

## A commutator description of the solvable radical of a finite group

Nikolai Gordeev, Fritz Grunewald, Boris Kunyavskii and Eugene Plotkin

**Abstract.** We are looking for the smallest integer  $k > 1$  providing the following characterization of the solvable radical  $R(G)$  of any finite group  $G$ :  $R(G)$  coincides with the collection of all  $g \in G$  such that for any  $k$  elements  $a_1, a_2, \dots, a_k \in G$  the subgroup generated by the elements  $g, a_i g a_i^{-1}, i = 1, \dots, k$ , is solvable. We consider a similar problem of finding the smallest integer  $\ell > 1$  with the property that  $R(G)$  coincides with the collection of all  $g \in G$  such that for any  $\ell$  elements  $b_1, b_2, \dots, b_\ell \in G$  the subgroup generated by the commutators  $[g, b_i], i = 1, \dots, \ell$ , is solvable. Conjecturally,  $k = \ell = 3$ . We prove that both  $k$  and  $\ell$  are at most 7. In particular, this means that a finite group  $G$  is solvable if and only if every 8 conjugate elements of  $G$  generate a solvable subgroup.

**Mathematics Subject Classification (2000).** 20F16, 20D05, 20D06, 20D08, 20D25, 20G40.

**Keywords.** Finite group, solvable radical, simple group.

### 1. Introduction

**1.1. Main results.** Let  $F_2 = F(x, y)$  be the free two generator group. Define a sequence  $\vec{e} = e_1, e_2, e_3, \dots$ , where  $e_i(x, y) \in F_2$ , by

$$e_1(x, y) = [x, y] = xyx^{-1}y^{-1}, \dots, e_n(x, y) = [e_{n-1}(x, y), y], \dots$$

An element  $g$  of a group  $G$  is called an Engel element if for every  $a \in G$  there exists a number  $n = n(a, g)$  such that  $e_n(a, g) = 1$ .

In 1957 R. Baer proved the following theorem [Ba], [H]:

**Theorem 1.1.** *The nilpotent radical of a noetherian group  $G$  coincides with the collection of all Engel elements of  $G$ .*

In particular, Baer's theorem is true for finite groups. Similar theorems have been established for many classes of infinite groups satisfying some additional conditions (see for example [Plo], [Pla]).

A tempting but difficult problem is to find a counterpart of Baer's theorem for the solvable radical of a finite group, in other words, to find an Engel-like sequence  $\bar{u} = u_n(x, y)$  such that an element  $g$  of a finite group  $G$  belongs to the solvable radical  $R(G)$  of  $G$  if and only if for any  $a \in G$  there exists a number  $n = n(a, g)$  such that  $u_n(a, g) = 1$ . The first results towards a solution of this problem have been obtained in [BGGKPP1], [BGGKPP2], [BWW], and [BBGKP].

In the paper [GKPS] a Thompson-like characterization of the solvable radical of finite groups (and, more generally, linear groups and PI-groups) has been obtained.

**Theorem 1.2** ([GKPS]). *The solvable radical  $R(G)$  of a finite group  $G$  coincides with the set of all elements  $g \in G$  with the following property: for any  $a \in G$  the subgroup generated by  $g$  and  $a$  is solvable.*

This theorem can be viewed as an implicit description of the solvable radical since it does not provide explicit formulas which determine if a particular element belongs to  $R(G)$ .

In the present paper our goal is to obtain a new characterization of the solvable radical  $R(G)$  of a finite group  $G$ .

**Theorem 1.3.** *The solvable radical of any finite group  $G$  coincides with the collection of all  $g \in G$  satisfying the following property: for any 7 elements  $a_1, a_2, \dots, a_7 \in G$  the subgroup generated by the elements  $g, a_i g a_i^{-1}, i = 1, \dots, 7$ , is solvable.*

The proof involves the classification of finite simple groups.

This theorem implies the following characterization of finite solvable groups:

**Theorem 1.4.** *A finite group  $G$  is solvable if and only if every 8 conjugate elements of  $G$  generate a solvable subgroup.*

We hope to sharpen these results.

**Conjecture 1.5.** *The solvable radical of a finite group  $G$  coincides with the collection of all  $g \in G$  satisfying the following property: for any 3 elements  $a, b, c \in G$  the subgroup generated by the conjugates  $g, a g a^{-1}, b g b^{-1}, c g c^{-1}$  is solvable.*

This statement implies

**Conjecture 1.6.** *A finite group  $G$  is solvable if and only if every 4 conjugate elements of  $G$  generate a solvable subgroup.*

**Remark 1.7.** *These characterizations are the best possible: in the symmetric groups  $S_n$  ( $n \geq 5$ ) any triple of transpositions generates a solvable subgroup.*

**Remark 1.8.** The main step in our proof of Theorem 1.3 is Theorem 1.11 below. To prove Conjecture 1.5 (and hence Conjecture 1.6), one has to extend the statement of Theorem 1.11 to all *almost simple* groups, i.e. to the groups  $H$  such that  $G \leq H \leq \text{Aut}(G)$  for some simple group  $G$ .

**Remark 1.9.** The statements of Theorems 1.3 and 1.4 remain true for arbitrary linear groups. The proof is similar to the proof of Theorem 4.1 in [GKPS]. Once Conjectures 1.5 and 1.6 are proved, they can also be extended to arbitrary linear groups.

Throughout the paper  $\langle a_1, \dots, a_k \rangle$  stands for the subgroup of  $G$  generated by  $a_1, \dots, a_k \in G$ . We define the commutator of  $x, y \in G$  by  $[x, y] = xyx^{-1}y^{-1}$ .

**Definition 1.10.** Let  $k \geq 2$  be an integer. We say that  $g \in G$  is a *k-radical element* if for any  $a_1, \dots, a_k \in G$  the subgroup  $H = \langle [a_1, g], \dots, [a_k, g] \rangle$  is solvable.

We prove the following result.

**Theorem 1.11.** *Let  $G$  be a finite nonabelian simple group. Then  $G$  does not contain nontrivial 3-radical elements.*

This theorem implies Theorems 1.3 and 1.4.

The proof goes by case-by-case inspection of simple groups (alternating groups, groups of Lie type, sporadic groups). In fact we prove a more precise result (Theorem 1.15) which distinguishes between 2-radical and 3-radical elements.

The following simple fact allows us to define a new invariant of a finite group.

**Proposition 1.12.** *Let  $G$  be a group which has no nontrivial solvable normal subgroups. Then for every  $g \in G$ ,  $g \neq 1$  the group  $H_g = \langle [g, G] \rangle$  is not solvable.*

*Proof.* For every  $x, y \in G$  we have

$$[g, x]^{-1}[g, y] = (xgx^{-1}g^{-1})(gyg^{-1}y^{-1}) = (xgx^{-1})(yg^{-1}y^{-1}) \in H_g.$$

Thus,  $C_g C_{g^{-1}} \subset H_g$  where  $C_g, C_{g^{-1}}$  are the corresponding conjugacy classes. Since the set  $C_g C_{g^{-1}}$  is invariant under conjugation, the subgroup  $F = \langle C_g C_{g^{-1}} \rangle \leq H_g$  is normal in  $G$  and therefore cannot be solvable.  $\square$

**Corollary 1.13.** *Let  $G$  be a finite group, and let  $R(G)$  denote the solvable radical of  $G$ . Then  $g \notin R(G)$  if and only if there exist an integer  $n$  and  $x_1, \dots, x_n \in G$  such that the subgroup  $\langle [g, x_1], \dots, [g, x_n] \rangle$  is not solvable.*

**Definition 1.14.** Denote by  $\kappa(g)$  the smallest possible  $n$  with the following property:  $g \notin R(G)$  if and only if there exist  $x_1, \dots, x_n \in G$  such that the subgroup  $\langle [g, x_1], \dots, [g, x_n] \rangle$  is not solvable. We call the number  $\kappa(G) := \max_{g \in G \setminus R(G)} \kappa(g)$  the radical degree of  $G$ .

In these terms we have to prove that the radical degree of a finite nonabelian simple group  $G$  is  $\leq 3$ . Our strongest result, which implies Theorem 1.11 and, correspondingly, Theorems 1.3 and 1.4, is the following

**Theorem 1.15.** *If  $G$  is a finite nonabelian simple group, then  $\kappa(G) \leq 3$ . If  $G$  is an alternating group  $G = A_n$ ,  $n \geq 5$ , or a group of Lie type over a field  $K$  with  $\text{char}(K) \neq 2$  and  $K \neq \mathbb{F}_3$ , or a sporadic group not isomorphic to  $Fi_{22}$  or  $Fi_{23}$ , then  $\kappa(G) = 2$ .*

**1.2. Notation and conventions.** First introduce some standard notation which mostly follows [St], [Ca1], [Ca2].

Denote by  $G = G(\Phi, K)$  a Chevalley group where  $\Phi$  is a reduced irreducible root system and  $K$  is a field. Assume that  $\Phi$  is generated by a set of simple roots  $\Pi = \{\alpha_1, \dots, \alpha_r\}$ , that is  $\Phi = \langle \alpha_1, \dots, \alpha_r \rangle$ . We number the roots according to [Bou]. Let  $W = W(\Phi)$  be the Weyl group corresponding to  $\Phi$ . Denote by  $\Phi^+$ ,  $\Phi^-$  the sets of positive and negative roots, respectively.

We use the standard notation  $u_\alpha(t)$ ,  $\alpha \in \Phi$ ,  $t \in K$ , for elementary root unipotent elements of  $G$ . Correspondingly, split semisimple elements will be denoted by  $h_\alpha(t)$ ,  $t \in K^*$ , where  $K^*$  is the multiplicative group of  $K$ . For  $\alpha \in \Phi$ , let  $U_\alpha$  denote the root subgroup generated by all elementary root unipotent elements  $u_\alpha(t)$ .

For the sake of completeness, recall that  $w_\alpha(t) = u_\alpha(t)u_{-\alpha}(-t^{-1})u_\alpha(t)$ ,  $w_\alpha = w_\alpha(1)$  and  $h_\alpha(t) = w_\alpha(t)w_\alpha^{-1}$ . Define the subgroups  $U = U^+ = \langle u_\alpha(t), \alpha \in \Phi^+, t \in K \rangle$ ,  $V = U^- = \langle u_\alpha(t), \alpha \in \Phi^-, t \in K \rangle$ ,  $T = \langle h_\alpha(t), \alpha \in \Phi, t \in K^* \rangle$ , and  $N = \langle w_\alpha(t), \alpha \in \Phi, t \in K^* \rangle$ .

As usual, the Borel subgroups  $B^\pm$  are  $B = B^+ = TU$ ,  $B^- = TV$ . The group  $N$  contains  $T$ , and  $N/T \cong W$ . Denote by  $\dot{w}$  a preimage of  $w \in W$  in  $N$ .

We also consider twisted Chevalley groups over finite fields. Assume that  $K$  is a finite field of characteristic  $p$  and  $|K| = q = p^s$ . By a twisted Chevalley group we mean the group  $G^F = G^F(\Phi, \bar{K})$  of fixed points of the simply connected Chevalley group  $G(\Phi, \bar{K})$  under the Frobenius map  $F$  (see [St], [Ca1], [Ca2]). Here  $\bar{K}$  stands for the algebraic closure of  $K$ . Let  $\theta$  be the field automorphism corresponding to  $F$ . Denote by  $k = K^\theta$  the subfield of  $\theta$ -fixed points for all cases except for the Suzuki groups and the Ree groups. For the latter groups suppose that  $k = K$ . Let  $\gamma$  be the graph automorphism corresponding to  $F$ . We denote by  $\Phi^\gamma$  the root system which determines the structure of the group  $G^F = G^F(\Phi, \bar{K})$ . Elementary root unipotent elements  $u_\alpha(t)$ ,  $\alpha \in \Phi^\gamma$ , have either one parameter  $t \in K$  or  $t \in k$ , or two parameters  $u_\alpha(t, u)$ ,  $t, u \in K$  (for the cases  ${}^2A_2$ ,  ${}^2B_2$ ,  ${}^2F_4$ ), or three parameters  $u_\alpha(t, u, v)$ ,  $t, u, v \in K$  (for  ${}^2G_2$ ), see [St]. Again, the root subgroups  $U_\alpha$  are generated by root unipotent elements. The subgroups  $B^F$ ,  $W^F$ ,  $T^F$ ,  $H^F$ ,  $U^{\pm F}$  in  $G^F$  are defined in a standard way, see [Ca2]. A maximal torus of  $G^F$  is a subgroup of the form  $T^F$ , where  $T$  is an  $F$ -stable maximal torus of  $G$ . A maximal torus  $T^F$  is called quasisplit if it is contained in  $B^F$ . Throughout the paper we suppress the map  $F$  in the notations.

We also suppress  $\gamma$  in the notation of the root system corresponding to the group  $G^F$ . Whenever we need to specify the type of a group, it will be written explicitly.

We follow [Ca2] in the notation of twisted forms. Thus unitary groups are denoted by  $\text{PSU}_n(q^2)$  (and not by  $\text{PSU}_n(q)$ ), the notation  ${}^2F_4(2^{2m+1})$  means that  $q = \sqrt{2^{2m+1}}$ , etc.

The paper is organized as follows. In Section 2 we reduce Theorem 1.4 to Theorem 1.15. In Sections 3–9 we prove Theorem 1.15 using case-by-case analysis.

**Acknowledgements.** Gordeev was partially supported by the INTAS grant N-05-1000008-8118. Kunyavskiĭ and Plotkin were partially supported by the Ministry of Absorption (Israel), the Israeli Science Foundation founded by the Israeli Academy of Sciences (Center of Excellence Program and grant 1178/06), the Minerva Foundation through the Emmy Noether Research Institute of Mathematics, and by the RTN network HPRN-CT-2002-00287. A substantial part of this work was done during Gordeev's visits to Bar-Ilan University in May 2005 and May 2006 (partially supported by the same RTN network) and the visit of Grunewald, Kunyavskiĭ and Plotkin to MPIM (Bonn) during the activity on "Geometry and Group Theory" in July 2006. The support of these institutions is highly appreciated.

We are very grateful to J. N. Bray, B. I. Plotkin, and N. A. Vavilov for useful discussions and correspondence. Our thanks also go to the anonymous referee for numerous remarks.

## 2. Reduction theorem

Let us show how Theorem 1.15 implies Theorem 1.4.

Suppose Theorem 1.15 is proven, and let us show that the solvable radical  $R(G)$  of a finite group  $G$  coincides with the collection of all  $g \in G$  satisfying the property: for any 7 elements  $a_1, a_2, \dots, a_7 \in G$  the subgroup generated by the elements  $g, a_i g a_i^{-1}, i = 1, \dots, 7$ , is solvable.

For the sake of convenience, let us call the elements  $g \in G$  satisfying the condition of the theorem, suitable.

Suppose  $g \in R(G)$ . Since  $R(G)$  is a normal subgroup,  $aga^{-1}$  belongs to  $R(G)$  for any  $a \in G$ . Hence for any  $k$  the subgroup  $\langle a_1 g a_1^{-1}, \dots, a_k g a_k^{-1} \rangle$ , where  $a_1, \dots, a_k \in G$ , is solvable. Therefore, all the elements of  $R(G)$  are suitable.

Suppose now that  $g \in G$  is a suitable element. We want to show that  $g$  belongs to  $R(G)$ . It is enough to prove that there are no nontrivial suitable elements in the semisimple group  $G/R(G)$ . So one can assume that the group  $G$  is semisimple in the sense that  $R(G) = 1$ .

As usual we consider a minimal counterexample  $G$  to the statement above.

Recall that any finite semisimple group  $G$  contains a unique maximal normal centreless completely reducible (CR) subgroup (by definition, CR means a direct

product of finite nonabelian simple groups) called the CR-radical of  $G$  (see [Ro, 3.3.16]). We call a product of the isomorphic factors in the decomposition of the CR-radical *an isotypic component* of  $G$ . Denote the CR-radical of  $G$  by  $V$ . This is a characteristic subgroup of  $G$ .

Let us show that  $V$  has only one isotypic component. Suppose  $V = N_1 \times N_2$ , where  $N_1 \cap N_2 = 1$ . Consider  $\bar{G} = G/N_1$  and denote  $\bar{R} = R(G/N_1)$ . Consider a suitable  $g \in G$ ,  $g \neq 1$  and denote by  $\bar{g}$  (resp.  $\bar{\bar{g}}$ ) the image of  $g$  in  $\bar{G}$  (resp.  $\bar{G}/\bar{R}$ ). Since  $\bar{G}/\bar{R}$  is semisimple and  $\bar{\bar{g}} \in \bar{G}/\bar{R}$  is suitable, we have  $\bar{\bar{g}} = 1$  (because  $G$  is a minimal counter-example) and hence  $\bar{g} \in R(G/N_1)$ . Consider  $V/N_1 \simeq N_2$ . Then  $V/N_1 \subset G/N_1$  is semisimple and therefore  $V/N_1 \cap R(G/N_1) = 1$ . Since  $\bar{g} \in R(G/N_1)$ , we have  $[\bar{g}, \bar{v}] = \bar{1}$  for every  $\bar{v} \in V/N_1$ . Hence  $[g, v] \in N_1$  for every  $v \in V$ . Similarly,  $[g, v] \in N_2$  for every  $v \in V$ . Therefore  $[g, v] = 1$ . Hence  $g$  centralizes every  $v \in V$ . Since the centralizer of  $V$  in  $G$  is trivial, we get  $g = 1$ . Contradiction.

Any  $g \in G$  acts as an automorphism  $\tilde{g}$  on  $V = H_1 \times \cdots \times H_n$ , where all  $H_i$ ,  $1 \leq i \leq n$ , are isomorphic nonabelian simple groups.

Suppose that  $g$  is a suitable element. Let us show that  $\tilde{g}$  cannot act on  $V$  as a non-identity element of the symmetric group  $S_n$ . Denote by  $\sigma$  the element of  $S_n$  corresponding to  $\tilde{g}$ .

By definition, the subgroup  $\Gamma = \langle g, x_i g x_i^{-1} \rangle$ ,  $i = 1, \dots, 7$ , is solvable for any elements  $x_i \in G$ . Evidently, the subgroup  $\langle [g, x_1], [g, x_2] \rangle$  lies in  $\Gamma$ .

Suppose  $\sigma \neq 1$ , and so  $\sigma(k) \neq k$  for some  $k \leq n$ . Take  $\bar{x}_1$  and  $\bar{x}_2$  of the form  $\bar{x}_i = (1, \dots, x_i^{(k)}, \dots, 1)$ , where  $x_i^{(k)} \neq 1$  lies in  $H_k$  ( $i = 1, 2$ ). Then we may assume  $(\bar{x}_i)^\sigma = (x_i^{(k)}, 1, \dots, 1)$ , and so  $[g, \bar{x}_i] = (\bar{x}_i)^\sigma \bar{x}_i^{-1} = (x_i^{(k)}, 1, \dots, (x_i^{(k)})^{-1}, \dots, 1)$ .

Since  $H_k$  is simple, it is generated by two elements, say  $a$  and  $b$ . On setting  $x_1^{(k)} = a$ ,  $x_2^{(k)} = b$ , we conclude that the group generated by  $[g, \bar{x}_1]$  and  $[g, \bar{x}_2]$  cannot be solvable because the first components of these elements,  $a$  and  $b$ , generate the simple group  $H_k$ . Contradiction with solvability of  $\Gamma$ .

So we can assume that a suitable element  $g \in G$  acts as an automorphism of a simple group  $H$ . Then we consider the extension of the group  $H$  with the automorphism  $\tilde{g}$ . Denote this almost simple group by  $G_1$ . We shall use the formula

$$y[x, g]y^{-1} = [x, g][[g, x], y].$$

Since  $G_1$  has no centre, one can choose  $x \in H$  such that  $[x, \tilde{g}] \neq 1$ . Evidently,  $[x, \tilde{g}]$  belongs to the simple group  $H$ . Then by Theorem 1.15, there exist  $y_1, y_2, y_3 \in H$  such that the subgroup  $\langle [[x, g], y_1], [[x, g], y_2], [[x, g], y_3] \rangle$  is not solvable. But

$$\begin{aligned} \langle [[x, g], y_1], [[x, g], y_2], [[x, g], y_3] \rangle &\leq \langle y_i [x, g] y_i^{-1}, [x, g] \mid i = 1, 2, 3 \rangle \\ &\leq \langle g, x^{-1} g x, y_i^{-1} g y_i, y_i^{-1} x^{-1} g x y_i \mid i = 1, 2, 3 \rangle. \end{aligned}$$

Since  $g$  is suitable, the latter subgroup must be solvable. Contradiction with the choice of  $y_i$ .

### 3. Alternating groups

**Proposition 3.1.** *Let  $G = A_n$ ,  $n \geq 5$ . Then  $\kappa(G) = 2$ .*

*Proof.* Let us proceed by induction. For  $n = 5$  the statement can be checked in a straightforward manner. Straightforward computations also work for  $n = 6, 7$ . Assume  $n \geq 8$ . Let  $y \in G$ ,  $y \neq 1$ . First suppose that  $y$  can be written in the form

$$y = \sigma\tau, \quad \sigma \in A_m, \quad \sigma \neq 1, \quad 5 \leq m < n, \quad (1)$$

where  $\sigma$  and  $\tau$  are disjoint (and thus commute). Then by induction hypothesis there exist  $\sigma_1, \sigma_2 \in A_m$  such that the subgroup generated by  $[\sigma, \sigma_1]$  and  $[\sigma, \sigma_2]$  is not solvable. Take  $x_i = \sigma_i\tau$ ,  $i = 1, 2$ . Then  $[y, x_i] = [\sigma, \sigma_i]$ , and we are done.

Suppose  $y$  cannot be represented in the form (1). Then we have one of the following cases: either  $n$  is odd and  $y = (12 \dots n)$ , or  $n$  is even and  $y = (12 \dots n-2)(n-1, n)$ . In any of these cases we take  $x_1 = (123)$  and  $x_2 = (345)$  and get  $\langle [x_1, y], [x_2, y] \rangle \cong A_5$ .  $\square$

### 4. Groups of Lie type of small rank over fields of large characteristic

**Proposition 4.1.** *Let  $G$  be one of the groups  $A_1(q)$  ( $q \neq 2, 3$ ),  ${}^2A_2(q^2)$  ( $q \neq 2$ ),  ${}^2B_2(2^{2m+1})$  ( $m \geq 1$ ),  ${}^2G_2(3^{2m+1})$  ( $m \geq 0$ ). Then  $\kappa(G) = 2$ .*

**Remark 4.2.** Obviously, it is enough to prove that  $\kappa(G_1) = 2$  for some group  $G_1$  lying between  $G$  and its simply connected cover. In each specific case the choice of  $G_1$  will depend on the convenience of the proof. In particular, we shall often assume the Chevalley group under consideration to be simply connected. We shall use this observation without any special notice.

We start with computations for simple groups of Lie type of small Lie rank defined over the finite fields of size 2, 3, 5. They will be used in several parts of our proof. The computations were made for all groups of rank 1 and 2 and also for certain groups of rank 3 and 4 needed for our arguments. The results of MAGMA computations for groups over  $\mathbb{F}_2$  and  $\mathbb{F}_3$  are exhibited in Table 1 (over  $\mathbb{F}_5$  these groups contain no nontrivial 2-radical elements). Each entry of Table 1 displays the number of nontrivial 2-radical elements in the corresponding group (up to conjugacy) and their orders (in parentheses). Dash means that the corresponding group either is solvable or does not exist (for this reason the types  $A_1$  and  ${}^2B_2$  do not appear at all). Asterisks mean that the corresponding group  $G$  is not simple, and computations were made for the derived subgroup  $G'$ , which is simple. It is worth recalling the isomorphisms  $B_2(q) \cong C_2(q)$ ,  $B_2(3) \cong C_2(3) \cong {}^2A_3(2^2)$ ,  $G_2(2)' \cong {}^2A_2(3^2)$ ,  $A_3(2) \cong A_8$ . Note

Table 1. 2-radical elements in simple groups of small Lie rank.

|           | $\mathbb{F}_2$ | $\mathbb{F}_3$ | Remarks                  |
|-----------|----------------|----------------|--------------------------|
| ${}^2A_2$ | —              | 0              |                          |
| ${}^2G_2$ | —              | 0*             | (*) Computed for $G'$    |
| $A_2$     | 0              | 0              |                          |
| $B_2$     | 0**            | 3 (2,3,3)      | (**) Computed for $G'$   |
| $C_2$     | 0**            | 3 (2,3,3)      |                          |
| $G_2$     | 0***           | 0              | (***) Computed for $G'$  |
| ${}^2A_3$ | 3 (2,3,3)      | 0              |                          |
| ${}^2A_4$ | 3 (2,3,3)      | 0              |                          |
| ${}^3D_4$ | 0              | 0              |                          |
| $A_3$     | 0              | 0              |                          |
| $B_3$     | 1 (2)          | 1 (2)          |                          |
| $C_3$     | 1 (2)          | 2 (3,3)        |                          |
| ${}^2F_4$ | 0****          | —              | (****) Computed for $G'$ |
| $D_4$     | 0              | 0              |                          |

that our computations show that whenever nontrivial 2-radical elements do exist, there are no nontrivial 3-radical elements.

Before starting the proof of the proposition, we recall the following result from [Gow] (compare with [EG2]) regarding conjugacy classes of semisimple elements in Chevalley groups. This fact is essential for our arguments.

**Theorem 4.3** ([Gow]). *Let  $G$  be a finite simple group of Lie type, and let  $g \neq 1$  be a semisimple element in  $G$ . Let  $C$  be a conjugacy class of  $G$  consisting of regular semisimple elements. Then there exist a regular semisimple  $x \in C$  and  $z \in G$  such that  $g = [x, z]$ .*

Let us now go over to the proof of Proposition 4.1.

*Proof.* First note that for the groups  $G = {}^2A_2(3^2)$  and  $G = {}^2G_2(3)$  the statement of the proposition follows from calculations presented in Table 1. So we exclude these groups from consideration in the rest of the proof. We start with several simple lemmas (recall that  $G$  is a finite group).

**Lemma 4.4.** *Let  $G = B \cup B\dot{w}B$  be a group of rank 1. Let  $1 \neq u \in U$ . If  $gug^{-1} \in U$ , then  $g \in B$ .*

*Proof.* Suppose  $g = u_2\dot{w}u_1$  where  $u_1, u_2 \in U$ . Then  $v = u_2\dot{w}u_1uu_1^{-1}\dot{w}^{-1}u_2^{-1} \in U$ . Hence

$$U \ni u_2^{-1}vu_2 = \dot{w}u_1uu_1^{-1}\dot{w}^{-1} \in U^-.$$



This contradicts the assumption  $u \neq 1$ .  $\square$

**Lemma 4.5.** *Let  $G$  be a group of rank 1. Then every nontrivial unipotent element is contained in only one Borel subgroup.*

*Proof.* Suppose  $1 \neq u \in U \leq B$  and  $u \in B'$ , where  $B' = xBx^{-1}$ ,  $x \notin B$  [St]. Then  $u = xv x^{-1}$  for some  $v \in U$ . By Lemma 4.4,  $x \in B$ , contradiction.  $\square$

**Lemma 4.6.** *Let  $G$  be a group of rank 1. Then, up to conjugacy, for every  $g \in G$  we have either  $g \in T$ , or  $g \in U$ , or  $g = tu$  with  $t \in T, u \in U, tu = ut$ , or  $g$  is a regular semisimple element which is not contained in any Borel subgroup.*

*Proof.* Indeed, let  $g = su = us$  be the Jordan decomposition of  $g$ . We may and shall assume  $u \in U$ . If  $s = 1$ , then  $g = u \in U$ , so we assume further  $s \neq 1$ . Suppose  $u \neq 1 \in U$ . Then  $sus^{-1} = u \in U$  and therefore, by Lemma 4.4, we have  $s \in B$ . Since  $s \in B$ ,  $s$  lies in some quasisplit torus. As all quasisplit tori are conjugate [Ca2], we have  $s' = bsb^{-1} \in T$  for some  $b \in B$ . Thus we get

$$bgb^{-1} = bsb^{-1}bub^{-1} = s'u'$$

with  $s' \in T, u' \in U$ . Suppose now  $u = 1$ . We have  $g = s$ , and if  $s$  lies in a Borel subgroup, then  $s$  is conjugate to an element of  $T$ , as above. Finally, if  $s$  is a semisimple element which does not belong to any Borel subgroup, then according to Lemma 4.4 it does not commute with any unipotent element, and thus  $g = s$  is a regular semisimple element.  $\square$

**Definition 4.7.** Let  $t \in T$ . Define

$$t^{[2]} := \dot{w}t^{-1}\dot{w}^{-1}t.$$

If  $G$  is of the type  $A_1, {}^2B_2$ , or  ${}^2G_2$ , we have  $t^{[2]} = t^2$ . If  $G$  is of the type  ${}^2A_2(q^2)$  and  $t = \text{diag}(\lambda, \lambda^{-1}\lambda^q, \lambda^{-q})$ , we have  $t^{[2]} = \text{diag}(\lambda\lambda^q, 1, \lambda^{-1}\lambda^{-q})$ .

**Lemma 4.8.** *Let  $G$  be a group of rank 1, let  $g \notin Z(G)$ , and let  $t$  be a generator of  $T$ . Suppose  $t^{[2]}$  is a regular element. Then there exists  $x \in G$  such that  $[g, x]$  is of the form  $\rho^{[2]}$  where  $\rho$  is a generator of a quasisplit torus of  $G$ .*

*Proof.* We may assume  $g = u\dot{w}$ . Put  $x = t^{-1}$ . Then

$$\sigma = [g, t^{-1}] = u\dot{w}t^{-1}\dot{w}^{-1}t^{-1}u^{-1}t = ut^{[2]}t^{-1}u^{-1}t$$

which is conjugate to  $t^{[2]}v$  for some  $v \in U$ . Since  $t^{[2]}$  and, correspondingly,  $t^{-[2]}$  are regular elements, there exists  $y$  such that  $v = [t^{-[2]}, y]$  (see, for example, [EG2]). Then  $yt^{[2]}y^{-1} = t^{[2]}[t^{-[2]}, y] = t^{[2]}v$ . Put  $\rho = yty^{-1}$ . Then  $\rho$  is a generator of a

quasisplit torus  $T' = yTy^{-1}$  and  $w_1 = y\dot{w}y^{-1}$  is a preimage of the generator of the Weyl group. We have

$$\begin{aligned} yt^{[2]}y^{-1} &= y\dot{w}t^{-1}\dot{w}^{-1}ty^{-1} = (y\dot{w}y^{-1})(yt^{-1}y^{-1})(y\dot{w}^{-1}y^{-1})(yty^{-1}) \\ &= \dot{w}_1\rho^{-1}w_1^{-1}\rho = \rho^{[2]}. \end{aligned} \quad \square$$

**Remark 4.9.** Explicit calculations with the matrices

$$\begin{aligned} t &= \text{diag}(\lambda, \lambda^{-1}), \\ t &= \text{diag}(\lambda, \lambda^{-1}\lambda^q, \lambda^{-q}), \\ t &= \text{diag}(\lambda, \lambda^{2\theta-1}, \lambda^{-1}, \lambda^{1-2\theta}), \\ t &= \text{diag}(\lambda^\theta, \lambda^{1-\theta}, \lambda^{2\theta-1}, 1, \lambda^{1-2\theta}, \lambda^{\theta-1}, \lambda^{-\theta}), \end{aligned}$$

corresponding, respectively, to the natural representation of  $\text{SL}_2(q)$ , natural representation of  $\text{SU}_3(q^2)$ , 4-dimensional representation of the Suzuki group and 7-dimensional representation of the Ree group, show that the hypothesis of Lemma 4.8 holds for every group from Proposition 4.1 except for  $A_1(5)$  and  ${}^2A_2(3^2)$ . These two groups were considered separately (note that  $\text{PSL}_2(5) \cong A_5$ ).

**Lemma 4.10.** *Let  $T'$  be a quasisplit torus in a group  $G$  of rank 1, and let  $S$  be a subgroup of  $T'$  such that  $C_G(S) = T'$ . Then  $N_G(S) = N_G(T')$ .*

*Proof.* Let  $B' = T'U'$  be a Borel subgroup containing  $T'$ , and let  $G = B' \cup B'\dot{w}'B'$  be the corresponding Bruhat decomposition. Let  $g \in N_G(S)$ . Suppose  $g = u_1\dot{w}'u_2$  where  $u_1, u_2 \in U'$ . Then for every  $s \in S$  we have

$$\begin{aligned} gsg^{-1} &= (u_1\dot{w}'u_2)s(u_2^{-1}\dot{w}'^{-1}u_1^{-1}) = s' \in S \\ &\implies B'^- \ni (\dot{w}'s\dot{w}'^{-1})(\dot{w}'[s^{-1}, u_2]\dot{w}'^{-1}) = s'[s'^{-1}, u_1^{-1}] \in B' \\ B'^- \cap B' &= T' \\ \implies [s^{-1}, u_2] &= [s'^{-1}, u_1^{-1}] = 1 \\ C_G(S) &= T' \\ \implies u_1 = u_2 &= 1 \\ \implies g &= \dot{w}'. \end{aligned}$$

Suppose  $g \in B'$ . Then  $g = tu$  for some  $t \in T'$ ,  $u \in U'$ , and for every  $s \in S$  we have

$$gsg^{-1} = st[s^{-1}, u]t^{-1} \in S \implies [s^{-1}, u] = 1 \stackrel{C_G(S)=T'}{\implies} u = 1.$$

Hence  $g \in N_G(T')$  and therefore  $N_G(S) \leq N_G(T')$ .

Further, using the same arguments as above (put  $S = T'$ ) one can see that  $N_G(T') = \langle T', \dot{w}' \rangle$ . Note that the conjugation with  $w'$  is an automorphism of  $T'$  and  $T'$  is a cyclic group. Hence the conjugation with  $w'$  is an automorphism of  $S$ . Thus  $N_G(T') \leq N_G(S)$ .  $\square$

**Lemma 4.11.** *Suppose the hypothesis of Lemma 4.8 holds. Suppose that for every nonregular  $s \in T$  and for every regular  $t \in T$  the element  $st$  is regular. Then for every  $g \notin Z(G)$  there exist  $x, y \in G$  such that the group  $H$  generated by  $\tau = [g, x]$  and  $\sigma = [g, y]$  is not contained in any Borel subgroup. Moreover,  $\tau \notin N_G(\langle \sigma \rangle)$ .*

*Proof.* We shall divide the proof into two cases: 1)  $g$  is not a regular semisimple element; 2)  $g$  is a regular semisimple element. Case 1, in turn, will be subdivided into two subcases: 1a)  $\text{char}(K) \neq 2$ ; 1b)  $\text{char}(K) = 2$ .

*Case 1a).* First suppose  $g$  is not a regular semisimple element. By Lemma 4.6, we have  $g \in B, g = su$  with  $su = us, s \in T$  is a nonregular element, and  $u \in U$ . Then we can get  $1 \neq \tau = [g, x] \in U$ . Indeed, if  $u \neq 1$ , we take  $x = s_1 \in T$  such that  $[u, s_1] \neq 1$ . Then  $[g, x] = [g, s_1] = [us, s_1] = [s, s_1]^u [u, s_1] = [u, s_1] = us_1 u^{-1} s_1^{-1} \in U$ . If  $u = 1$ , then  $s \notin Z(G)$ , and hence  $1 \neq [s, v] \in U$  for some  $v \in U$ .

Then by Lemma 4.8, we get  $\sigma = [g, y] = \rho^{[2]}$  where  $\rho$  is a generator of a quasisplit torus. Suppose  $\langle \tau, \sigma \rangle = H \leq B'$  for some Borel subgroup  $B'$ . Since  $\tau$  is a unipotent element, by Lemma 4.5 we have  $B' = B$  and therefore  $gyg^{-1}y^{-1} = \sigma \in B$ . Consider the element  $g^{-1}\sigma = u^{-1}s^{-1}\sigma$ . Since  $\sigma \in B$ , we have  $\sigma = s'u'$  where  $s' \in T$  is semisimple and  $u' \in U$ . Since  $\sigma$  is regular, so is  $s'$ . Then  $g^{-1}\sigma = u^{-1}s^{-1}s'u' = s^{-1}u^{-1}s'u' = s^{-1}s'u_1u' = s^{-1}s'u''$  for some  $u'' \in U$ . By the hypothesis of the lemma,  $s^{-1}s'$  is a regular semisimple element. Hence  $g^{-1}\sigma = s^{-1}s'u''$  is a regular semisimple element. Contradiction, since  $yg^{-1}y^{-1} = g^{-1}\sigma$  is not a regular semisimple element.

Let us now prove that  $\tau \notin N_G(\langle \sigma \rangle)$ . Assume the contrary. Since  $\sigma$  is a regular semisimple element, we have  $C_G(\sigma) = C_G(\langle \sigma \rangle) = T'$ . Lemma 4.10 gives  $N_G(\langle \sigma \rangle) = N_G(T')$ . Therefore  $\tau \in N_G(T')$ .

Hence  $\tau^2 \in T'$ . Indeed, since  $\tau \in N_G(T')$ , we have  $\tau = \dot{w}'$  where  $\dot{w}'$  is a preimage of an element of the Weyl group (possibly,  $w' = 1$ ) corresponding to  $T'$ . Thus  $\tau^2 \in T'$ . But  $\tau \in U$ . Hence  $\tau$  is a unipotent element of order 2 which contradicts to the assumption  $\text{char}(k) \neq 2$ .

*Case 1b).* Suppose  $g$  is not a regular semisimple element and  $\text{char}(k) = 2$ . In this case we may assume  $g = \dot{w}$ .

Indeed, let  $g = su$  be the Jordan form for  $g$ . Suppose the order of  $u$  is greater than 2. On setting  $x = t \in T$ , we get the element  $[g, x] \in U$  of order greater than 2. Then, by the arguments of Case 1a, we have  $\tau \notin N_G(\langle \sigma \rangle)$ . Thus the order of  $u$  is one or two. As  $\text{char}(k) = 2$ , every nonregular element of  $T$  lies in the centre of  $G$ , and therefore we may assume  $s = 1$ . Hence we may assume  $g = u$  to be an element of order 2.

As  $\text{char}(k) = 2$ , in each of the Lie rank 1 groups,  $\text{SL}_2(2^m), \text{SU}_3(2^{2m})$  and  ${}^2B_2(2^{2m+1})$ , all involutions are conjugate, and we may assume  $g = \dot{w}$ .

Therefore we can take  $\sigma = [g, t] = [\dot{w}, t] = t^{[2]}$ , and  $\tau = [g, u] = [\dot{w}, u] = \dot{w}u\dot{w}^{-1}u^{-1} = vu^{-1}$  where  $u \in U$  and  $1 \neq v \in U^-$ . Suppose  $\sigma, \tau \in B'$  for some

Borel subgroup  $B'$ . Then  $T \leq B'$  and therefore  $B' = B$  or  $B' = B^-$ . Contradiction, since  $\tau \notin B$ ,  $\tau \notin B^-$ .

Suppose now  $\tau = vu^{-1} \in N_G(\langle \sigma \rangle) = N_G(T)$ . This is impossible:

$$vu^{-1}tuv^{-1} = t' \in T \implies (B \setminus T) \ni u^{-1}tu = v^{-1}t'v \in (B^- \setminus T).$$

*Case 2.* Let  $g$  be a regular semisimple element. By [Gow], we can get  $\sigma = [g, y]$  to be a generator of a quasisplit torus and  $\tau = [g, x]$  to be a regular semisimple element which is not contained in any Borel subgroup.

We have

- $|T| = q - 1$  if  $G = \mathrm{SL}_2(q)$ ;
- $|T| = q^2 - 1$  if  $G = \mathrm{SU}_3(q^2)$  or  $G$  is a Suzuki or a Ree group.

Further,

- $(q + 1)$  divides  $|G|$  if  $G = \mathrm{SL}_2(q)$ ,  $(q + 1, q - 1) = 2$  or  $1$  (if  $q$  is even);
- $(q^2 - q + 1)$  divides  $|G|$  if  $G = \mathrm{SU}_3(q^2)$ ,  $(q^2 - 1, q^2 - q + 1)$  equals  $3$  or  $1$  (indeed,  $p$  divides  $(q - 1)$  implies  $q \equiv 1 \pmod{p}$ , hence  $q^2 - q + 1 \equiv 1 \pmod{p}$ ). Correspondingly,  $p \mid q + 1$  implies  $(q^2 - q + 1) \equiv 3 \pmod{p}$ ;
- $(q^4 + 1)$  divides  $|G|$  if  $G$  is a Suzuki group,  $q^2 = 2^{2m+1}$ ,  $(q^2 - 1, q^4 + 1) = 1$ ;
- $(q^4 - q^2 + 1)$  divides  $|G|$  if  $G$  is a Ree group,  $q^2 = 3^{2m+1}$ ,  $(q^4 - q^2 + 1, q^2 - 1) = 1$ .

Let now  $G = \mathrm{SL}_2(q)$ . Then the maximal nonsplit torus is a cyclic group of order  $q + 1$ . By [Gow], we can take  $\tau = [g, y]$  to be a generator of such a group. Then the order of  $\tau^2$  is equal to  $q + 1 > 2$  if  $q = 2^m$  or  $(q + 1)/2 > 2$  (note that  $q > 3$ ). Hence  $\tau \notin N_G(\langle \sigma \rangle) = N_G(T)$  (because  $\tau^2 \notin T$ ). Also  $\tau$  does not belong to a Borel subgroup.

Let  $G = \mathrm{SU}_3(q^2)$ . Suppose that  $3$  divides  $q^2 - q + 1$ . Then  $q \equiv -1 \pmod{3}$ , hence  $q \equiv 2, 5, 8 \pmod{9}$  and, therefore,  $9$  does not divide  $q^2 - q + 1$ . Then there exists a prime  $p \neq 2, 3$ ,  $p \mid q^2 - q + 1$ . By [Gow], we can obtain an element of order  $p$  of the form  $\tau = [g, y]$ . Then  $\tau \notin N_G(\langle \sigma \rangle)$ , and  $\tau$  does not belong to a Borel subgroup.

If  $G$  is of Suzuki or Ree type, take  $p \mid q^4 + 1$  or  $p \mid q^4 - q^2 + 1$ , respectively, and proceed as above.

Thus, in all the cases  $\tau \notin N_G(\langle \sigma \rangle)$ . □

**Remark 4.12.** The hypotheses of Lemma 4.11 hold for every group from Proposition 4.1. This can also be checked by explicit calculations with diagonal matrices (see [Ca2] and [KLM]).

**Lemma 4.13.** *There exist  $\tau = [g, x]$  and  $\sigma = [g, y]$  such that the subgroup  $H = \langle \sigma, \tau \rangle$  is not solvable.*

We choose  $\tau = [g, x]$  and  $\sigma = [g, y]$  as in the previous lemma.

It is enough to show that  $H$  does not contain abelian normal subgroups. Let  $A$  be a maximal abelian normal subgroup of  $H$ . We want to check that  $A$  is a reductive group. Suppose  $p = \text{char}(K)$  divides the order of  $A$ . Then the Sylow  $p$ -subgroup of  $A$  is normalized by  $H$ . By Lemma 4.6,  $H \leq B'$  for some Borel subgroup  $B'$ . This is impossible in view of Lemma 4.11. Hence the order of  $A$  is not divisible by  $p$ , and  $A$  is a reductive group.

Let us now view  $H$  as a subgroup of  $\text{GL}(V)$  where  $V$  is a finite dimensional vector space over an algebraically closed field and  $\dim V = 3$  (if  $G = \text{PSL}_2(q), q \neq 2^n$ ),  $\dim V = 2$  (if  $G = \text{SL}_2(2^m)$ ),  $\dim V = 8$  (if  $G = \text{PSU}_3(q^2)$ ),  $\dim V = 4$  (case  ${}^2B_2$ ), or  $\dim V = 7$  (case  ${}^2G_2$ ). Then  $A$  is diagonalizable in  $\text{GL}(V)$  and not all irreducible components of the  $A$ -module  $V$  are isomorphic (if  $A \neq Z(H)$ ). Thus there exists a nontrivial homomorphism  $\varphi: H \rightarrow S_k, k \leq 3, 2, 8, 4, 7$  which corresponds to permutations of isotypical components (otherwise,  $A \leq Z(H)$ ).

*Case 1.* Let  $G = \text{PSL}_2(q), q \neq 2^m$ . For  $q \leq 25$  the statement of the lemma is checked by explicit computer calculations with MAGMA. Let now  $q > 25$ . Recall that  $\sigma = t^2$  or  $\sigma = t$  for  $\langle t \rangle = T'$ , where  $T'$  is a split torus in  $G$ . Since the order of  $T'$  is  $\geq (q-1)/2$ , the order of  $\sigma$  is  $\geq (q-1)/4$ . Since  $\varphi(\sigma)$  lies in  $S_3$ , we have  $\varphi(\sigma^n) = 1$  for some  $n \leq 3$ . Thus  $\text{ord } \sigma^n \geq (q-1)/12 > 2$ . Hence  $C_G(\sigma^n) = T'$  because  $\sigma^n$  is a regular semisimple element of  $T'$ . Since  $\varphi(\sigma^n) = 1$ , we have  $\sigma^n \in C_H(A)$ .

**Sublemma 4.14.** i) *With the above notation, suppose there exists  $h \in H$  such that* 1.  $h \in C_H(A)$ ; 2.  $h \in T'$ ; 3.  $C_G(h) = T'$ . *Then  $A \subseteq T'$ .*

ii) *If, in addition, there exists  $a \in A$  such that  $C_G(a) = T'$ , then  $N_G(\langle h \rangle) = N_G(A) = N_G(T')$ .*

*Proof.* The first assertion of the sublemma is obvious: if  $h \in C_H(A)$ , then  $a \in C_G(h)$  for any  $a \in A$ . The second assertion follows from Lemma 4.10 applied to  $S = A$  and  $S = \langle h \rangle$ . □

On setting  $h = \sigma^n$ , we conclude that  $A \subseteq T'$ .

Suppose there exists  $a$  generating  $A$  such that  $C_G(a) = T'$ . Then by the above sublemma we have  $N_G(\langle \sigma^n \rangle) = N_G(A) = N_G(T')$ . On the other hand, we have  $N_G(T') = N_G(\langle \sigma \rangle)$ . (Indeed, the inclusion  $N_G(\langle \sigma \rangle) \subseteq N_G(\langle \sigma^n \rangle)$  is obvious, and the inclusion  $N_G(T') \subseteq N_G(\langle \sigma \rangle)$  follows from the fact that in the groups of Lie rank 1 the generator  $w$  of the Weyl group normalizes  $t \in T$  and hence  $\sigma$ .) Thus we conclude that  $N_G(\langle \sigma \rangle) = N_G(A) \supseteq H$ , which contradicts the choice of  $\tau$ .

Suppose now there is no  $a \in A$  such that  $C_G(a) = T'$ . Then  $A = \langle a \rangle$  is a cyclic subgroup of order 2 (all other elements of  $T'$  are regular). Since the order of  $a$  equals 2, we have  $N_G(A) = C_G(A)$ . On the other hand,  $C_G(A) = N_G(T') = N_G(\langle \sigma \rangle)$ . Again we get a contradiction since  $\tau$  belongs to  $H \subseteq N_G(A)$  but does not belong to  $N_G(\langle \sigma \rangle)$ .

*Case 2.* Let  $G = \mathrm{SL}_2(2^m)$ ,  $m > 1$ . In this case  $G$  has no centre, any element of  $T' = \langle t \rangle$  is regular, the order of  $t$  equals  $2^m - 1$ . Hence the order of  $\sigma^2$  equals  $2^m - 1 > 1$ . Therefore we can use the same argument as in the preceding case.

*Case 3.* Let  $G = \mathrm{PSU}_3(q^2)$ ,  $q > 3$ . In this case the semisimple element  $\sigma$  equals  $t$  or  $t^{[2]}$ . The order of the image of  $\sigma$  in  $\mathrm{PSU}_3(q^2)$  is  $\geq q - 1$  (recall that the centre of  $\mathrm{SU}_3(q^2)$  is nontrivial if and only if  $q + 1 = 3k$  for some  $k$ ). Note that  $\sigma^n$  is a nonregular nontrivial element if and only if  $\sigma^n = \mathrm{diag}(-1, 1, -1)$ . Hence if  $n \leq 8$  and  $q > 17$ , the order of  $\sigma^n \geq (q - 1)/8 > 2$  and therefore the image of  $\sigma^n$  in  $\mathrm{PSU}_3(q^2)$  is a regular element. Thus we may use the same arguments as in the previous case. Explicit computer calculations with MAGMA prove the statement for the remaining cases  $q \leq 17$ .

*Case 4.* Let  $G$  be a Suzuki or a Ree group. Every nontrivial element of  $T$  is regular if  $G$  is a Suzuki group [Ca2], and every element of  $T$  of order greater than two is regular if  $G$  is a Ree group [KLM]. Note that if  $G$  is a Ree group, then the order of a maximal torus  $T'$  is equal to  $3^{2m+1} - 1$ . Hence  $2 \mid |T'|$ ,  $4 \nmid |T'|$ . The element  $\sigma$  is a generator or the square of a generator of  $T'$ . In particular,  $\sigma$  is not an involution. So if  $n$  is less than the order of  $\sigma^2$ , then  $\sigma^n$  is a regular element of a maximal quasisplit torus.

Consider the permutation  $\varphi(\sigma) \in S_k$ . First suppose  $\varphi(\sigma) = 1$ . Arguing as in Case 1, we arrive at a contradiction with the choice of  $\tau$  whenever we can choose  $a \in A$  such that  $C_G(a) = A$ . This is always possible except for the case where  $G$  is a Ree group and  $A$  is generated by the (unique up to conjugacy) involution  $a$  of  $G$ . But in this latter case we have  $N_G(A) = C_G(a) = \mathbb{Z}/2 \times \mathrm{PSL}_2(3^{2m+1})$  [Gor2, Theorem 3.33 (iv)]. Hence  $H \leq \mathrm{PSL}_2(3^{2m+1})$ , and we are reduced to Case 1.

Thus we may assume  $\varphi(\sigma) \neq 1$ . Then the same argument as above with  $\sigma^n$  replacing  $\sigma$  shows that  $\varphi(\sigma^n) \neq 1$  for every  $n < \mathrm{ord} \sigma^2$ . This means that the restriction of  $\varphi$  to  $\langle \sigma^2 \rangle$  is faithful. But this is impossible since  $\varphi(\sigma^2) \in S_4$  for the Suzuki groups and the order of  $\varphi(\sigma)$  must be less than or equal to 4. However in this case  $\mathrm{ord} \varphi(\sigma^2) = \mathrm{ord} \sigma^2 = 2^{2m+1} - 1 > 4$ . The same situation takes place for the Ree groups:  $\mathrm{ord} \varphi(\sigma^2) = \mathrm{ord} \sigma^2 = (3^{2m+1} - 1)/2 > 12$ , and therefore  $\varphi(\sigma^2)$  cannot belong to  $S_7$ .

Thus in the Suzuki and Ree groups there are no nontrivial abelian normal subgroups in  $H$ , and hence  $H$  is not solvable.

Lemma 4.13 (and hence Proposition 4.1) is proved. □

To use Proposition 4.1 as induction base, we have to extend it from the *simple* groups of rank 1 to some *reductive* groups of semisimple rank 1, namely to the case where  $G$  is an extension of a simple group by a diagonal automorphism, because such groups appear as Levi factors of parabolic subgroups of simple groups of higher ranks; see Lemma 5.6 below.

**Proposition 4.15.** *Let  $G$  be one of the groups from the list of Proposition 4.1, let  $h$  be a diagonal automorphism of  $G$ , and let  $L$  denote the corresponding extension. Then  $\kappa(L) = 2$  with the sole exception  $L = \text{PGL}_2(5)$  for which we have  $\kappa(L) = 3$ .*

*Proof.* The exceptional case is not a surprise in light of the isomorphism  $\text{PGL}_2(5) \cong S_5$ . In order not to overload the reader with technicalities, we shall only sketch the proof. The key point is the following generalization of Gow’s Theorem 4.3:

**Theorem 4.16** ([Gord]). *Let  $L = \tilde{L}^F$  be the group of fixed points of the Frobenius map  $F$  acting on a connected reductive group  $\tilde{L}$  defined over  $\mathbb{F}_p$  such that the derived subgroup  $\tilde{L}'$  is a simple algebraic group, and denote  $L' = (\tilde{L}')^F$ . Suppose that  $([L : L'], p) = 1$ . Let  $\gamma, g \in L$  be semisimple elements such that  $\gamma$  is regular,  $g \in L'$ ,  $g \notin Z(L)$ . Then there exist  $g' \in C_g$  and  $x \in L$  such that  $g' = [\gamma, x]$ .  $\square$*

Note that the hypotheses of the theorem hold if  $L'$  is generated by the root subgroups of  $L$ . The proof goes along the same lines as in [Gow].

Furthermore, Lemmas 4.4–4.6 hold for all reductive groups of semisimple rank 1, and Lemmas 4.8, 4.11, 4.13 admit appropriate modifications. For example, the statement of Lemma 4.8 should be modified as follows:

**Lemma 4.17.** *Let  $L = HG$  be a reductive group of semisimple rank 1, where  $G$  is the derived subgroup of  $L$  and  $H$  is generated by a diagonal automorphism  $h$  of  $G$ . Let  $g \in L$ ,  $g \notin Z(G)$ , and let  $t$  be a generator of  $T$ . Suppose  $t^{[2]}$  is a regular element. Then there exists  $x \in G$  such that  $[g, x]$  is of the form  $\rho^{[2]}$  where  $\rho$  is a generator of a quasisplit torus of  $G$ .  $\square$*

Note that to prove the modified Lemma 4.13, additional MAGMA computations are needed to treat the reductive groups  $\text{PGL}_2(q)$  ( $q \leq 25$ ) and  $\text{PGU}_3(q)$  ( $q \leq 17$ ).  $\square$

### 5. Groups of Lie type of arbitrary rank over fields of large characteristic

**Theorem 5.1.** *Let  $G$  be a Chevalley group of rank  $> 1$  over a field  $K$ ,  $\text{char}(K) \neq 2$ ,  $K \neq \mathbb{F}_3$ . Then  $\kappa(G) = 2$ .*

*Proof.* We need several lemmas (most of whose statements are independent of the characteristic of the ground field).

**Lemma 5.2.** *Let  $\Pi = \{\alpha_1, \dots, \alpha_r\}$ ,  $r \geq 2$ , be a basis of an irreducible root system  $R \neq A_2$ , where the numbering of the simple roots is as in [Bou] in the case  $R \neq E_r$ , and  $\alpha_2$  and  $\alpha_3$  are interchanged in the case  $R = E_r$ . Denote by  $w_c = w_{\alpha_1} \dots w_{\alpha_r} w_{\alpha_2}$*

the corresponding Coxeter element. Then  $w_c(\alpha_1) > 0$ ,  $w_c(\alpha_1) \notin \Pi$  and  $w_c^{-1}(\alpha_2) > 0$ ,  $w_c^{-1}(\alpha_2) \notin \Pi$ .

*Proof.* Let  $r = 2$ . We proceed case by case.

1.  $R = B_2$ . We have  $\alpha_1 = \epsilon_1 - \epsilon_2$ ,  $\alpha_2 = \epsilon_2$ , and

$$w_c(\alpha_1) = \epsilon_1 + \epsilon_2 = \alpha_1 + 2\alpha_2, \quad w_c^{-1}(\alpha_2) = \epsilon_1 = \alpha_1 + \alpha_2.$$

2.  $R = C_2$ . We have  $\alpha_1 = \epsilon_1 - \epsilon_2$ ,  $\alpha_2 = 2\epsilon_2$ , and

$$w_c(\alpha_1) = \epsilon_1 + \epsilon_2 = \alpha_1 + \alpha_2, \quad w_c^{-1}(\alpha_2) = 2\epsilon_1 = 2\alpha_1 + \alpha_2.$$

3.  $R = G_2$ . Then  $\alpha_1 = \epsilon_1 - \epsilon_2$ ,  $\alpha_2 = -2\epsilon_1 + \epsilon_2 + \epsilon_3$ . We have

$$w_c(\alpha_1) = \epsilon_3 - \epsilon_2 = 2\alpha_1 + \alpha_2, \quad w_c^{-1}(\alpha_2) = 2\epsilon_3 - \epsilon_1 - \epsilon_2 = 3\alpha_1 + 2\alpha_2.$$

Let  $r > 3$ . Note that our numbering of roots gives  $\langle \alpha_1, \alpha_2 \rangle = A_2$ . Therefore

$$w_{\alpha_1}(\alpha_2) = \alpha_1 + \alpha_2, \quad w_{\alpha_2}(\alpha_1) = \alpha_1 + \alpha_2, \quad (2)$$

$$w_{\alpha_1}(\alpha_1 + \alpha_2) = \alpha_2, \quad w_{\alpha_2}(\alpha_1 + \alpha_2) = \alpha_1. \quad (3)$$

Put  $\omega = w_{\alpha_3} \dots w_{\alpha_r}$ . Since  $\omega$  has no factors  $w_{\alpha_{1,2}}$ , we have

$$\omega^{\pm 1}(\alpha_{1,2}) > 0. \quad (4)$$

Moreover,

$$\omega^{\pm 1}(\alpha_1) = \alpha_1, \quad \omega^{\pm 1}(\alpha_2) \notin \langle \alpha_1, \alpha_2 \rangle. \quad (5)$$

From (2)–(5) we get

$$\omega^{\pm 1}(\alpha_1 + \alpha_2) = \alpha_1 + \alpha_2 + \dots \neq \alpha_1 + \alpha_2, \quad \omega^{\pm 1}(\alpha_1 + \alpha_2) > 0. \quad (6)$$

From (6) we get

$$\begin{aligned} 0 < w_c(\alpha_1) &= w_{\alpha_1}\omega(\alpha_1 + \alpha_2) \notin \Pi, \\ 0 < w_c^{-1}(\alpha_2) &= w_{\alpha_2}\omega^{-1}(\alpha_1 + \alpha_2) \notin \Pi. \end{aligned} \quad \square$$

**Lemma 5.3.** *Let  $g = u^{-1}w_c^{-1}$ , where  $w_c$  is the Coxeter element from the previous lemma and  $u \in U$ . Then there exists  $x \in G$  such that  $[g, x] = u_{\alpha_1}u_{\alpha_2}u'$ , where  $u_{\alpha_1} \neq 1$ ,  $u_{\alpha_2} \neq 1$  are the corresponding root subgroup elements and  $u' \in U$  does not contain root subgroups factors of type  $u_{\alpha_1}, u_{\alpha_2}$ . Moreover, every  $u_{\alpha_1} \in U_{\alpha_1}$  can be obtained in such a way.*



*Proof.* Let  $R = A_2$ . Put  $1 \neq x = u'_{\alpha_2} \in U_{\alpha_2}$ . Then  $\dot{w}_c^{-1} u'_{\alpha_2} \dot{w}_c = u'_{\alpha_1} \in U_{\alpha_1}$  and

$$[g, x] = u^{-1}(\dot{w}_c^{-1} u'_{\alpha_2} \dot{w}_c) u u'^{-1}_{\alpha_2} = (u^{-1} u'_{\alpha_1} u) u'^{-1}_{\alpha_2} = u_{\alpha_1} u_{\alpha_2} u'$$

where  $u_{\alpha_1} = u'_{\alpha_1}$ ,  $u_{\alpha_2} = u'^{-1}_{\alpha_2}$ , and  $u' = u'_{\alpha_2} [u'^{-1}_{\alpha_1}, u^{-1}] u'^{-1}_{\alpha_2}$  does not contain factors from  $U_{\alpha_1}, U_{\alpha_2}$ .

On varying  $x = u'_{\alpha'_2}$ , we can get an arbitrary  $u_{\alpha_1}$ .

Let now  $R \neq A_2$ . We use Lemma 5.2. Put  $x = u'_{\alpha_2} u'_{\beta}$  where  $\beta = w_c(\alpha_1)$ . Then  $\dot{w}_c^{-1} u'_{\alpha_2} \dot{w}_c = u'_{\gamma}$ ,  $\gamma > 0$ ,  $\gamma \notin \Pi$ ,  $\dot{w}_c^{-1} u'_{\beta} \dot{w}_c = u'_{\alpha_1} \in U_{\alpha_1}$ , and

$$[g, x] = u^{-1}(\dot{w}_c^{-1} u'_{\alpha_2} u'_{\beta} \dot{w}_c) u u'^{-1}_{\beta} u'^{-1}_{\alpha_2} = (u^{-1} u'_{\gamma} u'_{\alpha_1} u) u'^{-1}_{\beta} u'^{-1}_{\alpha_2} = u_{\alpha_1} u_{\alpha_2} u',$$

with  $u'$  as required.  $\square$

**Lemma 5.4.** *Let  $g = u^{-1} \dot{w}_c^{-1}$ , where  $w_c$  is the Coxeter element from Lemma 5.2. Then there exists  $y \in G$  such that  $[g, y] = u_{-\alpha_1} u'$  where  $u_{-\alpha_1} \in U_{-\alpha_1}$ ,  $u' \in U$ . Moreover, every  $u_{-\alpha_1} \in U_{-\alpha_1}$  can be obtained in such a way.*

*Proof.* Put  $y = u^{-1}_{-\alpha_1}$ . We have  $\dot{w}_c^{-1} u^{-1}_{-\alpha_1} \dot{w}_c = u_{\beta}$ ,  $\beta > 0$ , and  $\beta \neq \alpha_1$  (this follows from the definition of  $w_c$ ). Then

$$\begin{aligned} [g, y] &= u^{-1} \dot{w}_c^{-1} u^{-1}_{-\alpha_1} \dot{w}_c u u_{-\alpha_1} = u^{-1} (\dot{w}_c^{-1} u^{-1}_{-\alpha_1} \dot{w}_c) u u_{-\alpha_1} \\ &= u^{-1} u_{\beta}^{-1} u u_{-\alpha_1} = u_{-\alpha_1} (u^{-1}_{-\alpha_1} u^{-1} u_{\beta}^{-1} u u_{-\alpha_1}) = u_{-\alpha_1} u'. \end{aligned}$$

The last equality follows from the fact that  $u^{-1} u_{\beta}^{-1} u$  belongs to the unipotent radical of the minimal parabolic subgroup corresponding to the root  $\alpha_1$ .  $\square$

**Lemma 5.5.** *Let  $G \neq A_1(2^m)$  be a quasisimple Chevalley group of rank 1. Then there exist  $u_1 \in U^{-}$ ,  $u_2 \in U^{+}$  such that  $\langle u_1, u_2 \rangle$  is not solvable.*

*Proof.* The proof immediately follows from Dickson's lemma (see [Gor2, Theorem 2.8.4] and [Nu]), where there are exhibited explicit pairs of unipotent elements  $u_1 \in U^{-}$ ,  $u_2 \in U^{+}$  such that the subgroup  $\langle u_1, u_2 \rangle$  is not solvable.  $\square$

The following (obvious) lemma allows us to reduce to groups of small semisimple rank.

**Lemma 5.6.** *Let  $P = LV$  be a parabolic subgroup of a Chevalley group  $G$  where  $L$  is a Levi factor and  $V$  is the unipotent radical of  $P$ . Further, let  $x_1, \dots, x_s, g \in P$ , and let  $\bar{x}_1, \dots, \bar{x}_s, \bar{g}$  be their images in  $L/Z(L)$  with respect to the natural homomorphism  $P \rightarrow L \rightarrow L/Z(L)$ . If the group  $\langle [\bar{g}, \bar{x}_1], \dots, [\bar{g}, \bar{x}_s] \rangle$  is not solvable, then the group  $\langle [g, x_1], \dots, [g, x_s] \rangle$  is not solvable too.*

Now we are able to finish the proof of the theorem. Let  $X \subset \Pi$ , and let  $X = X_1 \cup \dots \cup X_l$  be the decomposition of  $X$  into a disjoint union of subsets  $X_i$  generating irreducible subsystems of  $R$ . Put

$$w_{X_i} = \prod_{\alpha \in X_i} w_\alpha \tag{7}$$

where the product is taken in any order. Set

$$w_X = \prod_i w_{X_i}.$$

(If  $X = \emptyset$ , we set  $w_X = 1$ .) Then  $w_X$  is a generalized Coxeter element (see [GS]) corresponding to  $X$ . Denote  $\dot{W}_X = \langle \dot{w}_\alpha, \alpha \in \langle X \rangle \rangle$ , where  $\langle X \rangle$  stands for the root system generated by  $X$ . Since  $\text{char}(K) \neq 2$ ,  $G$  is not of type  ${}^2F_4$ , and we can use the following

**Proposition 5.7** ([GS, Proposition 6]). *Suppose  $G$  is not of type  ${}^2F_4$ , and let  $g \in G \setminus Z(G)$ . Then the conjugacy class of  $g$  intersects a generalized Coxeter cell  $B\dot{w}_X B$  for some  $X$ .*

**Remark 5.8.** For  $G = {}^2F_4$  it is not known whether the above statement is true or not.

Thus we may assume

$$g = u\dot{w}_X, \quad u \in U.$$

To finish the proof of Theorem 5.1, we now consider three separate cases. (Note that if  $X \neq \emptyset$ , we have  $|X_i| \neq \emptyset$  for every  $i$ .)

*Case 1.* Suppose  $X = \emptyset$ . Then  $g = hu$ ,  $u \in U$ ,  $h \in T$ . We may assume  $u \neq 1$  (otherwise we can conjugate  $g$  with an appropriate element from  $U$ ). Conjugating  $g$  with an appropriate element  $\dot{w}$  we can get an element  $g' = h'u'$  in the conjugacy class of  $g$  such that  $u' \in U$  and among root factors of  $u'$  there is a simple root subgroup factor  $u_\alpha$ .

Indeed, let

$$u = \prod_{\alpha \in M \subset R^+} u_\alpha, \quad u_\alpha \neq 1.$$

Let  $k = \min\{ht(\alpha) \mid \alpha \in M\}$ . Then there exists an element  $w \in W$  such that  $0 < \min\{ht(\alpha) \mid \alpha \in w(M)\} < k$ . Thus we can get  $\min\{ht(\alpha) \mid \alpha \in w(M)\} = 1$  for an appropriate  $w \in W$ .

Write  $g = hu_\alpha u''$ .

Put  $P = T\langle U_{\pm\alpha} \rangle U = B\langle \dot{w}_\alpha \rangle B$ . Now in the parabolic subgroup  $P$  we can take the Levi factor  $L_\alpha$  of rank 1 corresponding to the root  $\alpha$ . Denote by  $\bar{g}$  the image of  $g$  in

$\bar{L}_\alpha = L_\alpha/Z(L_\alpha)$ . First suppose that  $\bar{g}$  lies in the derived subgroup  $G_\alpha = L'_\alpha$  of  $L_\alpha$ . Since  $G_\alpha$  is a simple group of rank 1, we can apply Lemma 5.6 and Proposition 4.1 and get the result. If  $\bar{g}$  does not lie in  $G_\alpha$ , we can use Proposition 4.15 instead of Proposition 4.1 except for the case  $p = 5$ . In this latter case we have  $G_\alpha \cong \text{PGL}_2(5)$ , and we have a problem only when  $\bar{g}$  is a (unique up to conjugacy) 2-radical element of  $\text{PGL}_2(5)$ . One can show that in fact this case cannot occur. Indeed, this 2-radical element is an involution which can be represented by the matrix  $\begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} \in \text{PGL}_2(5)$ . One can easily show that this matrix is not triangulizable which contradicts the form of  $g$ .

*Case 2.* Suppose  $|X_i| > 1$  for every  $i$ . Put  $P = B\dot{W}_X B$ . Consider the group  $L_i = T\langle U_{\pm\alpha} \mid \alpha \in \langle X_i \rangle \rangle$ . This is a subgroup of a Levi factor  $L = T\langle U_{\pm\alpha} \mid \alpha \in \langle X \rangle \rangle$  of  $P$ . Let  $g_i = u_i w_{X_i}$  be the  $i^{\text{th}}$  component of  $g$ . We may assume that the order of simple reflections in (7) corresponds to the order in Lemmas 5.2–5.4. Then by Lemmas 5.3–5.4, given any  $u_{\pm\alpha_i} \in U_{\pm\alpha_i}$ , we have

$$[g_i, x] = u_{\alpha_i} u'', [g_i, y] = u_{-\alpha_i} u'$$

for some  $x, y \in G$  and  $u', u''$  as specified there. It remains to use Lemmas 5.5 and 5.6; note that Lemmas 5.3–5.6 hold for the reductive (not necessarily simple) groups appearing as Levi factors of parabolic subgroups.

*Case 3.* Suppose  $|X_i| = 1$  for some  $i$ . Let  $P = B\dot{W}_X B$ . Then there exists a simple component  $L_i$  of a Levi factor of  $P$  which is of rank 1. If  $p > 5$ , we can use Lemma 5.6 and Proposition 4.15. To treat the exceptional case  $p = 5$ , we reduce to consideration of the reductive groups of ranks 2, 3, 4 over  $\mathbb{F}_5$  (see Case 4 at the end of the next section for a more detailed argument). MAGMA computations show that these groups contain no nontrivial 2-radical elements, and we are done.

Theorem 5.1 is proved. □

## 6. Groups of Lie type over fields of small characteristic

**Proposition 6.1.** *Let  $G$  be a nonsolvable Chevalley group over a field  $K$  where either  $\text{char}(K) = 2$  or  $K = \mathbb{F}_3$ . Then  $\kappa(G) \leq 3$ .*

*Proof.* Throughout this section we assume  $G \neq {}^2F_4(q^2)$  leaving this case for separate consideration in the next section.

We have to prove that for every  $g \notin Z(G)$  one can find  $x_1, x_2, x_3 \in G$  such that the group  $F = \langle [g, x_1], [g, x_2], [g, x_3] \rangle$  is not solvable.

By Proposition 4.1, for any nonsolvable rank 1 group  $G$  we have  $\kappa(G) = 2$ . Thus we may and shall assume that  $\text{rank } G > 1$ .

First suppose  $\text{char}(K) = 2, |K| > 2$ . We use the same case-by-case subdivision as in the proof of Theorem 5.1 above. Cases 1 and 3 are treated in exactly the same

way (two commutators are enough). Suppose that we are in the conditions of Case 2, i.e.  $|X_i| > 1$  for every  $i$ . Arguing as in the proof of Theorem 5.1, we reduce to the case of  $L_\alpha/Z(L_\alpha)$ , where  $L_\alpha$  is a Levi factor of semisimple rank 1. If  $L_\alpha$  is not of type  $A_1(2^m)(m > 1)$ , we can use the same arguments as in Lemma 5.5 (once again, two commutators are enough). So we may and shall assume  $G$  of type  $A_1(2^m)(m > 1)$ .

Arguing as in the proofs of Lemmas 5.3–5.4, we conclude that there exist  $x_1, x_2, x_3 \in G$  such that  $[g, x_1] = v \in U^-, [g, x_2] = u' \in U, [g, x_3] = u \in U, u \notin \langle u' \rangle$ , where  $v, u', u$  are arbitrary given elements. Moreover, according to [EG1], [CEG], we can arrange our choice so that to make  $s = vu'$  a generator of a maximal split torus of  $G$ . Finally, note that  $u$  is a regular unipotent element (as all unipotent elements in  $SL_2(2^m)$ ).

Put  $\sigma = s, \tau = u$ . Since  $v, u'$  are involutions,  $u'$  belongs to  $N_G(\langle \sigma \rangle)$ . Indeed, we have  $u'\sigma u'^{-1} = u'\sigma u' = u'su' = u'vu'u' = u'v = (vu')^{-1} = \sigma^{-1}$ . Then  $\tau = u$  does not belong to  $N_G(\langle \sigma \rangle)$  (otherwise we would have  $u, u' \in N_G(\langle \sigma \rangle)$  and  $|\langle u, u' \rangle| = 4$ , contradiction to  $|N_G(\langle \sigma \rangle)| = 2(2^m - 1)$ ). Further,  $u$  and  $vu'$  cannot be in the same parabolic subgroup ( $u$  can belong only to  $B$  (Lemma 4.5), but  $vu' \notin B$ ). Now we can repeat the arguments used in the proof for rank 1 groups over a field of odd characteristic (see Lemmas 4.11 and 4.13).

Let now  $|K| = 2$  or  $|K| = 3$ .

*Case 1.*  $X = \emptyset$ . Then  $g = uh, u \in U, h \in T$ . We may assume  $u \neq 1$  (otherwise we can conjugate  $g$  with an appropriate element from  $U$ ). Conjugating  $g$  with an appropriate element  $\dot{w}$ , we can get  $g' = u'h'$  in the conjugacy class of  $g$  such that  $u' \in U$  and among root factors of  $u'$  there is a nontrivial simple root subgroup factor  $u_{\alpha_j}$  (see Case 1 in the end of the proof of Theorem 5.1). Let  $\alpha_j$  be any root adjacent (in the Dynkin diagram) to  $\alpha_i$ . Then we can reduce to the case of a Levi factor of semisimple rank 2, as above. For all groups of rank 2 over  $\mathbb{F}_2$  and  $\mathbb{F}_3$  we use explicit MAGMA computations. Table 1 contains the needed data for simple groups. As to reductive groups of semisimple rank 2, 2-radical elements can only appear in groups of type  $C_2$  (isomorphic to  $B_2$ ) and in  $PGU_4(2^2)$  (isomorphic to  $PSp_4(3)$ ); in all these cases there are no nontrivial 3-radical elements.

*Case 2.*  $|X_i| = 2$  for some  $i$ . Let  $P$  be a parabolic subgroup,  $P = B\dot{W}_X B$ . Then there exists a simple component  $L_i$  of a Levi factor of  $P$  which is of semisimple rank 2. Then we can use Lemma 5.6 and explicit MAGMA computations for the groups of rank 2, as in the previous case.

*Case 3.*  $|X_i| > 2$  for some  $i$ . In this case, the arguments based on the use of Lemmas 5.3–5.4 are not enough. Instead we shall use the following more subtle version of Lemma 5.4. Note that as Lemma 5.4, this lemma holds for the reductive, not necessarily simple, groups appearing as Levi factors of parabolic subgroups.

**Lemma 6.2.** *Let  $g = u^{-1}\dot{w}_c^{-1}$ , where  $w_c$  is the Coxeter element from Lemma 5.2. Then:*

1) there exists  $y \in G$  such that  $[g, y] = u_{-\alpha_1} u'$  where  $u_{-\alpha_1}$  is any prescribed element from  $U_{-\alpha_1}$  and  $u' \in U$ ;

2) there exists  $z \in G$  such that  $[g, z] = f u''$  where  $f \in \langle U_{\alpha_2}, U_{-\alpha_2} \rangle$ ,  $f \notin B$  and  $u'' \in U$ .

*Proof.* 1) See Lemma 5.4.

2) Recall that  $w_c = w_{\alpha_1} \dots w_{\alpha_r} w_{\alpha_2} = \omega w_{\alpha_2}$ . Since  $\omega$  does not contain the factor  $w_{\alpha_2}$ , we have  $\omega(\alpha_2) = \gamma > 0$  and  $w_c^{-1}(\gamma) = w_{\alpha_2} \omega^{-1}(\gamma) = w_{\alpha_2}(\alpha_2) = -\alpha_2$ . Put  $z = u_\gamma \in U_\gamma$ ,  $u_\gamma \neq 1$ . Then  $\dot{w}_c^{-1} z \dot{w}_c = u_{-\alpha_2} \in U_{-\alpha_2}$ . Further, for every  $0 < \beta \neq \alpha_2$  either  $\beta + (-\alpha_2)$  is not a root or  $\beta + (-\alpha_2) \in R^+$ . Hence  $u_\beta u_{-\alpha_2} u_\beta^{-1} = u_{-\alpha_2} v$  for some  $v \in U$ . Also, for every  $u'_{\alpha_2} \in U_{\alpha_2}$

$$u'_{\alpha_2} u_{-\alpha_2} u_{\alpha_2}'^{-1} \in \langle U_{-\alpha_2}, U_{\alpha_2} \rangle \quad \text{and} \quad u'_{\alpha_2} u_{-\alpha_2} u_{\alpha_2}'^{-1} \notin B.$$

Recall that  $g = u^{-1} \dot{w}_c^{-1}$ . We may assume  $u = v u'_{\alpha_2}$  where the element  $v \in U$  does not have factors from  $U_{\alpha_2}$ . We have

$$\begin{aligned} [g, z] &= u_{\alpha_2}'^{-1} v^{-1} (\dot{w}_c^{-1} u_\gamma \dot{w}_c) v u'_{\alpha_2} u_\gamma^{-1} = u_{\alpha_2}'^{-1} v^{-1} u_{-\alpha_2} v u'_{\alpha_2} u_\gamma^{-1} \\ &= u_{\alpha_2}'^{-1} u_{-\alpha_2} u_{\alpha_2}' v' u_\gamma^{-1} \end{aligned}$$

for some  $v' \in U$ . Put  $f = u_{\alpha_2}'^{-1} u_{-\alpha_2} u_{\alpha_2}'$  and  $u'' = v' u_\gamma^{-1}$ . We have

$$[g, z] = f u''$$

where  $f \in \langle U_{\alpha_2}, U_{-\alpha_2} \rangle$ ,  $f \notin B$  and  $u'' \in U$ . □

By Lemmas 5.2–5.6, we can come up with the situation when  $\Gamma \leq G$  corresponds to the root system generated by  $\alpha_1, \alpha_2$  (in our notation), i.e.  $\Gamma$  is of type  $A_2$  (here  $\Gamma$  denotes the derived subgroup of the Levi factor of the corresponding parabolic subgroup of  $G$ ). By Lemmas 5.3 and 6.2, we have got the following elements in  $\Gamma$  (which are images of commutators of  $G$ ):

$$v_1 = u_{-\alpha_1} v', \quad v_2 = f v'', \quad u = u_{\alpha_1} u_{\alpha_2} u',$$

where  $1 \neq u_{-\alpha_1} \in U_{-\alpha_1}$ ,  $v' \in U_\Gamma := \langle U_{\alpha_1}, U_{\alpha_2} \rangle$ ,  $f \in \langle U_{-\alpha_2}, U_{\alpha_2} \rangle$ ,  $f \notin B$ ,  $v'' \in U_\Gamma$ ,  $1 \neq u_{\alpha_1} \in U_{\alpha_1}$ ,  $1 \neq u_{\alpha_2} \in U_{\alpha_2}$ ,  $u' \in U_{\alpha_1 + \alpha_2}$ .

We have to show that the group  $\langle v_1, v_2, u \rangle$  is not solvable. Consider the groups

$$P = \langle v_1, u \rangle \leq \tilde{P} = \langle u_{-\alpha_1}, U_\Gamma \rangle, \quad P' = \langle v_2, u \rangle \leq \tilde{P}' = \langle u_{-\alpha_2}, U_\Gamma \rangle$$

and the natural homomorphisms

$$\theta: \tilde{P} \rightarrow \tilde{P}/R_u, \quad \theta': \tilde{P}' \rightarrow \tilde{P}'/R'_u$$

where  $R_u$  (resp.  $R'_u$ ) is the unipotent radical of  $\tilde{P}$  (resp.  $\tilde{P}'$ ). We have

$$\theta(\tilde{P}) = \tilde{P}/R_u \cong \mathrm{SL}_2(p), \quad \theta'(\tilde{P}') = \tilde{P}'/R'_u \cong \mathrm{SL}_2(p)$$

where  $p = 2, 3$ . Obviously,  $\langle u_{-\alpha_1}, u_{\alpha_1} \rangle \cong \mathrm{SL}_2(p)$ ,  $\langle f, u_{\alpha_2} \rangle \cong \mathrm{SL}_2(p)$  if  $p = 2, 3$ . Hence

$$\theta(P) = \langle u_{-\alpha_1}, u_{\alpha_1} \rangle \cong \mathrm{SL}_2(p), \quad \theta'(P') = \langle f, u_{\alpha_2} \rangle \cong \mathrm{SL}_2(p), \quad p = 2, 3.$$

Let us show that

$$\mathrm{Ker} \theta \cap P \neq 1, \quad \mathrm{Ker} \theta' \cap P' \neq 1.$$

Recall that  $u$  is regular, so if  $|K| = 2$ , then  $u^2 \in U_{\alpha_1+\alpha_2}$ , and thus the order of  $u$  equals 4. Hence  $u^2 \in \mathrm{Ker} \theta \cap P$  ( $u^2 \in \mathrm{Ker} \theta' \cap P'$ ). Let now  $|K| = 3$ . Take  $h \in P$  (or  $h \in P'$ ) such that  $\theta(h)$  (or  $\theta'(h)$ ) equals  $\mathrm{diag}(-1, -1) \in \mathrm{SL}_2(3)$ . Then explicit matrix calculations show that

$$[h, u] = u_{\alpha_2} u_{\alpha_1+\alpha_2} \in \mathrm{Ker} \theta \cap P \quad (\text{or } [h, u] = u_{\alpha_1} u_{\alpha_1+\alpha_2} \in \mathrm{Ker} \theta' \cap P').$$

We proved that  $\mathrm{Ker} \theta \cap P$  (resp.  $\mathrm{Ker} \theta' \cap P'$ ) is not trivial. Let us show that  $\mathrm{Ker} \theta \cap P = \mathrm{Ker} \theta$  (resp.  $\mathrm{Ker} \theta' \cap P' = \mathrm{Ker} \theta'$ ). Note that  $\mathrm{Ker} \theta \cong K^2$  is a 2-dimensional vector  $K$ -space on which  $P$  acts by conjugation. Since  $\theta(P) \cong \mathrm{SL}_2(p)$ , we have only one nonzero orbit of  $P$  in  $\mathrm{Ker} \theta \cong K^2$ . Hence  $\mathrm{Ker} \theta \cap P = \mathrm{Ker} \theta \cong K^2$ , and therefore  $P = \tilde{P}$ . By the same arguments,  $\mathrm{Ker} \theta' \cap P' = \mathrm{Ker} \theta'$  and  $P' = \tilde{P}'$ . Hence

$$P = \langle v_1, u \rangle = \tilde{P} = \langle u_{-\alpha_1}, U_\Gamma \rangle, \quad P' = \langle v_2, u \rangle = \tilde{P}' = \langle u_{-\alpha_2}, U_\Gamma \rangle.$$

Thus,  $U_\Gamma, u_{-\alpha_1}, u_{-\alpha_2}$  are all contained in  $\langle v_1, v_2, u \rangle$ , and therefore

$$\Gamma = \langle v_1, v_2, u \rangle \cong \mathrm{SL}_3(p).$$

*Case 4.*  $|X_i| = 1$  for every  $i$ . Since for all groups of rank 1 or 2 the proposition has been checked, we may assume  $\mathrm{rank} G > 2$ .

First suppose that the root system corresponding to  $G$  does not contain  $D_4$ , i.e. is of one of the types  $A_r, B_r, C_r, F_4$ . Suppose  $X_i = \{\alpha_j\}$ , where  $j$  is the number of the root in the standard numbering. Note that by construction of  $X$ , neither  $\alpha_{j-1}$ , nor  $\alpha_{j+1}$  belong to  $X$ . Suppose that  $\alpha_{j+2} \notin X$  or  $\alpha_{j-2} \notin X$  (in particular, this assumption holds if  $\alpha_{j\pm 2}$  does not exist). Then the subgroup  $L$  of  $G$  generated by  $U_{\pm\alpha_j}$  and  $U_{\pm\alpha_{j+1}}$  (or  $U_{\pm\alpha_{j-1}}$ ) commutes with the elements  $U_{\pm\beta}$  for every  $\beta \in X \setminus X_i$ . Thus we are reduced to the group  $L$  of rank 2, and the statement is proved. Let us now suppose that  $\alpha_{j+2} \in X$ . Then we can consider the group  $L = \langle U_{\pm\alpha_j}, U_{\pm\alpha_{j+1}}, U_{\pm\alpha_{j+2}} \rangle$  which commutes with the groups  $U_{\pm\beta}$ ,  $\beta \in X \setminus (X_i \cup \{\alpha_{j+2}\})$ . Hence we may assume  $\mathrm{rank} G = 3$  and  $g = \dot{w}_{\alpha_1} \dot{w}_{\alpha_3} u$  for some  $u \in U$ . Here we have to check

the groups  $A_3(p)$ ,  $B_3(p)$ ,  $C_3(p)$ ,  ${}^2D_4(p^2)$ ,  ${}^2A_5(p^2)$ ,  ${}^2A_6(p^2)$ ,  $p = 2, 3$ . We can exclude  ${}^2D_4(p^2)$ ,  ${}^2A_5(p^2)$ ,  ${}^2A_6(p^2)$ ,  $p = 2, 3$ , because these groups have a root subgroup  $G_\alpha$ ,  $\alpha = \alpha_1$  or  $\alpha = \alpha_3$ , which is isomorphic to  $SL_2(p^2)$ , and we can use our considerations for rank 1. Since  $A_3(2) \cong A_8$ ,  $B_3(2) \cong C_3(2)$ , it remains to calculate in the groups  $A_3(3)$ ,  $B_3(2)$ ,  $B_3(3)$ ,  $C_3(3)$ . These groups are checked by explicit MAGMA calculations. Table 1 contains the results for the simple groups. For the reductive groups of type  $A_3$  we have  $PGL_4(2) \cong PSL_4(2) \cong A_8$ , and we only have to compute  $PGL_4(3)$ . This group contains no nontrivial 2-radical elements.

Suppose now that the root system of  $G$  is of type  $D_r$  or  $E_r$ . Let  $\beta$  be the root corresponding to the node with 3 edges on the Dynkin diagram. First suppose  $\beta \in X$ . Then we can take  $\gamma \in \Pi$  which is joined with  $\beta$  and disjoint from all other roots. As  $\beta \in X$ , we have  $\gamma \notin X$ , and  $L = \langle U_{\pm\beta}, U_{\pm\gamma} \rangle$  commutes with every  $U_{\pm\delta}$ ,  $\delta \neq \beta, \delta \in X$ . Thus we may reduce our considerations to groups of rank 2. Let now  $\beta \notin X$ . Suppose  $r > 4$ . If none of  $\alpha_1, \alpha_2$  belongs to  $X$ , we are reduced to the case of type  $A_2$  treated above. If not, we are reduced to the case of groups of rank 1. So it remains to consider the case  $r = 4$ , i.e., the case of the groups  $D_4(p)$ ,  $p = 2, 3$ . This is checked by MAGMA (see Table 1).  $\square$

### 7. Groups ${}^2F_4(q^2)$

Recall that in light of Remark 5.8 we have to consider the groups of type  ${}^2F_4(q^2)$  separately.

If  $R$  is a root system and  $G_R$  is a connected reductive algebraic group with root system  $R$  defined over some algebraically closed field, we denote by  $\tilde{G}_R$  the universal cover of the derived group of  $G_R$ . If it is clear what is the root system under consideration, we often drop the subscript  $R$ . In particular, throughout this section we denote by  $G$  the twisted Chevalley group  ${}^2F_4(q^2)$ ,  $q = \sqrt{2^{2m+1}}$ , and by  $\tilde{G}$  the simple algebraic group of type  $F_4$  defined over  $\mathbb{F}_2$  (identifying it with its group of  $\overline{\mathbb{F}_2}$ -points). We have  $G \subset \tilde{G}$ . Correspondingly, tilde always indicates to subgroups of  $\tilde{G}$ . We denote  $K = \mathbb{F}_{q^2}$ .

**Theorem 7.1.** *Let  $G = {}^2F_4(q^2)$ . Then  $\kappa(G) = 2$ .*

*Proof.* For  $m = 0$ , the group  $G$  is not simple; its derived subgroup (the Tits group) is checked by MAGMA (see Table 1). So throughout below we assume  $m > 0$ .

Let  $1 \neq g \in G$ . First suppose  $g \in P$  for some parabolic subgroup  $P$ . Any parabolic subgroup is conjugate to a standard parabolic subgroup (see [Ca2]). We may thus assume  $P$  to be a standard parabolic subgroup. We have  $P = LV$ ,  $V = R_u(P)$ . We may assume that the image of  $g$  in  $P/Z(L)V$  is not trivial (as above) and reduce the consideration to the group  $L/Z(L)$  of semisimple rank 1.

Hence we may assume that  $g$  does not belong to any parabolic subgroup  $P$ . Then (see [Ca2, 6.4.5]) the order of  $C_G(g)$  is prime to  $p = 2$  (and so is an odd number). Hence  $g$  is a regular semisimple element, and by [Gow] we can get representatives of any two semisimple conjugacy classes of  $G$  in the form  $\sigma = [g, x]$ ,  $\tau = [g, y]$ .

Put  $H = \langle \sigma, \tau \rangle$ . Suppose  $H$  is solvable. Denote by  $I = \{p_1, \dots, p_k\}$  some set of prime divisors of  $|H|$  and by  $H_I$  a Hall subgroup of  $H$  corresponding to  $I$ . Let  $A$  be a maximal normal abelian subgroup of  $H_I$ .

Let us now consider two separate cases:  $m \geq 2$  and  $m = 1$ .

*General case*  $q = \sqrt{2^{2m+1}}$ ,  $m \geq 2$ . We have [Ca2, 2.9, p. 76]

$$\begin{aligned} |G| &= q^{24}(q^2 - 1)(q^6 + 1)(q^8 - 1)(q^{12} + 1) \\ &= (q^2)^{12}(q^2 - 1)^2(q^2 + 1)^2((q^2)^2 + 1)^2((q^2)^2 - q^2 + 1)((q^2)^4 - (q^2)^2 + 1), \end{aligned}$$

where  $q = \sqrt{2^{2m+1}}$ .

**Lemma 7.2.** *Let  $T$  be a maximal quasisplit torus of  $G$ . Then there exists  $t \in T$  such that  $t$  is a regular element of  $\tilde{G}$ , i.e.  $C_{\tilde{G}}(t) = \tilde{S}$  is a maximal torus in  $\tilde{G}$ .*

*Proof.* Let  $\tilde{S}$  be a maximal torus of  $\tilde{G}$  containing  $T$ . Let  $\alpha$  be a positive root of  $R = F_4$  corresponding to  $\tilde{S}$ , and let  $\alpha_T: T \rightarrow \overline{\mathbb{F}}_2^*$  be the restriction of  $\alpha$  to  $T$ .

Let us show that

$$\text{Im } \alpha_T = K^* \tag{8}$$

for every  $\alpha \in R(F_4)$ . We have the following simple root system

$$\alpha_1 = \epsilon_2 - \epsilon_3, \alpha_2 = \epsilon_3 - \epsilon_4, \alpha_3 = \epsilon_4, \alpha_4 = \frac{1}{2}(\epsilon_1 - \epsilon_2 - \epsilon_3 - \epsilon_4),$$

and

$$T = \langle h_1(t) = h_{\alpha_1}(t)h_{\alpha_4}(t^\theta), \quad h_2(s) = h_{\alpha_2}(s)h_{\alpha_3}(s^\theta) \rangle$$

where  $s, t \in K^*$ ,  $2\theta^2 = 1$ . Further,

$$\epsilon_1(h_1(t)) = t^\theta, \quad \epsilon_2(h_1(t)) = t^{1-\theta}, \quad \epsilon_3(h_2(s)) = s, \quad \epsilon_4(h_1(t)) = t^{-\theta}$$

(note that  $2(1 - \theta)(1 + \theta) = 2 - 2\theta^2 = 2 - 1 = 1$ ),

$$(\epsilon_1 + \epsilon_2)(h_1(t)) = t, \quad (\epsilon_1 - \epsilon_2)(h_1(t)) = t^{2\theta-1}$$

$((1 - 2\theta)(1 + 2\theta) = 1 - 4\theta^2 = 1 - 2 = -1)$ ,

$$\begin{aligned} (\epsilon_1 \pm \epsilon_3)(h_2(s)) &= s^{\pm 1}, & (\epsilon_1 \pm \epsilon_4)(h_2(s)) &= s^{\pm 1 \pm 2\theta}, \\ (\epsilon_2 \pm \epsilon_3)(h_2(s)) &= s^{\pm 1}, & (\epsilon_2 \pm \epsilon_4)(h_2(s)) &= s^{\pm 1 \pm 2\theta}, \\ (\epsilon_3 + \epsilon_4)(h_2(s)) &= s^{2\theta}, & (\epsilon_3 - \epsilon_4)(h_2(s)) &= s^{2-2\theta}, \end{aligned}$$



$$\frac{1}{2}(\epsilon_1 \pm \epsilon_2 \pm \epsilon_3 \pm \epsilon_4)(h_2(s)) = s^{\pm 1 \pm \theta} \quad \text{or} \quad s^{\pm \theta}.$$

Thus we have (8). From (8) we get

$$|\text{Ker } \alpha_T| = (q^2 - 1)$$

and

$$\left| \bigcup_{\alpha \in R^+(F_4)} \text{Ker } \alpha_T \right| < (q^2 - 1) \cdot 24 < (q^2 - 1)^2. \quad (9)$$

From (9) we conclude that the set  $M = T \setminus \bigcup_{\alpha \in R^+(F_4)} \text{Ker } \alpha_T$  is not empty. Any element  $t \in M$  is regular. The lemma is proved.  $\square$

**Lemma 7.3.** *There exists a prime  $p \neq 2, 3$ ,  $(p, q^2 - 1) = 1$  such that  $p \mid q^2 + 1$  or  $p \mid q^4 + 1$ .*

*Proof.* This follows from the fact that  $(q^2 - 1, q^2 + 1) = 1$  and  $(q^2 + 1, q^4 + 1) = 1$ .  $\square$

**Lemma 7.4.** *Let  $R$  be a root system, and let  $G_R$  be a connected reductive group. Further, let  $A \subseteq G_R$  be a finite abelian subgroup consisting of semisimple elements and such that  $(|A|, |W(R)|) = 1$ . Then there exists a maximal torus  $S$  in  $G_R$  such that  $A \subseteq S$ .*

*Proof.* Let  $G_R = S'G'_R$ , where  $S' \leq Z(G_R)$  is a torus of  $G_R$  and  $G'_R$  is semisimple. Hence  $Z(G_R) = S'A'$ , where  $A' = Z(G'_R)$  is a finite abelian group. Suppose  $A \subseteq Z(G_R)$ . Since  $(|A|, |W(R)|) = 1$ , we have  $(|A|, |A'|) = 1$  (because  $|W(R)|$  is divisible by  $|A'|$ ), and hence  $A \leq S'$ . Suppose  $a \notin Z(G)$  for some  $a \in A$ . Let  $S$  be a maximal torus of  $G_R$  containing  $a$ . By [Ca2, Theorem 3.5.3], we have

$$C_{G_R}(a) = \langle S, U_\alpha, \dot{w} \mid \alpha(a) = 1, w \in C_{W(R)}(a) \rangle,$$

$$C_G(a)^0 = \langle T_1, U_\alpha \mid \alpha(a) = 1 \rangle.$$

Hence  $|C_G(a)/C_G(a)^0|$  divides  $|W(R)|$ , and therefore  $A \leq C_G(a)^0 \neq G_R$ . To finish the proof, we use induction by  $|R|$ .  $\square$

Before going over to the proof of the assertion of the theorem, we shall describe some general construction (parallel to that of Lemma 4.10).

Let  $G_R$  be a connected semisimple group corresponding to a root system  $R$ , and let  $S$  be a maximal torus of  $G_R$ . Further, let  $M \subseteq S$ , let  $g \in N_{G_R}(M)$ , and let  $g = u\dot{w}v$  be a Bruhat decomposition of  $g$  in  $G_R$  with respect to a Borel subgroup containing  $S$ . We may assume  $\dot{w}v\dot{w}^{-1} \in U^-$ . Let  $s \in M$ . Then

$$gsg^{-1} = u\dot{w}vsv^{-1}\dot{w}^{-1}u^{-1} = uw(s)v'u^{-1} = s' \in M \subseteq S,$$

where  $v' \in U^-$ . Hence  $w(s)v' = u^{-1}s'u = s'[s'^{-1}, u^{-1}]$ . Since  $[s'^{-1}, u^{-1}] \in U$ ,  $v' = [w(s)^{-1}, v] \in U^-$ , we have  $[s'^{-1}, u^{-1}] = 1$ ,  $[w(s)^{-1}, v] = 1$ ,  $s' = w(s)$ . Since we can consider any  $s \in M$ , we have  $u, v \in C_{G_R}(M)$ . Now we have a homomorphism

$$\phi: N_{G(R)}(M) \rightarrow W(R)$$

with

$$\text{Ker } \phi = C_{G(R)}(\tilde{M})^0. \quad (10)$$

We can now go over to the proof of Theorem 7.1.

Set  $\sigma = t$ , where  $t$  is chosen as in Lemma 4.11. Let  $\tau$  be an element of order  $p$  (it exists by Lemma 7.3). Denote by  $I$  the set consisting of  $p$  and all prime divisors of  $q - 1$ . Since all Hall subgroups  $H_I$  are conjugate and each element of order  $p$  belongs to one of those, we may assume  $t \in H_I$  and some element  $\tau'$  of order  $p$  is also in  $H_I$ .

Note that  $2, 3 \nmid (q^2 - 1)$ . Since  $|W(F_4)| = 2^7 3^2$ , we have  $\sigma, \tau' \in C_{\tilde{G}}(A)^0$  (by (10) and Lemma 7.4). Then  $A \subseteq T \subseteq \tilde{T}$  where  $\tilde{T}$  is the unique maximal torus of  $\tilde{G}$  containing  $T$  (recall that  $T$  contains a regular semisimple element of  $\tilde{G}$ ).

Denote by  $R \subset R(F_4)$  the minimal (with respect to inclusion) root subsystem such that

$$\sigma, \tau' \in G_R = \langle \tilde{T}, U_\alpha \mid \alpha \in R \rangle.$$

First note that  $R \neq R(F_4)$  because otherwise we would have  $A \subseteq Z(F_4) = 1$  (recall that  $H \leq C_{\tilde{G}}(A)^0$ ). Second, note that  $R \neq \emptyset$  because  $\tau' \notin T = \tilde{T}^F$ . Set  $G'_R = \langle U_\alpha \mid \alpha \in R \rangle$ . Then  $G_R = SG'_R$  where  $S \leq \tilde{T} \cap Z(G_R)$  is a subtorus of  $\tilde{T}$ . Then  $Z(G_R) = SZ(G'_R)$ . Since the orders of  $\sigma, \tau'$  are prime to 2, 3, we have  $\sigma, \tau' \notin Z(G'_R)$ , and hence so are the orders of their images  $\bar{\sigma}, \bar{\tau}'$  in  $\bar{G}'_R = G'_R / (Z(G'_R) \cap S)$ . Now we have a semisimple group  $\bar{G}'_R$  with a maximal torus  $\bar{T} = \tilde{T}/S$  which contains the solvable group  $\bar{H}_I = \langle \bar{\sigma}, \bar{\tau}' \rangle \neq 1$ , where  $\bar{\sigma} \in \bar{T}$  is a regular element. Let  $A_1$  be a maximal abelian normal subgroup of  $\bar{H}_I$ . Then  $A_1 \subseteq \bar{T}$  and  $A_1 \not\subseteq Z(\bar{G}'_R)$  (note that 2, 3 are the only primes dividing both  $|W(R)|$  and  $Z(\bar{G}'_R)$ ). By (10), we have

$$\bar{\sigma}, \bar{\tau}' \in C_{\bar{G}'_R}(A_1)^0 = \langle \bar{T}', U_\beta \mid \beta(A_1) = 1 \rangle = \langle \bar{T}', U_\beta \mid \beta \in R' \subsetneq R \rangle.$$

Hence

$$\sigma, \tau' \in \langle \tilde{T}, U_\beta \mid \beta \in R' \rangle.$$

This is a contradiction with the choice of  $R$ .

Let us now consider the remaining special case  $m = 1$ .

*Case  $q = \sqrt{2^3}$ .* Here  $|G| = 2^{36} \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 19 \cdot 37 \cdot 109$ .

Let  $|\langle \sigma \rangle| = 109$ ,  $|\langle \tau \rangle| = 37$ , and let  $H_0 \subseteq H$  be a Hall subgroup of  $H$  of order  $37 \cdot 109$ . Since  $(37, 109 - 1) = 1$ , the group  $H_0 = \langle h \rangle$  is cyclic of order  $37 \cdot 109$ .

Let, as above,  $\tilde{G}$  denote the simple algebraic group of type  $F_4$  over the field  $\mathbb{F}_2$ , and let  $F$  be the Frobenius map of  $G$  such that  $G = \tilde{G}^F$ . Since  $h \in \tilde{G}^F$ , the centralizer  $C_{\tilde{G}}(h)$  is an  $F$ -stable connected reductive group ([Ca2, 3.5.6]) which, in turn, contains an  $F$ -stable maximal torus  $\tilde{T}$  (which is also a maximal torus of  $\tilde{G}$ ). Hence  $h \in \tilde{T}^F$ . But

$$|\tilde{T}^F| = \prod_{i=1}^4 (q - \epsilon_i)$$

where each  $\epsilon_i$  is a root of unity [Ca2, 3.3.5]. Since

$$|q - \epsilon_i| \leq q + 1 = \sqrt{8} + 1 \leq 4,$$

we conclude that  $|\tilde{T}^F| \leq 256 < 37 \cdot 109$ . Contradiction.

The theorem is proved. □

### 8. Groups generated by 3-transpositions

In this section we show that the estimate of Proposition 6.1 is sharp as follows from the case of groups generated by 3-transpositions (see [Fi], [As] for definitions and notation).

**Definition 8.1.** [Fi] Let  $G$  be a finite group generated by a class  $D$  of conjugate involutions such that any pair of non-commuting elements of  $D$  generates a dihedral group of order 6; then  $D$  is a class of *conjugate 3-transpositions* of  $G$ .

Equivalently, the product of any two involutions from  $D$  is of order 1, 2, or 3.

**Proposition 8.2.** *Let  $G$  be a finite group generated by a class  $D$  of conjugate 3-transpositions. Then any element of  $D$  is 2-radical.*

*Proof.* This is an immediate consequence of [Fi, Corollary 1.6]. □

**Corollary 8.3.** *Let  $G$  be one of the following groups:*

- a symmetric group  $S_n$ ;
- a symplectic group  $\text{Sp}(2n, 2) (n \geq 2)$ ;
- an orthogonal group  $\text{O}^\mu(2n, 2)$  for  $\mu \in \{-1, 1\}$  and  $n \geq 2$ ;
- a unitary group  $\text{PSU}(n, 2) (n \geq 4)$ ;
- an orthogonal group  $\text{O}^{\mu, \pi}(n, 3)$  for  $\mu \in \{-1, 1\}$ ,  $\pi \in \{-1, 1\}$ , and  $n \geq 4$ ;
- one of Fischer's groups  $Fi_{22}, Fi_{23}, Fi_{24}$ .

*Then  $G$  contains a nontrivial 2-radical element.*

*Proof.* This immediately follows from the above proposition taking into account the fact that all the listed groups are generated by a class of conjugate 3-transpositions [Fi].  $\square$

## 9. Sporadic groups

**Proposition 9.1.** *Let  $G$  be a sporadic simple group. Then  $\kappa(G) = 3$  for  $G = Fi_{22}$ ,  $Fi_{23}$  and  $\kappa(G) = 2$  for all the remaining groups.*

More precisely, we shall prove that if  $g \neq 1$  is a 2-radical element of a sporadic simple group  $G$ , then  $G = Fi_{22}$  or  $G = Fi_{23}$  and  $g$  is a 3-transposition. (In the latter cases MAGMA computations show that  $g$  is not a 3-radical element.)

The proof goes case by case. Apart from the theoretical arguments presented below, we used MAGMA for rechecking them (in all the cases except for the Monster). For larger sporadic groups we had to replace most standard MAGMA procedures with our own ones in order to avoid storing the whole group and large subgroups. In particular, to check whether a subgroup under consideration is not solvable, we used the Hall–Thompson criterion [Th]: a group  $H$  is nonsolvable if and only if it contains nonidentity elements  $a, b, c$  of pairwise coprime orders such that  $abc = 1$ .

Both in the theoretical proof and in the computer-aided one, we rely on the ATLAS classification of conjugacy classes of maximal cyclic subgroups [Wi].

Let us now prove the proposition. The exposition below is sometimes sketchy, we omit some cases where the proof uses arguments similar to earlier ones.

The main idea is very simple. We first consider the elements of prime order. It turns out that in most cases one can include a given element  $g$  of prime order  $p$  of a group  $G$  in its proper simple subgroup  $H$ . If there is a single conjugacy class of cyclic subgroups of order  $p$ , it is enough to indicate  $H$  whose order is divisible by  $p$ . In the case where there are several conjugacy classes of cyclic subgroups of order  $p$ , more subtle arguments are needed. We either use ATLAS information on elements  $h$  of order  $mp$  for some  $m$  whose powering gives  $g$  and try to include  $h$  in some proper simple subgroup  $H$ , or use some information on subgroup structure of  $G$  from the literature. Finally, if  $g$  is not contained in any proper simple subgroup of  $G$ , it happens that its normalizer  $N = N_G(g)$  is the unique maximal subgroup of  $G$  containing  $g$ . In that case, one can take  $x \in N$  and get  $a = [g, x] \in \langle g \rangle$ , and take  $y$  such that  $b = [g, y] \notin N$ . Then  $\langle a, b \rangle = G$  is not solvable.

If an element  $g$  under consideration is of a composite order  $mp$ , we note that it belongs to the centralizer of  $h = g^m$  which is of prime order  $p$ . It remains to use the information from ATLAS on the centralizers of elements of prime orders in sporadic groups. It turns out that in many cases the structure of  $C_G(h)$  is as follows: it contains a normal subgroup  $Z$  of small exponent such that the quotient  $G' = C_G(H)/Z$  is either a smaller simple group or an extension of a simple group by a group of small

exponent. Thus if  $g$  is a 2-radical element of sufficiently large exponent, then its image in  $G'$  is a nonidentity 2-radical element, and we arrive at a contradiction by induction. In some cases, elements of small exponents require separate consideration.

Below we mostly present theoretical arguments as above for elements of prime orders. We present a more detailed proof for the baby-monster  $B$  and a complete proof for the monster  $M$ .

We follow the subdivision of sporadic groups from the ATLAS.

*Mathieu groups:*  $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$ .

$M_{11}$ . The elements of orders 2, 3 and 5 are included in  $A_5$ , and those of order 11 in  $\text{PSL}_2(11)$ .

$M_{12}$ . Any element of order 11 is included in  $\text{PSL}_2(11)$ . All the remaining ones, of types 2A, 2B, 3A, 3B, 5A, are included in  $A_5$  (according to [CCNPW, p. 33],  $M_{12}$  contains  $A_5$ 's of types (2A, 3B, 5A) and (2B, 3A, 5A)).

$M_{22}$ . The elements of orders 2, 3, 5 and 7 are included in  $A_7$ , and the elements of order 11 are included in  $\text{PSL}_2(11)$ .

$M_{23}$ . The elements of orders 2, 3, 5 and 11 are included in  $M_{11}$ . The elements of order 7 are contained in  $A_7$ , and the normalizer  $N = 23 \cdot 11$  of an element  $g$  of order 23 is the unique maximal subgroup of  $M_{23}$  containing  $g$ , so we can apply the argument mentioned above.

$M_{24}$ . Any element of order 23 is included in  $\text{PSL}_2(23)$ . The elements of order 11 are included in  $M_{23}$ , and the elements of orders 7 and 5 are contained in  $\text{PSL}_2(7)$  and in  $A_5$ , respectively. According to [CCNPW, p. 96],  $M_{24}$  contains  $A_5$ 's of types (2B, 3A, 5A) and (2B, 3B, 5A), so it remains to consider the class 2A. Fix an element  $z$  of type 2B. We have  $C_G(z) = E_{26} \cdot S_5$ , where  $E_{26}$  is an elementary abelian subgroup. Let  $g$  be any involution of  $A_5 \subset S_5$ . Since  $g$  centralizes  $z$ , it cannot be conjugate to  $z$ , hence  $g$  is of type 2A, and we are done.

*Leech lattice groups:*  $HS, J_2, Co_1, Co_2, Co_3, McL, Suz$ .

Here we shall be a little sketchy describing only the largest Conway group  $Co_1$  among the three ones.

$HS$ . The elements of orders 3, 7 and 11 are included in  $M_{22}$ . According to [CCNPW, p. 80], there is an  $M_{11} < HS$  containing elements of types 2A and 5C, and there is an  $A_5$  containing elements of type 2B and 5A. The remaining class 5B also has a representative lying in  $A_5$  [GLS, p. 274].

$J_2$ . Any element of order 7 can be included in  $\text{PSL}_3(2)$ . According to [CCNPW, p. 42], there are  $A_5$ 's of types (2B, 3A, 5CD), (2A, 3B, 5AB), thus including the elements of all the other classes.

$McL$ . There are no problems with the elements of orders 2, 7 and 11, they can all be included, say, in  $M_{11}$ . By [CCNPW, p. 100], there is a subgroup  $\text{PSU}_3(5^2)$

containing representatives of 3B, 5A and 5B. It remains to consider the class 3A. Take an element of order 9 in  $\text{PSU}_4(3^2)$ . According to [Wi], its cube belongs to 3A.

*Suz.* Any element of order 13 belongs to a maximal subgroup  $G_2(4)$ , and hence to an even smaller subgroup  $\text{PSL}_2(13)$ . The elements of orders 7 and 11 belong to  $M_{11}$ . On [CCNPW, p. 131] we find an  $A_7$  containing representatives of 2B, 3C and 5B, a  $\text{PSL}_3(3)$  containing representatives of 3B, and a  $\text{PSL}_2(25)$  containing representatives of 5A and 5B. It thus remains to consider the classes 2A and 3A. To treat 2A, take an element of order 8 in  $M_{11}$ , then its cube is of type 2A [Wi]. Similarly, the fifth power of an element of order 15 in  $J_2$  is of type 3A.

*Co<sub>1</sub>.* The elements of orders 23 and 11 belong to  $M_{23}$ , and those of order 13 are included in *Suz*. The classification of  $A_5$ 's [Wi83] gives subgroups of types (2B, 3A, 5A), (2C, 3A, 5B), (2C, 3B, 5C), (2B, 3B, 5A), (2B, 3A, 5A). According to [Cu], the classes 7A and 7B have their representatives in  $A_7$  and  $\text{PSL}_2(7)$ , and the class 3D, as 3A, belongs to  $A_5$ . It remains to consider 2A. One can take an element of order 18 in  $Co_3$ , its 9th power is of type 2A.

*Monster sections: He, HN, Th, Fi<sub>22</sub>, Fi<sub>23</sub>, Fi<sub>24</sub>', B, M.*

Here we shall skip *HN* (which can be treated using [CCNPW, p. 166] and [NW]) and two larger Fischer groups.

*He.* The elements of order 17 belong to  $\text{PSp}_4(4)$ , and hence to  $\text{PSL}_2(16)$ . The elements of order 5 lie in  $A_5$ . We have to consider the classes 2A, 2B, 3A, 3B, 7A, 7C and 7D (7B is a power of 7A and 7E is a power of 7D). First we use the information on (2,3,7)-subgroups from [CCNPW, p. 104]: a subgroup of type (2A, 3B, 7C) is contained in  $7 : 3 \times \text{PSL}_3(2)$  (and hence 2A belongs to  $\text{PSL}_3(2)$ ), and a subgroup of type (2B, 3A, 7AB) is contained in  $S_4 \times \text{PSL}_3(2)$  (and hence 7A belongs to  $\text{PSL}_3(2)$  too). Next, we use the information on the centralizers of involutions [GLS, p. 277]. Since 7D and 3B commute with 2B, they both belong to  $\text{PSL}_3(2)$ . Since 3A commutes with 2A, it belongs to the centralizer of 2A, and hence to  $\text{PSL}_3(4)$ . As to 2A and 2B, the same argument as in the case  $M_{24}$  applies, and we conclude that 2A belongs to  $\text{PSL}_3(2)$  and 2B belongs to  $\text{PSL}_3(4)$ . Finally, since 7C commutes with 3A, it belongs to the centralizer of 3A and hence to  $A_7$ .

*Th.* The normalizer  $N = 31 \cdot 15$  of an element  $g$  of order 31 is the unique maximal subgroup of *Th* containing  $g$ , so we can proceed as in the case of an element of order 23 in  $M_{23}$ . Any element of order 19 belongs to  $\text{PSL}_2(19)$ , the elements of order 13 belong to  ${}^3D_4(2^3)$ , and the elements of orders 2, 5 and 7 are contained in  $A_7$ . It remains to treat three classes of elements of order 3. Take an element of order 21 in  $\text{PSL}_5(2)$ , its 7th power is of type 3A. Taking elements of orders 9 and 15 in  $2^{1+8} \cdot A_9$ , we obtain 3B and 3C as their 3rd and 5th power, respectively.

*Fi<sub>22</sub>.* First recall that this group does contain 2-radical elements, namely, those of the class 2A (3-transpositions), see Section 8 above. Any element of order 13 belongs to  $O_7(3)$ , and hence to  $\text{PSL}_3(3)$ . The elements of orders 5, 7, 11 lie in  $M_{22}$ .

We have to consider the classes 2B, 2C, 3A, 3B, 3C, 3D. According to [CCNPW, p. 163], there is an  $M_{12}$  containing representatives of 2B, 2C, 3C, 3D. We include 3A in  $A_{10}$  representing it as the 5th power of an element of order 15 in  $A_{10}$ . Similarly, we represent 3B as the 6th power of an element of order 18 in  $O_8^+(2)$ .

*B.* The normalizer  $N = 47 \cdot 23$  of an element  $g$  of order 47 is the unique maximal subgroup of  $B$  containing  $g$ , so we can proceed as above. The cases of elements of orders 31, 23, 19, 17, 13, 11 and 7 are easy: those of order 31 belong to  $PSL_2(31)$ , those of order 19 belong to  $Th$ , and all the remaining ones can be included, say, in  $Fi_{23}$ . Furthermore, we use the classification of  $A_5$ 's [Wi93, Theorems 5.1, 5.2]: in particular, there are subgroups of types (2B, 3A, 5A), (2D, 3B, 5B) and also those containing 2C. It remains to consider 2A. We get it as the 13th power of an element of order 26 in  $Fi_{23}$ .

Let now  $g$  be an element of composite order  $mp$ ,  $m \geq p$ . As  $p \leq 5$ , it suffices to use information on the centralizers of the elements of orders 2, 3 and 5. We have  $C_B(2A) = 2 \cdot ({}^2E_6(2^2)) : 2$ ,  $C_B(2B) = 2_+^{1+22} \cdot Co_2$ ,  $C_B(2C) = (2^2 \cdot F_4(2)) : 2$ ,  $C_B(2D) = 2^9 \cdot 2^{16} \cdot O_8^+(2) \cdot 2$ ,  $C_B(3A) = 3 \times Fi_{22} : 2$ ,  $C_B(3B) = 3_+^{1+8} : 2_-^{1+6} \cdot PSU_4(2^2)$ ,  $C_B(5A) = 5 \times HS : 2$ ,  $C_B(5B) = 5_+^{1+4} : 2_-^{1+4} \cdot A_5$ .

First suppose  $g$  is of odd order  $mp$ ,  $m > p$ . If  $p = 3$ , then  $g$  centralizes either 3A or 3B. As the exponent of the extraspecial group  $3_+^{1+8}$  equals 3, we get the image of  $g$  of order at least 5 in either  $Fi_{22}$  or  $PSU_4(2^2)$  whose 2-radical elements can only be of order 2 or 3. Thus  $g$  is not 2-radical. (Note that this argument does not work for the elements of order 9 which will be considered separately.) If  $p = 5$ , we have to consider the elements of orders 35 and 55 which all centralize 5A. Hence each of them maps to a nonidentity element of  $HS$ , and we are done. The elements of order 25 centralize 5B. As the exponent of the extraspecial group  $5_+^{1+4}$  equals 5, each of them maps to a nonidentity element of  $A_5$  which cannot be 2-radical. To finish with the case of odd order, it remains to consider the elements of order 9. According to [Wi], both 9A and 9B can be represented as the 4th power of an element of order 36. Hence any element of order 9 centralizes either 2B or 2D and thus belongs to either  $Co_2$  or  $O_8^+(2)$ , and we are done.

Suppose now  $g$  is of even order  $2m$  so that  $g$  centralizes an involution of  $B$ . If  $m$  is odd, then the image of  $g$  in the simple group involved in the centralizer of the corresponding involution is nonidentity, and we are done. So assume  $m$  to be even, i.e.  $g$  is of order  $4n$ . The elements of order 4 were checked by MAGMA, so suppose  $n > 1$ . According to [Wi], there are no elements of order  $4n$ ,  $n > 1$ , powering to 2A. If  $g$  centralizes 2B, then it maps to a nonidentity element of  $Co_2$ , and we are done. According to [Wi], the elements of order  $4n$ ,  $n > 1$ , powering to 2C are 12T, 20H and 52A, they were checked separately by MAGMA. Finally, suppose that  $g$  centralizes 2D. If  $n > 2$ , then taking into account that  $C_B(2D) < 2^9 \cdot 2^{16} \cdot PSp_8(2)$ , we conclude that  $g$  maps to a nonidentity 2-radical element of order greater than 2 in  $PSp_8(2)$  which contradicts to MAGMA computations in that group. Thus it remains

to check the elements of order 8 powering to 2D, i.e. 8G, 8J, 8K, 8M and 8N. This was also done by MAGMA.

*M*. In this case no additional MAGMA computations were needed, we only used the results for smaller groups. Our approach mimics the case of the baby-monster.

The normalizer  $N = 41 \cdot 40$  of an element  $g$  of order 41 is the unique maximal subgroup of  $M$  containing  $g$ , so we can proceed as above. Relying on the existing information on maximal subgroups of  $M$  [BrW], we include the elements of orders 71, 59, 47, 31, 29, 23, 19, 17, 11 in  $\text{PSL}_2(71)$ ,  $\text{PSL}_2(59)$ ,  $B$ ,  $B$ ,  $Fi'_{24}$ ,  $B$ ,  $B$ ,  $B$ ,  $B$ , respectively. Representatives of all the remaining classes appear in [No]: Table 1 on p. 201 gives 13A and 13B lying in  $\text{PSL}_3(3)$ , in Section 5 there are exhibited 7A and 7B lying in  $\text{PSL}_3(2)$ , and the list of  $A_5$ 's in Table 3 on p. 202 contains representatives of all classes of elements of orders 2, 3 and 5.

Let now  $g$  be an element of composite order  $mp$ ,  $m \geq p$ . Our arguments are similar to the previous case. As for  $B$ , we have  $p \leq 5$ , and it suffices to use information on the centralizers of the elements of orders 2, 3 and 5. We have  $C_M(2A) = 2 \cdot B$ ,  $C_M(2B) = 2_+^{1+24} \cdot Co_1$ ,  $C_M(3A) = 3 \times Fi'_{24}$ ,  $C_M(3B) = 3_+^{1+12} \cdot 2 \text{Suz}$ ,  $C_M(3C) = 3 \times Th$ ,  $C_M(5A) = 5 \times HN$ ,  $C_M(5B) = 5_+^{1+6} : 2J_2$ .

First suppose  $g$  is of odd order  $mp$ ,  $m \geq p$ . If  $p = 3$ , then  $g$  centralizes either 3A, or 3B, or 3C. As the exponent of the extraspecial group  $3_+^{1+12}$  equals 3, we get the image of  $g$  of order at least 5 in either  $Fi'_{24}$ , or  $\text{Suz}$ , or  $Th$  which do not contain 2-radical elements. Thus  $g$  is not 2-radical. If  $p = 5$ , we have to consider the elements of orders 25, 35, 45, 55, 95 and 105. Any of those centralizes either 5A or 5B and hence maps to a nonidentity element of either  $HN$  or  $J_2$ . (We use the fact that the exponent of the extraspecial group  $5_+^{1+6}$  equals 5.)

If  $g$  is of even order  $2m$ , it centralizes either 2A or 2B. If  $m > 2$ , then  $g$  maps to a nonidentity element of either  $B$  or  $Co_1$  which do not contain 2-radical elements. Thus  $g$  is not 2-radical and we are done. Let now  $g$  be of order 4. Any 4A-element is the 11th power of 44A and hence belongs to  $B$ . The square of a 4B-element belongs to 2A [Wi]. Therefore 4B centralizes 2A and thus maps to a nonidentity element of  $B$ . According to [Wi], the 4th power of any element of order 16 belongs to 4C, hence 4C lies, say, in  $Fi'_{24}$ . Finally, 4D is the cube of 12J whose 4th power is 3C. Therefore 12J centralizes 3C and hence so does 4D. Thus 4D belongs to  $Th$ , and we are done.

*Pariahs*:  $J_1, J_3, J_4, Ru, O'N, Ly$ .

$J_1$ . The normalizer  $N = 19 \cdot 6$  of an element  $g$  of order 19 is the unique maximal subgroup of  $J_1$  containing  $g$ , and the above argument applies. If the order of  $g$  equals 7, its normalizer  $N$  equals  $7 \cdot 6$  and is also a maximal subgroup of  $J_1$  but is contained in another maximal subgroup of order 168. However, taking  $x \in N$  and  $y$  of order 3, we get  $a = [g, x] \in \langle g \rangle$  and  $b = [g, y]$  of order 15. Since  $b$  is outside of both above mentioned maximal subgroups, we have  $\langle a, b \rangle = J_1$ . The elements of order 11 belong to  $\text{PSL}_2(11)$ , and the elements of orders 2, 3 and 5 belong to  $A_5$ .



$J_3$ . The elements of orders 2 and 5 belong to  $A_5$ , those of orders 17 and 19 belong to  $\mathrm{PSL}_2(17)$  and  $\mathrm{PSL}_2(19)$ , respectively. Taking an element of order 9 in  $\mathrm{PSL}_2(17)$ , we obtain 3B as its cube, and taking an element of order 15 in  $\mathrm{PSL}_2(16)$ , we obtain 3A as its 5th power.

$J_4$ . For  $p = 43$  or  $29$ , the normalizer of  $g$  of order  $p$  is the unique maximal subgroup containing  $g$ , and we apply the above argument. The elements of order 37 lie in  $\mathrm{PSU}_3(11^2)$ . Elements of order 31 are contained in  $\mathrm{PSL}_2(32)$ , and elements of orders 3, 5, 7, and 23 lie in  $M_{24}$ . It remains to consider the classes 2A, 2B, 11A, 11B. The centralizers of each of 2A and 2B contain  $M_{22}$ , and we embed both 2A and 2B in  $M_{22}$  using the same argument as in the case  $M_{24}$  above. According to [J, Propositions 22 and 26], we have  $11A \in C(2B)$  and  $11B \in C(2A)$ , so they are both included in  $M_{22}$  too.

$Ru$ . The elements of orders 29 and 13 lie in the corresponding  $\mathrm{PSL}$ 's, and those of orders 7 and 3 lie in  $A_7$ . The information on alternating subgroups in [CCNPW, p. 126] gives 2B, 5A and 5B contained there. 2A appears as the square of an element of order 4 in  $A_6$ .

$O'N$ . The elements of order 31 lie in  $\mathrm{PSL}_2(31)$  and those of order 19 are contained in  $\mathrm{PSL}_3(7)$ . Elements of orders 11, 5, 3 and 2 lie in  $M_{11}$ . As to the classes 7A and 7B, the first appears as the square of an element of order 14 in  $\mathrm{PSL}_3(7)$ , and the second belongs to  $\mathrm{PSL}_2(7)$  [Wi85, Section 4, p. 471].

$Ly$ . For  $p = 67$  and  $37$  we use the same maximal subgroup argument as above. The elements of order 31 belong to  $G_2(5)$ , and hence to  $\mathrm{PSL}_3(5)$ , and those of orders 11, 7 and 2 belong to  $A_{11}$ . The classification of  $A_5$ 's [Wi84, Section 6, p. 407] shows that 3B and 5B are included in  $A_5$ . Both 3A and 5A lie in  $G_2(5)$ : they can be obtained as the 3th power of an element of order 9 and the 4th power of an element of order 20, respectively.

To finish the proof of the proposition, it remains to check all small groups of Lie type appearing in the above arguments. This was done by straightforward computations.

Proposition 9.1, and hence Theorem 1.15 and Theorem 1.4, are proved.  $\square$

## References

- [As] M. Aschbacher, *3-transposition groups*. Cambridge Tracts in Math. 124, Cambridge University Press, Cambridge 1997 [Zbl 0883.20010](#) [MR 1423599](#)
- [Ba] R. Baer, Engelsche Elemente Noetherscher Gruppen. *Math. Ann.* **133** (1957), 256–270. [Zbl 0078.01501](#) [MR 0086815](#)
- [BBGKP] T. Bandman, M. Borovoi, F. Grunewald, B. Kunyavskiĭ, and E. Plotkin, Engel-like characterization of radicals in finite dimensional Lie algebras and finite groups. *Manuscripta Math.* **119** (2006), 365–381. [Zbl 05027339](#) [MR 2223628](#)

- [BGGKPP1] T. Bandman, G.-M. Greuel, F. Grunewald, B. Konyavskii, G. Pfister, and E. Plotkin, Two-variable identities for finite solvable groups. *C. R. Acad. Sci. Paris, Ser. I* **337** (2003), 581–586. [Zbl 1047.20014](#) [MR 2017730](#)
- [BGGKPP2] T. Bandman, G.-M. Greuel, F. Grunewald, B. Konyavskii, G. Pfister, and E. Plotkin, Identities for finite solvable groups and equations in finite simple groups. *Compositio Math.* **142** (2006), 734–764. [Zbl 1112.20016](#) [MR 2231200](#)
- [Bou] N. Bourbaki, *Groupes et algèbres de Lie*. Ch. I–III, Hermann, Paris, 1971/1972; Ch. IV–VI, Hermann, Paris, 1968. [Zbl 0213.04103](#) [Zbl 0244.22007](#) [Zbl 0186.33001](#) [MR 0271276](#) [MR 0573068](#) [MR 0240238](#)
- [BW] R. Brandl and J. S. Wilson, Characterization of finite soluble groups by laws in a small number of variables. *J. Algebra* **116** (1988), 334–341. [Zbl 0651.20039](#) [MR 0953155](#)
- [BWW] J. N. Bray, J. S. Wilson, and R. A. Wilson, A characterization of finite soluble groups by laws in two variables. *Bull. London Math. Soc.* **37** (2005), 179–186. [Zbl 1075.20008](#) [MR 2119017](#)
- [BrW] J. N. Bray and R. A. Wilson, Explicit representations of maximal subgroups of the Monster. *J. Algebra* **300** (2006), 834–857. [Zbl 1100.20019](#) [MR 2228224](#)
- [Ca1] R. W. Carter, *Simple Groups of Lie Type*. Pure Appl. Math. 28, John Wiley & Sons, London 1972. [Zbl 0248.20015](#) [MR 0407163](#)
- [Ca2] R. W. Carter, *Finite Groups of Lie Type. Conjugacy Classes and Complex Characters*. Pure Appl. Math. (N. Y.), John Wiley & Sons, New York 1985. [Zbl 0567.20023](#) [MR](#)
- [CEG] V. Chernousov, E. W. Ellers, and N. Gordeev, Gauss decomposition with prescribed semisimple part: short proof. *J. Algebra* **229** (2000), 314–332. [Zbl 0964.20024](#) [MR 1765783](#)
- [CCNPW] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups*. Clarendon Press, Oxford 1985. [Zbl 0568.20001](#) [MR 0827219](#)
- [Cu] R. T. Curtis, On subgroups of  $\cdot O$ , II. Local structure. *J. Algebra* **63** (1980), 413–434. [Zbl 0427.20010](#) [MR 0570721](#)
- [EG1] E. W. Ellers and N. Gordeev, Gauss decomposition with prescribed semisimple part in classical Chevalley groups. *Comm. Algebra* **22** (1994), 5935–5950; Gauss decomposition with prescribed semisimple part in Chevalley groups. II. Exceptional cases. *ibid.* **23** (1995), 3085–3098; Gauss decomposition with prescribed semisimple part in Chevalley groups. III. Finite twisted groups. *ibid.* **24** (1996), 4447–4475. [Zbl 0821.20028](#) [Zbl 0838.20054](#) [Zbl 0887.20022](#) [MR 1298758](#) [MR 1332168](#) [MR 1421200](#)
- [EG2] E. W. Ellers and N. Gordeev, On the conjectures of J. Thompson and O. Ore. *Trans. Amer. Math. Soc.* **350** (1998), 3657–3671. [Zbl 0910.20007](#) [MR 1422600](#)
- [Fi] B. Fischer, Finite groups generated by 3-transpositions, I. *Invent. Math.* **12** (1971), 232–246. [Zbl 0232.20040](#) [MR 0294487](#)
- [Gord] N. Gordeev, A theorem of Gow for finite reductive groups. Preprint.

- [GS] N. Gordeev and J. Saxl, Products of conjugacy classes in Chevalley groups, I: Extended covering numbers. *Israel J. Math.* **130** (2002), 207–248. [Zbl 1007.20041](#) [MR 1919378](#)
- [Gor1] D. Gorenstein, *Finite Groups*. Harper, New York 1968. [Zbl 0185.05701](#) [MR 0231903](#)
- [Gor2] D. Gorenstein, *Finite Simple Groups. An Introduction to Their Classification*. University Ser. in Math., Plenum Press, New York 1982. [Zbl 0483.20008](#) [MR 0698782](#)
- [GLS] D. Gorenstein, R. Lyons, and R. Solomon, *The Classification of the Finite Simple Groups*. Number 3, Math. Surveys Monogr. 40 (3), Amer. Math. Soc., Providence, RI, 1998. [Zbl 0890.20012](#) [MR 1490581](#)
- [Gow] R. Gow, Commutators in finite simple groups of Lie type. *Bull. London Math. Soc.* **32** (2000), 311–315. [Zbl 1021.20012](#) [MR 1750469](#)
- [GKPS] R. Guralnick, B. Kunyavskii, E. Plotkin, and A. Shalev, Thompson-like characterizations of the solvable radical. *J. Algebra* **300** (2006), 363–375. [Zbl 1118.20021](#) [MR 2228653](#)
- [H] B. Huppert, *Endliche Gruppen*, I. Grundlehren Math. Wiss. 134, Springer-Verlag, Berlin, New York 1979. [Zbl 0412.20002](#) [MR 0224703](#)
- [J] Z. Janko, A new finite simple group of order  $86 \cdot 775 \cdot 571 \cdot 046 \cdot 077 \cdot 562 \cdot 880$  which possesses  $M_{24}$  and the full covering group of  $M_{22}$  as subgroups. *J. Algebra* **42** (1976), 564–596. [Zbl 0344.20010](#) [MR 0432751](#)
- [KLM] G. Kemper, F. Lübeck, and K. Magaard, Matrix generators for the Ree groups  ${}^2G_2(q)$ . *Comm. Algebra* **29** (2001), 407–413. [MR 1842506](#)
- [No] S. P. Norton, Anatomy of the Monster, I. In *The Atlas of Finite Groups: Ten Years On*, London Math. Soc. Lecture Notes Ser. 249 Cambridge University Press, Cambridge 1998, 198–214. [Zbl 0908.20008](#) [MR 1647423](#)
- [NW] S. P. Norton and R. A. Wilson, Maximal subgroups of the Harada–Norton group. *J. Algebra* **103** (1986), 362–376. [Zbl 0595.20017](#) [MR 0860712](#)
- [Nu] Ya. N. Nuzhin, The structure of groups of Lie type of rank 1. *Mat. Zametki* (2) **36** (1984), 149–158; English transl. *Math. Notes* **36** (1984), 565–570. [Zbl 0561.20034](#) [MR 0759428](#)
- [Pla] V. P. Platonov, Engel elements and radical in PI-algebras and topological groups. *Dokl. Akad. Nauk SSSR* **161** (1965), 288–291; English transl. *Soviet Math. Dokl.* **6** (1965), 412–415. [Zbl 0136.29503](#) [MR 173711](#)
- [Plo] B. I. Plotkin, Notes on Engel groups and Engel elements in groups. Some generalizations. *Izv. Ural. Univ. Ser. Mat. Mekh.* **36** (7) (2005), 153–166. [MR 2190949](#) [arXiv:math.GR/0406100](#)
- [Ro] D. J. S. Robinson, *A Course in the Theory of Groups*. Grad. Texts in Math. 80, Springer-Verlag, New York 1996. [Zbl 0836.20001](#) [MR 1357169](#)
- [SS] T. Springer and R. Steinberg, *Conjugacy classes*. Seminar on Algebraic Groups and Related Finite Groups, Lecture Notes Math. 131, Springer-Verlag, Berlin 1970, 167–266. [Zbl 0249.20024](#) [MR 0268192](#)

- [St] R. Steinberg, *Lectures on Chevalley Groups*. Notes prepared by John Faulkner and Robert Wilson, Yale University, New Haven, Conn., 1968. [MR 0466335](#)
- [Th] J. Thompson, Non-solvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.* **74** (1968), 383–437. [Zbl 0159.30804](#) [MR 0230809](#)
- [Wi83] R. A. Wilson, The maximal subgroups of Conway's group  $Co_1$ . *J. Algebra* **85** (1983), 144–165. [Zbl 0525.20009](#) [MR 0723071](#)
- [Wi84] R. A. Wilson, The subgroup structure of the Lyons group. *Math. Proc. Cambridge Philos. Soc.* **95** (1984), 403–409. [Zbl 0542.20004](#) [MR 0755827](#)
- [Wi85] R. A. Wilson, The maximal subgroups of the O'Nan group. *J. Algebra* **97** (1985), 467–473. [Zbl 0577.20012](#) [MR 0812997](#)
- [Wi93] R. A. Wilson, More on maximal subgroups of the Baby Monster. *Arch. Math.* **61** (1993), 497–507. [Zbl 0823.20019](#) [MR 1254061](#)
- [Wi] R. A. Wilson et al., *A world-wide-web Atlas of group representations*. <http://brauer.maths.qmul.ac.uk/Atlas/>

Received November 5, 2006; revised April 11, 2007

N. Gordeev, Department of Mathematics, Herzen State Pedagogical University,  
48 Moika Embankment, 191186, St. Petersburg, Russia

E-mail: [nickgordeev@mail.ru](mailto:nickgordeev@mail.ru)

F. Grunewald, Mathematisches Institut der Heinrich-Heine-Universität Düsseldorf,  
Universitätsstr. 1, 40225 Düsseldorf, Germany

E-mail: [grunewald@math.uni-duesseldorf.de](mailto:grunewald@math.uni-duesseldorf.de)

B. Konyavskii, Department of Mathematics, Bar-Ilan University, 52900 Ramat Gan, Israel

E-mail: [kunyav@macs.biu.ac.il](mailto:kunyav@macs.biu.ac.il)

E. Plotkin, Department of Mathematics, Bar-Ilan University, 52900 Ramat Gan, Israel

E-mail: [plotkin@macs.biu.ac.il](mailto:plotkin@macs.biu.ac.il)