

## ON THE CONJECTURES OF J. THOMPSON AND O. ORE

ERICH W. ELLERS AND NIKOLAI GORDEEV

ABSTRACT. If  $G$  is a finite simple group of Lie type over a field containing more than 8 elements (for twisted groups  ${}^L X_n(q^l)$  we require  $q > 8$ , except for  ${}^2 B_2(q^2)$ ,  ${}^2 G_2(q^2)$ , and  ${}^2 F_4(q^2)$ , where we assume  $q^2 > 8$ ), then  $G$  is the square of some conjugacy class and consequently every element in  $G$  is a commutator.

### 1. INTRODUCTION

In 1951 Ore [O] proved that every element in the alternating group  $A_n$ , where  $n \geq 5$ , is a commutator. Towards the end of his paper he wrote: “It is possible that a similar theorem holds for any simple group of finite order, but it seems that at present we do not have the necessary methods to investigate the question.” Now this supposition is known as the Ore conjecture.

In the notes of Arad and Herzog [AH] (we do not know of any more direct reference) the following stronger conjecture is attributed to J. Thompson: “Every finite simple group  $G$  contains a conjugacy class  $C$  such that  $C^2 = G$ .” Obviously, this statement implies that every element in  $G$  is a commutator.

Ore’s remark that we lack the tools to prove his assertion in general is valid even now. The same, of course, is true for Thompson’s conjecture. There seems to be no general approach to either one of them. Theoretically for every finite simple group one can check, e.g. with a computer, both conjectures using character inequalities. Namely let  $G$  be a finite simple group; then (see [I])

- (i) every element in  $G$  is a commutator if and only if

$$\sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)}{\chi(1)} \neq 0 \quad \text{for every } g \in G,$$

and

- (ii)  $G = C^2$  for some conjugacy class  $C$  of  $G$  if and only if  $x, x^{-1} \in C$  for some  $x \in G$  and

$$\sum_{\chi \in \text{Irr}(G)} \frac{|\chi(x)|^2 \overline{\chi(g)}}{\chi(1)} \neq 0 \quad \text{for every } g \in G.$$

In order to use these inequalities we need some information about the conjugacy classes and characters. It is not clear how this can be obtained in general. The classification of finite simple groups, on the other hand, gives us a chance to prove both conjectures through a case by case analysis.

---

Received by the editors April 5, 1996 and, in revised form, October 10, 1996.

1991 *Mathematics Subject Classification*. Primary 20G15.

Research supported in part by NATO collaborative research grant CRG 950689.

©1998 American Mathematical Society

For the alternating groups the Ore conjecture has been proved by Ore himself, as mentioned above, and the Thompson conjecture has been proved by Cheng-hao Hsü [H] in 1965. Various papers were devoted to the determination of conjugacy classes in the alternating groups  $A_n$  whose squares cover  $A_n$  (see [AH] and [BrL]). For the sporadic groups the Thompson (and consequently the Ore conjecture) was verified in 1984 by Neubüser, Pahlings, and Cleavers; see [NPaCl]. The situation for finite simple groups of Lie type is the following. In 1961/62 R. C. Thompson proved the Ore conjecture for  $PSL_n(K)$ , where  $K$  is an arbitrary finite field. The Thompson conjecture for  $PSL_n(K)$  was proved by J. L. Brenner in 1983 for finite fields  $K$  containing more than  $n + 1$  elements (see [Br]), by A. R. Sourour in 1986 for fields  $K$  with  $|K| > n + 1$  (see [So]), and by A. Lev in 1994 for arbitrary fields (see [Le]). These conjectures have also been checked for some other groups of Lie type. If  $\text{char } K \neq 2$  and  $-1$  is a square in the field  $K$ , the Thompson conjecture was verified for  $PSp_n(K)$  by R. Gow in 1988 (see [Gow]). The Thompson conjecture was confirmed for  ${}^2B_2(q)$  by Arad, Chillag, and Moran (see [AH]) and for all finite simple groups with order less than  $10^6$  by S. Karni (see [AH]).

In 1993 O. Bonten [B] proved the following result, which gives an asymptotic solution of Ore's conjecture: Let  $G(q) = X_n(q), {}^lX_n(q^l)$  be a series of groups of Lie type. Then there exists a constant  $q_0$  such that every element in  $G(q)$  is a commutator if  $q > q_0$ . Here  $n$  and  $l$  are fixed, i.e.,  $q_0$  depends on  $n$ . In [B] only the existence of such numbers  $q_0$  is proved, but theoretically the methods used allow one to calculate an estimate for  $q_0$ . Using such estimates for groups of small Lie rank and using a computer for small  $q$ , Bonten [B] proved Ore's conjecture for all simple groups of the following Lie types:  $G_2(q), {}^2G_2(q^2), {}^3D_4(q^3), F_4(q), {}^2F_4(q^2)$ . Bonten's results are based on the inequalities (i) and (ii), estimates of the values of characters for groups of Lie type obtained by Gluck (see [G1], [G2], [G3]), and on the Deligne-Lusztig theory of characters for groups of Lie type.

In 1994–96 the authors of the present paper proved the following result (see [EGI], [EGII], [EGIII]):

**Theorem 1.** *Let  $G$  be a Chevalley group (untwisted or twisted) over a field  $K$  (here Chevalley group means a group generated by root subgroups  $X_\alpha$  (see [St]); in the twisted cases  $K$  is supposed to be finite). Let  $h_1$  and  $h_2$  be two regular semisimple elements in  $G$  from a maximal split torus and let  $C_1$  and  $C_2$  be the conjugacy classes of  $h_1$  and  $h_2$ , respectively. Then*

$$C_1C_2 \supset G \setminus Z(G).$$

This theorem immediately implies the Ore conjecture for any simple group  $G$  containing a regular semisimple element  $h$  in a maximal split torus, and the Thompson conjecture if this element is in addition real, i.e., if  $h$  and  $h^{-1}$  are conjugate. Estimates show that such a real regular element exists if  $|K| > (2r + 3)^2$ , where  $r$  is the Lie rank of  $G$  (more precise statements can be found in [EGI], [EGII], [EGIII]). Thus this theorem also gives an asymptotic solution for the Thompson and in turn for the Ore conjecture. Our estimates are not worse than those in [B], because there the group is also supposed to have a regular element in a maximal split torus. Moreover, Theorem 1 gives a solution of the Thompson conjecture and consequently for the Ore conjecture for untwisted Chevalley groups over arbitrary infinite fields.

The purpose of the present paper is to prove the Thompson conjecture for all groups of Lie type over fields containing more than 8 elements (for twisted groups

${}^lX_n(q^l)$  we require  $q > 8$ , except for  ${}^2B_2(q^2)$ ,  ${}^2G_2(q^2)$ , and  ${}^2F_4(q^2)$ , where we assume  $q^2 > 8$ ).

Thus now the situation with the conjectures of Thompson and Ore is the following: the Thompson conjecture has been confirmed for all groups of Lie type except for those over small fields  $k$ , where  $|k| = 2, 3, 4, 5, 7, 8$ . Actually, for most cases the bound is even better, see Table 1 below, e.g.  $|k| = 8$  needs to be checked only for  ${}^2F_4(8)$ . For the Ore conjecture the groups with small Lie ranks  $F_4(q)$ ,  ${}^2F_4(q^{2r+1})$ ,  $G_2(q)$ ,  ${}^2G_2$ ,  ${}^3D_4(q^3)$  and over small fields have been checked by computer (see [B]).

Finally, we mention a number of interesting results that are related to the conjectures of Thompson and Ore. The question of representation of a group element as a commutator has been considered for cases of infinite groups too. In 1949 M. Goto [Go] proved that every element in a connected compact semisimple group is a commutator. The same result for semisimple algebraic groups over the complex number field was obtained by S. Pasiencier and H. C. Wang [PW] and for semisimple algebraic groups over arbitrary algebraically closed fields by Ree [R]. In 1964 Ree proved that in a connected semisimple algebraic group defined over an algebraically closed field every element is a commutator (see [R]). In 1951 Shoda obtained results on commutators of matrices (see [S]). There are papers showing that certain simple groups are cubes of some conjugacy classes (see [MSaWe]); there are other papers showing that in certain simple groups every element is a product of two commutators (see [Wi]). For further results see [AH], [Wi], [VWh], and [L].

## 2. NOTATION AND TERMINOLOGY

A Chevalley group  $G = G(R, K)$ , over a field  $K$ , corresponding to the root system  $R$  is a group generated by root subgroups  $X_\alpha, \alpha \in R$ , where  $X_\alpha = \langle x_\alpha(t) | t \in K \rangle$  or  $X_\alpha = \langle x_\alpha(t, s) | t, s \in K \rangle$  or  $X_\alpha = \langle x_\alpha(t, s, r) | t, s, r \in K \rangle$ . The second and third possibilities occur only in the case of twisted Chevalley groups (see [C1], [St]). Thus  $G$  is a commutator subgroup of the group of rational points  $\tilde{G}(K)$  of the corresponding simple algebraic group  $\tilde{G}$ . When we use  $X_n(q)$  and  ${}^lX_n(q^l)$  we follow Carter [C1]. In the case of untwisted groups  $K$  is an arbitrary field. For twisted groups,  $K$  is a finite field,  $\theta : K \rightarrow K$  is the corresponding automorphism and  $K^\theta$  is the subfield of  $\theta$ -invariant elements of  $K$ .

We put

$$k = K \text{ if } G \text{ is untwisted or if it is of type } {}^2B_2, {}^2G_2 \text{ or } {}^2F_4$$

and

$$k = K^\theta \text{ in all other cases.}$$

Let  $K^*$  and  $k^*$  denote the multiplicative groups of the fields  $K$  and  $k$ , respectively.

We use the following notation:

$\Delta$  denotes a simple root system of  $R$ ,

$B = HU$  denotes a Borel subgroup of  $G$ , where  $U = \langle X_\alpha | \alpha \in R^+ \rangle$ ,  $H = \langle h_\alpha | \alpha \in \Delta \rangle$ ,  $U^- = \langle X_\alpha | \alpha \in R^- \rangle$ .

For groups of Lie type we have the Bruhat decomposition

$$G = BNB$$

where  $H \triangleleft N$  and  $W = N/H$  is the Weyl group of  $G$  (see [C1], [St]). We shall identify the elements of the group  $W$  with those of  $N$ .

A semisimple element  $h \in H$  is regular if the centralizer  $C_G(h) \subset N$ . This is equivalent to the usual definition (see [C2]). We shall also consider regular elements from groups of Lie type  $A_n$ . Then a preimage of such an element lies in  $SL_{n+1}(\bar{K})$ , where  $\bar{K}$  is the algebraic closure of  $K$ ; so the preimage has a canonical form, where distinct Jordan blocks have distinct eigenvalues.

An element  $g \in G$  is called real if  $g$  is conjugate to  $g^{-1}$ .

We use the notation of Bourbaki for root systems of untwisted groups (see [Bo]) and that of Carter (see [C1]) for twisted groups.

If  $\Delta_1$  is a subsystem of the simple root system  $\Delta$ , then  $\langle \Delta_1 \rangle$  denotes the root subsystem generated by  $\Delta_1$ .

### 3. THE MAIN THEOREM

Our main result is

**Theorem 2.** *Let  $G$  be a Chevalley group over  $K$  and  $k = K$  or  $k = K^\theta$  a field as defined above. If  $|k| > 8$ , then there is a real conjugacy class  $C \subset G$  such that*

$$C^2 \supset G \setminus Z(G).$$

**Corollary.** *If  $G$  is a simple group satisfying the conditions of Theorem 2, then the Thompson conjecture holds for  $G$ .*

*Proof of Corollary.* Clearly  $Z(G) = 1$ , and  $1 \in C^2$  because  $C$  is real. □

*Remark 1.* Here  $|K| = |k|$  or  $|K| = |k|^2$  or  $|K| = |k|^3$ . The last condition is only possible for  ${}^3D_4(q^3)$ . One can say that the Thompson conjecture holds for twisted groups if the corresponding field contains more than  $8^2$  or  $8^3$  elements. But for twisted groups, when  $|K| = |k|^2$  or  $|K| = |k|^3$ , the field  $K$  is determined by  $k$  and it is better to look at  $k$  to describe the unsolved cases.

*Remark 2.* In Table 1 we summarize results. We give a number  $d$ , depending on the type of the Chevalley group, indicating that the Thompson conjecture has been proved for all groups  $G$  provided that  $|k| \geq d$ . Thus if  $G$  is a finite group of type  $X_n(q)$  or  ${}^lX_n(q^l)$ , except for  ${}^2B_2(q^2), {}^2G_2(q^2), {}^2F_4(q^2)$ , the table gives a bound for  $q$ . In the cases  ${}^2B_2(q^2), {}^2G_2(q^2), {}^2F_4(q^2)$  the table gives a bound for  $q^2$ . Note that in some cases there is no group with  $|k| = d$ . (The statement is then trivially true.) These  $d$  have been chosen in order to allow us to give a reasonable global estimate in Theorem 2.

TABLE 1

type	$A_l$	$B_2$	$B_l$ ( $l > 2$ )	$C_l$	$D_{2l}$	$D_{2l+1}$	$E_6$	$E_7$	$E_8$	$F_4$	$G_2$
$d$	2	4	7	4	5	4	7	5	7	8	7

type	${}^2A_{2l-1}$	${}^2A_{2l}$	${}^2D_{l+1}$	${}^2E_6$	${}^3D_4$	${}^2B_2$	${}^2G_2$	${}^2F_4$
$d$	8	4	7	8	7	3	4	9

4. GAUSS DECOMPOSITION FOR CHEVALLEY GROUPS

Let  $G$  be a Chevalley group and  $H, \mathcal{U}, \mathcal{U}^-$  be the corresponding subgroups. Then every element in  $G$  belonging to the “big cell”  $\mathcal{U}^-HU$  has a unique decomposition  $g = u_1hu_2$ , where  $u_1 \in \mathcal{U}^-$ ,  $u_2 \in \mathcal{U}$ ,  $h \in H$ . This is called the Gauss decomposition of  $g$ .

Now let  $\Gamma$  be a group generated by  $G$  and a cyclic group  $\langle \sigma \rangle$  which normalizes  $G$  in  $\Gamma$  and acts as a diagonal automorphism on  $G$  (perhaps trivially). In [EGI], [EGII], [EGIII] the following theorem has been proved.

**Theorem 3.** *Let  $\gamma = \sigma g \in \Gamma$ ,  $g \in G$  and  $\gamma \notin Z(\Gamma)$ . If  $h$  is any fixed element in the group  $H$ , then there is an element  $\tau \in G$  such that*

$$\tau\gamma\tau^{-1} = \sigma u_1 h u_2,$$

where  $u_1 \in \mathcal{U}^-$  and  $u_2 \in \mathcal{U}$ .

*Remark.* This is a generalization of a theorem of Sourour for  $G = SL_n(K)$  and  $\Gamma \leq GL_n(K)$  (see [So]).

We shall refer to Theorem 3 as  $EG$ .

Clearly, Theorem 1 follows immediately from Theorem 3. Indeed, if  $h_1, h_2 \in H$  are regular elements, then the elements  $u_1 \in \mathcal{U}^-$  and  $u_2 \in \mathcal{U}$  can be presented as  $u_1 = v_1 h_1 v_1^{-1} h_1^{-1}$  and  $u_2 = h_2^{-1} v_2 h_2 v_2^{-1}$  for some  $v_1 \in \mathcal{U}^-$  and  $v_2 \in \mathcal{U}$  (see [EGI, Proposition 1]). Thus, if we consider any noncentral conjugacy class  $C \subset G$ , according to  $EG$  we can find a representative  $c \in C$  such that

$$c = u_1 h_1 h_2 u_2 = (v_1 h_1 v_1^{-1} h_1^{-1}) h_1 h_2 (h_2^{-1} v_2 h_2 v_2^{-1}) = (v_1 h_1 v_1^{-1}) (v_2 h_2 v_2^{-1}).$$

Moreover,  $EG$  implies other decompositions in Chevalley groups; e.g. if we choose  $h = 1$  in Theorem 3 we get the following.

**Corollary.** *Every noncentral element in a Chevalley group is a product of two unipotent elements. In particular, every noncentral element in a finite Chevalley group is a product of two  $p$ -elements, where  $p$  is the characteristic of the field  $k$ .*

5. PROOF OF THEOREM 2

The two main components of our proof are  $EG$  and the following theorem by Lev.

**Theorem (Lev [Le]).** *Let  $F$  be a field and let  $A, B \in GL_n(F)$  be regular matrices, where  $n \geq 3$  and  $|F| \geq 4$ . Assume that all eigenvalues of  $A$  or of  $B$  lie in  $F$ . Then, for every nonscalar matrix  $M \in GL_n(F)$  with  $\det A \cdot \det B = \det M$ , there are matrices  $A_1$  and  $B_1$  in  $GL_n(F)$  which are similar to  $A$  and  $B$ , respectively, such that  $A_1 B_1 = M$ . The same conclusion holds for  $n = 2$  if and only if either the eigenvalues of  $A$  or those of  $B$  are distinct or all eigenvalues of  $A$  and  $B$  lie in  $F$ .*

*Remark.* If  $Z$  is a subgroup of the centre of  $GL_n(F)$ , then we obviously can apply Lev’s theorem to the images  $\bar{A}, \bar{B}, \bar{M}$  of matrices  $A, B, M$  in  $GL_n(F)/Z$ .

Suppose  $\Delta_1 \subset \Delta$  and  $R_1 = \langle \Delta_1 \rangle$ . If  $R_1 = A_l$ , then

$$G_1 = \langle X_{\pm\alpha} | \alpha \in R_1 \rangle \approx SL_{l+1}(F)/Z$$

where  $F = K$  or  $F = k$  and  $Z \leq Z(SL_{l+1}(F))$ . Let  $u$  be a regular element in  $G_1$  and assume a preimage of  $u$  has all eigenvalues in  $F$ . Suppose every element in

$G_1$  that is  $GL_{l+1}(F)$ -conjugate to  $u$  is also  $HG_1$ -conjugate to  $u$ . Then by Lev's theorem every noncentral element  $g \in G_1$  is a product

$$g = u_1 u_2,$$

where  $u_1, u_2$  are elements which are  $HG_1$ -conjugate to  $u$ . In the situation just described we shall say that  $G_1 \setminus Z(G_1) \subset C^2$ , where  $C$  is the  $HG_1$ -conjugacy class of  $u$ , by Lev's theorem.

For  $\emptyset \neq \Delta_1 \subset \Delta$ , let  $R_1$  be the root subsystem generated by  $\Delta_1$ ,  $G_1 = \langle X_{\pm\alpha} | \alpha \in R_1 \rangle$ ,  $H_1 = H \cap G_1$ ,  $V = \langle X_{\alpha} | \alpha > 0, \alpha \in R \setminus R_1 \rangle$ ,  $V^- = \langle X_{\alpha} | \alpha < 0, \alpha \in R \setminus R_1 \rangle$ .

**Proposition 5.1.** *Let  $f$  be a real element in  $G$  belonging to  $HG_1$ , let  $C$  be the conjugacy class of  $f$ ,  $C_f$  and  $C_{f^{-1}}$  the  $HG_1$ -conjugacy classes of  $f$  and  $f^{-1}$ , respectively. Put  $C_1 = C_f \cup C_{f^{-1}}$ . Suppose*

1.  $H_1 \neq Z(G_1)$ ,
2.  $C_1^2 \supset G_1 \setminus Z(G_1)$ ,
3.  $f$  acts fixed-point freely on  $V_i/V_{i+1}$  for every  $i$ , where  $\{V_j\}$  is the central series of  $V$ , i.e.,  $V_0 = V$ ,  $V_1 = [V, V]$ ,  $V_2 = [V, V_1]$ ,  $\dots$ .

Then

$$C^2 \supset G \setminus Z(G).$$

If in addition  $G$  is simple, then  $C^2 \supset G$ .

In order to prepare the proof of Proposition 5.1 we make an observation and establish Lemma 5.1. Since  $f \in HG_1$ , any element of  $C_1$  normalizes  $V$  and  $V^-$ . Consequently the action of such elements on  $V_i/V_{i+1}$  or on  $V_i^-/V_{i+1}^-$  is defined.

**Lemma 5.1.** *If 3 of Proposition 5.1 holds, then for any  $\sigma_1, \sigma_2 \in C_1$  and for any  $v_1 \in V^-, v_2 \in V$  there are  $a_1 \in V^-$  and  $a_2 \in V$  such that*

$$\begin{aligned} v_1 &= a_1 \sigma_1 a_1^{-1} \sigma_1^{-1} = [a_1^{-1}, \sigma_1^{-1}], \\ v_2 &= \sigma_2^{-1} a_2 \sigma_2 a_2^{-1} = [\sigma_2, a_2^{-1}]. \end{aligned}$$

*Proof of Lemma 5.1.* Obviously every  $\sigma \in C_1$  acts on  $V_i/V_{i+1}$  fixed-point freely. Since  $V_i/V_{i+1}$  can be considered as a finite dimensional vector space over some subfield of  $K$ , the linear operator  $1 - \sigma$  is invertible on  $V_i/V_{i+1}$ . Thus for every  $v \in V$  there exists some  $x_1 \in V$  such that

$$x_1 \sigma x_1^{-1} \sigma^{-1} \equiv v \pmod{V_1}.$$

Further, if

$$x_i \sigma x_i^{-1} \sigma^{-1} \equiv v \pmod{V_i}$$

for some  $x_i \in V$ , there exists some  $y_i \in V_i$  such that

$$(x_i \sigma x_i^{-1} \sigma^{-1}) (y_i \sigma y_i^{-1} \sigma^{-1}) \equiv v \pmod{V_{i+1}}.$$

Hence  $(x_i y_i) \sigma (y_i^{-1} x_i^{-1}) \sigma^{-1} \equiv (x_i \sigma x_i^{-1} \sigma^{-1}) (y_i \sigma y_i^{-1} \sigma^{-1}) \equiv v \pmod{V_{i+1}}$ .  $\square$

*Proof of Proposition 5.1.* Let  $y \in G \setminus Z(G)$ . According to EG, for every  $h \in H$  there is some  $y_1$  conjugate to  $y$  such that

$$(1) \quad y_1 = u_1 h u_2$$

for some  $u_1 \in \mathcal{U}^-, u_2 \in \mathcal{U}$ . Since  $H_1 \neq Z(G_1)$  we can take  $h \in H_1 \setminus Z(G_1)$ . Further,

$$(2) \quad u_1 = v_1 \tilde{u}_1, \quad u_2 = \tilde{u}_2 v_2,$$

where  $v_1 \in V^-$ ,  $v_2 \in V$ ,  $\tilde{u}_1 \in \mathcal{U}^- \cap G_1 = \mathcal{U}_1^-$ ,  $\tilde{u}_2 \in \mathcal{U} \cap G_1 = \mathcal{U}_1$  (we can arrange the factors from the root subgroups in appropriate order). From (1) and (2) we get

$$(3) \quad y_1 = v_1 (\tilde{u}_1 h \tilde{u}_2) v_2.$$

Put  $g = \tilde{u}_1 h \tilde{u}_2$ . Then  $g \in G_1$  but  $g \notin Z(G_1)$ ; indeed, if  $\tilde{u}_1 h \tilde{u}_2 = h' \in Z(G_1)$ , then  $\tilde{u}_1 h = h' \tilde{u}_2^{-1} \in \mathcal{U}_1^- H_1 \cap H_1 \mathcal{U}_1 = H_1$  (see [C1, Corollary 7.1.3]). Thus  $\tilde{u}_1, \tilde{u}_2 \in H_1$ , which implies  $\tilde{u}_1 = \tilde{u}_2 = 1$  and  $h \in Z(G_1)$ , contradicting our choice of  $h$ . Therefore

$$(4) \quad g = \sigma_1 \sigma_2$$

for some  $\sigma_1, \sigma_2 \in C_1$ , according to 2 of Proposition 5.1. From Lemma 5.1 we get

$$(5) \quad \begin{aligned} a_1 \sigma_1 a_1^{-1} \sigma_1^{-1} &= v_1, \\ \sigma_2^{-1} a_2 \sigma_2 a_2^{-1} &= v_2 \end{aligned}$$

for some  $a_1 \in V^-$  and  $a_2 \in V$ . Applying (3), (4), and (5) we get

$$(a_1 \sigma_1 a_1^{-1}) (a_2 \sigma_2 a_2^{-1}) = (a_1 \sigma_1 a_1^{-1} \sigma_1^{-1}) \sigma_1 \sigma_2 (\sigma_2^{-1} a_2 \sigma_2 a_2^{-1}) = v_1 g v_2 = y_1.$$

Thus

$$(6) \quad C^2 \supset G \setminus Z(G).$$

If  $G$  is simple the equality  $C^2 = G$  follows from (6) because  $f$  is real. □

**Lemma 5.2.** *Let  $u$  be a real element in  $HG_1$  and  $h$  an element in  $H$ . Suppose*

- a.  $C_u^2 \supset G_1 \setminus Z(G_1)$ , where  $C_u$  is the  $HG_1$ -conjugacy class of  $u$ ,
- b.  $h \in C_G(G_1)$ ,
- c.  $whw^{-1} = h^{-1}$ ,  $wuw^{-1} \in C_u$  for some  $w \in W$ ,
- d. the element  $f = hu$  satisfies 3 of Proposition 5.1.

*Then  $f$  is a real element in the group  $G$  satisfying 2 of Proposition 5.1.*

*Proof.* From c we get

$$f_1 = wfw^{-1} = h^{-1}u_1$$

for some  $u_1 \in C_u$ . Since  $u$  is real in  $HG_1$ , there is some  $g \in HG_1$  such that  $gu_1g^{-1} = u^{-1}$ . Hence

$$f_2 = gf_1g^{-1} = gh^{-1}g^{-1}gu_1g^{-1} = h^{-1}u^{-1} = f^{-1}.$$

Therefore  $f$  is real in  $G$ . Moreover, for any  $v_1, v_2 \in C_u$  one can find  $g_1, g_2 \in HG_1$  such that  $v_1 = g_1u_1g_1^{-1}$ ,  $v_2 = g_2u^{-1}g_2^{-1}$ . Thus

$$(g_1fg_1^{-1})(g_2f^{-1}g_2^{-1}) = v_1hh^{-1}v_2 = v_1v_2$$

and we have 2 of Proposition 5.1. □

Note, that if  $|K| > 3$ , condition 1 of Proposition 5.1 holds. Thus, to prove Theorem 2 it is sufficient to find elements  $u$  and  $h$  satisfying a to d. In the proof that follows we shall check conditions a to d for appropriate  $u$  and  $h$ .

Since for infinite fields Theorem 2 is a consequence of Theorem 1, we shall consider in the following only the Chevalley groups over finite fields, i.e., we shall consider  $X_n(q)$  or  ${}^lX_n(q^l)$ .

In order to check condition a of Lemma 5.2 we use the following facts.

**Lemma 5.3.** *Let  $R_1 = \langle \epsilon_1 - \epsilon_2, \dots, \epsilon_l - \epsilon_{l+1} \rangle$  be a root subsystem of  $R$  of type  $A_l$  and let  $G_1 \approx SL_{l+1}(F)/Z$  for some  $Z \subset Z(SL_{l+1}(F))$ , where  $F = K$  or  $F = k$ . Let  $u$  be a regular unipotent element in  $G_1$ . Suppose one of the following conditions holds:*

1. *There exists an element  $h_0 \in H$  such that*

$$h_0 x_{\epsilon_i - \epsilon_j}(a) h_0^{-1} = x_{\epsilon_i - \epsilon_j}(\mu_{ij} a)$$

*for every  $a \in F$ ,  $i < j$ , where  $\mu_{ij} = 1$  if  $j \neq l + 1$ ,  $\mu_{il+1} = s$  for every  $i$  and  $\langle s \rangle = F^*$ .*

2. *There exists a root subsystem  $R^1 \subset R$  such that  $R_1 \subset R^1$  and  $R^1$  is of type  $A_{l+1}$ .*

*Then condition a of Lemma 5.2 holds for  $u$ .*

*Proof.* 1. We may assume for simplicity that  $G_1 \approx SL_{l+1}(F)$ , because the question considered is on the  $HG_1$ -conjugacy class of  $u$ . One easily sees that 1 implies  $\langle G_1, h_0, Z(GL_{l+1}(F)) \rangle = GL_{l+1}(F)$ . Now condition a follows from Lev.

2. We may assume the group generated by  $R^1$  is isomorphic to  $SL_{l+2}(F)$ . Thus  $G_1 \leq GL_{l+1}(F) \leq G$ . Now we can apply Lev again.  $\square$

**Lemma 5.4.** *Suppose  $R_1$  is of type  $A_l$ . Let  $u \in G_1$  be the image of the matrix*

$$\tilde{u} = \begin{pmatrix} \alpha & 0 & & \\ 0 & \alpha^{-1} & & \\ & & & J_{l-1} \end{pmatrix},$$

*where  $\alpha \neq \alpha^{-1}$ ,  $\alpha \in k^*$ , and  $J_{l-1}$  is a unipotent Jordan block ( $J_0 = \emptyset, J_1 = 1$ ). Then  $u$  satisfies condition a of Lemma 5.2.*

*Proof.* If any matrix from  $SL_{l+1}(K)$  is  $GL_{l+1}(K)$ -conjugate to  $\tilde{u}$ , then it is also  $SL_{l+1}(k)$ -conjugate to  $\tilde{u}$ . Thus our statement follows from Lev.  $\square$

In order to check c of Lemma 5.2 we shall use the following result.

**Lemma 5.5.** *Let  $u$  be a regular element in  $G_1$ . Assume either  $u$  is unipotent and the conditions of Lemma 5.3 hold, or  $u$  is an element as described in Lemma 5.4. Suppose  $-1_W \in W$  and also that for twisted groups the element  $h$  from Lemma 5.2 belongs to the subgroup  $\langle h_\alpha(t) \mid \alpha \in R, t \in k \rangle$ , where  $R$  is the root system of  $G$ . Then condition c of Lemma 5.2 holds.*

*Proof.* Clearly  $-1_W(h) = h^{-1}$  for every  $h \in H$ . Further,  $-1_W(u)$  is a regular unipotent element in  $G_1$  which is  $\langle G_1, h_0 \rangle$ -conjugate to  $u$  or  $-1_W(u)$  is an element in  $G_1$  which is a product of a regular unipotent element of a subgroup of type  $A_{l-2}$  and a semisimple element with eigenvalues  $\alpha$  and  $\alpha^{-1}$  which commutes with the first one. Thus,  $-1_W(u)$  is  $HG_1$ -conjugate to  $u$ .  $\square$

In order to check d of Lemma 5.2 we use the following statement.

**Lemma 5.6.** *Let  $f = g_s g_u \in HG_1$ , where  $g_s \in H, g_u \in \mathcal{U}$  and  $g_s g_u = g_u g_s$ . Suppose that for every  $\alpha \in R \setminus R_1, \alpha > 0$ , and for every  $a \in K$*

$$g_s x_\alpha(a) g_s^{-1} = x_\alpha(\mu_\alpha a), \quad \text{where } \mu_\alpha \neq 1,$$

*or, in the case where  $X_\alpha$  is a two parameter root subgroup, for every  $a, b \in K$*

$$g_s x_\alpha(a, b) g_s^{-1} = x_\alpha(\mu_\alpha a, \nu_\alpha b), \quad \text{where } \mu_\alpha, \nu_\alpha \neq 1,$$

or, in the case where  $X_\alpha$  is a three parameter root subgroup, for every  $a, b, c \in K$

$$g_s x_\alpha(a, b, c) g_s^{-1} = x_\alpha(\mu_\alpha a, \nu_\alpha b, \lambda_\alpha c), \quad \text{where } \mu_\alpha, \nu_\alpha, \lambda_\alpha \neq 1.$$

Then the element  $f$  satisfies 3 of Proposition 5.1.

*Proof.* We consider the action of  $f$  on  $V_i/V_{i+1}$  by conjugation. As a linear operator  $g_u$  acts as unipotent and  $g_s$  as semisimple operator with eigenvalues  $\{\mu_\alpha\}, \{\nu_\alpha\}, \{\lambda_\alpha\}$ . Since  $g_s g_u = g_u g_s$  and since there is no 1 among the eigenvalues of  $g_s$ , the operator  $f = g_s g_u$  also has no eigenvalue 1. This implies our statement.  $\square$

Now we consider different cases.

$B_2(q); q \geq 4$ . We put

$$\Delta_1 = \{\epsilon_2\}, \quad u = x_{\epsilon_2}(t), \quad h = h_{\epsilon_1}(s), \quad f = hu,$$

where  $t, s \in K^*$ , and  $\langle s \rangle = K^*$ . We check the conditions a to d of Lemma 5.2.

a. Put  $h_0 = h_{\epsilon_1 + \epsilon_2}(s)$ . Then

$$h_0 x_{\epsilon_2}(t) h_0^{-1} = x_{\epsilon_2}(st).$$

Therefore  $h_0$  satisfies the conditions of Lemma 5.3, and a follows.

b. This is obvious.

c. This is a consequence of Lemma 5.5.

d. Here  $V = \langle X_{\epsilon_1 \pm \epsilon_2}, X_{\epsilon_1} \rangle$ . So

$$h x_\alpha(t) h^{-1} = x_\alpha(s^2 t)$$

for  $\alpha = \epsilon_1, \epsilon_1 \pm \epsilon_2$ . Now we use Lemma 5.6.

$B_l(q); l > 2; q \geq 7$ . We put

$$\Delta_1 = \{\epsilon_1 - \epsilon_2, \dots, \epsilon_{l-1} - \epsilon_l\}, \quad \Delta_2 = \{\epsilon_3 - \epsilon_4, \dots, \epsilon_{l-1} - \epsilon_l\},$$

(if  $l < 4$  we put  $\Delta_2 = \emptyset$ ),  $G_2 = \langle X_{\pm\alpha} \mid \alpha \in \langle \Delta_2 \rangle \rangle$ . Let  $\tilde{u}$  denote a regular unipotent element in  $G_2$ ,  $u = h_{\epsilon_1 - \epsilon_2}(s) \tilde{u}$ , where  $\langle s \rangle = K^*$ ,  $h = h_{\epsilon_1}(s) \cdots h_{\epsilon_l}(s)$ ,  $f = hu$ .

We check the conditions a to d of Lemma 5.2.

a. This follows from Lemma 5.4.

b. This is obvious.

c. This follows from Lemma 5.5.

d. Here  $V = \langle X_{\epsilon_i}, X_{\epsilon_k + \epsilon_l} \rangle$ . We have

$$h h_{\epsilon_1 - \epsilon_2}(s) x_\alpha(t) h_{\epsilon_1 - \epsilon_2}^{-1}(s) h^{-1} = x_\alpha(\mu_\alpha t),$$

where

$$\mu_\alpha = \begin{cases} s^3 & \text{if } \alpha = \epsilon_1, \\ s & \text{if } \alpha = \epsilon_2, \\ s^2 & \text{if } \alpha = \epsilon_i, i > 2, \\ s^5 & \text{if } \alpha = \epsilon_1 + \epsilon_k, k > 2, \\ s^3 & \text{if } \alpha = \epsilon_2 + \epsilon_k, k > 2, \\ s^4 & \text{if } \alpha = \epsilon_1 + \epsilon_2. \end{cases}$$

Now we use Lemma 5.6.

$C_l(q); l \geq 3; q \geq 4$ . We put  $\Delta_1 = \{\epsilon_1 - \epsilon_2, \dots, \epsilon_{l-1} - \epsilon_l\}$ . Let  $u$  denote a regular unipotent element in  $G_1$ ,  $\langle s \rangle = K^*$ , and  $h = h_{2\epsilon_1}(s) \cdots h_{2\epsilon_l}(s)$ .

- a. Put  $h_0 = h_{2\epsilon_l}(s)$ . Then

$$h_0 x_{\epsilon_i - \epsilon_{i+1}}(t) h_0^{-1} = x_{\epsilon_i - \epsilon_{i+1}}(\mu_i t),$$

where  $\mu_i = 1$  if  $i < l - 1$  and  $\mu_i = s^{-1}$  if  $i = l - 1$ . Thus  $h_0$  satisfies the condition of Lemma 5.3, and a is proved.

- b. This is obvious.
- c. This follows from Lemma 5.5.
- d. Here  $V = \langle X_{\epsilon_i + \epsilon_j}, X_{2\epsilon_i} \rangle$ . So

$$h x_\alpha(t) h^{-1} = x_\alpha(s^2 t)$$

for every  $\alpha = \epsilon_i + \epsilon_j, 2\epsilon_i$ . Now we use Lemma 5.6.

$D_{2l}(q); 2l = n \geq 4; q \geq 5$ . We put

$$\Delta_1 = \{\epsilon_1 - \epsilon_2, \dots, \epsilon_{n-1} - \epsilon_n\}, \quad \Delta_2 = \{\epsilon_3 - \epsilon_4, \dots, \epsilon_{n-1} - \epsilon_n\},$$

$G_2 = \langle X_{\pm\alpha} | \alpha \in \langle \Delta_2 \rangle \rangle$ . Let  $\tilde{u}$  denote a regular unipotent element in  $G_2$ ,  $u = h_{\epsilon_1 - \epsilon_2}(s) \tilde{u}$ , where  $\langle s \rangle = K^*$ ,  $h = h_{\epsilon_1 + \epsilon_2}(s) \cdots h_{\epsilon_{n-1} + \epsilon_n}(s)$ ,  $f = hu$ .

- a. This follows from Lemma 5.4.
- b. This is obvious.
- c. This follows from Lemma 5.5.
- d. Here  $V = \langle X_{\epsilon_i + \epsilon_j} \rangle$ . We have

$$h h_{\epsilon_1 - \epsilon_2}(s) x_\alpha(t) h_{\epsilon_1 - \epsilon_2}^{-1}(s) h^{-1} = x_\alpha(\mu_\alpha t)$$

where

$$\mu_\alpha = \begin{cases} s^3 & \text{if } \alpha = \epsilon_1 + \epsilon_k, k > 2, \\ s & \text{if } \alpha = \epsilon_2 + \epsilon_k, k > 2, \\ s^2 & \text{if } \alpha = \epsilon_1 + \epsilon_2 \text{ or } \epsilon_i + \epsilon_j, i, j > 2. \end{cases}$$

Now we use Lemma 5.6.

$D_{2l+1}(q); n = 2l + 1 \geq 5; q \geq 4$ . Let  $\Delta_1 = \{\epsilon_2 - \epsilon_3, \dots, \epsilon_{n-1} - \epsilon_n\}$ . Let  $u$  denote a regular unipotent element in  $G_1$  and put  $h = h_{\epsilon_2 + \epsilon_3}(s) \cdots h_{\epsilon_{n-1} + \epsilon_n}(s)$ , where  $\langle s \rangle = K^*$ .

- a. This follows from Lemma 5.3.
- b. This is obvious.
- c. This follows from Lemma 5.5, because  $-1 \in W(D_{n-1})$ .
- d. Here  $V = \langle X_{\epsilon_1 \pm \epsilon_i}, X_{\epsilon_i + \epsilon_j} \rangle, i, j > 1$ ; then  $h x_\alpha(t) h^{-1} = x_\alpha(\mu_\alpha t)$ , where

$$\mu_\alpha = \begin{cases} s & \text{if } \alpha = \epsilon_1 + \epsilon_k, \\ s^{-1} & \text{if } \alpha = \epsilon_1 - \epsilon_k, \\ s^2 & \text{if } \alpha = \epsilon_i + \epsilon_j, i, j > 1. \end{cases}$$

Now we apply Lemma 5.6.

$E_6(q); q \geq 7$ . We put

$$\begin{aligned} \Delta_1 &= \{\epsilon_3 - \epsilon_2, \epsilon_4 - \epsilon_3, \epsilon_5 - \epsilon_4\}, \\ \beta &= \frac{1}{2}(\epsilon_8 - \epsilon_7 - \epsilon_6 + \epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4 + \epsilon_5), \\ \gamma &= \frac{1}{2}(\epsilon_8 - \epsilon_7 - \epsilon_6 + \epsilon_1 - \epsilon_2 - \epsilon_3 - \epsilon_4 - \epsilon_5), \\ \langle t_\gamma \rangle &= K^*, \quad t_\beta \in K^*, \quad t_\beta \neq t_\gamma^{\pm 1}, \quad t_\beta^2 \neq 1, \\ h &= h_\beta(t_\beta)h_\gamma(t_\gamma). \end{aligned}$$

Let  $u$  be a regular unipotent element in  $G_1$  and  $f = hu$ .

- a. This follows from Lemma 5.3.
- b. This can be confirmed by a simple calculation.
- c. Let  $w = w_\beta w_\gamma$ . It is easy to see that  $\alpha \pm \beta$  and  $\alpha \pm \gamma$  are not roots for any  $\alpha = \epsilon_k - \epsilon_l, k, l > 1$ . Clearly  $w_\beta w_\gamma = w_\gamma w_\beta$ , and  $w$  commutes with all elements in  $G_1$ . Therefore  $w(h) = h^{-1}$  and  $w(u) = u$ . This shows c.
- d. Here

$$V = \langle X_{\epsilon_k - \epsilon_1}, X_{\epsilon_i + \epsilon_j}, i, j, k \leq 5, X_\alpha \rangle,$$

where  $\alpha = \frac{1}{2}(\epsilon_8 - \epsilon_7 - \epsilon_6 + \sum_{i=1}^5 (-1)^{\nu(i)} \epsilon_i)$  with  $\sum_{i=1}^5 \nu(i) \equiv 0 \pmod{2}$ . Then

$$hx_\delta(a)h^{-1} = x_\delta(\mu_\delta a),$$

where  $\delta = \epsilon_k - \epsilon_1, \epsilon_i + \epsilon_j, \alpha$  and  $\mu_\delta = t_\beta^2, t_\gamma^2, t_\beta^{\pm 1}, t_\gamma^{\pm 1}, t_\beta^{\pm 1} t_\gamma^{\pm 1}$ . Now we apply Lemma 5.6.

$E_7(q); q \geq 5$ . We put  $\Delta_1 = \{\epsilon_2 - \epsilon_1, \epsilon_3 - \epsilon_2, \epsilon_4 - \epsilon_3, \epsilon_5 - \epsilon_4, \epsilon_6 - \epsilon_5\}$ . Let  $u$  be a regular unipotent element in  $G_1$ ,  $\langle s \rangle = K^*$ ,  $h = h_{\epsilon_8 - \epsilon_7}(s)h_{\epsilon_1 + \epsilon_2}(s)h_{\epsilon_3 + \epsilon_4}(s)h_{\epsilon_5 + \epsilon_6}(s)$ , and  $f = hu$ .

- a. This follows from Lemma 5.3.
- b. This requires only a simple calculation.
- c. Here  $-1 \in W(E_7)$ , and we can apply Lemma 5.5.
- d.  $V = \langle X_{\epsilon_i + \epsilon_j}, i, j \leq 6, X_{\epsilon_8 - \epsilon_7}, X_\alpha \rangle$ , where

$$\alpha = \frac{1}{2} \left( \epsilon_8 - \epsilon_7 + \sum_{i=1}^6 (-1)^{\nu(i)} \epsilon_i \right), \quad \sum_{i=1}^6 \nu(i) \equiv 1 \pmod{2}.$$

Then

$$\begin{aligned} hx_{\epsilon_i + \epsilon_j}(a)h^{-1} &= x_{\epsilon_i + \epsilon_j}(s^2 a), \\ hx_{\epsilon_8 - \epsilon_7}(a)h^{-1} &= x_{\epsilon_8 - \epsilon_7}(s^2 a), \\ hx_\alpha(a)h^{-1} &= x_\alpha(\mu_\alpha a), \end{aligned}$$

where  $\alpha = \frac{1}{2}(\epsilon_8 - \epsilon_7 + \sum_{i=1}^6 (-1)^{\nu(i)} \epsilon_i)$ ,  $\sum_{i=1}^6 \nu(i) \equiv 1 \pmod{2}$ ,  $\mu_\alpha = s, s^3, s^{-1}$ . Thus we can apply Lemma 5.6.

$E_8(q); q \geq 7$ . We put  $\Delta_1 = \{\epsilon_2 - \epsilon_1, \epsilon_3 - \epsilon_2, \epsilon_4 - \epsilon_3, \epsilon_5 - \epsilon_4, \epsilon_6 - \epsilon_5, \epsilon_7 - \epsilon_6\}$ . Let  $u$  be a regular unipotent element in  $G_1$ ,

$$\langle t \rangle = K^*, \quad h = h_{\epsilon_8 - \epsilon_7}(t^2)h_{\epsilon_8 + \epsilon_7}(t^2)h_{\alpha_0}(t),$$

where  $\alpha_0 = \frac{1}{2}(\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4 + \epsilon_5 + \epsilon_6 + \epsilon_7 + \epsilon_8)$ ,  $f = hu$ .

- This follows from Lemma 5.3.
- This is obvious.
- Clearly  $-1 \in W(E_8)$ , and we can use Lemma 5.5.
- Here

$$V = \langle X_{\epsilon_8 - \epsilon_k}, X_{\epsilon_8 + \epsilon_k}, k \leq 7, X_{\epsilon_i + \epsilon_j}, i, j \leq 7, X_\beta \rangle,$$

where  $\beta = \frac{1}{2}(\epsilon_8 + \sum_{i=1}^7 (-1)^{\nu(i)} \epsilon_i)$ ,  $\sum_{i=1}^7 \nu(i) \equiv 0 \pmod{2}$ . Then

$$hx_{\epsilon_i + \epsilon_j}(a)h^{-1} = x_{\epsilon_i + \epsilon_j}(ta),$$

and for  $k \leq 7$  we get

$$\begin{aligned} hx_{\epsilon_8 - \epsilon_k}(a)h^{-1} &= x_{\epsilon_8 - \epsilon_k}(t^4 a), \\ hx_{\epsilon_8 + \epsilon_k}(a)h^{-1} &= x_{\epsilon_8 + \epsilon_k}(t^5 a), \\ hx_\beta(a)h^{-1} &= x_\beta(\mu_\beta a), \end{aligned}$$

where  $\mu_\beta = t, t^2, t^3, t^4$ . Now we apply Lemma 5.6.

$F_4(q); q \geq 8$ . We put  $\Delta_1 = \{\epsilon_2 - \epsilon_3, \epsilon_3 - \epsilon_4\}$ . Let  $u$  be a regular unipotent element in  $G_1$ ,  $\beta_0 = \frac{1}{2}(\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4)$ ,  $\langle s \rangle = K^*$ ,  $h = h_{\beta_0}(s)h_{\epsilon_2}(s)h_{\epsilon_3}(s)h_{\epsilon_4}(s)$ .

- This follows from Lemma 5.3.
- This is obvious.
- Clearly  $-1 \in W(F_4)$ , and we can apply Lemma 5.5.
- $V = \langle X_{\epsilon_i + \epsilon_j}, i, j > 1, X_{\epsilon_i}, X_{\epsilon_1 - \epsilon_k}, X_{\epsilon_1 + \epsilon_k}, X_\beta \rangle$ , where  $\beta = \frac{1}{2}(\epsilon_1 \pm \epsilon_2 \pm \epsilon_3 \pm \epsilon_4)$ ,

$$\begin{aligned} hx_{\epsilon_i + \epsilon_j}(a)h^{-1} &= x_{\epsilon_i + \epsilon_j}(s^6 a), \\ hx_{\epsilon_i}(a)h^{-1} &= x_{\epsilon_i}(\mu_i a), \end{aligned}$$

where  $\mu_1 = s$  and  $\mu_i = s^3$  if  $i > 1$ ,

$$\begin{aligned} hx_{\epsilon_1 - \epsilon_k}(a)h^{-1} &= x_{\epsilon_1 - \epsilon_k}(s^{-2} a), \\ hx_{\epsilon_1 + \epsilon_k}(a)h^{-1} &= x_{\epsilon_1 + \epsilon_k}(s^4 a), \\ hx_\beta(a)h^{-1} &= x_\beta(\mu_\beta a), \end{aligned}$$

where  $\mu_\beta = s^5, s^{-4}, s^2, s^{-1}$ . Now we apply Lemma 5.6.

$G_2(q); q \geq 7$ . Let  $\langle s \rangle = K^*$ ,  $h = h_{\epsilon_1 - \epsilon_2}(s)h_{2\epsilon_3 - \epsilon_1 - \epsilon_2}(s)$ . For every  $\beta \in R$  we have

$$hx_\beta(a)h^{-1} = x_\beta(\mu_\beta a),$$

where  $\mu_\beta = s^{\pm 2}, s^{\pm 3}, s^{\pm 1}, s^{\pm 5}$ . Hence  $h$  is a regular element. Since  $-1 \in W(G_2)$ , the element  $h$  is real. Now we can apply Theorem 1 from [EGII].

${}^2A_{2l-1}(q^2)$ ;  $l \geq 2$ ;  $q \geq 8$ . We use the notation of [C1]. Put

$$\Delta_1 = \{e_1 - e_2, \dots, e_{l-1} - e_l\}, \quad \Delta_2 = \{e_3 - e_4, \dots, e_{l-1} - e_l\},$$

$$G_2 = \langle X_{\pm\alpha} | \alpha \in \langle \Delta_2 \rangle \rangle.$$

Let  $\tilde{u}$  be a regular unipotent element in  $G_2$ ,

$$\langle t \rangle = k^*, \quad u = h_{e_1 - e_2}(t)\tilde{u},$$

$$h = h_{2e_1}(t^2) \cdots h_{2e_l}(t^2), \quad f = hu.$$

- a. This follows from Lemma 5.4.
- b. This can be confirmed by a simple calculation:

$$h_{2e_i}(t^2)x_{e_k - e_m}(a)h_{2e_i}^{-1}(t^2) = x_{e_k - e_m}(\delta_i a),$$

where

$$\delta_i = \begin{cases} t^2 & \text{if } i = k, \\ t^{-2} & \text{if } i = m, \\ 1 & \text{if } i \neq k, m. \end{cases}$$

- c. Since  $-1 \in W(C_l)$  and the parameters in  $h$  and  $h_{e_1 - e_2}(t)$  belong to  $k$ , we can apply Lemma 5.5.
- d.  $V = \langle X_{e_i + e_j}, X_{2e_k} \rangle$ . Now

$$h_{e_1 - e_2}(t)x_{e_i + e_j}(a)h_{e_1 - e_2}^{-1}(t) = x_{e_i + e_j}(\mu_{ij} a),$$

where

$$\mu_{ij} = \begin{cases} t & \text{if } i = 1, j > 2, \\ t^{-1} & \text{if } i = 2, j > 2, \\ 1 & \text{if } i = 1, j = 2. \end{cases}$$

Further,  $h_{e_1 - e_2}(t)x_{2e_k}(a)h_{e_1 - e_2}^{-1}(t) = x_{2e_k}(\delta_k a)$ , where

$$\delta_k = \begin{cases} t^2 & \text{if } k = 1, \\ t^{-2} & \text{if } k = 2, \\ 1 & \text{if } k > 2. \end{cases}$$

Finally,

$$hx_\alpha(a)h^{-1} = x_\alpha(t^4 a)$$

for  $\alpha = e_i + e_j$  and  $\alpha = 2e_k$ . Thus

$$hh_{e_1 - e_2}(t)x_\alpha(a)h_{e_1 - e_2}^{-1}(t)h^{-1} = x_\alpha(\gamma a),$$

where  $\gamma = t^2, t^3, t^4, t^5, t^6$ . Now we apply Lemma 5.6.

${}^2A_{2l}(q^2)$ ;  $q \geq 4$ . If  $l = 1$  then we take  $h = \text{diag}(t, 1, t^{-1})$ , where  $t$  is a generator of  $k^*$ . It is easy to see that  $h$  is a real regular semisimple element in  $SU_3(q^2)$  if  $q \geq 4$ . Thus the image  $f$  of  $h$  in  $G$  is also real regular semisimple. Theorem 2 now is a consequence of Theorem 1.

Now let  $l > 1$  and put  $\Delta_1 = \{e_1 - e_2, \dots, e_{l-1} - e_l\}$ . Let  $u$  be a regular unipotent element in  $G$ ,  $\langle t \rangle = k^*$ ,  $h = h_{e_1}(t) \cdots h_{e_l}(t)$ ,  $f = hu$ .

- a. Put  $h_0 = h_{e_l}(s)$ , where  $\langle s \rangle = K^*$ . Then  $h_0$  commutes with all roots of the form  $x_{e_i - e_k}$  if  $i, k \neq l$ . One can check that

$$h_0 x_{e_i - e_l}(a) h_0^{-1} = x_{e_i - e_l}(s^{-1}a).$$

Thus we can apply Lemma 5.3.

- b. This follows by a simple calculation.
- c. Since  $-1 \in W(B_l)$  and the parameter  $t \in k$ , we can apply Lemma 5.5.
- d.  $V = \langle X_{e_i + e_j}, X_{e_k} \rangle$ . We have (see [St])

$$h_{e_i}(t) x_{e_i}(a, b) h_{e_i}^{-1}(t) = x_{e_i}(ta, t^2b).$$

Further,

$$\begin{aligned} h_{e_i}(t) x_{e_k}(a, b) h_{e_i}^{-1}(t) &= x_{e_i}(a, b) && \text{if } k \neq i, \\ h_{e_i}(t) x_{e_i + e_j}(a) h_{e_i}^{-1}(t) &= x_{e_i + e_j}(ta), \\ h_{e_i}(t) x_{e_k + e_m}(a) h_{e_i}^{-1}(t) &= x_{e_k + e_m}(a) && \text{if } k, m \neq i. \end{aligned}$$

Hence,

$$h x_{e_i}(a, b) h^{-1} = x_{e_i}(ta, t^2b), \quad h x_{e_i + e_j}(a) h^{-1} = x_{e_i + e_j}(t^2a).$$

Thus we can apply Lemma 5.6.

${}^2D_{l+1}(q^2); q \geq 7$ . Put

$$\Delta_1 = \{e_1 - e_2, \dots, e_{l-1} - e_l\}.$$

Let  $u$  be a regular unipotent element in  $G_1$ ,  $h = h_{e_1}(s) \cdots h_{e_l}(s)$ ,  $\langle s \rangle = k^*$ , and  $f = hu$ .

- a. This follows from Lemma 5.3 with  $h_0 = h_{e_l}(t)$ ,  $\langle t \rangle = K^*$ .
- b. This is obvious.
- c. This is true because  $-1 \in W(B_l)$  and the parameter  $s$  in  $h$  belongs to  $k$ .
- d.  $V = \langle X_{e_i}, X_{e_i + e_j} \rangle$ . Then

$$\begin{aligned} h(s) x_{e_i}(a) h^{-1}(s) &= x_{e_i}(s^2a), \\ h(s) x_{e_i + e_j}(a) h^{-1}(s) &= x_{e_i + e_j}(s^4a). \end{aligned}$$

So we have confirmed d.

${}^2E_6(q^2); q \geq 8$ . Here we have the root system of type  $F_4$ . If in the proof of the case  $F_4$  we put the parameter  $t \in k$ , we also have a proof for  ${}^2E_6(q^2)$ .

For the cases  ${}^3D_4(q^3)$ ,  $q \geq 7$ ,  ${}^2B_2(2^{2m+1})$ ,  $m \geq 1$ ,  ${}^2G_2(3^{2m+1})$ ,  $m \geq 1$ ,  ${}^2F_4(2^{2r+1})$ ,  $r \geq 2$ , there exist regular semisimple elements; see [EGIII, Section 4].

#### REFERENCES

- [AH] *Products of conjugacy classes in groups*, Lecture Notes in Mathematics, no. 1112 (Z. Arad and M. Herzog, eds.), Springer Verlag, New York, 1985. MR **87h**:20001
- [B] O. Bonten, *Über Kommutatoren in endlichen einfachen Gruppen*, Aachener Beiträge zur Mathematik, Bd. 7, Verlag der Augustinus-Buchhandlung, Aachen, 1993.
- [Bo] N. Bourbaki, *Groupes et algèbres de Lie IV, V, VI*, Hermann, Paris, 1968. MR **39**:1590
- [Br] J. L. Brenner, *Covering theorems for finisigs X*, Ars Combinatoria **16** (1983), 57–67. MR **85g**:20021
- [BrL] J. L. Brenner and R. J. List, *Application of partition theory to groups: Covering the alternating group by products of conjugacy classes*, Number Theory (J. M. De Koninck and C. Levesque, eds.), Walter de Gruyter, Berlin, New York, 1989, pp. 65–71. MR **90k**:20029

- [C1] R. W. Carter, *Simple Groups of Lie Type*, John Wiley & Sons, London, 1989. MR **90g**:20001
- [C2] R. W. Carter, *Finite Groups of Lie Type*, John Wiley & Sons, Chichester, 1993. MR **94k**:20020
- [EGI] E. W. Ellers and N. L. Gordeev, *Gauss decomposition with prescribed semisimple part in classical Chevalley groups*, *Comm Algebra* **22** (1994, no. 14), 5935–5950. MR **95m**:20052
- [EGII] E. W. Ellers and N. L. Gordeev, *Gauss decomposition with prescribed semisimple part in Chevalley groups II: Exceptional cases*, *Comm Algebra* **23** (1995, no. 8), 3085–3098. MR **96f**:20064
- [EGIII] E. W. Ellers and N. L. Gordeev, *Gauss decomposition with prescribed semisimple part in Chevalley groups III: Twisted groups*, *Comm Algebra* **24** (1996, no. 14), 4447–4475. MR **98a**:20048
- [G1] D. Gluck, *Character value estimates for groups of Lie type*, *Pacific J. Math.* **150** (1991), 279–307. MR **92k**:20014
- [G2] D. Gluck, *Character value estimates for non-semisimple elements*, *J. Algebra* **155** (1993), 221–237. MR **94b**:20023
- [G3] D. Gluck, *Sharper character value estimates for groups of Lie type*, *J. Algebra* **174** (1995), 229–266. MR **96m**:20021
- [Go] M. Goto, *A theorem on compact semisimple groups*, *J. Math. Soc. Japan* **1** (1949), 270–272. MR **11**:497d
- [Gow] R. Gow, *Commutators in the symplectic group*, *Arch. Math. (Basel)* **50** (1988), 204–209. MR **89g**:20071
- [H] C. Hsü (Xu), *The commutators of the alternating group*, *Sci. Sinica* **14** (1965), 339–342. MR **32**:1241
- [I] I. M. Isaacs, *Character theory of finite groups*, Academic Press, New York, 1976. MR **57**:417
- [L] T. J. Laffey, *Products of matrices*, *Generators and relations in groups and geometries*, (A. Barlotti, E. W. Ellers, P. Plaumann, K. Strambach, eds.), NATO ASI Series C, vol. 333, Kluwer Academic Publishers, Dordrecht, 1991, pp. 95–123. MR **93m**:15018
- [Le] A. Lev, *Products of cyclic similarity classes in the groups  $GL_n(F)$* , *Linear Algebra Appl.* **202** (1994), 235–266. MR **95e**:20062
- [MSaWe] G. Malle, J. Saxl, and T. Weigel, *Generation of classical groups*, *Geom. Dedicata* **40** (1994), 85–116. MR **95c**:20068
- [NPaCl] J. Neubüser, H. Pahlings and E. Cleuvers, *Each sporadic finasig  $G$  has a class  $C$  such that  $CC = G$* , *Abstracts AMS* **34** (1984), 6.
- [O] O. Ore, *Some remarks on commutators*, *Proc. Amer. Math. Soc.* **272** (1951), 307–314. MR **12**:671e
- [PW] S. Pasiencier and H. C. Wang, *Commutators in a complex semisimple Lie group*, *Proc. Amer. Math. Soc.* **13** (1962), 907–913. MR **30**:190
- [R] R. Ree, *Commutators in semi-simple algebraic groups*, *Proc. Amer. Math. Soc.* **15** (1964), 457–460. MR **28**:5148
- [S] K. Shoda, *Über den Kommutator der Matrizen*, *J. Math. Soc. Japan* **3** (1951), 78–81. MR **13**:425b
- [So] A. R. Sourour, *A factorization theorem for matrices*, *Linear and Multilinear Algebra* **19** (1986, no. 2), 141–147. MR **87j**:15028
- [St] R. Steinberg, *Lectures on Chevalley Groups*, Yale University, 1967. MR **57**:6215
- [VWh] L. N. Vaserstein and E. Wheland, *Commutators and companion matrices over rings of stable rank one*, *Linear Algebra Appl.* **142** (1990), 263–277. MR **92a**:19002
- [Wi] J. S. Wilson, *On simple pseudofinite groups*, *J. London Math. Soc. (2)* **51** (1995), 471–490. MR **96c**:20005

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO, TORONTO, ONTARIO, CANADA M5S 3G3

*E-mail address:* `ellers@math.utoronto.ca`

DEPARTMENT OF MATHEMATICS, RUSSIAN STATE PEDAGOGICAL UNIVERSITY, MOIJK 48, ST. PETERSBURG, RUSSIA 191-186

*E-mail address:* `algebra@ivt.rgpu.spb.ru`