similarly as in the proof of Lemma 7.1). By the definition of words $w_i = W_i(a, b, -a, b^2 - b)$ it follows that $u_\xi \in Z_\gamma$ where
$$Z_\gamma = \{w_\gamma b, w_\gamma(b^2 - b), \bar{w}_\gamma b, \bar{w}_\gamma(b^2 - b)\},$$
where $2^{\gamma - 1} = m_{n+2}$. Similarly,
$$u_\xi = v_1 \dots v_{m_{n+2}/m_{n+1}}$$
for $v_i \in R(m_{n+1})$.

Observe that for each i, $v_i \notin \sum_{i=1}^{n} E_i$, as otherwise $w_t b \in \sum_{i=1}^{n} E_i$, contradicting the inductive assumption. Therefore, by Lemma 11.1 applied to S-monomials v_i, we can choose mapping $T' : R(m_{n+1}) \to R(m_{n+1})$ such that $T'(v_i) \neq 0$ for all $i \leq m_{n+2}/m_{n+1}$ and $T'(\sum_{i=1}^{n} E_i \cap R(m_{n+1})) = 0$. Let T be as in Definition 11.2. Observe that $T(\sum_{i=1}^{n} E_i \cap R(m_{n+2})) = 0$ since $T'(\sum_{i=1}^{n} E_i \cap R(m_{n+1})) = 0$ (by Lemma 11.1). It follows that

$$T(u_\xi) = T(v_1 v_2 \dots v_{m_{n+2}/m_{n+1}}) \in T(E_{n+1}).$$

Notice that by the definition of the mapping T we get

$$T(v_1)T(v_2)\dots T(v_{m_{n+2}/m_{n+1}}) = T(v_1 v_2 \dots v_{m_{n+2}/m_{n+1}}) \in T(E_{n+1}).$$

By the definition of E_{n+1} it follows that

$$T(v_1 \dots v_\beta) \in T(E'_{n+1}),$$

where $\beta = 2^{2^{m_{n+1}}}/m_{n+1}$. Notice that $T(E'_{n+1})$ is the linear space spanned by coefficients of matrix $T({X_{n+1}}^{m_{n+1}\cdot\beta})$. Observe that $T(X_{n+1}^{m_{n+1}\cdot\beta}) = T(X_{n+1}^{m_{n+1}})^{\beta}$.

Therefore

$$T(v_1)\dots T(v_\beta) = T(v_1 \dots v_\beta) \in P(M^\beta),$$

where $M = T(X_{n+1}^{m_{n+1}})$.

Recall that $(v_1 \dots v_\beta) \cdot (v_{\beta+1} \dots v_{m_{n+1}/m_n}) = u_\xi \in \{w_\gamma b, w_\gamma(b^2 - b), \bar{w}_\gamma b, \bar{w}_\gamma(b^2 - b)\}$; hence by the definition of words w_i we get $v_1 \dots v_\beta = w_k b$ (since $\beta < m_{n+1}/m_n$). Therefore $w_{k+1} b = v_1 \dots v_\beta$, and hence $T(w_{k+1}b) = T(v_1 \dots v_\beta) \in P(M^\beta)$. □

Theorem 11.4. *Let $0 < m_1 < m_2 < \dots$ be such that each m_i is a power of two, $2^{2^{m_i}} < m_{i+1}$, and $2^{2^{m_i}}$ divides m_{i+1} for every i. Assume that $2^{m_1} > 17! \cdot 10$. Let R, I satisfy assumptions of Theorem 8.1 for these m_i. Let $R(i), S$ be as in Theorem 8.1. Let n be a natural number. Then $w_t b \notin \sum_{i=1}^{n} E_i$ for any t.*

Proof. We proceed by induction on n. For $n = 1$ the result holds by Theorem 10.3. Suppose now that $w_j b \notin \sum_{i=1}^{n} E_i$ for any j. We need to show that $w_j b \notin \sum_{i=1}^{n+1} E_i$ for all j. Suppose on the contrary that $w_t b \in \sum_{i=1}^{n+1} E_i$ for some t. Then by the definition of words w_i, $w_{t+j} b \in \sum_{i=1}^{n+1} E_i$ for every $j \geq 0$.

Let notation be as in Theorem 11.4. Then $w_k b = v_1 \dots v_\beta$ for some $v_1, \dots, v_\beta \in R(m_{n+1})$; moreover each v_i is an S-monomial. By Lemma 11.4 we know that $T(w_{k+1} b) \in P(M^\beta)$.

Let $c'_1, c'_2, \dots, c'_j \in \{v_1, \dots, v_\beta\}$ be distinct S-monomials such that elements $T'(c'_1), T'(c'_2), \dots, T'(c'_j)$ form a basis of the linear space $F \cdot T'(v_1) + \dots + F \cdot T'(v_\beta)$. By Lemma 11.3, for every k we can write $T(v_k) = T(c'_{i_k})\alpha_k$ for some i_k and some $0 \neq \alpha_k \in F$; moreover, as in Lemma 11.3, we denote $\beta = 2^{2^{m_{n+1}}}/m_{n+1}$ and $k = 2^{m_{n+1}}$. Denote $T(c'_i) = c_i$, for every i. Notice that $T(w_{k+1} b) = w' \cdot \alpha$ where $w' = c_{i_1} \dots c_{i_\beta}$ and $\alpha = \alpha_1 \dots \alpha_\beta$. It follows that $c_{i_1} \dots c_{i_\beta} \in P(M^\beta)$.

Denote

$$v = T'(v_1) \dots T'(v_{\beta/2}), v' = T'(v_{\beta/2+1}) \dots T'(v_\beta)$$

and

$$u = T'(c'_{i_1}) \dots T'(c'_{i_{\beta/2}}), u' = T'(c'_{i_{\beta/2+1}}) \dots T'(c'_{i_\beta});$$

then $w' = c_{i_1} \dots c_{i_\beta} = uu'$ and $u, u' \in R(2^{2^{m_{n+1}}}/2) = R(m_{n+1})^{\beta/2}$. Moreover there are $0 \neq \beta', \beta'' \in F$ such that $v = \beta'' \cdot u$ and $v' = \beta' \cdot u'$.

Notice that $u = c_{i_1} \dots c_{i_{\beta/2}}$ and $u' = c_{i_{\beta/2+1}} c_{i_\beta}$. By Lemma 7.6 we get that for $n' \geq 8d^3 \cdot (\alpha + 1)$ either u or u' has less than n' subwords of length n'; without restraining generality we can assume that it happens for u'. In our case $\alpha = (n+1) \cdot m_{n+1}$, $d = n+1$ because of assumptions on matrix $M = T(X_{n+1}^{m_{n+1}})$ (before Lemma 7.6), so we can take $n' = 8(n+2)^4 m_{n+1}$, so v' has less than n' subwords of degree n'. By Lemma 10.2 we get that

$$u' = cddd \dots d$$

for some words c, d such that c has length smaller than $n'! + n'!$ and d has length $n'!$, so $d \in R(n'! \cdot m_{n+1})$ and $c \in R(l \cdot m_{n+1})$ for some $l < n'! + n'!$.

It follows that

$$v' = \beta' \cdot cddd \dots d.$$

We know that $(v_1 \dots v_{\beta/2}) \cdot (v_{\beta/2+1} \dots v_\beta) = w_{k+1} b = (w_k b) \cdot (\bar{w}_k b)$; therefore $v' = T(\bar{w}_k b)$. Observe now that $v' = T(\bar{w}_k b)$ implies that

$$v' = T(w_{k-1}(b^2 - b)\bar{w}_{k-1} b).$$

By Lemma 9.3 we can write $w_{k-1} = ab_{2^{k-2}-1} \cdot b_{2^{k-2}-2} a \dots ab_2 \cdot ab_1 a$ where $b_i \in \{b, b^2 - b\}$. Then $v' = T(w_{k-1}(b^2 - b)\bar{w}_{k-1} b)$ gives

$$v' = T(ab_{2^{k-2}-1} \cdot ab_{2^{k-2}-2} \dots ab_2 \cdot ab_1 \cdot a(b^2 - b))(a\bar{b}_1 \cdot a\bar{b}_2 \dots a\bar{b}_{2^{k-2}-1} \cdot ab),$$

where $\bar{b} = b^2 - b$ and $\bar{b}^2 - b = b$.

Recall that $v' = \beta' \cdot cddd \dots d$ for some words c, d such that c has length smaller than $n'! + n'!$ and d has length $n'!$ where $n' = 8(n+2)^4 m_{n+1}$. By the assumptions $v' \in R(2^{2^{m_{n+1}}}/2) = R(m_{n+1})^{\beta/2}$. Observe that $\beta/2 > n'! \cdot 10 \cdot m_{n+1}$. Therefore we can write

$$\bar{w}_{k-1}(b^2 - b) w_{k-1} b = s \cdot p \cdot q \cdot r \cdot t$$

for some $s, t \in R$ and some $p, q, r \in R(n'! \cdot m_{n+1})$ with $s \cdot p \cdot q = w_{k-1}(b^2 - b)$.

Notice then that $s \in R(q \cdot m_{n+1})$ for some $q > n'! \cdot 2$. Then

$$v' = T(w_{k-1}(b^2 - b)\bar{w}_{k-1} b) = T(s \cdot p \cdot q \cdot r \cdot t).$$

Notice that $spq = w_{k-1}(b^2 - b)$ implies that $spq \in R(\gamma)$ for some γ divisible by m_{n+1}, as m_{n+1} is a power of two and $w_{k-1}(b^2 - b) \in R(2^{2^{m_{n+1}}}/4)$. By the definition of T, $v' = T(spq)T(qr)$. Because $p, q, r \in R(n! \cdot m_{n+1})$ we get

$$v' = T(s)T(p)T(q)T(r)T(t).$$

Then because $v' = cddd \dots \cdot \beta'$ and d has length $n'!$ we get $\gamma \cdot T(p) = \gamma' \cdot T(q) = \gamma'' \cdot T(r) = m$ for some $0 \neq \gamma, \gamma', \gamma'' \in F$ and some m (where m is a product of some elements $c_{i_1}, \dots, c_{i_\beta}$). Denote $\xi = n'! \cdot m_{j+1}$. Then $q = ab_{\xi-1} a \dots b_2 ab_1 a(b^2 - b)$, $r = a\bar{b}_1 a\bar{b}_2 a \dots a\bar{b}_\xi$, and $p = p' ab_\xi$, for some p' (for some $b_i \in \{b, b^2 - b\}$ where $\bar{b} = b^2 - b$ and $b^2 - b = b$). Recall that $\gamma \cdot T(p) = \gamma'' \cdot T(r)$. Recall also that by Lemma 11.1 we have $T(p) = s \cdot ab_\xi$ and $T(r) = s' \cdot a\bar{b}_\xi$ for some s, s'; it follows that $\bar{b}_\xi = b_\xi$, which is impossible, as $b_\xi \in \{b, b^2 - b\}$ and $\bar{b} = b^2 - b$ and $\bar{b}^2 - b = b$. We have obtained a contradiction. $\square$

Theorem 11.5. *There is a nil ring R such that the adjoint group of R^o is not an Engel group. Moreover R can be taken to be an algebra over an arbitrary countable field.*

Proof. Suppose first that F is an infinite field. Let $0 < m_1 < m_2 < \dots$ be such that each m_i is a power of two, $2^{2^{m_i}} < m_{i+1}$ and $2^{2^{m_i}}$ divides m_{i+1} for every i. Assume moreover that $2^{m_1} > 17! \cdot 10$. Let R, I satisfy assumptions of Theorem 8.1 for these m_i. By Theorem 11.4 we have $w_n b \notin \sum_{i=1}^{j} E_i$ for any n, j, where $w_n = W_n(a, b, -a, b^2 - b)$. By Theorem 8.1 we see that $I \subseteq \sum_{i=1}^{\infty} E_i + bE_i + b^2E_i + \langle a^2\rangle + \langle b^3\rangle$. Suppose that $w_n b \in I$ for some n. Then there is $w \in \sum_{i=1}^{\infty} E_i$ such that $w_n b - w \in bR + \langle a^2\rangle + \langle b^3\rangle$. We can assume that $w \in \sum_{i=1}^{\infty} R(i) + R(i)a$ where $R(i) = S^i$ and $S = F\cdot ab + F\cdot ab^2$. Observe that $(bR + \langle a^2\rangle + \langle b^3\rangle) \cap (\sum_{i=1}^{\infty} R(i) + R(i)a) = 0$ and so $w_n b - w = 0$, so $w_n b \in \sum_{i=1}^{\infty} E_i$, a contradiction. It follows that $w_n b \notin I$ for every n.

By Lemma 9.9 we have $v_n - 1 \notin I'$ for every n, and hence $(R/I)^{\circ}$ is not an Engel group (I' is as in Lemma 9.9). By Theorem 8.1, R/I is nil. Therefore R/I is a nil algebra over field F such that the adjoint group R/I^o of this algebra is not an Engel group.

If F is a finite field, then we proceed in the following way: Let $\bar{F}$ be the algebraic closure of F; then $\bar{F}$ is infinite. Hence there is a nil algebra A over $\bar{F}$ such that the adjoint group A^o is not nil. Let $x, y \in A$ be such that $[x[\dots[x[x, y]]]] \neq 1$ (n copies of x) for every n. Let A' be the smallest subring of A containing x, y and such that if $r \in A'$, then $f \cdot r \in A'$ for every $f \in F$. Then A' is an F-algebra which is generated as an F-algebra by x, y and which is nil. Since $x, y \in A'$ then the adjoint group A'^o is not an Engel group. □

Proof of Corollary 2.4. Let $(R, +, \cdot)$ be a ring such that R is nil and R^o is not an Engel group. Assume moreover that R is an algebra over a finite field of cardinality p for some prime number p. Let $(R, +, o)$ be the associated brace, so $a \circ b = a\cdot b + a + b$ for all $a, b \in R$, and the addition is the same as in the ring R. It follows that $(R, +, o)$ satisfies the thesis of Corollary 2.4. □

12. Zelmanov's question

Observe that in the case of algebras over uncountable fields we have the following result analogous to Lemma 6.1.

Lemma 12.1. *Let F be an uncountable field and let F' be a countable subfield of F. Let R be an F-algebra generated by elements a, b, and suppose that $a^2 = 0$ and $b^3 = 0$. Let $R[x_1, x_2, \dots]$ be the polynomial ring over R in infinitely many commuting variables $x_1, x_2, \dots$. Let $F'[x_1, x_2, \dots]$ be the polynomial ring over F' in infinitely many commuting variables $x_1, x_2, \dots$.*

Let S' be the F'-linear space spanned by elements abx_i and ab^2x_i for $0 \leq i$.

If all finite matrices with entries from S' are nilpotent, then R is a Jacobson radical ring.

Proof. Observe that if all finite matrices with entries from S are nilpotent, then after substituting arbitrary elements $\alpha_1, \alpha_2, \dots \in F$ for variables $x_1, x_2, \dots$ we get that all matrices with entries from F'-linear space spanned by elements $ab^i\alpha_j$ are nilpotent.

Therefore every matrix with entries in the F-linear space spanned by elements ab and ab^2 is nilpotent. By Lemma 6.1, R is a Jacobson radical F-algebra. □

We recall Amitsur's theorem.

Theorem 12.2. *Let R be a finitely generated algebra over an uncountable field. If R is a Jacobson radical algebra, then R is nil.*

We will now use Lemma 12.1 to give an analogue of Theorem 8.1.

Let F be a field and let F' be a countable subfield of F. Let R be as in Lemma 12.1 and let S be the F'-linear space spanned by elements ab and ab^2. Let $X = \{x_1, x_2, \ldots\}$ and let $F'[X]$ denote the polynomial ring over F' in infinitely many variables $x_1, x_2, \ldots$.

We can enumerate all finite matrices with entries from $S \cdot F'[X]$ as $X_1, X_2, \ldots$. We can assume that the matrix X_i is a d_i-by-d_i matrix where $d_i \leq i$ and X_i has entries in $S \cdot y_1 + S \cdot y_2 + \ldots + S \cdot y_i$ for some $y_1, y_2, \ldots, y_i \in F'[X]$ (if necessary taking $X_i = 0$ for some i). The following theorem has the same proof as Theorem 8.1.

Theorem 12.3. *Let F be an uncountable field, and let R, S and the matrices $X_1, X_2, \ldots$ be as above. Let $0 < m_1 < m_2 < \ldots$ be a sequence of natural numbers such that $2^{2^{m_i}}$ divides m_{i+1} for every $i \geq 1$. Denote $R(m) = F \cdot S^m$ for every m. Let E'_i be the linear space spanned by all coefficients of polynomials which are entries of the matrix $X_i^{2^{2^{m_i}}}$ and let*

$$E_i = \sum_{j=0}^{\infty} R(j \cdot m_{i+1}) E'_i S R.$$

Then there is an ideal I in R contained in $\sum_{i=1}^{\infty} E_i + bE_i + b^2E_i + \langle a^2 \rangle + \langle b^3 \rangle$ and such that R/I is a nil ring, where $\langle a^2 \rangle, \langle b^3 \rangle$ denote ideals in R generated by elements a^2 and b^3.

Proof. Observe first that the ideal I_k of R generated by coefficients of polynomials which are entries of the matrices $X_k^{2m_{k+1}}$ is contained in the subspace $E_k + bE_k + b^2E_k$. It follows because entries of every matrix X_k have degree one in the subring generated by S with elements of S of degree one. In general, if $n > m_{k+1} + 2^{2^{m_k}} + 1$, then every entry of matrix X_k^n belongs to $R(i)E'_kR(1)R$ for every $0 \leq i < n - m_{k+1} - 1$.

Define $I = \sum_{i=1}^{\infty} I_k + \langle a^2 \rangle + \langle b^3 \rangle$. Then $I \subseteq \sum_{i=1}^{\infty} E_i + bE_i + b^2E_i + \langle a^2 \rangle + \langle b^3 \rangle$. Observe also that, by Lemma 12.1 and Theorem 12.2, R/I is a nil ring. □

We will say that $M, R, F', S, r_1, r_2, m, d, \alpha$ satisfy assumption (3) if

1. R, F' are as in Lemma 12.1 and S is the F'-linear space spanned by elements ab and ab^2, and m, d, α are natural numbers.
2. M is a d-by-d matrix with entries from $S^m \cdot F[X]$. Moreover,

$$M \subseteq R + R \cdot y_1 + R \cdot y_2 + \ldots + R \cdot y_\alpha,$$

for some $y_1, y_2, \ldots, y_\alpha \in F[X]$, where $X = \{x_1, x_2, \ldots\}$ is an infinite set.

We now propose a generalisation of Lemma 7.6.

Lemma 12.4. *Let F be an infinite field. Let M, R, S, m, d, α satisfy assumption (3). Let q be a natural number. Let $c_1, \ldots, c_k$ be linearly independent elements* *from* $F \cdot S^m$, *and let* $r_1, r_2, \ldots, r_{\alpha+1}$ *be products of* q *elements from the set* $C = \{c_1, \ldots, c_k\}$. *If* $n > d^{\alpha+2} \cdot (\alpha+1)^{\alpha+1}$ *and for each* i, r_i *has more than* n *subwords of length* n, *then* $r_1 \cdot r_2 \ldots r_{\alpha+1} \notin P(M^j)$, *for any* j.

We say that w *is a subword of degree* n *in* r *if* w *is a product of* n *elements from* C, *and* $r = vwv'$ *for some* v, v' *which are also products of elements from* C.

Proof. Denote $r = r_1 \ldots r_{\alpha+1}$. Suppose on the contrary that $r \in P(M^j)$. Let $p_{1,i}, \ldots, p_{n,i}$ be subwords of degree n in r_i for all $i \leq \alpha+1$. Fix numbers $\beta(1), \ldots, \beta(\alpha+1) \leq \alpha+1$. Then there are $q_1, \ldots, q_\alpha$ such that

$$s = (\prod_{i=1}^{\alpha} p_{\beta(i),i} q_i) p_{\beta(\alpha+1),\alpha+1}$$

is a subword of r.

By Lemma 7.1, $r \in P(M^j)$ implies that $s \in P(M^{j'})$, for some j'.

Let $f : F \cdot S^m \to F$ be a linear map such that $f(c_i) \neq 0$, and let $f : F \cdot S^{m \cdot n'} \to F$ be as in Definition 7.2. Then $f(c_{i_1} c_{i_2} \ldots c_{i_{n'}}) = f(c_1) \ldots f(c_{n'}) \neq 0$ for every choice of $i_1, i_2, \ldots, i_{n'} \leq k$. By Lemma 7.3 applied several times we get that

$$(\prod_{i=1}^{\alpha} p_{\beta(i),i} f(q_i)) p_{\beta(\alpha+1),\alpha+1} \in P(\prod_{i=1}^{\alpha} M^n f(M^{\deg q_i}) M^n).$$

By an analogous argument to Lemma 7.5,

$$p_{\beta(1),1} p_{\beta(2),2} \cdots p_{\beta(\alpha+1),\alpha+1} \in P((\prod_{i=1}^{\alpha} M^n Q_i) M^n),$$

where $Q_i = \sum_{i=1}^{d+1} F \cdot f(M^i)$.

Notice that the linear space $P((\prod_{i=1}^{\alpha} M^n Q_i) M^n)$ has dimension at most $d^\alpha \cdot d^2 \cdot ((\alpha+1) \cdot n)^{\alpha+1}$.

Observe that since each $p_{i,j}$ is a product of n elements from the set C, then elements

$$p_{\beta(1),1} p_{\beta(2),2} \cdots p_{\beta(\alpha+1),\alpha+1}$$

span linear space over field F of dimension at least $n^{\alpha+1}$. Hence $d^\alpha \cdot d^2 \cdot ((\alpha+1) \cdot n)^\alpha < n^{\alpha+1}$, a contradiction with the assumptions on n. ☐

Proof of Theorem 1.5. We first obtain an analogue of Theorem 11.4 by using assumption (3) instead of assumption (2), and by using Theorem 8.1 instead of Theorem 12.3, and by using Lemma 12.4 instead of Lemma 7.6. Moreover, we need to use a stronger assumption that $2^{2^{2^{2^{m_i}}}}$ divides m_{i+1} (instead of the assumption that $2^{2^m_i}$ divides m_{i+1}). Once we have obtained an analogue of Theorem 11.4, we can prove Theorem 1.5 using the same proof as the proof of Theorem 11.5, where instead of Lemma 7.6 we use Lemma 12.4. ☐

Acknowledgments

I would like to thank Efim Zelmanov and Gunnar Traustason for their helpful comments on Engel groups and Tatyana Gateva-Ivanova for introducing me to research into braided groups, braces, and solutions to the Yang-Baxter equation. I am also grateful to Jan Krempa and Jan Okniński for their helpful suggestions. I am very grateful to Ferran Cedó and to the anonymous referee for reading the manuscript and for their very useful comments.

References

[1] Alireza Abdollahi, *Engel elements in groups*, Groups St Andrews 2009 in Bath. Volume 1, London Math. Soc. Lecture Note Ser., vol. 387, Cambridge Univ. Press, Cambridge, 2011, pp. 94–117. MR2858851

[2] Adel Alahmadi, Hamed Alsulami, S. K. Jain, and Efim Zelmanov, *Finite generation of Lie algebras associated with associative algebras*, J. Algebra **426** (2015), 69–78, DOI 10.1016/j.jalgebra.2014.10.056. MR3301901

[3] B. Amberg, O. Dickenschied, and Ya. P. Sysak, *Subgroups of the adjoint group of a radical ring*, Canad. J. Math. **50** (1998), no. 1, 3–15, DOI 10.4153/CJM-1998-001-9. MR1618706

[4] Bernhard Amberg and Lev Kazarin, *Nilpotent p-algebras and factorized p-groups*, Groups St. Andrews 2005. Vol. 1, London Math. Soc. Lecture Note Ser., vol. 339, Cambridge Univ. Press, Cambridge, 2007, pp. 130–147, DOI 10.1017/CBO9780511721212.005. MR2327319

[5] Bernhard Amberg and Yaroslav Sysak, *Radical rings and products of groups*, Groups St. Andrews 1997 in Bath, I, London Math. Soc. Lecture Note Ser., vol. 260, Cambridge Univ. Press, Cambridge, 1999, pp. 1–19. MR1676607

[6] Bernhard Amberg and Yaroslav P. Sysak, *Radical rings with soluble adjoint groups*, J. Algebra **247** (2002), no. 2, 692–702, DOI 10.1006/jabr.2001.8996. MR1877869

[7] Bernhard Amberg and Yaroslav P. Sysak, *Radical rings with Engel conditions*, J. Algebra **231** (2000), no. 1, 364–373. MR1779604

[8] J. C. Ault and J. F. Watters, *Circle groups of nilpotent rings*, Amer. Math. Monthly **80** (1973), 48–52, DOI 10.2307/2319260. MR0316493

[9] David Bachiller, *Counterexample to a conjecture about braces*, J. Algebra **453** (2016), 160–176, DOI 10.1016/j.jalgebra.2016.01.011. MR3465351

[10] David Bachiller, *Extensions, matched products, and simple braces*, arXiv:1511.08477v3 [math.GR], 13 June 2016.

[11] David Bachiller and Ferran Cedó, *A family of solutions of the Yang-Baxter equation*, J. Algebra **412** (2014), 218–229, DOI 10.1016/j.jalgebra.2014.05.011. MR3215955

[12] David Bachiller, Ferran Cedó, and Eric Jespers, *Solutions of the Yang-Baxter equation associated with a left brace*, J. Algebra **463** (2016), 80–102, DOI 10.1016/j.jalgebra.2016.05.024. MR3527540

[13] D. Bachiller, F. Cedó, E. Jespers, J. Okniński, *Iterated matched products of finite braces and simplicity; new solutions of the Yang-Baxter equation*, arXiv:1610.00477v1 [math.GR], 3 October 2016.

[14] F. Catino, M. M. Miccoli, and Ya. P. Sysak, *On the adjoint group of semiprime rings*, Comm. Algebra **35** (2007), no. 1, 265–270, DOI 10.1080/00927870601042084. MR2287569

[15] Francesco Catino and Roberto Rizzo, *Regular subgroups of the affine group and radical circle algebras*, Bull. Aust. Math. Soc. **79** (2009), no. 1, 103–107, DOI 10.1017/S0004972708001068. MR2486886

[16] Ferran Cedó, *Braces and the Yang-Baxter equation* (joint work with Eric Jespers and Jan Okniński), slides from the talk in Stuttgart, June 2012.

[17] Ferran Cedó, Tatiana Gateva-Ivanova, and Agata Smoktunowicz, *On the Yang-Baxter equation and left nilpotent left braces*, J. Pure Appl. Algebra **221** (2017), no. 4, 751–756, DOI 10.1016/j.jpaa.2016.07.014. MR3574204

[18] Ferran Cedó, Eric Jespers, and Jan Okniński, *Braces and the Yang-Baxter equation*, Comm. Math. Phys. **327** (2014), no. 1, 101–116, DOI 10.1007/s00220-014-1935-y. MR3177933

[19] Ferran Cedó, Eric Jespers, and Jan Okniński, *Retractability of set theoretic solutions of the Yang-Baxter equation*, Adv. Math. **224** (2010), no. 6, 2472–2484, DOI 10.1016/j.aim.2010.02.001. MR2652212

[20] Ferran Cedó, Eric Jespers, and Jan Okniński, *Nilpotent groups of class three and braces*, Publ. Mat. **60** (2016), no. 1, 55–79. MR3447734

[21] Ferran Cedó, Eric Jespers, and Ángel del Río, *Involutive Yang-Baxter groups*, Trans. Amer. Math. Soc. **362** (2010), no. 5, 2541–2558, DOI 10.1090/S0002-9947-09-04927-7. MR2584610

[22] Pavel Etingof, Travis Schedler, and Alexandre Soloviev, *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Math. J. **100** (1999), no. 2, 169–209, DOI 10.1215/S0012-7094-99-10007-X. MR1722951

[23] Tatiana Gateva-Ivanova, *Set-theoretic solutions of the Yang-Baxter equation, Braces, and Symmetric groups*, arXiv:1507.02602v2 [math.QA], 31 August 2015.

[24] Tatiana Gateva-Ivanova, *A combinatorial approach to the set-theoretic solutions of the Yang-Baxter equation*, J. Math. Phys. **45** (2004), no. 10, 3828–3858, DOI 10.1063/1.1788848. MR2095675

[25] Tatiana Gateva-Ivanova and Shahn Majid, *Matched pairs approach to set theoretic solutions of the Yang-Baxter equation*, J. Algebra **319** (2008), no. 4, 1462–1529, DOI 10.1016/j.jalgebra.2007.10.035. MR2383056

[26] Tatiana Gateva-Ivanova and Shahn Majid, *Quantum spaces associated to multipermutation solutions of level two*, Algebr. Represent. Theory **14** (2011), no. 2, 341–376, DOI 10.1007/s10468-009-9192-z. MR2776789

[27] Tatiana Gateva-Ivanova and Peter Cameron, *Multipermutation solutions of the Yang-Baxter equation*, Comm. Math. Phys. **309** (2012), no. 3, 583–621, DOI 10.1007/s00220-011-1394-7. MR2885602

[28] Tatiana Gateva-Ivanova and Michel Van den Bergh, *Semigroups of I-type*, J. Algebra **206** (1998), no. 1, 97–112, DOI 10.1006/jabr.1997.7399. MR1637256

[29] L. Guarnieri and L. Vendramin, *Skew braces and the Yang-Baxter equation*, Math. Comp. **86** (2017), no. 307, 2519–2534, DOI 10.1090/mcom/3161. MR3647970

[30] A. W. Hales and I. B. S. Passi, *The second augmentation quotient of an integral group ring*, Arch. Math. (Basel) **31** (1978/79), no. 3, 259–265, DOI 10.1007/BF01226446. MR521479

[31] Natalia Iyudu and Stanislav Shkarin, *Finite dimensional semigroup quadratic algebras with the minimal number of relations*, Monatsh. Math. **168** (2012), no. 2, 239–252, DOI 10.1007/s00605-011-0339-8. MR2984149

[32] Eric Jespers and Jan Okniński, *Monoids and groups of I-type*, Algebr. Represent. Theory **8** (2005), no. 5, 709–729, DOI 10.1007/s10468-005-0342-7. MR2189580

[33] Eric Jespers and Jan Okniński, *Noetherian semigroup algebras*, Algebra and Applications, vol. 7, Springer, Dordrecht, 2007. MR2301033

[34] T. Y. Lam, *A first course in noncommutative rings*, Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York, 1991. MR1125071

[35] Jiang-Hua Lu, Min Yan, and Yong-Chang Zhu, *On the set-theoretical Yang-Baxter equation*, Duke Math. J. **104** (2000), no. 1, 1–18, DOI 10.1215/S0012-7094-00-10411-5. MR1769723

[36] M. Lothaire, *Algebraic combinatorics on words*, Encyclopedia of Mathematics and its Applications, vol. 90, Cambridge University Press, Cambridge, 2002. A collective work by Jean Berstel, Dominique Perrin, Patrice Seebold, Julien Cassaigne, Aldo De Luca, Steffano Varricchio, Alain Lascoux, Bernard Leclerc, Jean-Yves Thibon, Veronique Bruyere, Christiane Frougny, Filippo Mignosi, Antonio Restivo, Christophe Reutenauer, Dominique Foata, Guo-Niu Han, Jacques Desarmenien, Volker Diekert, Tero Harju, Juhani Karhumaki and Wojciech Plandowski; With a preface by Berstel and Perrin. MR1905123

[37] Victor M. Petrogradsky, Ivan P. Shestakov, and Efim Zelmanov, *Nil graded self-similar algebras*, Groups Geom. Dyn. **4** (2010), no. 4, 873–900, DOI 10.4171/GGD/112. MR2727670

[38] B. I. Plotkin, *Notes on Engel groups and Engel elements in groups. Some generalizations* (English, with English and Russian summaries), Izv. Ural. Gos. Univ. Mat. Mekh. **7(36)** (2005), 153–166, 192–193. MR2190949

[39] Derek J. S. Robinson, *A course in the theory of groups*, 2nd ed., Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996. MR1357169

[40] Derek J. S. Robinson, Finiteness Conditions and Generalized Soluble Groups. Springer-Verlag, Berlin-Heidelberg-New York, 1972. MR0332989, MR0332990

[41] Louis Halle Rowen, *Graduate algebra: noncommutative view*, Graduate Studies in Mathematics, vol. 91, American Mathematical Society, Providence, RI, 2008. MR2462400

[42] Wolfgang Rump, *Modules over braces*, Algebra Discrete Math. **2** (2006), 127–137. MR2320986

[43] Wolfgang Rump, *The brace of a classical group*, Note Mat. **34** (2014), no. 1, 115–144. MR3291816

[44] Wolfgang Rump, *Braces, radical rings, and the quantum Yang-Baxter equation*, J. Algebra **307** (2007), no. 1, 153–170, DOI 10.1016/j.jalgebra.2006.03.040. MR2278047

[45] Wolfgang Rump, *A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation*, Adv. Math. **193** (2005), no. 1, 40–55. MR2132760

[46] Aner Shalev, *On associative algebras satisfying the Engel condition*, Israel J. Math. **67** (1989), no. 3, 287–290, DOI 10.1007/BF02764947. MR1029903

[47] Layla Sorkatti and Gunnar Traustason, *Nilpotent symplectic alternating algebras I*, J. Algebra **423** (2015), 615–635, DOI 10.1016/j.jalgebra.2014.10.031. MR3283734

[48] I. P. Shestakov and E. Zelmanov, *Some examples of nil Lie algebras*, J. Eur. Math. Soc. (JEMS) **10** (2008), no. 2, 391–398, DOI 10.4171/JEMS/114. MR2390328

[49] Agata Smoktunowicz, *How far can we go with Amitsur's theorem in differential polynomial rings?*, Israel J. Math. **219** (2017), no. 2, 555–608, DOI 10.1007/s11856-017-1491-1. MR3649600

[50] Agata Smoktunowicz, *The Jacobson radical of rings with nilpotent homogeneous elements*, Bull. Lond. Math. Soc. **40** (2008), no. 6, 917–928, DOI 10.1112/blms/bdn086. MR2471940

[51] Ya. P. Sysak, *The adjoint group of radical rings and related questions*, Ischia group theory 2010, World Sci. Publ., Hackensack, NJ, 2012, pp. 344–365, DOI 10.1142/9789814350051_0027. MR3185324

[52] Yaroslav P. Sysak, *Products of groups and local nearrings*, Note Mat. **28** (2008), no. suppl. 2, 181–216 (2009). MR2799412

[53] Antonio Tortora, Maria Tota, and Gunnar Traustason, *Symplectic alternating nil-algebras*, J. Algebra **357** (2012), 183–202, DOI 10.1016/j.jalgebra.2012.02.012. MR2905248

[54] Gunnar Traustason, *Engel groups*, Groups St Andrews 2009 in Bath. Volume 2, London Math. Soc. Lecture Note Ser., vol. 388, Cambridge Univ. Press, Cambridge, 2011, pp. 520–550. MR2866724

[55] L. Vendramin, *Extensions of set-theoretic solutions of the Yang-Baxter equation and a conjecture of Gateva-Ivanova*, J. Pure Appl. Algebra **220** (2016), no. 5, 2064–2076, DOI 10.1016/j.jpaa.2015.10.018. MR3437282

[56] I. Wisliceny, *Konstruktion nilpotenter assoziativer Algebren mit wenig Relationen* (German), Math. Nachr. **147** (1990), 75–82, DOI 10.1002/mana.19901470109. MR1127311

[57] E. I. Zel′manov, *Some problems in the theory of groups and Lie algebras* (Russian), Mat. Sb. **180** (1989), no. 2, 159–167; English transl., Math. USSR-Sb. **66** (1990), no. 1, 159–168. MR993451

[58] E. I. Zel′manov, *Solution of the restricted Burnside problem for groups of odd exponent* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **54** (1990), no. 1, 42–59, 221; English transl., Math. USSR-Izv. **36** (1991), no. 1, 41–60. MR1044047

[59] E. I. Zel′manov, *Solution of the restricted Burnside problem for* 2*-groups* (Russian), Mat. Sb. **182** (1991), no. 4, 568–592; English transl., Math. USSR-Sb. **72** (1992), no. 2, 543–565. MR1119009

School of Mathematics, The University of Edinburgh, James Clerk Maxwell Building, The King's Buildings, Peter Guthrie Tait Road, Edinburgh EH9 3FD, United Kingdom

Email address: A.Smoktunowicz@ed.ac.uk