

## TWO-VARIABLE IDENTITIES IN GROUPS AND LIE ALGEBRAS

F. Grunewald, B. Kunyavskii, D. Nikolova, and E. Plotkin

UDC 512.546.6;  
512.8.15

We study two-variable Engel-like relations and identities characterizing finite-dimensional solvable Lie algebras and, conjecturally, finite solvable groups and introduce some invariants of finite groups associated with such relations. Bibliography: 29 titles.

### 1. MOTIVATION

Our primary interest in the problems discussed in the present paper came from a paper by Segev [25], where the Margulis–Platonov conjecture had been related to some properties of the commuting graph of a finite simple group. (Given a finite group  $F$ , its commuting graph  $\Gamma(F)$  has vertices indexed by the elements of  $F$  different from 1;  $x, y \in F$  are joined by an edge if and only if they commute.) In a more recent paper [26], the expected properties of this graph have been proved.

In its simplest form, the Margulis–Platonov conjecture asserts that if  $G$  is any (absolutely almost) simple linear algebraic group defined over a number field  $k$ , then the group of rational points  $G(k)$  contains no noncentral normal subgroups if and only if the same is true for all groups  $G(k_v)$ , where  $v$  runs over all places of  $k$  and  $k_v$  stands for the completion of  $k$  at  $v$  (see [22, 9.1]). The most difficult case of this conjecture is that of anisotropic groups of type  $A_n$ . In the case of the inner forms, Potapchik and Rapinchuk [24] reduced the conjecture to a purely algebraic statement that the multiplicative group of any finite-dimensional division  $k$ -algebra has no non-Abelian finite simple quotients. For this purpose, Segev proved [25] that if  $D$  is a finite-dimensional division algebra over an arbitrary field and  $F$  is a finite simple non-Abelian group whose commuting graph  $\Gamma(F)$  is either balanced (see [25] for the definition) or is of diameter greater than 4, then  $F$  cannot be a quotient of  $D^*$ . In [26], it is proved that the commuting graph of any finite non-Abelian simple group is either balanced or of diameter greater than 4. This completes the proof.

All the above shows that  $\Gamma(F)$  is a powerful invariant of  $F$ . After Segev's lecture on this topic, B. Plotkin suggested two natural generalizations of the commuting graph of a group. Namely, it is natural to consider graphs of nilpotency and solvability of an arbitrary group  $G$ . To define them, we need to formulate conditions of nilpotency and solvability as two-variable relations between the elements of  $G$ . This is done in Sec. 2. In Sec. 3, we consider Lie-algebraic analogs of these conditions. In Sec. 4, we focus on the case of linear algebraic groups and groups of their rational points. In Sec. 5, we return to the case of finite groups, which was the main motivation for this paper.

**Notation.** If  $G$  is a group and  $x, y \in G$ , let  $[x, y] = x^{-1}y^{-1}xy$ . If  $L$  is a Lie algebra and  $x, y \in L$ , we use the same symbol  $[x, y]$  for the Lie product.

### 2. NEW INVARIANTS OF FINITE GROUPS

Our primary goal is to introduce some new invariants of a group  $G$  associated with two-variable relations between elements of  $G$ .

**Definition 2.1.** Let  $G$  be an arbitrary group, and let  $\rho$  be a binary relation on  $G$ . We define a (directed) graph  $\Gamma^+ = \Gamma_\rho^+(G)$  (the  $\rho$ -graph of  $G$ ) as follows: the vertices of  $\Gamma^+$  are indexed by the elements of  $G$  different from 1, and vertices  $g$  and  $h$  form an edge directed from  $g$  to  $h$  if and only if  $g \neq h$  and  $g \rho h$  holds. We denote by  $\Gamma$  the nondirected graph obtained from  $\Gamma^+$  by forgetting orientation and deleting multiple edges.

**Remark.** If  $\rho$  is symmetric, we only consider the nondirected graph  $\Gamma_\rho(G)$ .

**Example.** If  $\rho$  is the commuting relation (i.e.,  $g \rho h$  if and only if  $gh = hg$ ), we obtain the commuting graph of  $G$  studied in [25].

First we consider “nilpotency relations.” Denote Engel words by  $v_1 = v_1(x, y) = [x, y]$ ,  $v_2 = [v_1, y], \dots, v_n = [v_{n-1}, y], \dots$

---

Published in *Zapiski Nauchnykh Seminarov POMI*, Vol. 272, 2000, pp. 161–176. Original article submitted October 11, 2000.

**Definition 2.2.** Let  $G$  be an arbitrary group. We say that elements  $g, h \in G$  are in  $n$ -Engel relation  $\nu_n$  if  $v_n(g, h) = 1$ . Elements  $g$  and  $h$  are said to be in nilpotency relation  $\nu$  if they are in  $n$ -Engel relation for some  $n$ .

Recall that a finite group  $G$  is nilpotent if and only if the identity  $v_n(x, y) \equiv 1$  holds in  $G$  for some  $n$ , or, in terms of the above definition, if and only if  $g\nu h$  holds for all  $g, h \in G$ . Note that  $v_k \equiv 1$  implies  $v_l \equiv 1$  for all  $l > k$ .

**Definition 2.3.** The graph  $\Gamma_\nu(G)$  (respectively,  $\Gamma_\nu^+(G)$ ) is called the nilpotency graph (respectively, the directed nilpotency graph) of  $G$ . The diameters of these graphs are denoted by  $d_\nu(G)$  and  $d_\nu^+(G)$ , respectively. (If there are vertices  $g$  and  $h$  with no path from  $g$  to  $h$ , the diameter is defined to be infinite.)

**Problem 2.4.** To investigate nilpotency graphs of finite simple groups and to estimate their diameters.

We now turn to “solvability relations.” Here we immediately encounter the following problem.

**Problem 2.5.** Find a sequence of words  $\{e_n(x, y)\}_{n=1}^\infty$  in two variables  $x$  and  $y$  such that a finite group  $G$  is solvable if and only if for some  $n$  the identity  $e_n \equiv 1$  holds in  $G$ .

**Remark.** Similarly to the nilpotency case, we require that the identity  $e_k \equiv 1$  would imply  $e_l \equiv 1$  for all  $l > k$ .

With such a sequence at our disposal, we could define the solvability relation in  $G$  and the corresponding graphs by repeating, word for word, Definitions 2.2–2.3.

There is strong evidence that Problem 2.5 has a positive solution, and finite solvable groups can be characterized by two-variable identities.

**Theorem 2.6** (see [28, 8]). Let  $G$  be a finite group in which every two elements generate a solvable subgroup. Then  $G$  is solvable.

However, Theorem 2.6 does not provide any explicit two-variable laws for finite solvable groups. We present several candidates for such  $e_n$ ’s.

**Definition 2.7.** Let  $\{e_n(x, y)\}_{n=1}^\infty$  be defined by one of the following three formulas:

$$\begin{aligned} e_1 &= [x, y], \\ e'_1 &= [e_1, x], \quad e''_1 = [e_1, y], \quad e_2 = [e'_1, e''_1], \dots \\ e'_n &= [e_n, x], \quad e''_n = [e_n, y], \quad e_{n+1} = [e'_n, e''_n], \dots \end{aligned} \tag{1}$$

$$e_1 = [x, y], e_2 = [xe_1x^{-1}, ye_1y^{-1}], \dots, e_{n+1} = [xe_nx^{-1}, ye_ny^{-1}], \dots \tag{2}$$

$$\begin{aligned} e'_1 &= x, e''_1 = y, e_1 = [e'_1, e''_1], \dots \\ e'_{n+1} &= [[e'_n, e''_n], e'_n], e''_{n+1} = [[e''_n, e'_n], e''_n], e_{n+1} = [e'_{n+1}, e''_{n+1}], \dots \end{aligned} \tag{3}$$

We call sequences (1)–(3) reasonable.

Note that for all reasonable sequences,  $e_k \equiv 1$  implies  $e_l \equiv 1$  for all  $l > k$ .

**Remark.** There is a natural way to produce reasonable sequences generalizing (2). Namely, let  $w$  be a word in  $x, y, x^{-1}, y^{-1}$ . Define

$$e_1^w = w, e_{n+1}^w = [xe_n^wx^{-1}, ye_n^wy^{-1}], \dots$$

A clever choice of  $w$  might lead to a sequence with good properties. We shall discuss the matter in detail in our forthcoming paper.

**Definition 2.8.** Fix a reasonable sequence  $\{e_i\}$ . Let  $G$  be an arbitrary group. We say that elements  $g, h \in G$  are in relation  $\sigma_n$  (with respect to  $\{e_i\}$ ) if  $e_n(g, h) = 1$ . Elements  $g$  and  $h$  are said to be in solvability relation  $\sigma$  if and only if they are in relation  $\sigma_n$  for some  $n$ . We call the  $\sigma$ -graph  $\Gamma_\sigma(G)$  (respectively,  $\Gamma_\sigma^+(G)$ ) the solvability graph (respectively, the directed solvability graph) of  $G$ .

To justify the above definition, one must prove the following analog of the Engel property.

**Conjecture 2.9** (B. Plotkin). *Let  $\{e_i\}$  be a reasonable sequence. A finite group  $G$  is solvable if and only if for some  $n$  the identity  $e_n \equiv 1$  holds in  $G$ .*

Clearly, if  $G$  is solvable of derived length  $n$ , then  $e_n \equiv 1$  holds in  $G$ .

**Remark.** There is another way to define nilpotency and solvability relations:  $g, h \in G$  are in relation  $\nu$  (respectively,  $\sigma$ ) if and only if the subgroup of  $G$  generated by  $g$  and  $h$  is nilpotent (respectively, solvable). Such relations have the advantage of being symmetric and the disadvantage of being less constructive. We do not consider them in the present paper. We refer the reader to [23] for yet another definition of the solvability graph and another relationship with abstract algebraic geometry over groups.

There are several results concerning the characterization of solvable groups in terms of two-variable identities [19, 20, 5]. Namely, it was proved in [19, 20] that if a finite group  $G$  satisfies the identity  $v_2 \equiv v_n$  for some  $n$ , where  $\{v_i\}$  is the sequence of Engel words, then  $G$  is solvable. However, it is easy to find a solvable group satisfying no identity of the form  $v_2 \equiv v_n$ . For example, as  $G$  we take a finite nilpotent group of class 3 such that the identity  $v_2 \equiv 1$  does not hold in  $G$ . Since  $v_3 \equiv 1$ , the group  $G$  cannot satisfy any identity of the form  $v_2 \equiv v_m$ . However,  $G$  is solvable.

In [5], it was proved that the identity  $v_3 \equiv v_n$  can hold in certain finite simple groups such as  $\mathrm{PSL}(2, 4)$ ,  $\mathrm{PSL}(2, 8)$ , etc. Let us also mention a pioneering result of N. Gupta [10]: any finite group satisfying the identity  $v_1 \equiv v_n$  is Abelian.

At this point, let us introduce some new invariants of finite groups. Our first remark is that, given any infinite sequence of distinct words in  $m$  variables  $\{w_i(x_1, \dots, x_m)\}_{i=1}^{\infty}$ , any finite group  $G$  satisfies a law of the type

$$w_k(x_1, \dots, x_m) \equiv w_l(x_1, \dots, x_m).$$

for some  $k$  and  $l$ . (Indeed, the set of values of the  $w_i$ 's is finite.)

The next definition goes back to [11]. It generalizes the notion of Engel depth (cf., [4, 5]).

**Definition 2.10.** *A pair  $(k, l)$  for which the identity  $v_k(x, y) \equiv v_l(x, y)$  holds, with minimal  $k + l$ , is called the Engel invariant of  $G$ .*

**Remark.** To justify the above definition, one needs to check that the pair  $(k, l)$  with the required properties is unique. Indeed, suppose we have two Engel identities in  $G$ :  $v_k \equiv v_l$  and  $v_m \equiv v_n$  with  $k < m < n < l$  and  $k + l = m + n$  minimal with this property.

We have  $v_m(x, y) = v_n(x, y)$  for all  $x, y$ . Plug in  $v_{l-n}(x, y)$  instead of  $x$ . We obtain  $v_{l-n+m}(x, y) = v_l(x, y)$  for all  $x, y$ . Hence  $v_k(x, y) = v_{l-n+m}(x, y)$  for all  $x, y$ . Therefore, because of the minimality of  $k + l$ , we have  $k + (l - n + m) \geq k + l$ , i.e.,  $m - n \geq 0$ , a contradiction. The Engel invariant is thus well defined.

This remark also shows that the number  $k$  in Definition 2.10 coincides with the Engel depth of  $G$  as defined in [4, 5]. However, the second parameter  $l$  is also important as the following beautiful result shows [11, Theorem 4.3]: with the notation of Definition 2.10, if  $k + l$  is odd then  $G$  is solvable.

**Problem 2.11.** *To compute Engel invariants for special classes of finite groups.*

In [18], Engel invariants were computed in some groups, classes of groups, and varieties of groups: some groups of small order; the class of dihedral groups  $D_p$ , where  $p$  is an odd prime; the solvable locally finite varieties of groups  $A_k A_l$  for  $k$  and  $l$  powers of one and the same prime number  $p$ , and for  $k$  and  $l$  coprime integers; infinite series of simple groups (the alternating groups  $A_n$  for  $n > 5$  and the special projective groups  $\mathrm{PSL}(2, q)$  for some of the first groups in the series).

One may consider analogs of Definition 2.10 and Problem 2.11 with the Engel sequence replaced by one of the reasonable (in the sense of Definition 2.7) sequences.

**Definition 2.12.** *Let  $\{e_i\}$  be a reasonable sequence. A pair  $(k, l)$  for which the identity  $e_k(x, y) \equiv e_l(x, y)$  holds, with minimal  $k + l$ , is called a  $\sigma$ -invariant of  $G$ . If there are several such pairs, we choose among them the pair with minimal  $k$  and define it to be  $\sigma(G)$ .*

**Problem 2.13.** *To compute  $\sigma$ -invariants for special classes of finite groups.*

### 3. LIE-ALGEBRAIC ANALOGS

On replacing commutators by Lie products (and 1 by 0), we obtain sequences similar to (1)–(3) for Lie algebras. We also call them reasonable. Here the situation is much more clear (at least, in the finite-dimensional case). We restrict our consideration to the Lie analog of sequence (1).

**Theorem 3.1.** Let  $L$  be a finite-dimensional Lie algebra over an infinite field  $k$  of characteristic  $p > 5$ . Let  $\{e_i\}$  be defined by formulas (1). Then  $L$  is solvable if and only if for some  $n$  the identity  $e_n \equiv 0$  holds in  $L$ .

*Proof.* Obviously, if  $L$  is solvable, then it satisfies an identity of the form  $e_n(x, y) \equiv 0$ , because for any  $X, Y \in L$  the value  $e_n(X, Y)$  belongs to the corresponding term of the derived series. Conversely, let  $L$  satisfy the identity  $e_n \equiv 0$ . First assume that  $k$  is algebraically closed. If  $L$  is not solvable, then  $L^{\text{ss}} = L/\text{rad}(L)$  is semisimple and nonzero (here  $\text{rad}(L)$  denotes the solvable radical of  $L$ , i.e., its maximal solvable ideal). If  $\text{char}(F) = 0$ , denote by  $\{E_\alpha, H_\alpha, E_{-\alpha}\}$  the standard basis of  $sl_2$ . Then  $[E_\alpha, E_{-\alpha}] = H_\alpha$ ,  $[H_\alpha, E_\alpha] = 2E_\alpha$ , and  $[H_\alpha, E_{-\alpha}] = -2E_{-\alpha}$ . Set  $x = E_\alpha$  and  $y = E_{-\alpha}$ . Then

$$\begin{aligned} e_1 &= H_\alpha, & e'_1 &= 2E_\alpha, & e''_1 &= -2E_{-\alpha}, \\ e_2 &= -4H_\alpha, & \dots & & & \end{aligned}$$

i.e.,  $e_n = mH_\alpha$  with  $m \neq 0$ . Thus, for any  $n$  we have  $e_n(E_\alpha, E_{-\alpha}) \neq 0$ .

Now let  $\text{char}(k) = p > 5$ . First assume that  $L$  is restricted (see [27, 2.1] for the definition; we refer to the same work for all background material in modular Lie algebras). Then we can use the classification theorem of [2] in order to mimic the proof in characteristic zero. To be more precise, [2] says that all simple restricted Lie algebras are given by the list predicted by the Kostrikin–Shafarevich conjecture. One can then verify that each such algebra contains  $sl_2$ . For the algebras of classical type this is obvious. As to the algebras of Cartan type, one must consider them as graded Lie algebras (see [27, Chapter 4]) and note that the zero component  $L_0$  contains  $sl_2$ . Indeed,  $S(n; 1)_0 \cong sl_n$  ([27, Proposition 3.3.4]),  $H(2r; 1)_0 \cong sp_{2r}$  ([27, Proposition 4.4.4]),  $K(2r+1; 1)_0$  contains  $sp_{2r}$  ([27, Exercise 4.5.3]), and  $W(n; 1)_0 \cong gl_n$  ([27, Proposition 2.2.4]). In this last case, for  $n = 1$  one must consider the algebra  $L_{-1} \oplus L_0 \oplus L_1$ ; one can show that it is isomorphic to  $sl_2$ .

If  $L$  is not restricted, one needs more subtle arguments.

**Lemma 3.2.** Every simple Lie algebra  $L$  defined over a field of characteristic  $p > 5$  contains a subalgebra  $S$  with quotient isomorphic to  $sl_2$ .<sup>1</sup>

*Proof.* Assume the contrary. Let  $L$  denote a counterexample of minimal dimension to the lemma. Let  $L^\circ$  denote a maximal subalgebra of  $L$ . We wish to show that  $L^\circ$  is solvable. If not, then  $L^{\text{ss}} = L^\circ/\text{rad}(L^\circ)$  is a nonzero semisimple Lie algebra. By [1, Theorem 9.3],  $L^{\text{ss}}$  contains a simple algebra  $S$ . Let  $S_1 = \pi^{-1}(S)$  be the preimage of  $S$  with respect to the natural projection  $\pi: L^\circ \rightarrow L^{\text{ss}}$ ; we have  $S_1/\ker \pi \cong S$ . Since  $\dim S < \dim L$ , there is a subalgebra  $T \subseteq S$  and an ideal  $J$  in  $T$  such that  $T/J \cong sl_2$ . Denote  $T_1 = \pi^{-1}(T)$  and  $J_1 = \pi^{-1}(J)$ . We have  $T_1/J_1 \cong sl_2$ , a contradiction. We have thus proved that  $L^\circ$  is solvable. By [29, Corollary 1.4],  $L$  must be isomorphic either to  $sl_2$  or to the Zassenhaus algebra  $W(1; m)$ . In the first case, we are done. In the second case,  $L$  is graded, and we set  $S = L_{-1} \oplus L_0 \oplus L_1$ . Each of the three components is one-dimensional, and a straightforward computation using the table of structure constants shows that  $S \cong sl_2$ . The lemma is proved.  $\square$

Let us continue the proof of the theorem. We have a Lie algebra  $L$  satisfying the identity  $e_n(x, y) \equiv 0$ . We wish to prove that  $L$  is solvable. Assume the contrary. Then, arguing as in the proof of Lemma 3.2 (i.e., considering  $L/\text{rad}(L)$  and using [1, Theorem 9.3]), we conclude that  $L$  has a simple subalgebra  $S$ . From Lemma 3.2 it follows that  $S$  (and hence  $L$ ) has a subfactor isomorphic to  $sl_2$ . Since identities remain true in sub- and quotient algebras,  $e_n \equiv 0$  must hold in  $sl_2$ , a contradiction. We have thus proved the “if” part of the theorem in the case where  $k$  is algebraically closed.

Now let  $k$  be an arbitrary infinite field, and suppose that  $L$  is a Lie algebra over  $k$  satisfying an identity  $w(x, y) \equiv 0$ , where  $w$  stands for one of the  $e_n$ ’s. We wish to prove that the identity  $w(x, y) \equiv 0$  also holds in the Lie algebra  $\bar{L} = L \otimes_k \bar{k}$  defined over an algebraic closure  $\bar{k}$  of  $k$ . Indeed, let  $\{E_1, \dots, E_d\}$  denote a  $k$ -basis of  $L$ . On writing arbitrary  $x, y \in L$  with respect to this basis,  $x = \sum \alpha_i E_i$ ,  $y = \sum \beta_i E_i$ , we translate the identity  $w(x, y) \equiv 0$  into identities of the form

$$P_i(\alpha_1, \dots, \alpha_d, \beta_1, \dots, \beta_d) = 0, \quad i = 1, \dots, d,$$

where  $P_i$  are polynomials. Since all the values of each  $P_i$  are zero and  $k$  is infinite, we conclude that the  $P_i$  are zero polynomials (see, for example, [15, Chapter IV, §1, Corollary 1.7]). Now let  $\bar{x}, \bar{y} \in \bar{L}$  be arbitrary elements. On writing them with respect to the same basis  $\{E_i\}$  (with coefficients from  $\bar{k}$ ) and plugging them into the expression for  $w(\bar{x}, \bar{y})$ , we obtain the same polynomials  $P_i$  as the coefficients of the  $E_i$ . But we have already proved that they are zero. Hence  $w(\bar{x}, \bar{y}) = 0$ .

<sup>1</sup>A. Premet informed us that one can modify the proof to be valid for all  $p > 2$ .

The theorem is proved.  $\square$

Note one more result in the same spirit (cf. [10, 11, 19, 20, 5] for the group case). Recall that  $\{v_i\}$  is the Engel sequence,  $v_i(x, y) = [[[x, y], y] \dots y]$  (for brevity, we denote this expression by  $[x, y_i]$ ).

**Proposition 3.3.** *Let  $L$  be a finite-dimensional Lie algebra over a field of characteristic different from 2 such that the identity  $v_k \equiv v_l$  holds in  $L$ . Then  $L$  is solvable. Moreover, if  $L$  satisfies  $v_1 \equiv v_l$ , then  $L$  is Abelian.*

*Proof.* As in the preceding theorem, we can reduce this to the case where the ground field is algebraically closed. First consider the characteristic zero case. Again, if  $L$  is not solvable, then  $L^{\text{ss}} = L/\text{rad}(L)$  is nonzero and contains  $sl_2$ . Set  $x = H_\alpha$  and  $y = E_\alpha$ . We have  $v_1 = 2E_\alpha$ ,  $v_2 = 4E_\alpha, \dots$ ; thus  $v_k \equiv v_l$  leads to  $2^k E_\alpha = 2^l E_\alpha$ , a contradiction. In the positive characteristic, we just reproduce the arguments from Theorem 3.1.

Now let  $v_1 \equiv v_l$ . We proceed by induction on  $\dim L$ . If  $\dim L = 1$ , then  $L$  is Abelian. Suppose that all subalgebras of dimension less than  $n = \dim L$  are Abelian. By the first part of the proposition,  $L$  is solvable. Hence  $L' = [L, L]$  is of dimension less than  $n$  and therefore is Abelian. We must prove that  $L' = 0$ . Take any  $[x, z] \in L'$ . By assumption,  $[x, z] = [x, z_l]$ . Let  $z = [x, y]$ . Then  $[x, [x, y]] = [x, [x, y]_l] = 0$  since  $L'$  is Abelian. Therefore,  $[[x, y], x] = 0$  and hence  $[[y, x], x] = 0$  and  $[y, x_l] = 0$ . Applying our assumption once again, we obtain  $[y, x] = 0$ , so that  $L' = 0$  and thus  $L$  is Abelian.  $\square$

**Remark.** As in the case of finite groups, one can note that the identity  $v_2 \equiv v_l$  gives only a sufficient condition for a finite-dimensional Lie algebra to be solvable.

#### 4. IDENTITIES IN LINEAR GROUPS

One of the most promising approaches to the proof of Conjecture 2.9 is related to the study of identities in finite linear groups. To be more precise, the following question seems to be critical: let  $\{e_i\}$  denote one of the reasonable sequences (see formulas (1)–(3)), and let  $G = \text{PSL}(2, p)$ ,  $p > 3$ ; is it true that neither of the formulas for  $e_n$  is an identity in  $G$ ? (See the next section for more details.) It is known [21; 17, Corollary 52.12] that any finite group  $G$  has a finite basis of identities, but for  $\text{PSL}(2, p)$  explicit bases are known only for  $p \leq 13$  (see [6] and the references therein). Clearly, the identities in  $\text{PSL}(2, p)$  heavily depend on  $p$ , because  $\text{PSL}(2, \mathbb{Z})$  has no identities at all. Thus, looking at  $\mathcal{G} = \mathcal{PSL}(2, \cdot)$  as a group scheme, one can say that different values of  $\mathcal{G}$  have different identities. On the other hand, if an affine group scheme  $\mathcal{G}$  is assumed to be either Abelian, or nilpotent, or solvable, then all its values inherit the corresponding identities. Therefore, given a linear group  $G \subset \text{GL}(n, k)$  isomorphic to the group  $\mathcal{G}(k)$  of  $k$ -rational points of an affine group scheme  $\mathcal{G}$ , it is important to distinguish its “structural” identities (i.e., coming from  $\mathcal{G}$ ) from those arising from the special choice of  $k$ .

Now we make all above considerations more precise. First introduce some notation. Given an affine group scheme  $\mathcal{G}$ , we denote

- $\mu: \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}$ , multiplication,
- $i: \mathcal{G} \rightarrow \mathcal{G}$ , inversion,
- $e: \mathcal{E} \rightarrow \mathcal{G}$ , unit (where  $\mathcal{E} = \{e\}$  is the final object in the category of affine group schemes),
- $c: \mathcal{G} \rightarrow \mathcal{G}$ , constant morphism,  $c(g) = e$ , (i.e.,  $c: \mathcal{G} \rightarrow \mathcal{E} \xrightarrow{e} \mathcal{G}$ , where  $\mathcal{G} \rightarrow \mathcal{E}$  is a unique morphism from  $\mathcal{G}$  to  $\mathcal{E}$ ),
- $\text{id}: \mathcal{G} \rightarrow \mathcal{G}$ , identity,
- $t: \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G} \times \mathcal{G}$ , transposition, i.e.,  $t = (\text{pr}_2, \text{pr}_1)$ .

We wish to define the commutator  $u: \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}$ . Let  $\tilde{\mu}: \mathcal{G} \times \mathcal{G} \times \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}$  be the composition  $(\mathcal{G} \times \mathcal{G}) \times (\mathcal{G} \times \mathcal{G}) \xrightarrow{\mu \times \mu} \mathcal{G} \times \mathcal{G} \xrightarrow{\mu} \mathcal{G}$ . We then define  $u$  as the composite morphism  $u: \mathcal{G} \times \mathcal{G} \xrightarrow{(i \times i, \text{id} \times \text{id})} \mathcal{G} \times \mathcal{G} \times \mathcal{G} \times \mathcal{G} \xrightarrow{\tilde{\mu}} \mathcal{G}$ .

**Observation.** A group scheme  $\mathcal{G}$  is commutative if and only if  $u = c$ .

**Remark.** Of course, one can express the commutativity condition without using commutators, just saying that  $\mu \circ t = \mu$ .

We now want to generalize the above construction. We define, by induction,

$$\begin{aligned} e_1 &= u = [x, y] = x^{-1} y^{-1} x y, \dots \\ e_{n+1} &= [[e_n, x], [e_n, y]], \dots \end{aligned} \tag{4}$$

More formally, we first define  $e'_n = [e_n, x]$  and  $e''_n = [e_n, y]$  as follows:

$$\begin{aligned} e'_n: \mathcal{G} \times \mathcal{G} &\xrightarrow{(e_n, \text{pr}_1)} \mathcal{G} \times \mathcal{G} \xrightarrow{u} \mathcal{G}, \\ e''_n: \mathcal{G} \times \mathcal{G} &\xrightarrow{(e_n, \text{pr}_2)} \mathcal{G} \times \mathcal{G} \xrightarrow{u} \mathcal{G}. \end{aligned} \tag{5}$$

Then  $e_{n+1}$  is defined as the composite morphism

$$e_{n+1}: \mathcal{G} \times \mathcal{G} \xrightarrow{(e'_n, e''_n)} \mathcal{G} \times \mathcal{G} \xrightarrow{u} \mathcal{G}.$$

The other two reasonable sequences (see formulas (2)–(3)) can be defined in a similar way.

**Proposition 4.1.** *Let  $\mathcal{G}$  be a connected affine algebraic group over a field  $k$ . Then  $\mathcal{G}$  is solvable if and only if  $e_n = c$  for some  $n \geq 1$ .*

*Proof. Necessity.* We prove by induction that the image of  $e_n$  lies in the  $n$ th derived subgroup  $D^n\mathcal{G}$  of  $\mathcal{G}$ . For  $n = 1$  this is obvious. Since  $D^n\mathcal{G}$  is a normal subgroup in  $\mathcal{G}$ , by the induction hypothesis each of the  $e'_n$  and  $e''_n$  maps  $\mathcal{G} \times \mathcal{G}$  into  $D^n\mathcal{G}$ . Hence  $e_{n+1}$  maps  $\mathcal{G} \times \mathcal{G}$  into  $D^{n+1}\mathcal{G}$ .

*Sufficiency.* First note that the condition  $e_n = c$  is equivalent to the fact that all groups  $\mathcal{G}(A)$ , where  $A$  is any  $k$ -algebra, satisfy the identity  $e_n(x, y) \equiv 1$ . This property is thus hereditary with respect to sub- and factor groups. Suppose that  $\mathcal{G}$  satisfies  $e_n = c$  but is not solvable. In view of the above remark, the quotient  $\mathcal{G}^{\text{red}} = \mathcal{G}/\mathcal{G}^{\text{u}}$ , where  $\mathcal{G}^{\text{u}}$  stands for the unipotent radical of  $\mathcal{G}$ , is a nontrivial reductive group satisfying  $e_n = c$ . Furthermore, its derived group  $\mathcal{G}^{\text{ss}} = [\mathcal{G}^{\text{red}}, \mathcal{G}^{\text{red}}]$  is a nontrivial semisimple group satisfying the same property. Hence the  $k$ -group  $\mathcal{SL}_2$  as a subgroup of  $\mathcal{G}^{\text{ss}}$  must satisfy the same law. Its quotient  $\mathcal{PSL}_2$  thus also satisfies  $e_n = c$ . Therefore, the identity  $e_n(x, y) \equiv 1$  must hold in all groups  $\mathcal{PSL}_2(A)$  where  $A$  is a  $k$ -algebra, which is impossible [14].  $\square$

Now we pass on to a “structural” analog of the Engel law. Define  $v_1 = u$  and, by induction,

$$v_{n+1}: \mathcal{G} \times \mathcal{G} \xrightarrow{(v_n, \text{pr}_2)} \mathcal{G} \times \mathcal{G} \xrightarrow{u} \mathcal{G}.$$

**Proposition 4.2.** *Let  $\mathcal{G}$  be a connected affine algebraic group over a field  $k$ . Then  $\mathcal{G}$  is nilpotent if and only if  $v_n = c$  for some  $n \geq 1$ .*

*Proof.* Let  $C^n\mathcal{G}$  denote the  $n$ th term of the lower central series. Then  $v_n$  maps  $\mathcal{G} \times \mathcal{G}$  into  $C^n\mathcal{G}$ . This proves the “only if” part. Now let  $v_n = c$ . Then, as in the proof of Proposition 4.1, we conclude that  $\mathcal{G}$  is solvable. Hence  $\overline{\mathcal{G}} = \mathcal{G}(\bar{k})$  is solvable (here  $\bar{k}$  stands for a (fixed) algebraic closure of  $k$ ). According to [7, IV, 4.1.5], we only need to prove that  $\overline{\mathcal{G}}$  is nilpotent. Since  $\overline{\mathcal{G}}$  is solvable and connected, it is isomorphic to a semidirect product  $T \ltimes U$ , where  $T$  is a torus and  $U$  is nilpotent. If  $T = \{e\}$  or  $U = \{e\}$ , then  $\overline{\mathcal{G}}$  is nilpotent. Hence we may assume that  $\dim T \geq 1$  and  $\dim U \geq 1$ . If  $T$  is central in  $\overline{\mathcal{G}}$ , then  $\overline{\mathcal{G}}$  is nilpotent [3, 10.6(3)]. If not,  $U$  contains a one-dimensional subgroup  $U_1$  that does not commute with  $T$ . Since  $\bar{k}$  is algebraically closed,  $U_1$  is isomorphic to the additive group  $\mathbf{G}_a$ . Hence  $T$  acts on  $U_1$  as follows:  $t^{-1}ut = \lambda(t)u$ , where  $u \in U_1$ ,  $t \in T$ , and  $\lambda: T \rightarrow \mathbf{G}_m$  is a character of  $T$  (cf. [3, 10.10]). Thus,  $t^{-1}u^{-1}t = \lambda(t)^{-1}u^{-1}$  and  $t^{-1}u^{-1}tu = \lambda(t)^{-1}$ , consequently  $[u, t] = \lambda(t) \neq 1$  for  $u \neq 1$  and  $t \neq 1$ . By induction, we obtain  $v_n(u, t) \neq 1$  for any  $n$ , which is a contradiction.  $\square$

## 5. THE MAIN CONJECTURE

In this section, we return to Conjecture 2.9. Our first observation is that by standard arguments one can restrict the consideration to a finite number of series of finite simple groups. To be more precise, one can easily derive Conjecture 2.9 from the following conjecture.

**Conjecture 5.1.** *Let  $G$  be one of the following groups:*

1.  $\text{PSL}(2, p)$  ( $p = 5$  or  $p \equiv \pm 2 \pmod{5}$ ,  $p \neq 3$ ),
2.  $\text{PSL}(2, 2^p)$ ,
3.  $\text{PSL}(2, 3^p)$  ( $p$  odd),
4.  $\text{Sz}(2^p)$  ( $p$  odd),
5.  $\text{PSL}(3, 3)$ .

Let  $\{e_i\}$  be one of the sequences (1)–(3). Then neither of the identities  $e_n \equiv 1$  holds in  $G$ .

Indeed, in accordance with [28], the list in Conjecture 5.1 is precisely the list of minimal finite nonsolvable groups (that is, the groups every subgroup of which is solvable). On our way to proving Conjecture 5.1, we proceed by a case-by-case computer investigation. In order to prove that  $e_n \equiv 1$  is not a law in  $G$ , it is enough to show that for some  $k < l$  the equation  $e_k(x, y) = e_l(x, y)$  has a nontrivial solution  $(x_0, y_0) \in G \times G$  (nontrivial means that  $e_k(x_0, y_0) = e_l(x_0, y_0) \neq 1$ ; by the construction of the sequences, it suffices to check that the right-hand side is not equal to 1).

The case  $G = \mathrm{PSL}(3, 3)$  is the easiest one. Say, if the  $e_n$  are taken from sequence (1), the matrices

$$x_0 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 2 & 1 & 1 \end{pmatrix}, \quad y_0 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

give a solution to the equation  $e_{17} = e_{21}$ , and thus  $e_n \equiv 1$  is not a law in  $\mathrm{PSL}(3, 3)$ .

For  $G = \mathrm{PSL}(2, p)$ , a computer search gives a solution to  $e_2 = e_4$  (where the  $e_i$  are taken from the sequence (seq. 2)) for all  $p < 1000$  except for  $p = 293$  (as in chess,  $e_2 - e_4$  usually wins!). The equation  $e_3 = e_5$  has a solution in  $\mathrm{PSL}(2, p)$  for all  $p < 1000$ , and this result remains true for all  $p < 1500$ , except, possibly, for  $p = 1163$ , for which calculations take too much time.

See the Appendix for more details concerning numerical experiments.

To conclude, we present the following model case that can be viewed as a testing ground for proving Conjecture 5.1.

**Proposition 5.2.** *Let the sequence  $\{e_i\}$  be given by formulas (1). If the identity  $e_2 \equiv 1$  holds in a finite group  $G$ , then  $G$  is solvable.*

*Proof.* As above, it is enough to prove that the identity  $e_2 \equiv 1$  does not hold in the minimal nonsolvable groups. For  $G = \mathrm{PSL}(3, 3)$  it is proved above. Now let  $G = \mathrm{PSL}(2, q)$ . Take

$$x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$$

with  $t \neq 0$ . Then  $e_2(x, y) = A(t)$  can be viewed as a polynomial matrix in the indeterminate  $t$ . Its entry  $A_{1,2}$  equals  $-2t^3(t+1)f(t)$ , where  $f(t) = t^8 + t^7 - t^6 - 4t^5 - 8t^4 - 5t^3 + t^2 + 4t + 2$ . Since  $A_{1,2}(t)$  can only vanish at  $t = 0$ ,  $t = -1$ , and at the roots of  $f(t)$ , we conclude that for odd  $q \geq 11$  the identity  $e_2 \equiv 1$  cannot hold in  $\mathrm{PSL}(2, q)$ . For  $q = 5$  and  $q = 7$  we have  $A_{1,2}(1) \neq 0$ . Thus, we have proved the proposition for  $G = \mathrm{PSL}(2, p)$  and  $G = \mathrm{PSL}(2, 3^p)$ .

Next consider the case  $G = \mathrm{PSL}(2, 2^p)$ . Take

$$x = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} t & 1 \\ 1 & 0 \end{pmatrix}.$$

As above, we have  $e_2(x, y) = B(t)$ , a polynomial matrix in one variable  $t$  running over the finite field  $\mathbb{F}_q$ ,  $q = 2^p$ , with  $B_{1,2} = t(t^8 + 1)$ . One can easily see that  $B_{1,2}(t)$  cannot vanish at all  $t \in \mathbb{F}_q$ .

It only remains to consider the case of Suzuki groups  $G = \mathrm{Sz}(q)$ . We recall (see, for example, [13, Chapter XI, §3]) that as a subgroup of  $\mathrm{GL}(4, q)$  the group  $G$  is generated by the matrices

$$S(\alpha, \beta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \alpha^z & 1 & 0 & 0 \\ \beta & \alpha & 1 & 0 \\ \alpha^{2z+1} + \alpha^z\beta + \beta^{2z} & \alpha^{1+z} + \beta & \alpha^z & 1 \end{pmatrix}, \quad \alpha, \beta \in \mathbb{F}_q,$$

$$M(\zeta) = \begin{pmatrix} \zeta^z & 0 & 0 & 0 \\ 0 & \zeta^{1-z} & 0 & 0 \\ 0 & 0 & \zeta^{z-1} & 0 \\ 0 & 0 & 0 & \zeta^{-z} \end{pmatrix}, \quad \zeta \in \mathbb{F}_q^*,$$

$$\text{and } J = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Here  $z = 2^{\frac{p-1}{2}}$ . Now we take  $x = J$  and  $y = S(1, t)$ . As above, a straightforward computation (using MAPLE) gives  $e_2(x, y)$  as a polynomial matrix  $C(t)$ . Its entry  $C_{4,1}(t)$  equals  $t^{2z}(t^z + 1)$ . The number of roots of  $t^z + 1$  in  $\mathbb{F}_q$  does not exceed  $z$ , which is strictly smaller than  $q - 1$ , and thus  $C_{4,1}(t)$  cannot vanish at all  $t \in \mathbb{F}_q$ .  $\square$

**Remark.** Probably, one can characterize neither finite nilpotent groups of a fixed class nor finite solvable groups of a fixed derived length by means of two-variable identities. For example, there exists a nonmetabelian solvable group  $G$  such that all its 2-generator subgroups are metabelian [16, 9].

#### APPENDIX

We present here some results of computer experiments. In Table 1, for each  $p < 200$  we exhibit one solution  $(x, y)$  to the equation  $e_2(x, y) = e_4(x, y)$ , where the  $e_i$  are taken from sequence (2). In the next two tables for  $p < 80$  we present the number of solutions of the above equation for sequences (1) and (2), respectively.

TABLE 1: Solutions to  $e_2 = e_4$  (formulas (1))

$p$	$x$	$y$	$p$	$x$	$y$
5	$(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} -2 & -1 \\ 1 & 0 \end{smallmatrix})$	7	$(\begin{smallmatrix} 0 & -1 \\ 1 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} -3 & 2 \\ -2 & 1 \end{smallmatrix})$
11	$(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} -5 & -5 \\ 0 & 2 \end{smallmatrix})$	13	$(\begin{smallmatrix} 0 & -1 \\ 1 & 6 \end{smallmatrix})$	$(\begin{smallmatrix} -3 & -5 \\ -6 & -1 \end{smallmatrix})$
17	$(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} -8 & -5 \\ 3 & 6 \end{smallmatrix})$	19	$(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} -9 & -8 \\ 1 & 5 \end{smallmatrix})$

23	$(\begin{smallmatrix} 0 & -1 \\ 1 & 11 \end{smallmatrix})$	$(\begin{smallmatrix} -11 & -11 \\ -10 & -8 \end{smallmatrix})$	29	$(\begin{smallmatrix} 0 & -1 \\ 1 & 5 \end{smallmatrix})$	$(\begin{smallmatrix} -14 & -13 \\ -6 & 13 \end{smallmatrix})$
31	$(\begin{smallmatrix} 0 & -1 \\ 1 & 5 \end{smallmatrix})$	$(\begin{smallmatrix} -15 & -15 \\ -2 & 0 \end{smallmatrix})$	37	$(\begin{smallmatrix} 0 & -1 \\ 1 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} -18 & -12 \\ 11 & -3 \end{smallmatrix})$
41	$(\begin{smallmatrix} 0 & -1 \\ 1 & 12 \end{smallmatrix})$	$(\begin{smallmatrix} -20 & -14 \\ -3 & 4 \end{smallmatrix})$	43	$(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} -21 & -20 \\ 1 & 5 \end{smallmatrix})$
47	$(\begin{smallmatrix} 0 & -1 \\ 1 & 16 \end{smallmatrix})$	$(\begin{smallmatrix} -23 & -21 \\ -20 & 4 \end{smallmatrix})$	53	$(\begin{smallmatrix} 0 & -1 \\ 1 & 19 \end{smallmatrix})$	$(\begin{smallmatrix} -26 & -24 \\ -18 & 18 \end{smallmatrix})$
59	$(\begin{smallmatrix} 0 & -1 \\ 1 & 24 \end{smallmatrix})$	$(\begin{smallmatrix} -29 & -24 \\ 23 & 19 \end{smallmatrix})$	61	$(\begin{smallmatrix} 0 & -1 \\ 1 & 29 \end{smallmatrix})$	$(\begin{smallmatrix} -30 & -28 \\ -12 & 3 \end{smallmatrix})$
67	$(\begin{smallmatrix} 0 & -1 \\ 1 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} -33 & -28 \\ 17 & -12 \end{smallmatrix})$	71	$(\begin{smallmatrix} 0 & -1 \\ 1 & 34 \end{smallmatrix})$	$(\begin{smallmatrix} -35 & -32 \\ -26 & 33 \end{smallmatrix})$
73	$(\begin{smallmatrix} 0 & -1 \\ 1 & 22 \end{smallmatrix})$	$(\begin{smallmatrix} -36 & -36 \\ 12 & 14 \end{smallmatrix})$	79	$(\begin{smallmatrix} 0 & -1 \\ 1 & 29 \end{smallmatrix})$	$(\begin{smallmatrix} -39 & -39 \\ 36 & 38 \end{smallmatrix})$
83	$(\begin{smallmatrix} 0 & -1 \\ 1 & 34 \end{smallmatrix})$	$(\begin{smallmatrix} -41 & -35 \\ -40 & -20 \end{smallmatrix})$	89	$(\begin{smallmatrix} 0 & -1 \\ 1 & 39 \end{smallmatrix})$	$(\begin{smallmatrix} -44 & -44 \\ 38 & 40 \end{smallmatrix})$
97	$(\begin{smallmatrix} 0 & -1 \\ 1 & 13 \end{smallmatrix})$	$(\begin{smallmatrix} -48 & -45 \\ -3 & -19 \end{smallmatrix})$	101	$(\begin{smallmatrix} 0 & -1 \\ 1 & 45 \end{smallmatrix})$	$(\begin{smallmatrix} -50 & -45 \\ -17 & 17 \end{smallmatrix})$
103	$(\begin{smallmatrix} 0 & -1 \\ 1 & 19 \end{smallmatrix})$	$(\begin{smallmatrix} -51 & -44 \\ 8 & 19 \end{smallmatrix})$	107	$(\begin{smallmatrix} 0 & -1 \\ 1 & 47 \end{smallmatrix})$	$(\begin{smallmatrix} -53 & -31 \\ -1 & -43 \end{smallmatrix})$
109	$(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} -54 & -49 \\ 5 & -52 \end{smallmatrix})$	113	$(\begin{smallmatrix} 0 & -1 \\ 1 & 47 \end{smallmatrix})$	$(\begin{smallmatrix} -56 & -56 \\ -11 & -9 \end{smallmatrix})$
127	$(\begin{smallmatrix} 0 & -1 \\ 1 & 8 \end{smallmatrix})$	$(\begin{smallmatrix} -63 & -55 \\ -11 & -58 \end{smallmatrix})$	131	$(\begin{smallmatrix} 0 & -1 \\ 1 & 11 \end{smallmatrix})$	$(\begin{smallmatrix} -65 & -58 \\ 13 & -65 \end{smallmatrix})$
137	$(\begin{smallmatrix} 0 & -1 \\ 1 & 11 \end{smallmatrix})$	$(\begin{smallmatrix} -68 & -54 \\ -59 & -65 \end{smallmatrix})$	139	$(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} -69 & -68 \\ -1 & 5 \end{smallmatrix})$
149	$(\begin{smallmatrix} 0 & -1 \\ 1 & 40 \end{smallmatrix})$	$(\begin{smallmatrix} -74 & -69 \\ 20 & 73 \end{smallmatrix})$	151	$(\begin{smallmatrix} 0 & -1 \\ 1 & 64 \end{smallmatrix})$	$(\begin{smallmatrix} -75 & -73 \\ -21 & 48 \end{smallmatrix})$
157	$(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} -78 & -68 \\ 10 & 55 \end{smallmatrix})$	163	$(\begin{smallmatrix} 0 & -1 \\ 1 & 58 \end{smallmatrix})$	$(\begin{smallmatrix} -81 & -30 \\ -59 & -44 \end{smallmatrix})$
167	$(\begin{smallmatrix} 0 & -1 \\ 1 & 14 \end{smallmatrix})$	$(\begin{smallmatrix} -83 & -76 \\ -83 & -74 \end{smallmatrix})$	173	$(\begin{smallmatrix} 0 & -1 \\ 1 & 37 \end{smallmatrix})$	$(\begin{smallmatrix} -86 & -63 \\ -23 & -41 \end{smallmatrix})$
179	$(\begin{smallmatrix} 0 & -1 \\ 1 & 53 \end{smallmatrix})$	$(\begin{smallmatrix} -89 & -88 \\ -59 & 4 \end{smallmatrix})$	181	$(\begin{smallmatrix} 0 & -1 \\ 1 & 49 \end{smallmatrix})$	$(\begin{smallmatrix} -90 & -86 \\ -20 & 3 \end{smallmatrix})$
191	$(\begin{smallmatrix} 0 & -1 \\ 1 & 88 \end{smallmatrix})$	$(\begin{smallmatrix} -95 & -85 \\ -41 & -95 \end{smallmatrix})$	193	$(\begin{smallmatrix} 0 & -1 \\ 1 & 84 \end{smallmatrix})$	$(\begin{smallmatrix} -96 & -94 \\ -62 & 78 \end{smallmatrix})$
197	$(\begin{smallmatrix} 0 & -1 \\ 1 & 24 \end{smallmatrix})$	$(\begin{smallmatrix} -98 & -86 \\ -20 & 93 \end{smallmatrix})$	199	$(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} -99 & -95 \\ 4 & 38 \end{smallmatrix})$

TABLE 2: Numbers of solutions to  $e_2 = e_4$  (formulas (1))

$p$	5	7	11	13	17	19	23	29	31	37
$N_1$	0	84	96	300	668	80	88	360	760	440
$p$	41	43	47	53	59	61	67	71	73	79
$N_1$	664	848	1312	428	712	480	1616	1432	1168	1904

TABLE 3: Numbers of solutions to  $e_2 = e_4$  (formulas (2))

$p$	5	7	11	13	17	19	23	29	31	37
$N_2$	22	16	134	28	36	304	136	526	670	296
$p$	41	43	47	53	59	61	67	71	73	79
$N_2$	990	590	760	428	1064	728	402	1136	584	2050

**Acknowledgments.** This work was done while D. Nikolova was visiting the Bar-Ilan University and Ben-Gurion University of the Negev, Israel, and the National University of Ireland, Galway. The paper was completed while B. Kunyavskii and E. Plotkin were visiting SFB 343 “Diskrete Strukturen in der Mathematik” (University of Bielefeld). The authors gratefully appreciate the hospitality and support of these institutions. We thank M. Borovoi, R. Farnsteiner, A. Premet, and N. Vavilov for very useful discussions and correspondence. Our special thanks go to B. Plotkin, whose ideas and encouragement were indispensable, and to A. Feldman and R. Shklyar for their help with the computer experiments.

This research was supported by the Israel Science Foundation founded by the Israel Academy of Sciences and Humanities – Center of Excellence Program.

Partially supported by the Ministry of Absorption (Israel) and the Minerva Foundation through the Emmy Noether Research Institute of Mathematics.

## REFERENCES

1. R. E. Block, “Determination of differentially simple rings with a minimal ideal,” *Ann. Math.* (2) **90**, 433–459 (1969).
2. R. E. Block and R. L. Wilson, “Classification of the restricted simple Lie algebras,” *J. Algebra*, **114**, 115–259 (1988).
3. A. Borel, *Linear Algebraic Groups*, Springer-Verlag, Berlin (1991).
4. R. Brandl, “On groups with small Engel depth,” *Bull. Austral. Math. Soc.*, **28**, 101–110 (1983).
5. R. Brandl and D. Nikolova, “Simple groups of small Engel depth,” *Bull. Austral. Math. Soc.*, **33**, 245–251 (1986).
6. J. Cossey, S. Oates, R. Macdonald, and A. P. Street, “On the laws of certain finite groups,” *J. Austral. Math. Soc.*, **11**, 441–489 (1970).
7. M. Demazure and P. Gabriel, *Groupes Algébriques*, Masson, Paris & North-Holland, Amsterdam (1970).
8. P. Flavell, “Finite groups in which every two elements generate a soluble group,” *Invent. Math.*, **121**, 279–285 (1995).
9. C. K. Gupta, “2-Metabelian groups,” *Arch. Math. (Basel)*, **19**, 584–587 (1968).
10. N. D. Gupta, “Some group laws equivalent to the commutative law,” *Arch. Math. (Basel)*, **17**, 97–102 (1966).
11. N. D. Gupta and H. Heineken, “Groups with a two-variable commutator identity,” *Math. Z.*, **95**, 276–287 (1967).
12. H. Heineken and P. Neumann, “Identical relations and decision procedures for groups,” *J. Austral. Math. Soc.*, **7**, 39–47 (1967).
13. B. Huppert and N. Blackburn, *Finite Groups III*, Springer-Verlag, Berlin (1982).
14. G. A. Jones, “Varieties and simple groups,” *J. Austral. Math. Soc.*, **17**, 163–173 (1974).
15. S. Lang, *Algebra*, 3rd ed., Addison-Wesley (1993).
16. B. N. Neumann, “On a conjecture of Hanna Neumann,” *Proc. Glasgow Math. Assoc.*, **3**, 13–17 (1956).
17. H. Neumann, *Varieties of Groups*, Springer-Verlag, Berlin (1967).
18. D. Nikolova, “Groups with a 2-variable commutator identity,” Ph.D. thesis, Sofia Univ. (1983).
19. D. Nikolova, “Groups with a two-variable commutator identity,” *C. R. Acad. Bulgare Sci.*, **36**, 721–724 (1983).
20. D. Nikolova, “Solvability of finite groups with a two-variable commutator identity,” *Serdica*, **11**, 59–63 (1985).
21. S. Oates and M. B. Powell, “Identical relations in finite groups,” *J. Algebra*, **1**, 11–39 (1964).
22. V. P. Platonov and A. S. Rapinchuk, *Algebraic Groups and Number Theory* [in Russian], Nauka, Moscow (1991).
23. B. Plotkin, E. Plotkin, and A. Tsurkov, “Geometrical equivalence of groups,” *Comm. Algebra*, **27**, 4015–4025 (1999).

24. A. Potapchik and A. Rapinchuk, “Normal subgroups of  $SL_{1,D}$  and the classification of finite simple groups,” *Proc. Indian Acad. Sci. (Math. Sci.)*, **106**, 329–368 (1996).
25. Y. Segev, “On finite homomorphic images of the multiplicative group of a division algebra,” *Ann. Math.*, (2) **149**, 219–251 (1999).
26. Y. Segev and G. Seitz, “Anisotropic groups of type  $A_n$  and the commuting graph of finite simple groups,” to appear.
27. H. Strade and R. Farnsteiner, *Modular Lie Algebras and Their Representations*, Marcel Dekker, New York–Basel (1988).
28. J. Thompson, “Non-solvable finite groups all of whose local subgroups are solvable,” *Bull. Amer. Math. Soc.*, **74**, 383–437 (1968).
29. B. Weisfeiler, “On subalgebras of simple Lie algebras of characteristic  $p > 0$ ,” *Trans. Amer. Math. Soc.*, **286**, 471–503 (1984).