Normal subgroups of $\mathbf{SL}_{1,D}$ and the classification of finite simple groups

Andrei Rapinchuk and Alexander Potapchik

1. Introduction

Let G be a simple simply connected algebraic group over an algebraic number field K. There is a conjecture due to Platonov and Margulis (*cf.* [PR3], ch. IX) that the normal subgroup structure of the group of K-rational points $G(K)$ should be as follows:

(PM) *let T be the set of all non-archimedean places v of K such that G is K_v-anisotropic; then for any noncentral normal subgroup $N \subset G(K)$ there should be an open normal subgroup $W \subset G(K,T) = \prod_{v\in T} G(K_v)$ such that $N = G(K) \cap W$; in particular, if $T = \emptyset$ (which is always the case if G is not of type A_n) then $G(K)$ should not have any proper noncentral normal subgroups (i.e. should be projectively simple).*

By now, this conjecture has been proved for almost all K-isotropic groups and most K-anisotropic groups of type different from A_n (*cf. loc. cit*). So, major attention is currently focused on the main remaining case of anisotropic groups of type A_n. The first result dealing with (PM) for this case was obtained in [PR1]; it was shown that for $G = \mathbf{SL}_{1,D}$, D a quaternion division algebra such that $T = \emptyset$, the group $G(K)$ is perfect (i.e. $G(K) = [G(K), G(K)]$). Note that for $G = \mathbf{SL}_{1,D}$, the set T introduced in the statement of (PM) coincides with the set of non-archimedean places v of K such that $D_v = D \otimes_K K_v$ is a division algebra. Using some methods from [PR1], Margulis [M2] proved (PM) for $G = \mathbf{SL}_{1,D}$ where D is an arbitrary quaternion algebra, in full. The technique of [PR1] was extended in [PR2] to division algebras of arbitrary index to prove (under some minor restriction on the dyadic ramification places of D) that the commutator subgroup $[G(K), G(K)]$ is always T-adically open in $G(K)$ (by the T-adic topology we mean the topology induced from the group $G(K,T) = \prod_{v\in T} G(K_v)$). Subsequently, Raghunathan [Ra] lifted the restriction imposed on D in [PR2] and proved that, more generally, the commutator subgroup $[U,U]$ of any T-adically open subgroup $U \subset G(K)$ is again T-adically open. Finally, Tomanov [To] gave reduction of (PM) for $G = \mathbf{SL}_{1,D}$ to division algebras of odd index; in particular he proved (PM) for all algebras of index 2^d. In the present paper we prove (PM) for $G = \mathbf{SL}_{1,D}$ where D is a division algebra of index 3. This is the first result on (PM) for division algebras of odd index, and by Tomanov's Theorem it implies (PM) also for all division algebras of index $3 \cdot 2^d$.

Theorem 1.1 *Let D be a central division algebra over K of index 3, $G = \mathbf{SL}_{1,D}$. Then the normal subgroup structure of $G(K)$ is given by* (PM).

The proof of this theorem is based on methods which are essentially different from those employed in the previous works on (PM). Its main feature is the usage of (CSG), the classification of finite simple groups. (By (CSG) we mean the statement that any finite non-abelian simple group is either a group of Lie type or an alternating group, or else is one of the 26 sporadic groups, *cf.* [Atlas]). To be more precise, (CSG) is used at two places in the proof of Theorem 1.1. One of them is so-called Push-up Theorem (*cf.* Theorem 2.1) which claims that if for $G = \mathbf{SL}_{1,D}$, D a division algebra of arbitrary index, the group $G(K)$ fails to satisfy (PM) then there exists a normal subgroup $N \subset D^*$ such that the quotient D^*/N is a finite simple group. Actually, the proof of this assertion uses not (CSG) itself but its following important consequence (Theorem 2.4): any class-preserving automorphism of a finite simple group F is inner.

This result suggests the following conjecture which can be regarded as a generalization of (PM) to division algebras over arbitrary field: *let D be a finite dimensional algebra over an arbitrary field; then D^* does not have any normal subgroup N such that D^*/N is a non-abelian finite simple group.*

In the present paper, we prove this conjecture for algebras of degree 2 and 3, which yields Theorem m 1.1 and gives an alternate proof of Margulis' Theorem [M2]. The argument for algebras of degree 2 actually imitates the proof of Theorem 3 in [PR1] and does not use (CSG), while consideration of algebras of degree 3 is based on a new approach.

First, we show that all quotients of D^*, D a division algebra of degree 3, satisfy a certain abstract property (called here property (C), *cf.* §3), and then prove that, on the contrary, none of the (known) finite simple groups has this property (*cf.* Theorem 3.5). The proof of Theorem 3.5 takes the major part of this paper, and it is the other spot in the proof of Theorem 1.1 which depends on (CSG) (note that here the dependence on (CSG) is stronger than in the proof of the Push-up Theorem, viz. to handle the sporadic groups, we use the detailed information about centralizers of elements from [Atlas]).

We hope to apply the technique of this paper also to other division algebras. Apparently, this can be done via a more thorough analysis of "additive" properties of multiplicative normal subgroups in D^* of finite index. (Some important results in this direction were obtained in [BS], [Tu].) So, in §7 we describe the additive properties that would enable us to prove (PM).

During the preparation of this paper, the first-named author was visiting the University of Bielefeld on a Fellowship awarded by the Alexander von Humboldt Foundation (Bonn). The second-named author was at that time a research co-worker at the SFB 343 "Diskrete Strukturen in der Mathematik" (Universität Bielefeld). The support of all these institutions is thankfully acknowledged. Also, it is our great pleasure to thank Herbert Abels for his encouragement and help without which this work would have hardly been done.

2. A Push-up Theorem

Theorem 2.1 *Let D be a finite dimensional division algebra over an algebraic number field K. If $\mathbf{SL}_{1,D}$ fails to satisfy* (PM) *then there exists a normal subgroup $N \subset D^*$ such that D^*/N is a non-abelian finite simple group.*

Proof. It is easy to show (*cf.* [PR3], Lemma 9.2) that the assertion of (PM) is true for a normal subgroup $N \subset \mathrm{SL}_1(D)$ if and only if N is T-adically closed (in $\mathrm{SL}_1(D)$). Therefore, our assumption entails the existence of a normal subgroup $M \subset \mathrm{SL}_1(D)$ such that $M \neq \overline{M}$ where the bar denotes closure in $\mathrm{SL}_1(D)$ with respect to the T-adic topology. Obviously, $\overline{M}$ contains a T-adically open subgroup $V \subset G(K)$ which is normalized by D^*. Then $\overline{M \cap V} = \overline{M} \cap V = V$ and

$$(\overline{M \cap V})/(M \cap V) \simeq \overline{M}/M \neq \{e\},$$

so we may (and we will) assume that $\overline{M}$ is normalized by D^*. Furthermore, by Margulis' Finiteness Theorem (*cf.* [M1]), M is of finite index in $\mathrm{SL}_1(D)$; in particular, the group $\overline{M}/M$ is finite. Pick a subgroup B, with $M \subset B \subset \overline{M}$, which is normal in $\overline{M}$ and such that $F = \overline{M}/B$ is a nontrivial simple group. As we mentioned in the introduction, by Raghunathan's Theorem (*cf.* [Ra] or [PR3], Theorem 9.3) the commutator subgroup $[\overline{M}, \overline{M}]$ is T-adically open; therefore, F cannot be abelian, as $\overline{B} = \overline{M}$. If $m = [\mathrm{SL}_1(D) : M]$ then M contains the subgroup $C = \langle x^m \rangle$ generated by m-th powers of all elements $x \in \mathrm{SL}_1(D)$. Then C is normalized by D^* and, again by Margulis' theorem, has finite index in $G(K)$. Since

$$C \subset R = \bigcap_{g \in D^*} (g^{-1}Bg),$$

R has finite index in $\mathrm{SL}_1(D)$ as well. For any $g \in D^*$, we have $g^{-1}Bg \subset \overline{M}$ and

$$\overline{M}/(g^{-1}Bg) \simeq \overline{M}/B = F$$

implying that $\overline{M}/R$ is a direct product of a certain number of copies of F; in particular, $\overline{M}/R$ is a perfect group. To show that in fact $R = B$, or equivalently, B is normalized by D^*, we need the following statement (*cf.* [Ra], *Prop. 3*, or [PR3], *Prop. 9.3*).

Proposition 2.2 *Assume that $N \subset \mathrm{SL}_1(D)$ is a non-central subgroup normalized by D^*, and for $x \in D^*$ let $C(x) = \{y \in D^* \mid [x, y] \in N\}$ (where, as usually, $[x, y] = xyx^{-1}y^{-1}$). Then for any $x \in \overline{N}$ we have $D^* = C(x)\overline{N}$.*

An automorphism of a group is called class-preserving if it preserves all conjugacy classes.

Corollary 2.3 *Inner automorphisms of D^* induce class-preserving automorphisms of $\overline{N}/N$. In particular, any intermediate subgroup P, $N \subset P \subset \overline{N}$, normalized by $\overline{N}$, is a normal subgroup in D^*.*

To apply this fact in our situation, notice that $\overline{R} = \overline{M}$. Indeed, being of finite index in $\mathrm{SL}_1(D)$, the subgroup R cannot be central, and then, it follows from the structure of local division algebras (*cf.* [Ri]) that $\overline{M}/\overline{R}$ is soluble; on the other hand, as we have seen above, in our case $\overline{M}/\overline{R}$ is perfect. Now, we obtain from the corollary above that B is a normal subgroup in D^*, as required. Using this corollary once more, we conclude that the action of D^* on $F = \overline{M}/B$ induced by inner automorphisms is class-preserving, and we may apply the following fact from the theory of finite simple groups (W. Feit, private communication).

Theorem 2.4 *Let F be a finite simple group. Then every class-preserving automorphism of F is inner.*

It follows that the image of the homomorphism $\alpha : D^* \to \mathrm{Aut}(F)$ defined by the above action, coincides with $\mathrm{Int}(F)$. So, letting $N = \mathrm{Ker}(\alpha)$ we have $D^*/N \simeq \mathrm{Int}(F) \simeq F$. Theorem 2.1 is proved. ■

Corollary 2.5 *(PM) for $\mathbf{SL}_{1,D}$ is equivalent to the non-existence of normal subgroups $N \subset D^*$ such that D^*/N is a non-abelian finite simple group.*

Indeed, as we already mentioned in the proof of Theorem 2.1, it follows from [Ri], that for any T-adically open normal subgroup $M \subset \mathrm{SL}_1(D)$ the quotient $\mathrm{SL}_1(D)/M$ is soluble. This fact combined with (PM) implies that for any normal subgroup $N \subset D^*$ of finite index, the image of $\mathrm{SL}_1(D)$ in D^*/N is soluble, and therefore the group D^*/N is itself soluble since $\mathrm{SL}_1(D) = [D^*, D^*]$.

At present, there does not seem to be a reasonable way to control all possible quotients of the multiplicative group of a division algebra; however, the following conjecture, which can be regarded as a generalization of (PM) to division algebras over arbitrary fields, appears to be plausible.

Conjecture (FSQ). *Let D be a finite dimensional division algebra over an arbitrary field. Then D^* does not have any normal subgroup N such that D^*/N is a non-abelian finite simple group.*

The rest of the paper is devoted to proving this fact for two particular cases.

Theorem 2.6 *Conjecture (FSQ) holds true for division algebras of degree two and three.*

3. Proof of Theorem 2.6

First, we consider the case of D a quaternion division algebra. The argument here is based on the following statement.

Lemma 3.1 *(cf. Lemma 4 in [PR1]) Fix some maximal subfield $L \subset D$. Then any element $z \in \mathrm{SL}_1(D)$ can be written in the form $z = [x, y]$ for suitable $x \in D^*$, $y \in L^*$ where $[x, y] = xyx^{-1}y^{-1}$ is the commutator of x and y.*

Proof. Fix $z \in \mathrm{SL}_1(D)$ and consider the following linear homogeneous equation for y:

$$\mathrm{Trd}_{D/K}(y) = \mathrm{Trd}_{D/K}(zy). \tag{1}$$

Since $\dim_K(L) = 2$, (1) has a non-zero solution $y \in L$. Then the elements y and zy have the same characteristic polynomial and therefore, they are conjugate in D by the Skölem-Noether Theorem. Thus, $zy = xyx^{-1}$ for some $x \in D^*$, and $z = [x, y]$ as required. ■

Let now $N \subset D^*$ be a normal subgroup such that $F = D^*/N$ is a finite non-abelian simple group. Pick a maximal subfield $L \subset D$ and let A denote the image of L^* in F. Then by Lemma 3.1, the set of commutators $\{[x, y] \mid x \in F, y \in A\}$ coincides with F and the proof is completed by the following elementary

Lemma 3.2 *Let F be a finite simple group. If for some abelian subgroup $A \subset F$ the set of commutators $Y(A) = \{[x, y] \mid x \in F, y \in A\}$ coincides with F then $F = \{e\}$.*

Proof. We have

$$Y(A) = \bigcup_{a \in A} Y(a)$$

where $Y(a) = \{[x, a] \mid x \in F\}$. Since A is abelian, any two elements in the same right coset modulo A define the same commutator implying that

$$\#Y(a) \leq [F : A]$$

for any $a \in A$. Besides, for the unity element $e \in A$ we have $Y(e) = \{e\}$. Therefore,

$$\#F = \#Y(A) \leq \sum_{a \in A \setminus \{e\}} Y(a) + 1 \leq (\#A - 1)[F : A] + 1 = \#F + (1 - [F : A]),$$

forcing $F = A$ and eventually $F = \{e\}$. ■

The given proof of Theorem 2.6 for quaternion division algebras is close to the proof of Theorem 3 in [PR1]. Note, that Theorem 3 in [PR1] combined with Theorem 2.4 above (which, as turned out later, was already known at that time) implies that if for a quaternion algebra D over an algebraic number field, the set T introduced in the statement of (PM), is empty then $\mathrm{SL}_1(D)$ is projectively simple (Kneser's conjecture [K] generalized later in the form of (PM), and proved in that form for quaternions by Margulis [M2]).

The proof of Theorem 2.6 for division algebras of degree 3 is much more complicated (and longer). First of all, we need to introduce one group-theoretic property. Let F be an abstract group. For any $x \in F$ let $C_F(x)$ denote the centralizer of x in F, and for $x,\ y \in F$ let

$$C_F(x,y) = \bigcup_{z \in yC_F(x)} C_F(z),$$

$$E_F(x,y) = C_F(x,y)C_F(x)C_F(x,y).$$

Definition 3.3 *We say that F has property* (C) *if $E_F(x,y) = F$ for any $x, y \in F$.*

This property looks rather odd and, to the best of our knowledge, has never appeared in the literature before. However due to the following statement, it plays an important role in the proof of Theorem 2.6.

Proposition 3.4 *Let D be a division algebra of index 3. Then its multiplicative group D^* satisfies property* (C)*, and so does any of its quotients.*

Proof. Clearly, it suffices to prove (C) for D^*. Fix $x,\ y \in D^*$ and put $L = K(x)$. Then obviously $L^* \subset C(x)$ (we shall ommit the subscript D^*), and there is nothing to prove if either $x \in K$ or $y \in L$. Otherwise, $V = L + yL$ is a 6-dimensional K-subspace in D, and since $\dim_K D = 9$, we have $V \cap (aV) \neq (0)$ for any $a \in D^*$; in other words, $a \in (V\backslash(0))(V\backslash(0))^{-1}$. To prove that $E(x,y) = D^*$, it remains to notice that $V\backslash(0) \subset C(x,y)C(x)$. Indeed, let $t = c + yd$ where $c,\ d \in L^*$. If $c = 0$ then $t = yd \in C(y)C(x) \subset C(x,y)C(x)$. Otherwise,

$$t = (1 + y(dc^{-1}))c \in C(y(dc^{-1}))C(x) \subset C(x,y)C(x).$$

Proposition 3.4 is proved. ■

Now, Theorem 2.6 is a consequence of the following result which seems to be of independent interest.

Theorem 3.5 *None of the (known) finite simple groups has property* (C).

(Note, that by a "known" finite simple group we mean one of the following: an alternating group, a finite group of Lie type or one of 26 sporadic groups, and (CSG) is the statement that all finite simple groups are known).

4. Proof of Theorem 3.5 for groups of Lie type: generic case.

For most groups of Lie type and for the alternating groups, it is possible to prove a stronger result than Theorem 3.5. Namely, with notations as in the previous section, for elements x, y of a group F we let $R_F(x,y)$ denote the subgroup in F generated by $C_F(x)$ and $C_F(x,y)$. Then we have

Theorem 4.1 *Let F be either an alternating group A_n ($n \geq 5$, $n \neq 8$) or one of simple (adjoint) Chevalley groups (normal or twisted) not in the following list:*

(i) $PSL_n(q)$, *where either* $q = 2$, *or* $n = 3$, $q = 4$, *or else* $n = 4$, $q = 3$;
(ii) $PSU_n(q^2)$, *where* $q = 2$ *or* $q = 3$, $n = 4$;
(iii) $PSp_{2n}(q)$, $P\Omega_n(f,q)$, $E_7(q)$, $E_8(q)$, *and* $F_4(q)$ *where* $q = 2$ *or 3;*
(iv) ${}^3D_4(q)$, $E_6(q)$ *and* ${}^2E_6(q^2)$, $q = 2$;
(v) $G_2(q)$, $q = 3$.

Then there exist elements x, $y \in F$ such that $R_F(x,y) \neq F$; in particular F does not have property (C).

We begin the proof with the alternating groups which naturally require a sort of special analysis, while all other groups of Lie type are treated in a more or less uniform way.

Alternating groups. Let $F = A_n$. First, consider the case of even $n \geq 10$. Letting $l = (n-4)/2$, we introduce the following subsets I_j $(j = 1,2,3)$ of the set $I = \{1,2,...,n\}$:

$$I_1 = \{1,2\},\ I_2 = \{3,...,2+l\},\ I_3 = \{3+l,...,3+2l = n-1\}.$$

Obviously, $\#I_2 = l, \#I_3 = l+1$, and since $n \geq 10$, we have $l > 2$. Now, let $x = x_1x_2x_3$, where x_j is a cyclic permutation of I_j. Then each of I_j's is invariant under the centralizer $C_F(x)$. Pick $y \in F$ such that $y(n) = n$ and $y(I_j) \cap I_j = \emptyset$ for each $j = 1,2,3$; for example, one can take

$$\begin{cases} (1,3,3+l)(2,n-1)\cdot\prod_{j=4}^{2+l}(j,j+l), & \text{for } l \text{ even;} \\ (1,3,3+l)(2,n-1)(4,4+l,5,5+l)\cdot\prod_{j=6}^{2+l}(j,j+l), & \text{for } l \text{ odd.} \end{cases}$$

For any $z \in C_F(x)$, and $t = yz$ we have the following: $t(n) = n$ and $t(I_j) \cap I_j = \emptyset$ for each $j = 1,2,3$, in particular the fixed point set I^t is $\{n\}$. So, n is fixed by every centralizer $C_F(t)$, $t \in yC_F(x)$, and therefore also by $R_F(x,y)$, implying that $R_F(x,y) \neq F$.

Next, we consider the case of $n \equiv 1 \bmod (4)$, $n \geq 17$. Here we let $l = (n-7)/2$ and define the subsets $I_j \subset I = \{1,2,...,n\}$ $(j = 1,2,3,4)$ as follows:

$$I_1 = \{1,2\},\ I_2 = \{3,4,5\},\ I_3 = \{6,...,5+l\},$$

$$I_4 = \{6+l,...,6+2l = n-1\}.$$

Since $\#I_3 = l$, $\#I_4 = l+1$, and $l > 3$, the element $x = x_1x_2x_3x_4$ where x_j is a cyclic permutation of I_j, has the property that each of I_j's is invariant under $C_F(x)$. Then letting

$$y = (1,3,6,6+l)(2,4,7,7+l)(5,n-1)\cdot\prod_{j=8}^{5+l}(j,j+l).$$

we see just as above that the group $R_F(x,y)$ fixes n, and therefore is a proper subgroup of F.

For $n \equiv 3 \bmod (4)$, $n \geq 7$, we set $l = (n-1)/2$,

$$I_1 = \{1, ..., l\}, \; I_2 = \{l+1, ..., 2l\},$$

and let $x = x_1 x_2$ where x_j is a cyclic permutation of I_j. Since l is odd, the centralizer $C_F(x)$ is generated by x_1 and x_2; and therefore leaves each of I_j's invariant. Then one can take

$$y = (1, l+1)(2, l+2, ..., l, 2l)$$

and argue as above.

Remaining small n's require special treatment.

Assume that $n = 5$ and let $x = (1,2)(3,4)$ and $y = (1,2,3)$. Then the centralizer $C_F(x)$ is the Klein group

$$\{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\},$$

so any $t = yz$, where $z \in C_F(x)$, has order 3. This implies that $C_F(t) = \langle t \rangle$, so $R_F(x,y)$ fixes 5, and $R_F(x,y) \neq F$.

Since $A_6 \simeq PSL_2(9)$, and the group $PSL_2(9)$ will be considered later, we don't write out here x and y for this case.

If $n = 9$ let $x = (1,2,3,4,5,6,7)$ and $y = (2,4,3,7,5,6)(8,9)$. One can readily verify that $C_F(x) = \langle x \rangle$, $C_F(y) = \langle y \rangle$ and $y^{-1}xy = x^3$. The last relation implies that the coset $yC_F(x)$ coincides with the conjugacy class $t^{-1}yt$, $t \in \langle x \rangle$. So $R_F(x,y)$ is generated by $\{x, y\}$, and therefore $R_F(x,y) \neq F$.

If $n = 10$ let $x = (1,2)(3,4,5)(6,7,8,9)$ and $y = (1,3,6)(2,7)(4,8,5,9)$. Then $C_F(x) = \langle (1,2)(6,7,8,9), \; (3,4,5) \rangle$ leaves invariant each of the following sets

$$I_1 = \{1,2\}, I_2 = \{3,4,5\}, I_3 = \{6,7,8,9\},$$

and y has the property that $y(I_j) \cap I_j = \emptyset$ for each $j = 1,2,3$; so arguing as above, we obtain that $R_F(x,y)$ fixes 10.

For $n = 13$ we argue exactly as in the previous case, with

$$x = (1,2,3)(4,5)(6,7)(8,9,10,11,12)$$

and

$$y = (1,4)(2,8)(3,9)(5,10)(6,11)(7,12).$$

We will describe now the general strategy of the proof of Theorem 4.1 for the groups of Lie type (excluding those listed above). So, let G be a finite simple (adjoint) Chevalley group, $\tilde{G}$ be the corresponding simply connected Chevalley group, and $\varphi : \tilde{G} \to G$ be the natural epimorphism. Then $\tilde{G}$ can be obtained as the group of fixed points of a suitable algebraic endomorphism $\sigma : \mathbf{G} \to \mathbf{G}$ of the corresponding simply connected algebraic group $\mathbf{G}$ over the algebraic closure K of a finite field. To recall the description of endomorphisms which occur in this set-up, we fix a maximal split torus $\mathbf{T} \subset \mathbf{G}$ and consider the associated root system $R = R(\mathbf{T}, \mathbf{G})$. Let Π be a system of simple roots in R, R_+ be the corresponding system of positive roots, $\mathbf{B}$ be the associated Borel subgroup, and $\mathbf{U}$ be the unipotent radical of $\mathbf{B}$. Then the endomorphism σ required to define $\tilde{G}$ can be written in the form

$$\sigma = \theta \circ \tau \tag{2}$$

where θ is the automorphism of $\mathbf{G}$ corresponding to a power of the Frobenius automorphism $\mathbf{p}$ of K where $p = \mathrm{char} K$ (in the sequel, θ will be used also to denote the underlying field automorphism), and τ is either an algebraic automorphism of $\mathbf{G}$ corresponding to a symmetry of Π (in this case the order of τ can be 1, 2 or 3) or an algebraic endomorphism switching positive multiples of short and long roots (this occurs only for the types $B_2 = C_2$ and F_4 if $p = 2$, and for the type G_2 if $p = 3$). Let k be the field of fixed under θ elements, and let l be the fixed field of θ^d if τ is an automorphism of order d, and the fixed field of $\mathbf{p}\theta^2$ if τ is an endomorphism but not an automorphism.

With this notations in mind, we proceed with our argument. Let U be the group of σ-fixed elements in $\mathbf{U}$ (i.e. $U = \mathbf{U} \cap \tilde{G}$). Lemma 4.2 below shows that U always contains a regular element $\tilde{x}$. Suppose there exists an element $\tilde{y} \in T = \mathbf{T} \cap \tilde{G}$ with the following properties:

(A) *the centralizer* $C_{\mathbf{G}}(\tilde{y})$ *is contained in a proper standard* σ*-invariant parabolic subgroup* $\mathbf{P} \subset \mathbf{G}$;
(B) $C_G(\varphi(\tilde{y})) = \varphi(C_{\tilde{G}}(\tilde{y}))$.

Then the elements $x = \varphi(\tilde{x})$ and $y = \varphi(\tilde{y})$ are as required. Indeed, since $\tilde{x}$ is regular unipotent,

$$C_{\tilde{G}}(\tilde{x}) = Z(\tilde{G}) \cdot C_U(\tilde{x})$$

and

$$C_G(x) = \varphi(C_{\tilde{G}}(\tilde{x}))$$

(in the above $Z(\tilde{G})$ denotes the center of $\tilde{G}$). We will show that $R_G(x, y)$ is contained in $\varphi(P)$ where $P = \mathbf{P} \cap \tilde{G}$. Since P is a proper subgroup of $\tilde{G}$ (Lemma 4.2 (ii)) and $\tilde{G}$ is its own commutator subgroup, we obtain that $\varphi(P) \neq G$ yielding the required result. Now, we pick an arbitrary $u \in C_G(x)$, and writing it as $u = \varphi(v)$ for a suitable $v \in C_U(\tilde{x})$ let $z = yu$ and $\tilde{z} = \tilde{y}v$. Letting p be the characteristic of k as before, we can put $\tilde{z}$ in the form $\tilde{z} = z_1 z_2$ where both z_1 and z_2 belong to the cyclic subgroup generated by $\tilde{z}$, and the order of z_1 (resp. z_2) is prime to p (resp. is a power of p). Clearly T is a maximal subgroup of the soluble group $B = \mathbf{B} \cap \tilde{G}$ of order prime to p

(recall that $B = TU$, a semi-direct product) so it follows from the P. Hall Theorem (*cf.* [H], §9.3) that $t = gz_1g^{-1} \in T$ for a suitable $g \in U$. We have

$$t = z_1(z_1^{-1}gz_1g^{-1}) = \tilde{z}z_2^{-1}(z_1^{-1}gz_1g^{-1}) = \tilde{y}[vz_2^{-1}(z_1^{-1}gz_1g^{-1})].$$

Since U is a normal Sylow p-subgroup of B, the expression in the square brackets belongs to U, and we conclude that $t = \tilde{y}$. Furthermore, as $\varphi(z_1)$ is a power of z, the centralizer of the latter is contained in the centralizer of the former, so we obtain the inclusion

$$C_G(z) \subset C_G(\varphi(g^{-1}\tilde{y}g)) = \varphi(g)^{-1}\varphi(C_{\tilde{G}}(\tilde{y}))\varphi(g) \subset \varphi(P).$$

Eventually $R_G(x, y) \subset \varphi(P)$, as we claimed.

Lemma 4.2 *(i) U contains a regular element;*
(ii) $\tilde{G}$ is not contained in any proper σ-invariant standard parabolic subgroup $\mathbf{P} \supset \mathbf{B}$.

Proof. For $\alpha \in R$, let $x_\alpha : K^+ \to \mathbf{U}_\alpha \subset \mathbf{G}$ be the root one-parameter subgroup. Then any element $u \in \mathbf{U}$ can be uniquely written in the form

$$u = \prod_{\alpha \in R_+} x_\alpha(u_\alpha) \tag{3}$$

(with arbitrary but fixed order of positive roots), and regular elements are determined by the condition

$$u_\alpha \neq 0 \text{ for all } \alpha \in \Pi$$

(*cf.* [SpSt], ch. III, 1.13). The endomorphism τ involved in the above description of σ induces an automorphism τ^* of the vector space $V = \mathbf{X}(\mathbf{T}) \otimes_{\mathbb{Z}} \mathbb{R}$ where $\mathbf{X}(\mathbf{T})$ is the character group of $\mathbf{T}$. Let us consider the orthogonal projection $\pi_\tau : V \to V_\tau$ on the space $V_\tau \subset V$ of τ^*-fixed elements and define the equivalence relation on R as follows: $\alpha \sim \beta$ iff $\pi_\tau(\alpha) = c\pi_\tau(\beta)$ for some $c > 0$ (details can be found in [St], §11). Let E denote the set of equivalence classes with respect to $\sim$, and let E_+ be the set of classes having a representative in R_+. Then for the proof of the lemma it is convenient to combine the factors in (3) as follows:

$$u = \prod_{\mathfrak{a} \in E_+}(\prod_{\alpha \in \mathfrak{a}} x_\alpha(u_\alpha)).$$

We will show that given any $\mathfrak{a} \in E_+$, there exists a $u(\mathfrak{a}) \in U$ such that

$$u(\mathfrak{a}) = \prod_{\alpha \in \mathfrak{a}} x_\alpha(u_\alpha) \tag{4}$$

and

$$u_\alpha \neq 0 \quad \text{for all} \quad \alpha \in \mathfrak{a} \cap \Pi \tag{5}$$

It is known that the roots belonging to $\mathfrak{a} \in E_+$ form a system of positive roots in a certain root system $R(\mathfrak{a})$, and for each case there is an explicit description of the set $U_\mathfrak{a}$ of elements of the form (4) which are fixed by σ, i.e. belong to U (*cf.* [St], §11). To be more precise, the full list of possibilities looks as follows (the fields l and k and the field automorphism θ are as introduced above):

(a) $R(\mathfrak{a}) = A_1$ and $\mathfrak{a} = \{\alpha\}$; then $U_\mathfrak{a} = \{x_\alpha(t) \mid t \in k\}$;
(b) $R(\mathfrak{a}) = (A_1)^n$ where $n = 2$ or 3; then $U_\mathfrak{a} = \{x \cdot \sigma(x) \cdot ... \mid x = x_\alpha(t),$ $\alpha \in \mathfrak{a}, t \in l\}$;
(c) $R(\mathfrak{a}) = A_2$ and $\mathfrak{a} = \{\alpha, \beta, \alpha+\beta\}$; then $U_\mathfrak{a} = \{x_\alpha(t)x_\beta(t^\theta)x_{\alpha+\beta}(u) \mid t, u \in l$ and $tt^\theta + u + u^\theta = 0\}$;
(d) $R(\mathfrak{a}) = C_2$ and $\mathfrak{a} = \{\alpha, \beta, \alpha+\beta, \alpha+2\beta\}$; then $U_\mathfrak{a} = \{x_\alpha(t)x_\beta(t^\theta)x_{\alpha+2\beta}(u) \cdot$ $\cdot x_{\alpha+\beta}(t^{1+\theta} + u^\theta) \mid t, u \in l\}$.
(e) $R(\mathfrak{a}) = G_2$ and $\mathfrak{a} = \{\alpha, \beta, \alpha+\beta, \alpha+2\beta, \alpha+3\beta, 2\alpha+3\beta\}$; then $U_\mathfrak{a} =$ $= \{x_\alpha(t)x_\beta(t^\theta)x_{\alpha+3\beta}(u)x_{\alpha+\beta}(u^\theta - t^{1+\theta})x_{2\alpha+3\beta}(v)x_{\alpha+2\beta}(v^\theta - t^{1+2\theta}) \mid$ $t, u, v \in l\}$.

From this description, the existence of $u \in U_\mathfrak{a}$ satisfying (5) follows immediately for all cases except (c), and to handle (c) one can take $t = 1$ and then notice that since the trace map $\mathrm{Tr}_{l/k}$ is surjective, one can find $u \in l$ to satisfy the required equation, proving (i).

To prove (ii) suppose that our parabolic corresponds to a (proper) subset $\Delta \subset \Pi$. Let $\alpha \in \Pi \setminus \Delta$ and $\mathfrak{a} \in E_+$ be the class containing α. Consider the corresponding root system $R(\mathfrak{a})$ and the group $\mathbf{G}_\mathfrak{a}$ generated by root subgroups $\mathbf{U}_\alpha$ for $\alpha \in R(\mathfrak{a})$. Then $\mathbf{G}_\mathfrak{a}$ is stable under σ and $\mathbf{P} \cap \mathbf{G}_\mathfrak{a} = \mathbf{B} \cap \mathbf{G}_\mathfrak{a}$. On the other hand, arguing as above, one can show that $\mathbf{G}_\mathfrak{a}$ always contains a non-identity σ-fixed element of the form

$$u(-\mathfrak{a}) = \prod_{\alpha \in (-\mathfrak{a})} x_\alpha(u_\alpha),$$

which belongs to $\tilde{G}$ but not to $\mathbf{P}$. The lemma is proved. ■

For convenience of reference, we formulate here one simple group-theoretic statement.

Lemma 4.3 *Let $\phi : G_1 \to G_2$ be a surjective homomorphism of finite groups such that $N = \mathrm{Ker}(\phi)$ is contained in the center of G_1, and let $x \in G_1$. Then*
(i) $\#C_{G_2}(\phi(x)) \leq \#C_{G_1}(x)$;
(ii) if n is the exponent of N, then $C_{G_2}(\phi(x)) \subset \phi(C_{G_1}(x^n))$.

Proof. Let $C_1 = C_{G_1}(x)$, $C_2 = C_{G_2}(\phi(x))$. For $g \in C_2$ we pick a lift $\tilde{g} \in \phi^{-1}(g)$ and consider the commutator $[\tilde{g}, x]$. SInce N is central in G_1, this commutator depends only on g, but not on the choice of $\tilde{g}$ and therefore can be denoted simply $c(g)$. Furthermore, one easily verifies that for $g \in C_2$, $c(g) \in N$, and the map

$$\theta : C_2 \to N, \quad g \mapsto c(g)$$

is a homomorphism of groups the kernel of which is exactly $\phi(C_1)$. It follows that

$$\#C_2 \leq (\#\phi(C_1)) \cdot (\#N).$$

On the other hand, $N \subset C_1$ and therefore

$$\#\phi(C_1) = \frac{\#C_1}{\#N},$$

and we obtain *(i)*. TO prove *(ii),* it remains to observe that with notations as above, we have

$$[\tilde{g}, x^n] = [\tilde{g}, x] \cdot (x[\tilde{g}, x]x^{-1}) \cdots (x^{n-1}[\tilde{g}, x]x^{-(n-1)}) = [\tilde{g}, x]^n,$$

implying that $[\tilde{g}, x^n] = 1$, and $\tilde{g} \in C_{G_1}(x^n)$. ∎

While Lemma 4.2 and the preceding remarks provide a uniform construction of the element $\tilde{x}$, the choice of $\tilde{y}$ requires a case-by-case consideration of all types.

Groups $PSL_n(q)$. Here $\tilde{y}$ can be presented explicitly in the matrix form, without appealing to the root notations. For the Borel subgroup $\mathbf{B}$ (resp. the maximal torus $\mathbf{T}$) we take the group of the upper triangular (resp. diagonal) matrices in $\mathbf{G} = \mathbf{SL}_n$. Suppose $k = \mathbf{F}_q$, the field of q elements. We will show that except for the cases listed in Theorem 4.1 and also the group $PSL_2(5)$ one can take $\tilde{y} = \mathrm{diag}(s, s^{-1}, 1, ..., 1)$ where s is a generator of $\mathbf{F}_q^*$. Since $q \neq 2$, the centralizer $C_{\tilde{G}}(\tilde{y})$ is always contained in the parabolic subgroup $\mathbf{P} \subset \mathbf{G}$ consisting of matrices of the form

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ 0 & 0 & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & a_{n3} & \dots & a_{nn} \end{pmatrix}.$$

Now, let $\varphi : \tilde{G} = SL_n(q) \to PSL_n(q) = G$ be the canonical homomorphism, and $y = \varphi(\tilde{y})$.

Lemma 4.4 *If $q \neq 2$ then except for the following cases:*

1) $n = 2$, $q = 3, 5$;
2) $n = 3$, $q = 4$;
3) $n = 4$, $q = 3$,

we have $C_G(y) = \varphi(C_{\tilde{G}}(\tilde{y}))$.

Proof. Let $u = \varphi(v) \in C_G(y) \setminus \varphi(C_{\tilde{G}}(\tilde{y}))$. Then $v\tilde{y}v^{-1} = z\tilde{y}$ where $z = diag(\xi, ..., \xi)$, and $1 \neq \xi \in \mathbf{F}_q^*$ satisfies $\xi^n = 1$. If $n > 4$ then $\tilde{y}$ has eigenvalue 1 with multiplicity $n-2 > 2$, and since the only eigenvalue with this multiplicity for $z\tilde{y}$ is ξ we obtain $\xi = 1$, a contradiction. If $n = 4$ and $q > 3$, then again $\tilde{y}$ has eigenvalue 1 with multiplicity

2, and the only eigenvalue with this multiplicity for $z\tilde{y}$ is ξ. For $n = 3$, v belongs to $C_{\tilde{G}}(\tilde{y}^3)$ (*cf.* the proof of Lemma 4.3) which coincides with $C_{\tilde{G}}(\tilde{y})$ unless $s^3 = \pm 1$, i.e. if $q \neq 4$ or 7. However, for $q = 7$, $\tilde{y}$ has eigenvalue 1 while $z\tilde{y}$ does not. In the last remaining case $n = 2$, we have $v \in C_{\tilde{G}}(\tilde{y}^2)$ which equals $C_{\tilde{G}}(\tilde{y})$ provided $s^2 \neq \pm 1$, i.e. if $q \neq 3, 5$. ■

Now, to complete consideration of $G = PSL_n(q)$, it remains to observe that for $n = 2$, $q = 3$ the group G is not simple, and therefore is automatically excluded from our consideration, and for $n = 2$, $q = 5$, G is isomorphic to the alternating group A_5 which has been considered earlier.

Groups $PSU_n(q^2)$. The group $SU_n(q^2)$ is obtained as the subgroup of $\mathbf{G} = \mathbf{SL}_n$ consisting of elements fixed by the automorphism σ of $\mathbf{G}$ given by the formula:

$$\sigma(x) = F^{-1}x^*F$$

where $x^*_{ij} = (\theta(x_{ji}))$, θ is the field automorphism $x \mapsto x^q$, and

$$F = \begin{pmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{pmatrix}.$$

Obviously, in this case $k = \mathbf{F}_q$, $l = \mathbf{F}_{q^2}$. Besides, since $SU_2(q^2)$ is isomorphic to $SL_2(q)$, we may assume that $n \geq 3$. As in the previous case, one can take for $\mathbf{B}$ (resp. $\mathbf{T}$) the group of upper triangular (resp. diagonal) matrices in $\mathbf{G}$.

If $n \geq 4$, we let $\tilde{y} = \mathrm{diag}(s, s^{-1}, 1, ..., 1, \theta(s), \theta(s)^{-1})$ where s is a generator of l^*. Since $q > 2$, all the elements in the set $\{s, s^{-1}, \theta(s), \theta(s)^{-1}, 1\}$ are distinct, and therefore $C_{\mathbf{G}}(\tilde{y})$ is contained in a parabolic $\mathbf{P} \supset \mathbf{B}$. As in the previous case, to verify (B) it suffices to show that the matrices $\tilde{y}$ and $z\tilde{y}$ where $z = \mathrm{diag}(\xi, ..., \xi)$ with ξ satisfying $\xi^n = 1$ and $\xi\theta(\xi) = 1$, are not conjugate unless $\xi = 1$. For $n \geq 6$ this follows from the fact that $\tilde{y}$ has eigenvalue 1 with multiplicity $n - 4 \geq 2$, and the only eigenvalue of this multiplicity for $z\tilde{y}$ is ξ. For $n = 5$, one should observe that 1 is an eigenvalue for $\tilde{y}$ but not for $z\tilde{y}$ unless $\xi = 1$, since the order of s is $q^2 - 1 \geq 8$.

Suppose now that $n = 4$. If $\xi \neq 1$, then for s to be contained in the set of eigenvalues of $z\tilde{y}$, ξ should equal one of the elements s^2, $s\theta(s^{-1})$ or $s\theta(s)$. The orders of these elements are respectively $(q^2-1)/2$, $q+1$, $q-1$, and the conditions on ξ imply that $q = 3$ which is excluded in Theorem 4.1.

In the case $n = 3$ we let $\tilde{y} = \mathrm{diag}(s, s^{-1}\theta(s), \theta(s)^{-1})$ where s is as above. Since $q > 2$, all the elements s, $s^{-1}\theta(s)$ and $\theta(s)^{-1}$ are distinct, and therefore $C_{\mathbf{G}}(\tilde{y}) = \mathbf{T}$. In verifying (B) we may assume that $q > 3$. If $q \geq 5$ then all eigenvalues of $\tilde{y}^3$ are also distinct, so $C_{\mathbf{G}}(\tilde{y}) = C_{\mathbf{G}}(\tilde{y}^3)$ and $C_G(y) \subset \varphi(C_{\tilde{G}}(\tilde{y}^3)) = \varphi(C_{\tilde{G}}(\tilde{y}))$, as required. In the last remaining case $q = 4$, if s is contained in the set of eigenvalues of $z\tilde{y}$ and $\xi \neq 1$, then ξ can be only either s^2 or s^5. Using the properties of ξ, we easily check that none of these is possible.

Table 1:

γ	$\lvert\gamma(r)\rvert$
$\varepsilon_1-\varepsilon_2$	$-1+2^{m+1}$
$\varepsilon_1+\varepsilon_2$	1
$2\varepsilon_1$	2^{m+1}
$2\varepsilon_2$	$2-2^{m+1}$

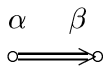
Groups $PSp_{2n}(q)$, $n \geq 2$. Here $\mathbf{G} = \mathbf{Sp}_{2n}(f)$ where f is an alternating form with the matrix

$$\begin{pmatrix} 0 & J \\ -J & 0 \end{pmatrix}, \quad J = \begin{pmatrix} & & 1 \\ & \cdot^{\cdot^{\cdot}} & \\ 1 & & \end{pmatrix}.$$

For $\mathbf{B}$ (resp. $\mathbf{T}$) one can take the group of upper triangular (resp. diagonal) matrices in $\mathbf{G}$. Let $\tilde{y} = \mathrm{diag}(s, 1, ..., 1, s^{-1})$ where s is a generator of the multiplicative group of $k = \mathbf{F}_q$. Since the cases $q = 2$ or 3 are excluded in Theorem 4.1, $s \neq s^{-1}$ implies that $C_{\mathbf{G}}(\tilde{y})$ is contained in a proper standard parabolic, hence (A). If $p = 2$, then the center of $\mathbf{G}$ is trivial, and (B) is satisfied automatically. Otherwise, for $q > 3$, $\tilde{y}$ is not conjugate to $-\tilde{y}$, and again (B) follows.

Groups ${}^2C_2(2^{2m+1})$. Since the group ${}^2C_2(2)$ is soluble, we may assume that $m \geq 1$. In this case $k = \mathbf{F}_{2^m}$, $l = \mathbf{F}_{2^{2m+1}}$ and σ acts on the root elements as follows:

$$\sigma : \begin{cases} x_\alpha(t) \to x_\beta(t^{2^m}), \\ \\ x_\beta(t) \to x_\alpha(t^{2^{m+1}}), \end{cases}$$



(In the realization of $R = C_2$ as $\{\pm 2\varepsilon_1, \pm 2\varepsilon_2, \pm\varepsilon_1 \pm \varepsilon_2\}$ given in ([Bo], Table III) we have $\alpha = 2\varepsilon_2$, $\beta = \varepsilon_1 - \varepsilon_2$.) Then σ acts on the elements $h_\alpha(t)$, $h_\beta(t)$ by similar formulas, implying that T consists of elements of the form $r(s) = h_\alpha(s) h_\beta(s^{2^m})$, $s \in l^*$. Since the center of $\tilde{G}$ is trivial, it suffices to show that for a generator s of l^*, the element $r = r(s)$ is regular. Obviously, for any root γ, the value $\gamma(r)$ is a certain power of s, to be denoted as $|\gamma(r)|$. For positive γ's, the value $|\gamma(r)|$ are given in Table 1, which shows that there is no γ such that $\gamma(r) = 1$, hence regularity of r.

Groups $P\Omega_n(f, q)$, $n \geq 5, q > 3$. For a non-degenerate quadratic form f over k in n variables we let $\Omega_n(f)$ denote the commutator subgroup of the special orthogonal group $SO_n(f)$, and then $P\Omega_n(f) = \Omega_n(f)$ if n is odd or else if $p = 2$, and $P\Omega_n(f) = \Omega_n(f)/\{\pm 1\}$ otherwise. (Recall that if f is isotropic, which is always the case over a finite field, then $\Omega_n(f)$ coincides with the kernel of the spinor norm for $p \neq 2$ and $\Omega_n(f) = SO_n(f)$ for $p = 2$.)

For the groups $P\Omega_n(f)$ the above method requires some minor modifications. Let f_0 be the split form in n variables, i.e. $f_0 = x_1 x_n + ... + x_r x_{r-1}$ if $n = 2r$, and $f_0 = x_1 x_n +$

$... + x_r x_{r+2} + x_{r+1}^2$ if $n = 2r+1$. It is more convenient to think of the occuring groups as obtained not from the simply connected spinor group $\mathbf{Spin}_n(f_0)$, but rather from the special orthogonal group $\mathbf{G} = \mathbf{SO}_n(f_0)$. We fix the maximal torus $\mathbf{T} \subset \mathbf{G}$ consisting of matrices of the form $\mathrm{diag}(t_1, ..., t_r, t_r^{-1}, ..., t_1^{-1})$ (resp. $\mathrm{diag}(t_1, ..., t_r, 1, t_r^{-1}, ..., t_1^{-1})$) for $n = 2r$ (resp., $n = 2r+1$), and also the Borel subgroup $\mathbf{B} \subset \mathbf{G}$ consisting of the upper triangular matrices in $\mathbf{G}$ whose diagonal part is in $\mathbf{T}$. Then the split orthogonal group $SO_n(f_0)$ over $k = \mathbf{F}_q$ is obtained as the group of σ-fixed points for $\sigma = \theta$ where θ corresponds to the field automorphism $x \mapsto x^q$, while non-split (but quasi-split) group $SO_n(f)$ where $n = 2r$, $f = x_1 x_n + ... + x_{r-1} x_{r+2} + x_r^2 + d x_{r+1}^2$, $d \notin (-1)^r k^{*2}$ if $p \neq 2$, and $f = x_1 x_n + ... + x_{r-1} x_{r+2} + d x_r^2 + x_r x_{r+1} + d x_{r+1}^2$, $d \in k^*$ is such that the polynomial $dt^2 + t + d$ is irreducible over k if $p = 2$, is isomorphic to the group of σ-fixed points for $\sigma = \tau \circ \theta$ where θ is as above, and $\tau = \mathrm{Int}(s)$,

$$s = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 0 & 1 & & \\ & & 1 & 0 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}.$$

Let $\tilde{G} = \Omega_n(f)$, $G = P\Omega_n(f)$ and $\varphi : SO_n(f) \to PSO_n(f)$ be the canonical projection. The same argument as before shows that it suffices to find $\tilde{y}$ in $T = \tilde{G} \cap \mathbf{T}$ with the following properties.

(A′) $C_{\mathbf{G}}(\tilde{y})$ *is contained in a proper parabolic* $\mathbf{P} \subset \mathbf{G}$ *containing* $\mathbf{B}$*;*
(B′) $C_G(\varphi(\tilde{y})) = \varphi(C_{\tilde{G}}(\tilde{y}))$

(obviously (B′) is satisfied automatically if either n is odd or $p = 2$). Now, suppose that $q > 3$, and let s be the generator of k^* and

$$\tilde{y} = \mathrm{diag}(s, s, 1, ..., 1, s^{-1}, s^{-1}).$$

One easily verifies that $\tilde{y}$ is fixed by σ and has the spinor norm one in both split and non-split cases, so $\tilde{y} \in T$. Since $s \neq s^{-1}$, $C_{\mathbf{G}}(\tilde{y})$ is contained in a proper parabolic containing $\mathbf{B}$, hence (A′). Finally, if $u = \varphi(v)$ is in $C_G(\varphi(\tilde{y}))$ but not in $\varphi(C_{\tilde{G}}(\tilde{y}))$ then $v^{-1}\tilde{y}v = -\tilde{y}$ which is impossible since the eigenvalue 1 or $\tilde{y}$ is not an eigenvalue for $-\tilde{y}$.

Verification of (A) and (B) for groups of other types is based on the root technique, so let us recall some facts and fix notations. For a subset $\Delta \subset \Pi$, the standard parabolic subgroup $\mathbf{P} = \mathbf{P}_\Delta$ corresponding to Δ is generated by $\mathbf{B}$ and $\mathbf{U}_\alpha$, for all $\alpha \in -[\Delta]$ where $[\Delta]$ denotes the set of roots which are linear combinations of roots from Δ with non-negative coefficients. On the other hand, for $\tilde{y} \in \mathbf{T}$, the centralizer $C_{\mathbf{G}}(\tilde{y})$ is generated by $\mathbf{T}$ and $\mathbf{U}_\alpha$ for $\alpha \in \Phi(\tilde{y}) = \{\alpha \in R_+ \mid \alpha(\tilde{y}) = 1\}$; this is a consequence of the Bruhat decomposition and the following fact proved in [SpSt], ch. II, §4: in the simply connected case, the centralizer $C_W(\tilde{y})$ in the Weil group $W = W(\mathbf{T},\mathbf{G})$ is generated by reflections w_α for $\alpha \in \Phi(\tilde{y})$. So, to ensure (A) we need to find $\tilde{y} \in T$ such that

$$\Phi(\tilde{y}) \subset [\Delta] \tag{6}$$

for a suitable proper subset $\Delta \subset \Pi$. Such an element $\tilde{y}$ will be presented in the form $\tilde{y} = \chi_1(t_1)...\chi_m(t_m)$ where $\chi_1, ..., \chi_m$ are (multiplicative) one-parameter subgroups in $\mathbf{T}$. The group $\mathbf{X}_*(\mathbf{T})$ of one-parameter subgroups which is identifiable with the dual group $\mathrm{Hom}(\mathbf{X}(\mathbf{T}), \mathbb{Z})$ of the character group, coincides in the simply connected case with the $\mathbb{Z}$-lattice $Q(R^\vee)$ generated by the dual roots $\alpha^\vee = \frac{2\alpha}{(\alpha|\alpha)}$, and the one-parameter subgroup corresponding to $\alpha^\vee$ is H_α in the notations of Steinberg [St]. Also, let $P(R^\vee)$ be the dual group to the subgroup $Q(R) \subset \mathbf{X}(\mathbf{T})$ generated by the roots $\alpha \in R$. Then $Q(R^\vee)$ is embeddable into $P(R^\vee)$ as a subgroup of finite index in such a way that the pairing between $P(R^\vee)$ and $Q(R)$ is compatible with that between $\mathbf{X}(\mathbf{T})$ and $\mathbf{X}_*(\mathbf{T})$, and the index $e = [P(R^\vee) : Q(R^\vee)]$ is called *the connectedness index* (l'indice de connexion) of R.

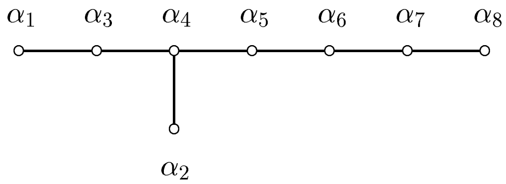
If $\Pi = \{\alpha_1, ..., \alpha_r\}$, then $P(R^\vee)$ is a free $\mathbb{Z}$-module with the basis $\omega_1, ..., \omega_r$ such that $\langle \omega_i, \alpha_j \rangle = \delta_{ij}$. Then $\chi_i = e\omega_i \in \mathbf{X}_*(\mathbf{T})$, and in some cases for $\tilde{y}$ one can take an element of the form $\tilde{y} = \chi_i(s)$ for some i, where s is a generator of k^*. To describe the precise conditions when this is possible, let us denote the coefficient of $\beta \in Q(R)$ at α_i as $n_i(\beta)$. Also, let $\tilde{\alpha} = n_1\alpha_1 + ... + n_r\alpha_r$ be the highest root. We claim that if

$$s^{e(n_i)!} \neq 1, \tag{7}$$

then the element $\tilde{y} = \chi_i(s)$ satisfies (6) with $\Delta = \Pi \backslash \{\alpha_i\}$, thereby yielding (A). Indeed, let $\alpha \in \Phi(\tilde{y})$ and $\alpha \notin [\Delta]$; then $n_i(\alpha) \neq 0$ and $n_i(\alpha) \leq n_i$. This means that $s^{e(n_i)!}$ is a power of $\alpha(\tilde{y}) = s^{en_i(\alpha)}$, and then (7) gives a contradiction.

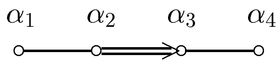
One can easily check (7) for the groups of types E_8, F_4, G_2 (for these types $e = 1$, implying that the center of $\tilde{G}$ is trivial (*cf.* [St], §3) and (B) is satisfied automatically).

Groups $E_8(q)$, $q > 3$. Labeling simple roots as in [Bo], Table VII



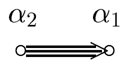
we have $\tilde{\alpha} = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 6\alpha_4 + 5\alpha_5 + 4\alpha_6 + 3\alpha_7 + 2\alpha_8$, and (7) is satisfied for $i = 1$.

Groups $F_4(q)$, $q > 3$. We have the following Dynkin diagram (*cf.* [Bo], Table VIII):



and the highest root $\tilde{\alpha} = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4$. Obviously (7) is satisfied for $i = 1$.

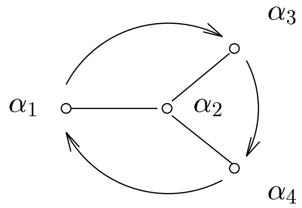
Groups $G_2(q)$, $q > 3$. The Dynkin diagram is



and the highest root is $\tilde{\alpha} = 3\alpha_1 + 2\alpha_2$ (*cf.* [Bo] Table IX). Then (7) is satisfied for $i = 2$.

Other groups require more detailed treatment.

Groups ${}^3D_4(q)$, $q \geq 3$. Here $\tilde{G}$ is the group of σ-fixed points for the automorphism σ of the group $\mathbf{G}$ of type D_4 of the form $\sigma = \tau \circ \theta$ where τ is the algebraic automorphism of $\mathbf{G}$ corresponding to the following symmetry of the Dynkin diagram:



and θ is induced by the field automorphism $x \to x^q$ (in this case $k = \mathbf{F}_q$, $l = \mathbf{F}_{q^3}$). Then R can be realized as $\{\pm\varepsilon_i \pm \varepsilon_j \mid 1 \leq i < j \leq 4\}$ with the following system of simple roots:

$$\alpha_1 = \varepsilon_1 - \varepsilon_2,\ \alpha_2 = \varepsilon_2 - \varepsilon_3,\ \alpha_3 = \varepsilon_3 - \varepsilon_4,\ \alpha_4 = \varepsilon_3 + \varepsilon_4$$

(*cf.* [Bo], Table IV). The center of $\tilde{G}$ is trivial, and we need only to find $\tilde{y} \in T$ satisfying (A), i.e. such that $\Phi(\tilde{y}) \subset [\Delta]$ for some proper subset $\Delta \subset \Pi$. Let t be a generator of l^*. Assume now that $q > 3$, and so we may pick an element $s \in k^*$ different from 1 and $N_{l/k}(t)$. Then the element

$$\tilde{y} = h_{\alpha_1}(t) h_{\alpha_3}(t^q) h_{\alpha_4}(t^{q^2}) h_{\alpha_2}(s)$$

is fixed by σ, and the values at $\tilde{y}$ of positive roots containing α_1 are given in Table 2. Going through the table, one easily ascertains that all values are different from 1, i.e. $\Phi(\tilde{y}) \subset [\Delta]$ for $\Delta = \{\alpha_2, \alpha_3, \alpha_4\}$. In fact, one can say even more: since $\tilde{y}^\sigma = \tilde{y}$, then using the action of τ on the Dynkin diagram, we conclude that $\Phi(\tilde{y}) \subset [\Delta]$ for $\Delta = \{\alpha_2\}$. On the other hand, $\alpha_2(\tilde{y}) = s^2 \cdot N_{l/k}(t)^{-1}$; so picking $s \in k^*$ such that in addition $s^2 \neq N_{l/k}(t)$ (this is always possible if $q \geq 5$; for $p \neq 2$ one can take $s = -1$), we obtain a regular $\tilde{y}$. For $q = 3$, we take

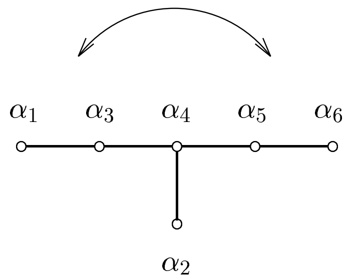
$$\tilde{y} = h_{\alpha_1}(t^2) h_{\alpha_3}(t^{2q}) h_{\alpha_4}(t^{2q^2}) h_{\alpha_2}(-1).$$

Then again with the help of Table 2 we verify that $\Phi(\tilde{y}) \subset [\Delta]$ for $\Delta = \{\alpha_2, \alpha_3, \alpha_4\}$.

Groups $E_6(q)$ and ${}^2E_6(q^2)$, $q > 2$. The Dynkin diagram looks as follows:

Table 2:

γ	$\lvert\gamma(\tilde{y})\rvert$
$\varepsilon_1 - \varepsilon_2$	$t^2 \cdot s^{-1}$
$\varepsilon_1 + \varepsilon_2$	s
$\varepsilon_1 - \varepsilon_3$	$t^{1-q-q^2} s$
$\varepsilon_1 + \varepsilon_3$	$N_{l/k}(t) \cdot s^{-1}$
$\varepsilon_1 - \varepsilon_4$	$t^{1+q-q^2} \cdot s$
$\varepsilon_1 + \varepsilon_4$	t^{1-q+q^2}



and ${}^2E_6$ is the group of σ-fixed points for $\sigma = \tau \circ \theta$ where θ is associated with the field automorphism $x \mapsto x^q$, and τ is the algebraic automorphism corresponding to the symmetry indicated above (in this case $k = \mathbf{F}_q, l = \mathbf{F}_{q^2}$).

First, let $q > 3$. Then $\omega_2 \in Q(R^\vee) = \mathbf{X}_*(\mathbf{T})$ (*cf.* [Bo], Table V); let $\tilde{y} = \omega_2(s)$ where s is a generator of k^*. Since $n_2 = 2$ and $s^2 \neq 1$, we obtain $\Phi(\tilde{y}) \subset [\Delta]$ for $\Delta \subset \Pi \setminus \{\alpha_2\}$, proving (A). To verify (B), pick a $u = \varphi(v)$ which is in $C_G(\varphi(\tilde{y}))$ but not in $\varphi(C_{\tilde{G}}(\tilde{y}))$. Then $v^{-1}\tilde{y}v = z\tilde{y}$ for some non-trivial element z of the center $Z(\tilde{G})$, and there exists $w \in W = W(\mathbf{T}, \mathbf{G})$ such that

$$w\tilde{y}w^{-1} = z\tilde{y} \tag{8}$$

It is easy to check that $Z(\mathbf{G})$ is generated by the element

$$z_0 = h_{\alpha_1}(\xi)h_{\alpha_3}(\xi^2)h_{\alpha_5}(\xi)h_{\alpha_6}(\xi^2)$$

where ξ is a prime 3^{rd} root of unity, and therefore (8) implies that for $\beta = \omega_2 - w(\omega_2)$ we have

$$n_i(\beta) \equiv 0 \bmod (q-1), \ i = 2, 4 \tag{9}$$

Obviously $w \in C_{\mathbf{G}}(\tilde{y})$; since for $q = 5$ the order of $\tilde{y}$ is four, we obtain $C_{\mathbf{G}}(\tilde{y}^3) = C_{\mathbf{G}}(\tilde{y})$ implying that $z = 1$. On the other hand, for $q \geq 7$ we can never have (9) for $i = 2$, since $n_2(\omega_2) = 2$ and $\mid n_2(w(\omega_2)) \mid \leq 2$. So, it remains to consider the case $q = 4$. Since $n_2(\omega_2) = 2$ and $n_4(\omega_2) = 3$, we can have (9) only if

$$n_2(w(\omega_2)) = 2 \text{ or -1}, \ n_4(w(\omega_2)) = 0 \text{ or } \pm 3 \tag{10}$$

Using the table of roots in [Bo], one can see that the possibilities for $w(\omega_2)$ are the following:

$$\omega_2, -\alpha_2, -(\omega_2-\alpha_2)$$

However, in the first case $z=1$, and in the last two cases we respectively have

$$\beta = -\alpha_1 - 3\alpha_2 - 2\alpha_3 - 3\alpha_4 - 2\alpha_5 - \alpha_6$$

and

$$2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 6\alpha_4 + 4\alpha_5 + 2\alpha_6,$$

and therefore

$$w^{-1}\tilde{y}w\tilde{y}^{-1} = h_{\alpha_1}(s)h_{\alpha_3}(s^2)h_{\alpha_5}(s^2)h_{\alpha_6}(s)$$

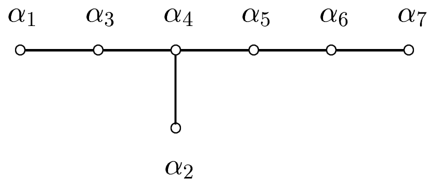
or

$$h_{\alpha_1}(s^{-2})h_{\alpha_3}(s^{-4})h_{\alpha_5}(s^{-4})h_{\alpha_6}(s^{-2}),$$

but neither of these elements belongs to $Z(\mathbf{G})$, and (B) is established.

Finally, if $q=3$, then both groups $E_6(3)$ and ${}^2E_6(9)$ have trivial centers, so we need only to check (A). Since $n_1=n_6=1$, in the non-twisted case one can take $\tilde{y}=\chi_1(-1)\in T$ where $\chi_1 = 3\omega_1 \in \mathbf{X}_*(\mathbf{T})$ to ensure that $\Phi(\tilde{y})\subset[\Delta]$ for $\Delta=\Pi\setminus\{\alpha_1\}$. In the twisted case we let $\tilde{y}=\chi_1(s)\chi_6(\theta(s))$ where s is a generator of the multiplicative group of $l=\mathbf{F}_9$, θ is the field automorphism $x\mapsto x^3$, and $\chi_6=3\omega_6$. Then for $\alpha\notin[\Delta]$ where $\Delta=\Pi\setminus\{\alpha_1,\alpha_2\}$, the value $\alpha(\tilde{y})$ is one of the following: $s,\theta(s)$ or $s\theta(s)$, and neither of these is 1.

Groups $E_7(q)$, $q>3$. Labeling the simple roots as in [Bo]:



we have $\omega_1\in Q(R^\vee)=\mathbf{X}_*(\mathbf{T})$ (*cf. loc. cit.*, Table VI); let $\tilde{y}=\omega_1(s)$ where s is a generator of the multiplicative group of $k=\mathbf{F}_q$. Then, since $n_1=2$ and $s^2\neq 1$, we have $\Phi(\tilde{y})\subset[\Delta]$ for $\Delta=\Pi\setminus\{\alpha_1\}$, hence (A). If (B) fails then, as above, there exists $w\in W=W(\mathbf{T},\mathbf{G})$ such that $w\tilde{y}w^{-1}=z\tilde{y}$. Then w is contained in $C_W(\tilde{y}^2)$ which, as we mentioned above, is generated by w_α for $\alpha\in\Phi(\tilde{y}^2)$. For any such α we have

$$\alpha(\tilde{y}^2) = s^{2n_1(\alpha)} = 1, \tag{11}$$

and since $q>3$, we conclude that $n_1(\alpha)>1$. However it follows from the table that there exists the only positive root in the root system of type E_7 with $n_1(\alpha)>1$, namely $\tilde{\alpha}=\omega_1$, the highest root; besides in this case $n_1(\tilde{\alpha})=2$, and therefore (11) holds only if $q=5$. So, $C_W(\tilde{y}^2)$ is generated by w_α for α not containing α_1, and also by $w_{\tilde{\alpha}}$

Table 3:

γ	$\lvert\gamma(r)\rvert$	$\lvert\gamma(r)\rvert$ for $m = 1$
ε_1	2^m	2
ε_2	$1 - 2^m$	-1
ε_3	$1 - 2^m$	-1
ε_4	$-2 + 3 \cdot 2^m$	4
$\varepsilon_1 - \varepsilon_2$	$-1 + 2^{m+1}$	3
$\varepsilon_1 + \varepsilon_2$	1	1
$\varepsilon_1 - \varepsilon_3$	$-1 + 2^{m+1}$	3
$\varepsilon_1 + \varepsilon_3$	1	1
$\varepsilon_1 - \varepsilon_4$	$2 - 2^{m+1}$	-2
$\varepsilon_1 + \varepsilon_4$	$-2 + 2^{m+2}$	6
$\varepsilon_2 - \varepsilon_3$	0	0
$\varepsilon_2 + \varepsilon_3$	$2 - 2^{m+1}$	-2
$\varepsilon_2 - \varepsilon_4$	$3 - 2^{m+2}$	-5
$\varepsilon_2 + \varepsilon_4$	$-1 + 2^{m+1}$	3
$\varepsilon_3 - \varepsilon_4$	$3 - 2^{m+2}$	-5
$\varepsilon_3 + \varepsilon_4$	$3 - 2^{m+1}$	3
$\frac{1}{2}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4)$	2^m	2
$\frac{1}{2}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3 - \varepsilon_4)$	$2 - 2^{m+1}$	-2
$\frac{1}{2}(\varepsilon_1 + \varepsilon_2 - \varepsilon_3 + \varepsilon_4)$	$-1 + 2^{m+1}$	3
$\frac{1}{2}(\varepsilon_1 + \varepsilon_2 - \varepsilon_3 - \varepsilon_4)$	$1 - 2^m$	-1
$\frac{1}{2}(\varepsilon_1 - \varepsilon_2 + \varepsilon_3 + \varepsilon_4)$	$-1 + 2^{m+1}$	3
$\frac{1}{2}(\varepsilon_1 - \varepsilon_2 - \varepsilon_3 + \varepsilon_4)$	$2 - 3 \cdot 2^m$	4
$\frac{1}{2}(\varepsilon_1 - \varepsilon_2 - \varepsilon_3 - \varepsilon_4)$	0	0
$\frac{1}{2}(\varepsilon_1 - \varepsilon_2 + \varepsilon_3 - \varepsilon_4)$	$1 - 2^m$	-1

for $q = 5$. So, if the element $x = w\tilde{y}w^{-1}\tilde{y}^{-1}$ is non-trivial, then it equals $\omega_1(-1)$. But $\omega_1(-1) = h_{\alpha_3}(-1)h_{\alpha_5}(-1)h_{\alpha_7}(-1)$ while the non-trivial element in the center is $h_{\alpha_2}(-1)h_{\alpha_5}(-1)h_{\alpha_7}(-1)$. Thus $z \notin Z(\mathbf{G})$, which proves (B).

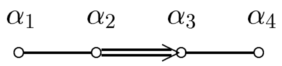
Groups ${}^2F_4(2^{m+1})$. Since the group ${}^2F_4(2)$ is not simple (however, simple is its derived subgroup ${}^2F_4(2)'$ known as Tits' sporadic group, considered in Section 5), we may assume that $m \geq 1$. We will be using the realization of the root system of type F_4 given in [Bo], Table VIII:

$$R = \{\pm\varepsilon_i, \varepsilon_i \pm \varepsilon_j \mid 1 \leq i < j \leq 4\} \cup \{\frac{1}{2}(\pm\varepsilon_1 \pm \varepsilon_2 \pm \varepsilon_3 \pm \varepsilon_4)\}.$$

Then the system of simple roots consists of the following elements:

$$\alpha_1 = \varepsilon_2 - \varepsilon_3,\ \alpha_2 = \varepsilon_2 - \varepsilon_3,\ \alpha_3 = \varepsilon_4,\ \alpha_4 = \frac{1}{2}(\varepsilon_1 - \varepsilon_2 - \varepsilon_3 - \varepsilon_4)$$

and the corresponding Dynkin diagram looks as follows:



Then $\tilde{G}$ is obtained as the group of σ-fixed elements of the endomorphism σ of the group $\mathbf{G}$ of type F_4 acting on the root elements as follows:

$$\sigma = \begin{cases} x_{\alpha_1}(t) \to x_{\alpha_4}(t^{2^m}), \\ x_{\alpha_2}(t) \to x_{\alpha_3}(t^{2^m}), \\ x_{\alpha_3}(t) \to x_{\alpha_2}(t^{2^{m+1}}), \\ x_{\alpha_4}(t) \to x_{\alpha_1}(t^{2^{m+1}}). \end{cases} \tag{12}$$

In this case $k = \mathbf{F}_{2^m}$, $l = \mathbf{F}_{2^{2m+1}}$. It follows from (12) that elements of the form

$$r(s) = h_{\alpha_1}(s)h_{\alpha_2}(s^2)h_{\alpha_3}(s^{2^{m+1}})h_{\alpha_4}(s^{2^m}),\ s \in l^* \tag{13}$$

are fixed by σ. Recall that the center of $\tilde{G}$ is trivial, and therefore all we need to do is to find $\tilde{y}$ of the form (13) such that $\Phi(\tilde{y}) \subset [\Delta]$ for some proper subset $\Delta \subset \Pi$. Let $s \in l^*$ be a generator. We will show that

$$\Phi(r(s)) \subset [\Delta] \quad \text{for} \quad \Delta = \{\alpha_1, \alpha_2\} \tag{14}$$

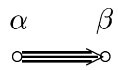
For a root $\gamma \in R$, let $|\gamma(r)|$ be the integer such that $\gamma(r) = s^{|\gamma(r)|}$ where $r = r(s)$. The values of $|\gamma(r)|$ for all positive roots are shown in Table 3. For $m = 1$, s has order 7, but no number in the third column (except two zeroes) is divisible by 7, and (14) follows. For $m > 1$, (14) is easily obtained via elementary estimations.

Table 4:

γ	$\lvert\gamma(r)\rvert$
α	$2-3^{m+1}$
β	$-1+2\cdot 3^m$
$\alpha+\beta$	$1-3^m$
$\alpha+2\beta$	3^m
$\alpha+3\beta$	$-1+3^{m+1}$
$2\alpha+3\beta$	1

Groups ${}^2G_2(3^{2m+1})$. In this case, $\tilde{G}$ is obtained as the group of σ-fixed points of the automorphism σ of the group $\mathbf{G}$ of type G_2 acting on the root elements as follows:

$$\sigma = \begin{cases} x_\alpha(t) \to x_\beta(t^{3^m}), \\ \\ x_\beta(t) \to x_\alpha(t^{3^{m+1}}). \end{cases}$$



Then $k = \mathbf{F}_{3^m}$, $l = \mathbf{F}_{3^{2m+1}}$. Since the group ${}^2G_2(3)$ is not simple, we may assume that $m \geq 1$. One easily verifies that σ-fixed elements of $\mathbf{T}$ are parameterized as follows: $r(s) = h_\alpha(s)h_\beta(s^{3^m})$, $s \in l^*$. Since the center of $\tilde{G}$ is trivial, it suffices to show that for a generator s of l^*, the element $r = r(s)$ is regular. The values of $|\gamma(r)|$ for all positive roots are given in Table 4, and simple analysis shows that there is no root γ such that $\gamma(r) = 1$, hence the required result.

5. Proof of Theorem 3.5 for groups of Lie type: exceptional cases.

First, we outline the basic idea of constructing the required elements in the Chevalley groups which are not covered by Theorem 3.5 and then present these for each type (we will see in the next section that the method used here is also applicable to the sporadic groups).

Lemma 5.1 *Let G be a finite group, x, $y \in G$. Then*

$$\#E(x,y) \leq c^3 d^2 \tag{1}$$

where c is the order of $C = C_G(x)$ and $d = \max(\#C_G(z))$, z runs through the coset yC. If y normalizes C and $C \cap C_G(y) = (e)$, then $d = \#C_G(y)$ and (1) can be sharpened to:

$$\#E(x,y) \leq \frac{c^3 d^2}{\mathrm{ord}(y)} \tag{2}$$

Proof. Obviously, the number of elements in

$$C_G(x,y) = \bigcup_{z \in yC} C_G(z)$$

cannot exceed cd, and (1) is immediate. Furthermore, if y is as in the second statement, the map

$$\mu : C \to C,\ c \mapsto y^{-1}c^{-1}yc,$$

is a bijection. This implies that any element $z \in yC$ can be written as $c^{-1}yc$ for a suitable $c \in C$; in particular, $\#C_G(z) = \#C_G(y)$. Besides, in this case

$$E(x,y) = CC_G(y)CC_G(y)C, \tag{3}$$

and writing $C_G(y)$ as $C_G(y) = \bigcup_{i=1}^{t} z_i D$ where $D = \langle y \rangle$, $t = [C_G(y) : D]$, and using the fact that y normalizes C, we obtain

$$\#E(x,y) \le c^3 \cdot d \cdot t = \frac{c^3 \cdot d^2}{\mathrm{ord}(y)}.$$

The lemma is proved. ∎

The basic construction for producing the required elements x, y in most types of Chevalley groups is as follows. Let $k = \mathbf{F}_q$, the field of q elements, l/k be the extension of degree n, and $\rho_{l/k} : l \to M_n(k)$ be the regular representation. Then $T_0 = \rho(l^*)$ and $T_1 = \rho(l^{(1)})$ are cyclic subgroups of $G_0 = GL_n(k)$; let x_0 (resp. x_1) be a generator of T_0 (resp. T_1). Obviously, x_0 is a regular element in $\mathbf{GL}_n$ implying that its centralizer C_0 in G_0 coincides with the cyclic subgroup $\langle x_0 \rangle$. We claim that x_1 is also regular, and therefore its centralizer in G_0 (resp. $G_1 = SL_n(k)$) coincides with C_0 (resp. $C_1 = \langle x_1 \rangle$). To see the regularity it suffices to observe that if $s \in l^{(1)}$ is a generator, then all the elements $s, s^q, ..., s^{q^{n-1}}$, obtained by applying the consecutive powers of the Frobenius automorphism, are pairwise distinct (since for any i, j between 0 and $n-1$, the difference $q^i - q^j$ is strictly less than the order of s which is equal to $(q^n - 1)/(q-1)$).

Next, let σ be a generator of $\mathrm{Gal}(l/k)$. Since $N_{l/k}(l^*) = k^*$, the Skolem-Noether Theorem easily implies the existence of an element $y_1 \in G_1$ which normalizes T_0 and is such that the inner automorphism $\mathrm{Int}(y_1)$ induces on $\rho_{l/k}(l)$ the automorphism $\rho_{l/k} \circ \sigma \circ \rho_{l/k}^{-1}$. Then any element $y \in y_1 C_0$ enjoys the latter two properties as well, and obviously the intersection $C_0 \cap C_{G_0}(y)$ coincides with $\rho_{l/k}(k^*)$ which is the center of G_0. Another property of y to be used in the sequel is given by the following statement.

Lemma 5.2 *Any $y \in y_1 C_0$ is conjugate in $GL_n(k)$ to a matrix of the form*

$$w(\alpha) = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ \alpha & 0 & \dots & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ & & \ddots & \vdots & \vdots \\ & & & 1 & 0 \end{pmatrix}$$

for some $\alpha \in k^*$. In particular, y is a regular element in $\mathbf{GL}_n$.

Proof. Since $y^n \in C_0 \cap C_{G_0}(y_1)$, we have $y^n = \alpha E_n$ for some $\alpha \in k^*$ (where E_n is the unity matrix). Let us show that y is conjugate to the corresponding matrix $w = w(\alpha)$, it being sufficient to establish the conjugacy in $\mathbf{GL}_n$. Obviously, y normalizes the torus $\mathbf{T}_0 = \mathbf{R}_{l/k}(\mathbb{G}_m)$, and therefore under conjugation which brings $\mathbf{T}_0$ to the diagonal form, it is taken to a certain monomial matrix μ. To every monomial matrix there corresponds in an obvious way a permutation of indices $\{1, ..., n\}$, and the permutation corresponding to μ is by our construction a cycle of length n. This means that conjugating μ by a suitable permutation matrix, if necessary, we may assume that μ looks as follows

$$\mu(\alpha_1, ..., \alpha_n) = \begin{pmatrix} 0 & 0 & \dots & 0 & \alpha_n \\ \alpha_1 & 0 & \dots & 0 & 0 \\ & \alpha_2 & & 0 & 0 \\ & & \ddots & \vdots & \vdots \\ & & & \alpha_{n-1} & 0 \end{pmatrix}.$$

The conjugation by the diagonal matrix

$$\mathrm{diag}(1, \alpha_2 \cdots \alpha_n, ..., \alpha_{n-1}\alpha_n, \alpha_n)$$

brings $\mu(\alpha_1, ..., \alpha_n)$ to the form $w(\beta)$, $\beta = \alpha_1, ..., \alpha_n$. However, since $w(\beta)^n = \beta E_n$, we conclude that $\beta = \alpha$.

Recall now the following criterion for regularity (*cf.* [RBC], §1): $g \in \mathbf{GL}_n$ is regular if and only if for any λ in some algebraically closed field containing the entries of g, the rank of the matrix $(g - \lambda E_n)$ is $\geq n - 1$. To verify this criterion for y, notice that deleting the first row and the last column in the matrix $w(\alpha) - \lambda E_n$, we obtain the matrix

$$\begin{pmatrix} \alpha & -\lambda & & & \\ 0 & 1 & -\lambda & & \\ & & 1 & & \\ & & & \ddots & -\lambda \\ & & & & 1 \end{pmatrix}$$

implying that $\mathrm{rank}(y - \lambda E_n) = \mathrm{rank}(w(\alpha) - \lambda E_n) \geq n - 1$. ■

Using this information, we are already in a position to consider

Groups $PSL_n(q)$. First, let $q = 2$. Then $G = PSL_n(q)$ is isomorphic to $SL_n(q) = GL_n(q)$. Since the group $SL_2(2)$ is not simple and $SL_3(2)$ is isomorphic to $PSL_2(7)$, we may assume that $n \geq 4$. We will prove that for $x = x_1$ and $y = y_1$

$$E(x, y) \neq G. \tag{4}$$

This will be done by estimating the number of elements in $E(x, y)$ and comparing it to the order of G. Since in our setting $C_G(x) \cap C_G(y) = (e)$, $\#C_G(x) \leq 2^n - 1$ and

$\#C_G(y) \leq 2^n - 1$ (the last inequality follows from the fact that the centralizer of a regular element in M_n is a vector space of dimension n), we obtain from Lemma 5.1 that

$$\#E(x,y) \leq \frac{2^{5n}}{n}.$$

Let $\alpha_n = 2^{5n}/n$, $\beta_n = \#SL_n(\mathbf{F}_2)$. We will show that for any $n \geq 5$

$$\alpha_n < \beta_n, \tag{5}$$

proving (4) for all $n \neq 4$. To establish (5), observe that for $n \geq 3$ we have

$$\frac{\alpha_{n+1}}{\alpha_n} \leq \frac{\beta_{n+1}}{\beta_n}. \tag{6}$$

Indeed, obviously

$$\frac{\alpha_{n+1}}{\alpha_n} = 2^5 \cdot \frac{n}{n+1} < 2^5,$$

while, using the formula for β_n (*cf.* [St]), we obtain

$$\frac{\beta_{n+1}}{\beta_n} = \frac{(2^{n+1}-1)(2^{n+1}-2)\cdots(2^{n+1}-2^n)}{(2^n-1)(2^n-2)\cdots(2^n-2^{n-1})} = 2^n \cdot (2^{n+1}-1) > 2^5.$$

By virtue of (6), the inequality $\alpha_n < \beta_n$ implies $\alpha_{n+1} < \beta_{n+1}$, so it suffices to prove (5) for $n = 5$, which is done by direct computations:

$$\alpha_5 = \frac{33,554,432}{5}, \ \beta_5 = 9,999,360.$$

The case $n = 4$ requires slightly more delicate estimations. Since $y^4 = E_4$, y is a regular unipotent element, and therefore $\#C_G(y) = 8$. Thus, $C_G(y) = \{1, z\} \cdot \langle y \rangle$, and in view of (3) we obtain

$$E(x,y) = (C\{1,z\}C\{1,z\}C) \cdot \langle y \rangle.$$

Then

$$\#E(x,y) \leq (15^3 + 2 \cdot 15^2 + 15) \cdot 4 = 15,360$$

while $\#SL_4(\mathbf{F}_2) = 20,160$.

Now, consider one of the two remaining cases: $G = PSL_4(\mathbf{F}_3)$. Let $\tilde{G} = SL_4(\mathbf{F}_3)$ and $\varphi : \tilde{G} \to G$ be the canonical homomorphism. Let $x = \varphi(x_1)$ and $y = \varphi(y_1)$, and show that for this elements we have (4). Indeed, it is easy to see that if s is a generator of $l^{(1)}$ where l is the extension of $k = \mathbf{F}_3$ of degree 3, then $k(s^2) = l$, implying that $C_G(x) = \varphi(C_{\tilde{G}}(x_1))$, and therefore $\#C_G(x) = 20$. Next the characteristic polynomial of any $z \in yT_1$ has the form $\lambda^4 + 1$, implying that the algebra $\mathbf{F}_3[z_1]$ is isomorphic to $\mathbf{F}_9 \oplus \mathbf{F}_9$, and therefore $C_{\tilde{G}}(z_1)$ is of order 32. There exists an element $t \in T_1$ such that

$y_1ty_1^{-1} = -t$, and then $z_1tz_1^{-1} = -t$ for any $z_1 \in y_1T_1$. Then for $z = \varphi(z_1)$ we have: $C_G(z) = \{1, \varphi(t)\} \cdot D$, where $D = \varphi(C_{\tilde{G}}(z_1))$ is of order 16. Using (3), we obtain the following estimation:

$$\#E(x,y) \leq 20^3 \cdot 16^2 = 2,048,000$$

while $\#G = 6,065,280$, and (4) is proved.

The last case $G = PSL_3(4)$ could be treated similarly, however we prefer to bring out at this point one technical statement which is applicable in a number of cases (in particular, to all sporadic groups).

Lemma 5.3 *Let G be a finite group, and let $x \in G$ be an element of a prime order p, such that the centralizer C of x in G coincides with the cyclic group $\langle x \rangle$. Suppose that p^2 does not divide the order of G, and that G has $c(p)$ conjugacy classes of elements of order p. Then*

(i) $N_G(C)$ contains an element y of order $d(p) = (p-1)/c(p)$;

(ii) if m is the maximum of orders of the centralizers of elements of order $d(p)$ in G, then

$$\#E(x,y) \leq f(x,y) = \frac{m^2p^3}{d(p)}.$$

(As was pointed out by B. Fischer, the condition that p^2 does not divide the order of G is superfluous).

Proof. Consider the homomorphism $\mu : N_G(C) \to \mathrm{Aut}(C)$ sending $g \in N_G(C)$ to the restriction of the inner automorphism $\mathrm{Int}(g)$. It follows from our assumptions, that any element of order p in G is conjugate to an element of C, and therefore $c(p)$ is equal, in fact, to the number of orbits of $\mathrm{Im}(\mu)$ on the set $X = \{x, ..., x^{p-1}\}$. Since $\mathrm{Aut}(C)$ is a cyclic group acting simply transitively on X, we obtain that $c(p) = [\mathrm{Aut}(C) : \mathrm{Im}(\mu)]$, implying that $\mathrm{Im}(\mu)$, and consequently also $N_G(C)$, contain an element of order $d(p)$.

Part (ii) is immediate from Lemma 5.1. ■

So, to prove that $E(x,y) \neq G$ it suffices to verify that $f(x,y) < \#G$. This is done by using information from [Atlas] about the centralizers of elements. For example, if $G = PSL_3(4)$, one finds in [Atlas], p. 24, that an element $x \in G$ of order 7 satisfies the assumptions of Lemma 5.3. Besides, $c(7) = 2$ and for y we take an element of order $d(7) = 3$. Again from the table in [Atlas] we conclude that $m = 9$. Thus $f(x,y) = 9,261$ while $\#G = 20,160$.

Alternating groups. The only case left out in Theorem 3.5 is $G = A_8$. This group, however, is known to be isomorphic to $SL_4(2)$ which has already been considered above.

To exhibit the required elements x, y in the groups of other classical types, we embed into these a suitable group $GL_n(q)$ or $SL_n(q)$ and take the images of x_0 (or x_1) and y_1 under this embedding. The calculation of the centralizer of the element x thus obtained is based on the following statement.

Lemma 5.4 *Assume that $n \geq 3$. It x is one of the matrices x_0 or x_1 constructed above, then x does not have any common eigenvalues with $-x$ (if* char $\neq 2$*) and $\pm x^{-1}$. In particular, the matrix* $\mathrm{diag}(x, {}^t x^{-1})$ *is regular in GL_{2n}.*

Proof. If λ is one eigenvalue of x, then all others are $\lambda^q, ..., \lambda^{q^{n-1}}$. It follows that if λ is common to x and $-x$, then $\lambda = -\lambda^{q^i}$ for some $1 \leq i \leq n-1$. Since the order of λ is either $(q^n - 1)$ (if $x = x_0$) or $l(n,q) = (q^n - 1)/(q-1)$ (if $x = x_1$), we obtain

$$2(q^i - 1) \equiv 0 \bmod l(n,q)$$

which is impossible for $n \geq 3$, as is easily seen. Similarly, if λ is common to x and $\pm x^{-1}$, there should be i, $1 \leq i \leq n-1$ such that

$$2(q^i + 1) \equiv 0 \bmod l(n,q)$$

which is not possible either. The lemma is proved. ∎

Groups $PSp_{2m}(q), m > 1, q = 2$ or 3. The group $PSp_4(3)$ requires special treatment and will be considered at the end of this subsection; therefore, since the group $PSp_4(2)$ is not simple, we may assume that $m \geq 3$. Now it is convenient to use presentation of $Sp_{2m}(q)$ other than the one used in §4. Namely, the corresponding alternating matrix I will be taken in the following form

$$I = \begin{pmatrix} 0 & E_m \\ -E_m & 0 \end{pmatrix},$$

and then $Sp_{2m}(q) = \{x \in M_{2m}(q) \mid {}^t x I x = I\}$. In this realization we have the embedding $\varepsilon : GL_m(q) \to Sp_{2m}(q)$ given by the formula

$$\varepsilon : a \to \begin{pmatrix} a & 0 \\ 0 & ({}^t a)^{-1} \end{pmatrix}.$$

Also, let $\varphi : \tilde{G} = Sp_{2m}(q) \to PSp_{2m}(q) = G$ be the natural projection (note that $\mathrm{Ker}(\varphi) = 1$ for $q = 2$), $\tilde{x} = \varepsilon(x_0)$, $\tilde{y} = \varepsilon(y_0)$, and $x = \varphi(\tilde{x})$, $y = \varphi(\tilde{y})$.

It follows from Lemma 5.4 that $C_{\tilde{G}}(\tilde{x})$ is the cyclic group $\langle \tilde{x} \rangle$. Besides, the matrices $\tilde{x}$ and $-\tilde{x}$ are not conjugate if char $\neq 2$, implying that $C_G(x) = \varphi(C_{\tilde{G}}(\tilde{x}))$. Thus,

$$\#C_G(x) = \begin{cases} 2^m - 1, & \text{if } q = 2, \\ 1/2 \cdot (3^n - 1), & \text{if } q = 3. \end{cases}$$

Furthermore, it follows from Lemma 5.2 that any $\tilde{z} \in \tilde{y} C_{\tilde{G}}(\tilde{x})$ is conjugate in $\tilde{G}$ to a matrix of the form $s = \mathrm{diag}(w, {}^t w^{-1})$ where $w = w(\alpha)$ for some $\alpha \in \mathbf{F}_q^*$. However, since $q = 2$ or 3, w is orthogonal (i.e. ${}^t w w = E_m$), implying that $C_{\tilde{G}}(\tilde{z})$ is identifiable with the unitary group $U_2(R)$ over the ring $R = \mathbf{F}_q[w]$ defined by the equation

$$a^* J a = J,$$

where $J = \begin{pmatrix} 0 & e \\ -e & 0 \end{pmatrix}$ ($e \in R$ is the multiplicative identity), $(a_{ij})^* = (\tau(a_{ji}))$, τ being the involution of R defined by taking the matrix transpose. To estimate the order of $U_2(R)$, consider the subgroup $H \subset GL_2(R)$ consisting of matrices of the form $\mathrm{diag}(r, e)$, $r \in R^*$. Obviously, H has trivial intersection with $U_2(R)$, hence

$$\#(H \cdot U_2(R)) = (\#H) \cdot (\#U_2(R)) \leq \#GL_2(R)$$

and

$$\#U_2(R) \leq \frac{\#GL_2(R)}{\#R^*} = \#SL_2(R).$$

However, as is well-known, $\#SL_2(R) \leq (\#R)^3$, and we obtain the estimation:

$$\#C_{\tilde{G}}(\tilde{y}) \leq q^{3m}.$$

Also, recall that the order of G is given by the formula (*cf.* [St]):

$$\#G = \gamma \cdot q^{m^2}(q^2-1)(q^4-1)\cdots(q^{2m}-1) \tag{7}$$

where $\gamma = 1$ if char $= 2$, and $\gamma = 1/2$ otherwise. Now, let us verify (4). First, let $q = 2$. It follows from the above that $C_G(x) \cap C_G(y) = (e)$, and therefore by Lemma 5.1,

$$\#E(x,y) \leq \frac{(\#C_G(x))^3 \cdot (\#C_G(y))^2}{\mathrm{ord}(y)} \leq \frac{2^{9m}}{m}. \tag{8}$$

Then, using (7) one easily verifies that $\#E(x,y) < \#G$ for any $m \geq 4$. For $q = 3$, we obtain the following estimation

$$\#E(x,y) \leq (\#C_G(x))^3 \cdot (\#C_G(y))^2 \leq \frac{1}{8} \cdot 3^{9m}, \tag{9}$$

and again it is easy to check that $\#E(x,y) < \#G$ for any $m \geq 4$.

The case $m = 3$ requires slightly sharper estimations. With the notations as above, let W be the image of the (R)-determinant on $U_2(R)$; obviously W is intermediate between

$$U_1(R) = \{a \in R^* \mid a \cdot \tau(a) = 1\} \text{ and } (R^*)^{1-\tau} = \{a/\tau(a) \mid a \in R^*\}.$$

Then

$$\#U_2(R) = (\#W) \cdot (\#SU_2(R)).$$

One the other hand, direct computation show that $SU_2(R) = SL_2(R_0)$ where $R_0 = R^\tau$ is the subring of τ-symmetric elements. If $m = 3$, $q = 2$, then $R = \mathbf{F}_2[t]/(f(t))$ where $f(t) = t^3 - 1$, i.e. $R = \mathbf{F}_2 \oplus \mathbf{F}_4$. Besides, τ acts trivially on $\mathbf{F}_2$ and non-trivially on $\mathbf{F}_4$. Obviously, $U_1(R) = (R^*)^{1-\tau}$ has order 3 and $R_0 = \mathbf{F}_2 \oplus \mathbf{F}_2$, implying

$$\#U_2(R) = (\#U_1(R)) \cdot (\#SL_2(\mathbf{F}_2))^2 = 108.$$

For $m = 3$, $q = 3$ we have $R = \mathbf{F}_3[t]/(f(t))$ where $f(t) = t^3 \pm 1$. So, R is identifiable with the ring $\mathbf{F}_3[\delta]$, $\delta^3 = 0$, with τ sending δ to $2\delta \pm \delta^2$. Obviously, under the homomorphism $R \to \mathbf{F}_3$ sending δ to zero, $U_2(R)$ is mapped onto $Sp_2(\mathbf{F}_3)$, and therefore W is contained in $(1 + \delta \mathbf{F}_3[\delta])$. Using this fact, it is easy to show that W has order 3. Also, R_0 coincides with the subring generated by δ^2, and consequently

$$\#U_2(R) = (\#W) \cdot (SL_2(R_0)) = 1944.$$

Thus, we have shown that if $m = 3$, the order of $C_{\tilde{G}}(\tilde{y})$ is 108 for $q = 2$, and is 1944 for $q = 3$.

Using the figures in (8), we obtain for $m = 3$, $q = 2$ that

$$\#E(x, y) \leq \frac{1}{3} \cdot 7^3 \cdot 108^2 = 1,333,584,$$

while the order of G equals $1,451,520$. For $m = 3$, $q = 3$, one should observe that $C_G(x) \cap C_G(y) = (e)$ (this is the case for any odd m) and therefore (9) can be sharpened to

$$\#E(x, y) \leq \frac{1}{24} \cdot (\#C_G(x))^3 \cdot (\#C_G(y))^2,$$

using which it is easy to verify that again $\#E(x, y) < \#G$.

The last remaining case is $G = PSp_4(3)$. It follows from [Atlas] that G has a single conjugacy class of elements of order 5, and if x is one of them, then C, the centralizer of x in G, is $\langle x \rangle$. By Lemma 5.3, $N_G(C)$ contains an element y of order 4, and then

$$\#E(x, y) \leq \frac{5^3 \cdot (\#C_G(y))^2}{4}. \tag{10}$$

[Atlas] provides two possibilities for the order of $C_G(y)$: 8 or 48. Unfortunately, the value 48 does not allow us to show vis (10) that $\#E(x, y) < \#G$. So, we need to show that in our case $\#C_G(y) = 8$, and then (10) easily yields the required result (observe, that $\#G = 25,920$). Let $\tilde{x} \in Sp_4(3)$ be an element of order 10 in $\varphi^{-1}(x)$, and $\tilde{y} \in \varphi^{-1}(y)$. It is easy to see that $\tilde{x}$ has 4 distinct eigenvalues in the natural action on the 4-dimensional space, and the conjugation by $\tilde{y}$ induces a cyclic permutation of the lines spanned by the corresponding eigenvectors. Now, it follows from the proof of Lemma 5.2, that $\tilde{y}$ is a regular element in GL_4. Thus, the centralizer of $\tilde{y}$ in $Sp_4(3)$ is a 2-dimensional torus splitting over the quadratic extension of $\mathbf{F}_3$, easily implying that the order of $C_{\tilde{G}}(\tilde{y})$ is ≤ 16, hence $\#C_G(y) = 8$.

Groups $PSU_n(q^2)$. As is well-known, the group $G = PSU_n(q^2)$ for $n = 3$, $q = 2$, is not simple, and for $n = 4$, $q = 2$ is isomorphic to $PSp_4(3)$ which has already been considered. Besides, the following cases are easily considered with the help of Lemma 5.1, using elements of the indicated orders:

$$\begin{array}{lll} n = 4, & q = 3, & \operatorname{ord}(x) = 5, \\ n = 5, & q = 2, & \operatorname{ord}(x) = 11, \\ n = 6, & q = 2, & \operatorname{ord}(x) = 7. \end{array}$$

So, throughout this subsection $n \geq 7$ and $q = 2$. We let $k = \mathbf{F}_2$, $k_0 = \mathbf{F}_4$, and let $x \to \overline{x}$ denote the natural automorphism of k_0 over k. Also, for $x = (x_{ij})$ in $GL_m(k_0)$ we let $x^* = (\overline{x_{ji}})$.

Lemma 5.5 *Let $x \in GL_m(k_0)$ be one of the matrices x_0 or x_1. Then for any $\mu \in k_0$, x does not have common eigenvalues with μx ($\mu \neq 1$) and $\mu(x^*)^{-1}$.*

Proof. As in the proof of Lemma 5.4, if λ is one of the eigenvalues of x, then all others are: $\lambda^4, ..., \lambda^{4^{m-1}}$. Thus, if λ is common to x and μx ($\mu \neq 1$), it satisfies a relation of the form: $\lambda = \mu\lambda^{4^i}$, for some $i = 1, ..., m-1$. This implies the congruence $9(4^i - 1) \equiv 0 \bmod (4^m - 1)$, which never holds true. Similarly, if λ is common to x and $\mu(x^*)^{-1}$, then for some i we have $\lambda = \mu\lambda^{-2\cdot 4^i}$, implying $9 \cdot (2 \cdot 4^i + 1) \equiv 0 \bmod (4^m - 1)$, which is again impossible for $m \geq 3$. The lemma is proved. ■

First, we consider the case $n = 2m$, $m \geq 4$. It is convenient to use the following realization of the unitary group:

$$U_n = \{x \in GL_n(\mathbf{F}_4) \mid x^* I x = I\} \tag{11}$$

where

$$I = \begin{pmatrix} 0 & E_m \\ E_m & 0 \end{pmatrix}$$

and $(x_{ij})^* = (\overline{x_{ji}})$. Let $\varepsilon : GL_m(\mathbf{F}_4) \to U_n$ be the embedding given by the formula

$$\varepsilon : a \mapsto \begin{pmatrix} a & 0 \\ 0 & (a^*)^{-1} \end{pmatrix}.$$

Obviously, for $\tilde{G} = SU_n$ one has $\varepsilon^{-1}(\tilde{G}) = SL_m(\mathbf{F}_4)$. Let $\tilde{x} = \varepsilon(x_1)$, $\tilde{y} = \varepsilon(y_1)$, and $x = \varphi(\tilde{x})$, $y = \varphi(\tilde{y})$. It follows from Lemma 5.5 that the centralizer $C_G(x)$ is equal to $(\varphi \circ \varepsilon)(T_1)$, and therefore its order is $\leq \frac{1}{3}(4^m - 1)$. Any $z \in yC_G(x)$ is of the form $z = \varphi(\tilde{z})$ where $\tilde{z} \in \tilde{y}\varepsilon(T_1)$, and it suffices to estimate the order of $C_{\tilde{G}}(\tilde{z})$ (which is $\geq \#C_G(z)$). Actually, for the case of n odd we will need the estimation of the order of the centralizer in U_n (for n even) of any $z \in \tilde{y}\varepsilon(T_0)$. For this reason, we produce here the latter estimation, which is also the upper bound for $C_{\tilde{G}}(\tilde{z})$. It follows from Lemma 5.2 that $\tilde{z}$ is conjugate in U_n to the matrix $w = \mathrm{diag}(w(\alpha), (w(\alpha)^*)^{-1})$, for some $\alpha \in k_0^*$. Since $\alpha\overline{\alpha} = 1$, the matrix $w(\alpha)$ is unitary, and therefore the centralizer of w in U_n is isomorphic to the unitary group $U_2(R)$ over the ring $R = k_0[w(\alpha)]$ (which is the centralizer of $w(\alpha)$ in $M_m(k_0)$), provided with the involution τ, acting as * on $w(\alpha)$ and as $^-$ on k_0, and with respect to the matrix

$$J = \begin{pmatrix} 0 & e \\ e & 0 \end{pmatrix}.$$

To estimate the order of $U_2(R)$, observe that $SU_2(R) = SL_2(R_0)$ where $R_0 = R^\tau$ (since char $= 2$), and therefore

$$\#SU_2(R) \leq (\#R_0)^3 = 2^{3m}.$$

Then
$$\#U_2(R) \le 2^{3m} \cdot d \tag{12}$$
where d is the order of the subgroup $U_1(R)$ of elements $r \in R^*$ satisfying $\tau(r)r = e$. In particular, since the order of the multiplicative group of R^* is $< 2^{2m}$, we obtain that
$$\#U_2(R) \le 2^{5m}.$$
Then
$$\#E(x,y) \le \frac{2^{16m}}{27},$$
and using the formula for the order of G:
$$\#G = \gamma \cdot 2^{(2m-1)m}(2^2-1)(2^3+1)\cdots(2^{2m-1}+1)(2^{2m}-1)$$
where γ is 1 or 1/3, we easily obtain that $\#E(x,y) < \#G$ for any $m \ge 4$.

Now, let $n = 2m+1$, $m \ge 3$. Then U_n can again be presented in the form (11) where
$$I = \begin{pmatrix} \begin{matrix} 0 & E_m \\ E_m & 0 \end{matrix} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \begin{matrix} 0 & \dots & 0 \end{matrix} & 1 \end{pmatrix},$$
and we may consider the embedding $\varepsilon : GL_m(k_0) \to SU_n$ given by the formula
$$\varepsilon : a \mapsto \begin{pmatrix} \begin{matrix} a & 0 \\ 0 & (a^*)^{-1} \end{matrix} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \begin{matrix} 0 & \dots & 0 \end{matrix} & \chi(a) \end{pmatrix},$$
where $\chi(a) = (\det(a))^{-1}(\overline{\det(a)})$. Let $\tilde{x} = \varepsilon(x_0)$, $\tilde{y} = \varepsilon(y_0)$ and $x = \varphi(\tilde{x})$, $y = \varphi(\tilde{y})$.

It easily follows from Lemma 5.5 that the centralizer $C_G(x)$ is equal to $(\varphi \circ \varepsilon)(T_0)$, hence its order is $\le 4^m - 1$. To estimate the order of $C_{\tilde{G}}(\tilde{z})$ for $\tilde{z} \in \tilde{y}\varepsilon(T_0)$, observe that if $\tilde{z}(e_n) = \lambda e_n$, then the λ-eigenspace V of $\tilde{z}$ in the natural action on $\mathbf{F}_4^n$ is at most 3-dimensional (since any element in $y_1 T_0$ is regular). Obviously, V is invariant under $C_{\tilde{G}}(\tilde{z})$, and therefore the index in $C_{\tilde{G}}(\tilde{z})$ of the subgroup B fixing e_n, does not exceed the number of elements in V, i.e. 2^6. On the other hand, B is isomorphic to the centralizer in U_{2m} of an element of the form similar to that of $\tilde{z}$, and we obtain that $\#C_{\tilde{G}}(\tilde{z}) \le 2^{5m+6}$. The corresponding estimation for $\#E(x,y)$ looks as follows:
$$\#E(x,y) \le 2^{16m+12},$$
using which and the formula for the order of G:
$$\#G = \gamma \cdot 2^{(2m+1)m} \cdot (2^2-1)(2^3+1)\cdots(2^{2m}-1)(2^{2m+1}+1),$$

we easily obtain that $\#E(x,y) < \#G$ for all $m \geq 4$.

The case $n = 7$ requires slightly more careful estimations. Assume that $\lambda = 1$, i.e. $\tilde{z}(e_n) = e_n$. Observe now that the index $[C_{\tilde{G}}(\tilde{z}) : B]$ cannot exceed, in fact, the number of elements in the subspace V defined above, of length 1. Using Witt's Theorem, and the fact that V is non-degenerate in this case, it is easy to calculate that this number is 36. On the other hand, we *a priori* know that the centralizer of the corresponding element in SU_6 cannot exceed 2^{15}, and from the information in [Atlas], we conclude that this bound, in fact, can be reduced to 1944. Thus, $\#C_{\tilde{G}}(\tilde{z}) \leq 36 \cdot 1944$, using which, it is easy to compute that $\#E(x,y) < \#G$ also in this case.

Now, assume that $\lambda \neq 1$. Then one easily checks that the corresponding λ-eigenspace V is 1-dimensional and the algebra R introduced above is the field $\mathbf{F}_{4^3}$. It follows that $U_1(R)$ is of order 9, and therefore according to (12),

$$\#U_2(R) \leq 9 \cdot 2^9.$$

Eventually, we obtain that $\#C_{\tilde{G}}(\tilde{z}) \leq 9 \cdot 2^9$, using which one easily checks again that $\#E(x,y) < \#G$.

Groups $P\Omega_n(f)$, $q = 2$ or 3. First, let $n = 2m$, $m \geq 4$ and f has Witt index m, i.e. $f(x_1, ..., x_{2m}) = x_1 x_{m+1} + ... + x_m x_{2m}$. Then we have the embedding $\varepsilon : GL_m(q) \to SO_n(f)$ given by the formula:

$$\varepsilon : a \mapsto \begin{pmatrix} a & 0 \\ 0 & ({}^t a)^{-1} \end{pmatrix}.$$

Note that for $q = 2$ we have $GL_m(q) = SL_m(q)$ and $SO_n(f) = \Omega_n(f)$, while for $q = 3$ we have $\varepsilon^{-1}(\Omega_n(f)) = SL_m(q)$. Also, let

$$\varphi : \tilde{G} = \Omega_n(f) \to P\Omega_n(f) = G$$

be the canonical projection; obviously $\mathrm{Ker}(\varphi) = 1$ if either $q = 2$ or $q = 3$ and m is odd. Let $\tilde{x} = \varepsilon(x_1)$, $\tilde{y} = \varepsilon(y_1)$, and $x = \varphi(\tilde{x})$, $y = \varphi(\tilde{y})$. It follows from Lemma 5.5 that the centralizer $C_G(x)$ coincides with $(\varphi \circ \varepsilon)(T_1)$, and therefore has order $(q^m - 1)/(q - 1)$.

To estimate the order of $C_{\tilde{G}}(\tilde{z})$, $\tilde{z} \in \tilde{y}\varepsilon(T_1)$ observe that $\tilde{z}$ is conjugate in $SO_n(f)$ to a matrix of the form $\mathrm{diag}(w, w)$ where $w = w(\alpha)$, $\alpha = \pm 1$. Then $C_{\tilde{G}}(\tilde{z})$ embeds into the unitary group $U_2(R)$ of the ring $R = \mathbf{F}_q[w]$ with the involution induced by taking the matrix transpose and with respect to the matrix

$$J = \begin{pmatrix} 0 & e \\ e & 0 \end{pmatrix}.$$

One easily verifies that the subgroup $H \subset GL_2(R)$ consisting of matrices of the form $\mathrm{diag}(a, e)$, $a \in R^*$, has trivial intersection with $U_2(R)$, implying that

$$\#(U_2(R) \cdot H) = (\#U_2(R)) \cdot (\#H) \leq \#GL_2(R)$$

and, consequently,

$$\#U_2(R) \leq \frac{\#GL_2(R)}{\#H} = \#SL_2(R) \leq q^{3m}. \tag{13}$$

For $q = 2$, we have $C_G(x) \cap C_G(y) = (1)$, so by Lemma 5.1

$$\#E(x, y) \leq \frac{(2^m)^3 \cdot (2^{3m})^2}{m} = \frac{2^{9m}}{m}. \tag{14}$$

Similarly, for $q = 3$

$$\#E(x, y) \leq \frac{3^{9m}}{8}. \tag{15}$$

On the other hand, the order of G is given by the formula

$$\#G = \gamma \cdot q^{m(m+1)}(q^2 - 1)(q^4 - 1)\cdots(q^{2m-2} - 1)(q^m - 1), \tag{16}$$

where $\gamma = 1$ for $q = 2$, and $\gamma = 1/2$ or $1/4$ for $q = 3$. Using (14), (15) and (16), it is easy to show that $\#E(x, y) < \#G$ for any $m \geq 5$. The case $m = 4$ is considered using Lemma 5.1 and elements of the following orders:

$$\begin{array}{lll} m = 4, & q = 2, & \mathrm{ord}(x) = 7, \\ m = 4, & q = 3, & \mathrm{ord}(x) = 13. \end{array}$$

Next, let $n = 2m + 1$ and $f(x_1, ..., x_{2m+1}) = x_1 x_{m+1} + ... + x_m x_{2m} + x_{2m+1}^2$. In view of the isomorphism $B_n(2) \simeq C_n(2)$, we need to consider here only the case $q = 3$. Take the following embedding $\varepsilon : GL_m(q) \to SO_n(f)$,

$$\varepsilon : a \mapsto \begin{pmatrix} a & 0 & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ 0 & ({}^t a)^{-1} & \\ 0 & \ldots\ 0 & 1 \end{pmatrix};$$

obviously, $G = P\Omega_n(f)$ coincides with $\Omega_n(f)$ and $\varepsilon^{-1}(\Omega_n) = SL_m(q)$. Let $x = \varepsilon(x_1)$, $y = \varepsilon(y_1)$. As usual, it follows from Lemma 5.5 that $C_G(x) = \varepsilon(T_1)$, and therefore has order $1/2 \cdot (3^m - 1)$. To estimate $C_G(z)$ for $z \in y\varepsilon(T_1)$, we let V be the 1-eigenspace for z. Obviously, V is invariant under $C_G(z)$, contains the last basic vector e_n and is of dimension ≤ 3. It follows that the subgroup D of $C_G(z)$ fixing e_n is of index at most $\#V = 3^3$, and from (13) we derive the estimation:

$$\#C_G(z) \leq 3^{3m+3}.$$

Then

$$\#E(x, y) \leq (\frac{1}{2} \cdot 3^m)^3 \cdot (3^{3m+3})^2 = \frac{3^{9m+6}}{8}.$$

Since

$$\#G = \frac{1}{2}3^{m^2} \cdot (3^2-1)(3^4-1)\cdots(3^{2m}-1),$$

we obtain that $\#E(x,y) < \#G$ for any $m \geq 5$. To consider the case $m=4$, notice that here $y_1^4 = -E_4$, in particular, y_1 does not have eigenvalue 1; therefore V is 1-dimensional and $[C_G(z) : D] \leq 3$. Using [Atlas] we see that the order of the centralizer of an element of order 4 in $P\Omega_8$ is $\leq 14 \cdot 10^3$ which implies that $\#C_G(z) \leq 6 \cdot 10^4$, and eventually that $\#E(x,y) < \#G$.

The case $m=3$, $q=3$ requires special consideration. It follows from [Atlas] that G has a single conjugacy class of elements of order 15; let x be one of them. Then $C = C_G(x)$ coincides with $\langle x \rangle$, and the quotient-group $N_G(\langle x \rangle)/\langle x \rangle$ is isomorphic to $(\mathbb{Z}/15\mathbb{Z})^* \simeq (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$. Let S be a Sylow 2-subgroup in $N_G(\langle x \rangle)$. Then S projects isomorphically onto $(\mathbb{Z}/15\mathbb{Z})^*$; let $y \in S$ be the element corresponding to the pair $(-1 \bmod (3), 2 \bmod (5))$. Obviously, $\mathrm{Int}(y)$ acts on $\langle x \rangle$ without fixed points, and therefore

$$E(x,y) = CC_G(y)CC_G(y)C.$$

Now, writing $C_G(y)$ as a union of cosets modulo S and using the fact that S normalizes C, we conclude that

$$\#E(x,y) \leq \frac{(\#C)^3 \cdot (\#G_G(y))^2}{8} \leq \frac{15^3 \cdot (2880)^2}{8} < 3.5 \cdot 10^9$$

while $\#G > 4.5 \cdot 10^9$.

Finally we consider the case: $n = 2m$, $m \geq 4$ and $f(x_1, ..., x_{2m}) = x_1 x_m + ... + x_{m-1}x_{2m-2} + g(x_{2m-1}, x_{2m})$ where g is an anisotropic binary form over $\mathbf{F}_q$. Consider the embedding $\varepsilon : GL_{m-1}(q) \to SO_n(f)$ given by the formula:

$$\varepsilon : a \to \begin{pmatrix} a & 0 & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ 0 & ({}^t a)^{-1} & \begin{matrix} \vdots \\ 0 \end{matrix} \\ 0 & \dots \quad 0 & E_2 \end{pmatrix}.$$

The commutator subgroup $\Omega_n(f)$ coincides with $SO_n(f)$ if $q=2$, and is a subgroup of index 2 if $q=3$; moreover, in the latter case $\varepsilon^{-1}(\Omega_n(f)) = SL_{m-1}(q)$. As before, let $\varphi : \tilde{G} = \Omega_n(f) \to P\Omega_n(f) = G$ be the natural homomorphism (note that $\mathrm{Ker}(\varphi) = 1$ if $q=2$), and let $\tilde{x} = \varepsilon(x_1)$, $\tilde{y} = \varepsilon(y_1)$, and $x = \varphi(\tilde{x})$, $y = \varphi(\tilde{y})$. As usual, it follows from Lemma 5.5 that $C_G(x) = \varphi(C)$, where $C = (\varepsilon(T_0) \times SO_2(g)) \cap \Omega_n(f)$. Taking into account that in the case $q=3$, $-E_n \in \Omega_n(f)$ if and only if m is odd, we see that the order of $C_G(x)$ is as follows:

$$\#C_G(x) = \begin{cases} 3(2^{m-1}-1); & q=2, \\ 2(3^{m-1}-1); & q=3 \text{ and } m \text{ even}, \\ 3^{m-1}-1; & q=3 \text{ and } m \text{ odd}. \end{cases} \tag{17}$$

The estimation of the order of $C_{\tilde{G}}(\tilde{z})$ for $\tilde{z} \in \tilde{y}C$ is based on the reduction to the case of split form in $2(m-1)$ variables. Namely, if $B \subset C_{\tilde{G}}(\tilde{z})$ is the subgroup fixing the last two basic vectors e_{n-1}, e_n , then we already know that $\#B \leq q^{3(m-1)}$, and it suffices to estimate the index $d = [C_{\tilde{G}}(\tilde{z}) : B]$. Let $\tilde{z} = \tilde{y}c$ where $c = \mathrm{diag}(a, b)$, $a = \varepsilon(t)$, $t \in T_0$ and $b \in SO_2(g)$.

Case 1: $b = \pm 1$. Let V be respectively $(+1)$ or (-1)-eigenspace for $\tilde{z}$. Then V is invariant under $C_{\tilde{G}}(\tilde{z})$ and has dimension 2 or 4. In the first case V coincides with $V_1 = \langle e_{n-1}, e_n \rangle$ implying that d is bounded by the order of the orthogonal group $O(V_1)$ which is 3 for $q = 2$ and 8 for $q = 3$. Now, assume that $\dim V = 4$, and let V_2 be the orthogonal complement of V_1 in V. Then there are two possibilities: either V_1 is non-degenerate of Witt index 1 (this happens if, respectively, $+1$ or -1 is a simple eigenvalue for $y_1 t$) or the restriction of f to V_2 is zero. Obviously,

$$d \leq \frac{\#O(V)}{\#O(V_2)},$$

and in the first case

$$\frac{\#O(V)}{\#O(V_2)} = \frac{q^2(q^4-1)}{q-1} = q^2(q^3+q^2+q+1),$$

this number being equal to 60 if $q = 2$, and 360 if $q = 3$, while in the second case

$$\frac{\#O(V)}{\#O(V_2)} = \frac{(\#GL_2(q)) \cdot q^4 \cdot (\#O(V_1))}{\#GL_2(q)} = q^4 \cdot (\#O(V_1))$$

which is 48 for $q = 2$ and 648 for $q = 3$.

Case 2: $b \neq \pm 1$. Then b has order 3 if $q = 2$, and order 4 if $q = 3$. If $y_1 t$ and b have no common eigenvalues, then $V_1 = \langle e_{n-1}, e_n \rangle$ is invariant under $C_{\tilde{G}}(\tilde{z})$ and $d \leq \#O(V_1)$. Now, let λ be a common eigenvalue for $y_1 t$ and b; λ belongs to $\mathbf{F}_{q^2}$, but not to $\mathbf{F}_q$. Obviously, the λ-eigenspace $V(\lambda)$ for $\tilde{z}$ in $\mathbf{F}_{q^2}^n$ is 3-dimensional and $C_{\tilde{G}}(\tilde{z})$-invariant. If v is the λ-eigenvector for b in V_1 and for $h \in C_{\tilde{G}}(\tilde{z})$ we have $h(v) = v$, then at the same time $h(\overline{v}) = \overline{v}$ where the bar denotes the nontrivial automorphism of $\mathbf{F}_{q^2}/\mathbf{F}_q$, and therefore h acts on V_1 identically, i.e. $h \in B$. This implies that

$$d \leq \#(V(\lambda) - \{0\})$$

which is 63 if $q = 2$, and is 728 if $q = 3$.

Putting the above information together, we obtain that

$$C_G(z) \leq \begin{cases} 63 \cdot 2^{3(m-1)}, & \text{if } q = 2, \\ 728 \cdot 3^{3(m-1)}, & \text{if } q = 3. \end{cases} \tag{18}$$

Using (17), (18) and the formula for the order of G:

$$\#G = \gamma \cdot q^{m(m-1)}(q^2-1)(q^4-1)\cdots(q^{2m-2}-1)(q^m+1)$$

where $\gamma = 1$ for $q = 2$ and $\gamma = 1/2$ or $1/4$ for $q = 3$, one easily shows that $\#E(x,y) < \#G$ for any $m \geq 6$.

The case $q = 3$, $m = 5$ requires slightly more precise estimations. First of all, observe that if in the above argument $b = \pm 1$, then necessarily $t \in T_1$ and therefore $(y_1 t)^4 = -1$. This implies that $y_1 t$ and b have no common eigenvalues and

$$\#C_{\tilde{G}}(\tilde{z}) \leq 8 \cdot 3^{12} < 4.3 \cdot 10^6.$$

On the contrary, if b has order 4, then $t \in T_0 \setminus T_1$, implying that $y_1 t$ is conjugate to the matrix $w = w(1)$ (notations as in Lemma 5.2). To estimate the order of the centralizer of $s = \mathrm{diag}(w,w)$ in $\Omega_8(g)$ where g has Witt index 4, write $\mathbf{F}_3^8$ as

$$\mathbf{F}_3^8 = V_+ \perp V_- \perp V_0,$$

where V_+ (resp. V_-) is $(+1)$ (resp. (-1)) eigenspace of s, and V_0 is the orthogonal complement of $V_+ \perp V_-$. Obviously, each of these spaces is invariant under $C_{\tilde{G}}(\tilde{z})$, and we obtain the estimation

$$\#C_{\tilde{G}}(\tilde{z}) \leq 728 \cdot \frac{1}{4}(\#O(V_+)) \cdot (\#O(V_-)) \cdot (\#O(V_0)) = 728 \cdot 4 \cdot 2 \cdot 24^2 < 4.3 \cdot 10^6.$$

Using the value $4.3 \cdot 10^6$ as the upper bound for the order of $C_{\tilde{G}}(\tilde{z})$, we obtain by direct computation that $\#E(x,y) < \#G$.

To consider the following cases, one applies Lemma 5.1 to the elements of the indicated order:

$$m = 4, \quad q = 2, \qquad \mathrm{ord}(x) = 7,$$
$$m = 5, \quad q = 2, \qquad \mathrm{ord}(x) = 17.$$

The case ${}^2D_4(3)$ requires special treatment. Here $G = P\Omega_8(f)$ where f is a quadratic form in 8 variables over $\mathbf{F}_3$ of Witt index 3. Obviously, in this case G is identifiable with $\tilde{G} = \Omega_8(f)$. Let F denote the matrix of f, and τ be the involution of $M_8(\mathbf{F}_3)$ given by the formula $\tau(a) = F^{-1}({}^t a)F$. Then $O_8(f)$ is defined by the equation $\tau(g)g = E_8$. The order computation shows that $\tilde{G} = \Omega_8(f)$ contains an element x of order 41. Then $L = \mathbf{F}_3[x]$, the subalgebra generated by x, is τ-invariant and is, in fact, a field extension of $\mathbf{F}_3$ of degree 8. One easily finds that $T = \{l \in L \mid \tau(l) \cdot l = 1\}$ has order 82, and therefore $T = \pm\langle x \rangle$ and $T \cap \Omega_8(f) = \langle x \rangle$. This allows to conclude that the centralizer $C = C_G(x)$ is $\langle x \rangle$.

Let $g \in GL_8(3)$ be the element such that $\mathrm{Int}(g)$ induces on L an automorphism of order 8. Since the restrictions of τ and $\mathrm{Int}(g)$ on L commute, we obtain that $g\tau(g) \in L^\tau$, and then for a suitable $l \in L^*$ we have $g\tau(g) = l\tau(l)$, and therefore $s = l^{-1}g$ satisfies $s\tau(s) = 1$. If we assume that $\det(s) = 1$, the characteristic polynomial of s would be $\lambda^8 + 1$, and therefore $-E_8 = s^8 \in \Omega_8(f)$ - a contradiction; hence $\det(s) = -1$, and the characteristic polynomial of s is $\lambda^2 - 1$, i.e. every 8-th root of unity is eigenvalue of s with multiplicity 1. Let y be the one of the elements s^2 or $-s^2$ which belongs to $\Omega_8(f)$. Then $\mathrm{Int}(y)$ induces on L an automorphism of order 4,

$$E(x,y) = CC_G(y)CC_G(y)C,$$

and

$$\#E(x,y) \le \frac{(\#C)^3 \cdot (\#C_G(y))^2}{4}.$$

To estimate $\#C_G(y)$, observe that y has the following eigenvalues: 1, -1, i, $-i$, (where $i^2 = -1$), each with multiplicity 2. We have the following decomposition:

$$\mathbf{F}_3^8 = V_+ \perp V_- \perp V_0$$

where V_+ and V_- are $(+1)$ and (-1)-eigenspaces for y, and V_0 is the orthogonal complement of $V_+ \perp V_-$. Each of these spaces is invariant under y, and the restriction of y to V_0 is not scalar. It follows that

$$\#C_G(y) < (O(V_+) \times O(V_-) \times H) \cap \Omega_8(f)$$

where H is *a proper* subgroup of $O(V_0)$, and therefore

$$\#C_G(y) \le \frac{8 \cdot 8 \cdot 720}{4} = 11,520.$$

Thus,

$$\#E(x,y) \le 2 \cdot 29 \cdot 10^{12}$$

while $\#G > 10^{13}$.

The group $^3D_4(2)$. It follows from [Atlas] that the group G of this type has a single conjugacy class of elements of order 7 having the centralizer of order 49; let x be one of them, and $C = C_G(x)$. Then $N_G(\langle x \rangle)/C$ is the cyclic group of order 6, and therefore there exists an element $y \in N_G(\langle x \rangle)$ of order 6. Again using [Atlas] we see that the order of $C_G(y)$ can be either 72 or 24. Since neither of these numbers is divisible by 7, we conclude that the action of $\mathrm{Int}(y)$ on C is fixed-point free implying the fact

$$E(x,y) = CC(y)CC(y)C.$$

Therefore

$$\#E(x,y) \le \frac{49^2 \cdot 72^2}{6} < 1.20 \cdot 10^8$$

which is less than $\#G$ $(> 2.1 \cdot 10^8)$.

The groups $^2E_6(4)$, $F_4(2)$ *and* $G_2(3)$ are considered by applying Lemma 5.1 to the elements of the following orders:

$$\begin{array}{ll} {}^2E_6 & \mathrm{ord}(x) = 13, \\ F_4(2) & \mathrm{ord}(x) = 13, \\ G_2(3) & \mathrm{ord}(x) = 7. \end{array}$$

Tits group $^2F_4(2)'$ is considered using Lemma 5.1, if one takes for x an element of order 13.

For consideration of the remaining types we need the following proposition.

Table 5:

r	$\#D(k)$
1	$< q^3$
2	$< 2 \cdot q^{11}$
3	$< 2 \cdot q^{21}$
4	$< q^{36}$
5	$< q^{55}$

Proposition 5.6 *1) Let* $\mathbf{D}$ *be a semisimple group of rank* r *over the field* $k = \mathbf{F}_q$. *Assume that* $\mathbf{D}$ *does not contain any factors of type* G_2. *Then for* $r \leq 5$ *we have the estimations for the order of* $\mathbf{D}(k)$ *given in Table 5.*

2) $\#E_7(q) > \frac{1}{2^8} \cdot q^{133}$ *and* $\#E_8(q) < \frac{1}{2^8} \cdot q^{248}$. *Besides,* $\#E_6(2) > 2 \cdot 10^{23}$ *and* $\#F_4(3) > 5 \cdot 10^{24}$.

Proof. The proof easily follows from the formulas for the order of finite Chevalley groups (*cf.* [St]). ∎

The group $E_6(2)$. Let $\mathbf{G}_1$ (resp.$\mathbf{G}_2$) be the subgroup of the simple simply connected group $\mathbf{G}$ of type E_6 over $k = \mathbf{F}_2$ generated by the root subgroups $\mathbf{G}_\alpha$ for $\alpha \in \{\alpha_1, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$ (resp. for $\alpha = \tilde{\alpha}$), simple roots being labeled as in the previous section. Then $\mathbf{G}_1 = \mathbf{SL}_6$, $\mathbf{G}_2 = \mathbf{SL}_2$, and besides, $\mathbf{G}_1$ and $\mathbf{G}_2$ commute. Let $\mathbf{T}_1$ be the following subtorus in $\mathbf{G}_1$:

$$\mathbf{T}_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \in \mathbf{R}^{(1)}_{l/k}(\mathbb{G}_m) \right\}$$

where l/k is the extension of degree five, and $\mathbf{T} = (\mathbf{R}_{l/k}(\mathbb{G}_m) \times \mathbb{G}_m) \cap \mathbf{SL}_6$ be the maximal torus of $\mathbf{SL}_6$ which contains $\mathbf{T}_1$. A simple computation with roots shows that $C_{\mathbf{G}}(\mathbf{T}_1) = \mathbf{T} \times \mathbf{G}_2$. (Indeed, $\mathbf{T}_1$ is conjugate in $\mathbf{G}_1$ to the subgroup generated by h_α, $\alpha \in \{\alpha_3, \alpha_4, \alpha_5, \alpha_6\}$, and one easily checks that the roots orthogonal to these α_i's are $\pm\tilde{\alpha}$.) Now, let x_1 be a generator of $\mathbf{T}_1(k)$; $\mathrm{ord}(x_1) = 31$. We claim that again $C_{\mathbf{G}}(x_1) = \mathbf{T} \cdot \mathbf{G}_2$. Assume the contrary. Since $\mathbf{T} = \mathbf{T}_1 \cdot \mathbb{G}_m$ and $\mathbf{T}_1$ does not have any proper k-defined subtori, the maximal central subtorus in $C_{\mathbf{G}}(x_1)$ would reduce to $\mathbb{G}_m$. But the group of the form $\mathbb{G}_m \cdot \mathbf{Z}$ where $\mathbf{Z}$ is center of some semisimple group of rank ≤ 5 cannot contain an element of order 31. Let $x = x_1 x_2$ where x_2 is some non-trivial unipotent element in $\mathbf{G}_2(k)$. Then the above argument shows that $C_G(x) = \mathbf{T}(k) \times \langle x_2 \rangle$, and therefore has order 62.

Next, let $y = \mathrm{diag}(y_0, 1) \in \mathbf{G}_1$ where $y_0 \in \mathbf{SL}_5(k)$ is such that $\mathrm{Int}(y_0)$ induces on l an automorphism of order 5, and let $z \in yC_G(x)$. Then $z = ytx_2^\varepsilon$ ($\varepsilon = 0$ or 1), and $C_{\mathbf{G}}(z) \subset C_{\mathbf{G}}(yt)$, so in estimating the order of $C_G(z)$ we may assume that $z = yt$ is an element of order 5 in $\mathbf{G}_1$. Obviously, z is contained in a k-defined subtorus $\mathbf{S} \subset \mathbf{G}_1$ of the form $\mathbf{R}_{m/k}(\mathbb{G}_m)$ where m is the extension of degree 4, and the maximal central torus in $C_{\mathbf{G}}(\mathbf{S}_1)$ is $\mathbf{S} = \mathbf{R}_{m/k}(\mathbb{G}_m)$. Suppose $C_{\mathbf{G}}(z)$ is different from $C_{\mathbf{G}}(\mathbf{S}_1) = C_{\mathbf{G}}(\mathbf{S})$. Then z is a k-element in a group of the form $\mathbf{S}' \cdot \mathbf{Z}$ where $\mathbf{S}' \subset \mathbf{S}$ is a proper k-subtorus different from $\mathbf{S}_1$ and $\mathbf{Z}$ is the center of a certain group of rank ≤ 5. Since $\mathbf{Z}(k)$ does not contain elements of order 5, we conclude that $\mathbf{S}'$ must contain such an element, implying that $\mathbf{S}' \supset \mathbf{S}_1$ - a contradiction.

It follows that $C_{\mathbf{G}}(z) = \mathbf{S} \cdot \mathbf{D}$ where $\mathbf{D}$ is some semisimple group of rank ≤ 2. Using Table 5, we conclude that

$$\# C_G(z) \leq 5 \cdot 2^{12}.$$

Therefore

$$\# E(x, y) \leq 62^3 \cdot 5^2 \cdot 2^{24} < 5 \cdot 10^9$$

while $\# G > 2 \cdot 10^{23}$.

The group $E_7(2)$. Let $\mathbf{G}_1$ be the subgroup of the group $\mathbf{G}$ of type E_7 over $k = \mathbf{F}_2$ generated by $\mathbf{G}_\alpha$ for $\alpha \in \{\tilde{\alpha}, \alpha_1, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7\}$; $\mathbf{G}_1 \simeq \mathbf{SL}_8$. Let $\mathbf{T} \subset \mathbf{G}_1$ be the maximal torus of the form:

$$\mathbf{T} = (\mathbf{R}_{l_1/k}(\mathbb{G}_m) \times \mathbf{R}_{l_2/k}(\mathbb{G}_m)) \cap \mathbf{SL}_8$$

where l_1 and l_2 are extensions of degree 5 and 3, respectively. Put $\mathbf{T}_i = \mathbf{R}^{(1)}_{l_i/k}(\mathbb{G}_m)$ $(i = 1, 2)$ and $\mathbf{T}_3 = \mathbf{T}_1 \times \mathbf{T}_2$. A simple computation with roots shows that $C_{\mathbf{G}}(\mathbf{T}_3) = \mathbf{T}$. Picking generators $x_i \in \mathbf{T}_i(k)$ for $i = 1, 2$, we let $x = x_1 x_2$ (note that x_1 and x_2 have orders 31 and 7, respectively, so the order of x is 217). We claim that $C_{\mathbf{G}}(x) = \mathbf{T}$. Indeed, if $C_{\mathbf{G}}(x) = \mathbf{T}' \cdot \mathbf{D}$ where $\mathbf{T}'$ is the central torus, $\mathbf{D}$ is semisimple, then $x \in \mathbf{T}' \cdot Z(\mathbf{D})$. Obviously, it is impossible that $\dim \mathbf{T}' = 1$. However, if $\dim \mathbf{T}' > 1$ then $\dim \mathbf{T}_3 \cap \mathbf{T}' \geq 1$, and since $\mathbf{T}_3$ does not have any k-defined subtori except for $\mathbf{T}_1$ and $\mathbf{T}_2$, we conclude that $\mathbf{T}'$ contains at least one of them. On the other hand, $\mathbf{T}'(k)$ contains an element of order 217. Suppose, for example, that $\mathbf{T}_1 \not\subset \mathbf{T}'$. We have: $\mathbf{T} = \mathbf{T}_1 \times \mathbf{T}_2 \times \mathbb{G}_m$, and therefore $\mathbf{T}/(\mathbf{T}_1 \times \mathbb{G}_m) = \mathbf{T}_2$. Comparing the orders, we see that $\mathbf{T}' \not\subset \mathbf{T}_1 \times \mathbb{G}_m$, therefore $\mathbf{T}'$ projects surjectively onto $\mathbf{T}_2$. But this immediately implies that $\mathbf{T}' \supset \mathbf{T}_3$, so $C_{\mathbf{G}}(x) = \mathbf{T}$, and $\# C_G(x) = 217$.

Next, let $y_1 \in \mathbf{SL}_5(k)$ and $y_2 \in \mathbf{SL}_3(k)$ be the elements inducing on l_1 and l_2 the automorphisms of orders 5 and 3, respectively; let $y = y_1 y_2 \in \mathbf{G}_1(k)$. Clearly, any $z \in y\mathbf{T}(k)$ has order 15.

Lemma 5.7 $\# C_G(z) \leq 45 \cdot 2^{36}$.

Proof. Obviously, z is contained in a maximal k-torus $\mathbf{S} \subset \mathbf{G}_1$ of the form $\mathbf{S} = ((\mathbb{G}_m)^2 \times \mathbf{R}_{m_1/k}(\mathbb{G}_m) \times \mathbf{R}_{m_2/k}(\mathbb{G}_m)) \cap \mathbf{SL}_8$ where m_1 and m_2 are extensions of degrees 4 and 2, respectively. Let $C_{\mathbf{G}}(z) = \mathbf{S}' \cdot \mathbf{D}$. We claim that rank$\mathbf{D} \leq 4$. Indeed, $z = (y_1 t_1)(y_2 t_2)$ where $t_i \in \mathbf{T}_i(k)$ and $\mathbf{C}_{\mathbf{G}}(z) = \mathbf{C}_{\mathbf{G}}(y_1 t_1) \cap \mathbf{C}_{\mathbf{G}}(y_2 t_2)$. Since there is a unipotent element in $C_{\mathbf{G}}(y_1 t_1)$ which does not commute with $y_2 t_2$, the semisimple rank of $C_{\mathbf{G}}(z)$ cannot exceed that of $C_{\mathbf{G}}(y_1 t_1)$ minus one. So, it remains to be shown that for $z_1 = y_1 t_1$ the semisimple rank is ≤ 5. Assume that $C_{\mathbf{G}}(z_1) = \mathbf{S}'_1 \cdot \mathbf{D}_1$ and $\mathrm{rank}\mathbf{D}_1 = 6$, i.e. $\dim \mathbf{S}'_1 = 1$. But $z_1 \in \mathbf{S}'_1 \cdot Z(\mathbf{D}_1)$ and since $\#\mathbf{S}'_1(k) \leq 3$ and no k-defined quotient of $Z(\mathbf{D}_1)$ can contain elements of order 5, we obtain a contradiction. So, using Table 5, we get

$$\#C_G(z) = (\#\mathbf{S}'(k))(\#\mathbf{D}(k)) \leq 45 \cdot 2^{36},$$

as required. ∎

Now, we obtain that

$$\#E(x,y) \leq (217)^3 \cdot (45 \cdot 2^{36})^2 \leq 2.1 \cdot 10^{10} \cdot 2^{72},$$

on the other hand, $\#G > 2^{125}$, and one easily checks that $\#E(x,y) < \#G$.

The group $E_7(3)$. We will use the same subgroup $\mathbf{G}_1 \subset \mathbf{S}$ as in the previous case and let

$$\mathbf{T} = (\mathbf{R}_{l_1/k}(\mathbb{G}_m) \times \mathbf{R}_{l_2/k}(\mathbb{G}_m)) \cap \mathbf{SL}_8$$

where l_1 and l_2 are extensions of degrees 5 and 2, respectively. Let $\mathbf{T}_i = \mathbf{R}^{(1)}_{l_i/k}(\mathbb{G}_m)$, $(i = 1,2)$ and $\mathbf{T}_3 = \mathbf{T}_1 \times \mathbf{T}_2$. Again, a simple computation shows that $C_{\mathbf{G}}(\mathbf{T}_3) = \mathbf{T}$. Picking arbitrary generators $x_i \in \mathbf{T}_i(k)$, let $x_0 = x_1 x_2$; the order of x_0 is 484. We claim that $C_{\mathbf{G}}(x_0) = \mathbf{T}$. Indeed, if $C_{\mathbf{G}}(x) = \mathbf{T}' \cdot \mathbf{D}$ then $x \in \mathbf{T}' \cdot Z(\mathbf{D})$, and $\mathbf{T}'$ must contain an element of order 121. Comparing the orders, we see that the projection of $\mathbf{T}'$ on $\mathbf{R}_{l_1/k}(\mathbb{G}_m)$ must contain $\mathbf{T}_1$; in particular, $\dim \mathbf{T}' \geq 4$. It follows that $\dim(\mathbf{T}' \cap \mathbf{T}_3) \geq 2$, and since $\mathbf{T}_3$ does not have any k-defined subtorus other than $\mathbf{T}_1$ and $\mathbf{T}_2$, we get $\mathbf{T}' \supset \mathbf{T}_1$. Now, the centralizer $C_{\mathbf{G}}(\mathbf{T}_1)$ has semisimple rank ≤ 3, and on the other hand, contains a unipotent element which does not commute with x_2. It follows, that $\mathrm{rank}\mathbf{D} \leq 2$. However, then the exponent of the 2-component of $Z(\mathbf{D})$ is at most 2, and therefore $\mathbf{T}'$ contains an element of order $4 \cdot 121$. Now, the image of the projection of $\mathbf{T}'$ on $\mathbf{R}_{l_2/k}(\mathbb{G}_m)$ has to contain $\mathbf{T}_2$ and eventually $\mathbf{T}' = \mathbf{T}_3$, i.e. $C_{\mathbf{G}}(x_0) = \mathbf{T}$. Let x'_2 be a generator of l_2^*; put $\tilde{x} = \mathrm{diag}(x_1, x'_2, -1)$. Then the above argument shows that $C_{\mathbf{G}}(\tilde{x}^2) = \mathbf{T}$ implying that if $\varphi : \tilde{G} = \mathbf{G}(k) \to G$ is the canonical projection then for $x = \varphi(\tilde{x})$ we have $C_G(x) = \varphi(\mathbf{T}(k))$, and therefore $\#C_G(x) = 968$.

Now, let $y_1 \in \mathbf{SL}_5(k)$ and $y_2 \in \mathbf{SL}_2(k)$ be the elements which induce on l_1 and l_2 the automorphisms of orders 5 and 2, respectively. Put $\tilde{y} = \mathrm{diag}(y_1, y_2, 1)$ and $y = \varphi(\tilde{y})$.

Lemma 5.8 *For any $z \in yC_G(x)$, $\#C_G(z) \leq 1280 \cdot 3^{36}$.*

Proof. If suffices to estimate the order of $C_{\tilde{G}}(\tilde{z})$ where

$$\tilde{z} = \tilde{y}t, \quad t = \mathrm{diag}(t_1, t_2, t_3) \in \mathbf{T}(k).$$

First of all, we are going to show that the semisimple rank of $C_{\mathbf{G}}(\tilde{z})$ is ≤ 4. Write t_1 in the form $t_1 = \varepsilon t'_1$ where $t'_1 \in \mathbf{R}^{(1)}_{l_1/k}(\mathbb{G}_m)$, $\varepsilon = \pm 1$, and let $t'_2 = \mathrm{diag}(\varepsilon, t_2, t_3)$. Then $\tilde{z} = z_1 z_2$ where $z_i = y_i t_i$ and

$$C_{\mathbf{G}}(\tilde{z}) = C_{\mathbf{G}}(z_1) \cap C_{\mathbf{G}}(z_2).$$

Obviously, $C_{\mathbf{G}}(z_1)$ contains a unipotent element which does not commute with z_2, therefore it suffices to show that the semisimple rank of $C_{\mathbf{G}}(z_1)$ is ≤ 5. Write $C_{\mathbf{G}}(z_1) = \mathbf{S}' \cdot \mathbf{D}$; then $z_1 \in \mathbf{S}' \cdot Z(\mathbf{D})$. If we assume that rank$\mathbf{D} = 6$, then dim $\mathbf{S}' = 1$. However, this is impossible since $\#\mathbf{S}'(k) \leq 4$ and none of k-defined quotients of $Z(\mathbf{D})$ can contain a k-element of order 5. Obviously, $\mathbf{S}'$ is a subtorus in a maximal k-torus $\mathbf{S} \subset \mathbf{G}_1$ of the form $(\mathbb{G}_m \times \mathbf{R}_{m_1/k}(\mathbb{G}_m) \times \mathbf{B} \times \mathbb{G}_m) \cap \mathbf{SL}_8$ where m_1 is the extension of degree 4, and $\mathbf{B}$ is either $(\mathbb{G}_m)^2$ or $\mathbf{R}_{m_2/k}(\mathbb{G}_m)$, $[m_2 : k] = 2$. In either case

$$\#C_{\tilde{G}}(\tilde{z}) = (\#\mathbf{S}'(k)) \cdot (\#\mathbf{D}(k)) \leq (\#\mathbf{S}(k)) \cdot (\#\mathbf{D}(k)) \leq 1280 \cdot 3^{36}.$$

The lemma is proved. ■

Now,

$$\#E(x,y) \leq (968)^3 \cdot (1280 \cdot 3^{36})^2 < 2 \cdot 10^{15} \cdot 3^{72}.$$

On the other hand, $\#G > (1/2^8) \cdot 3^{133}$, and one can easily see that $\#E(x,y) < \#G$.

The group $E_8(2)$. Let $\mathbf{G}_1 \subset \mathbf{G}$ be the subgroup generated by the root subgroups $\mathbf{G}_\alpha$ for $\alpha \in \{\alpha_1, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8, \tilde{\alpha}\}$; $\mathbf{G}_1 = \mathbf{SL}_9$. Let $\mathbf{T} = \mathbf{R}^{(1)}_{l/k}(\mathbb{G}_m)$ be the maximal torus in $\mathbf{G}_1$ corresponding to the extension l of $k = \mathbf{F}_2$ of degree 9, and $x \in \mathbf{T}(k)$ be a generator (ord$(x) = 7 \cdot 73 = 511$). We claim that x is a regular element. Assume the contrary. Then $x \in \mathbf{T}' \cdot \mathbf{Z}$ where $\mathbf{T}' \subset \mathbf{T}$ is a proper subtorus and $\mathbf{Z}$ is the center of some semisimple group of rank ≤ 7. It follows that $\mathbf{T}'(k)$ contains an element of order 73 which immediately implies that $\mathbf{T}' = \mathbf{T}$, a contradiction. Now, let $y \in \mathbf{G}_1(k)$ be an element such that Int(y) induces on l an automorphism of order 9.

Lemma 5.9 *For any* $z \in y\mathbf{T}(k)$, *we have* $\#C_G(z) \leq 2^{23} \cdot 10^2$.

Proof. Obviously, z has order 9 and therefore is contained in a maximal torus $\mathbf{S} \subset \mathbf{G}_1$ of the form $(\mathbf{R}_{m_1/k}(\mathbb{G}_m) \times \mathbf{R}_{m_2/k}(\mathbb{G}_m) \times \mathbf{R}_{m_3/k}(\mathbb{G}_m)) \cap \mathbf{SL}_9$ where m_1, m_2, m_3 are extensions of degrees 6, 2 and 1 respectively. Let $\mathbf{R} = C_{\mathbf{G}}(z)$ and write $\mathbf{R}$ as $\mathbf{R} = \mathbf{S}' \cdot \mathbf{D}$, almost direct product of the central torus $\mathbf{S}'$ and a semisimple group $\mathbf{D}$. Then $z \in \mathbf{S}' \cdot Z(\mathbf{D})$. We claim that the three component $\mathbf{Z}_3$ of the center of any semisimple group of rank ≤ 7 has the following property: for any k-defined subgroup $\mathbf{Z}'_3 \subset \mathbf{Z}_3$ the map $\pi(k) : \mathbf{Z}'_3(k) \to (\mathbf{Z}_3/\mathbf{Z}'_3)(k)$ is surjective.

First of all, notice that it suffices to prove that

$$\pi(f) : \mathbf{Z}_3(f) \to (\mathbf{Z}_3/\mathbf{Z}'_3)(f)$$

where $[f : k] = 3$ is surjective. Indeed, then for $t \in (\mathbf{Z}_3/\mathbf{Z}'_3)(k)$ the fiber $\pi(f)^{-1}(f)$ is non-empty and Gal(f/k) invariant, hence contain a Gal(f/k) stable point, since Gal(f/k) has order 3. But $\mathbf{Z}_3$ is f-isomorphic to direct product of factors isomorphic to μ_3, the group of the 3^{rd} roots of unity, or $\mu_3^{(1)} = \mathbf{R}^{(1)}_{m/k}(\mu_3)$, $[m : k] = 2$, and our assertion can be easily checked.

Applying this fact to the morphism $Z(\mathbf{D}) \to Z(\mathbf{D})/Z(\mathbf{D}) \cap \mathbf{S}'$ we obtain that $\mathbf{S}'(k)$ contains an element of order 9, and therefore $\dim \mathbf{S}' \geq 5$, i.e. the rank of $\mathbf{D}$ is ≤ 3. It follows from Table 5 that $\#\mathbf{D}(k) \leq 2^{22}$. On the other hand, $\#\mathbf{S}'(k) \leq \#\mathbf{S}(k) = 189$, hence our estimation. ■

Now,

$$\#E(x,y) \leq (511)^3 \cdot (2^{23} \cdot 10^2)^2 < 2 \cdot 10^{27},$$

while $\#G > 3 \cdot 10^{74}$.

The group $E_8(3)$. Let $\mathbf{G}_1 \subset \mathbf{S}$ be the same as in the previous case, and let $\mathbf{T} \subset \mathbf{G}_1$ be a maximal k-torus of the form

$$\mathbf{T} = (\mathbf{R}_{l_1/k}(\mathbb{G}_m) \times \mathbf{R}_{l_2/k}(\mathbb{G}_m)) \cap \mathbf{SL}_9$$

where l_1 and l_2 are extensions of degrees 7 and 2, respectively. Put $\mathbf{T}_i = \mathbf{R}^{(1)}_{l_i/k}(\mathbb{G}_m)$ $(i = 1, 2)$ and $\mathbf{T}_3 = \mathbf{T}_1 \times \mathbf{T}_2$. A simple computation shows that $C_{\mathbf{G}}(\mathbf{T}_3) = \mathbf{T}$. Pick generators $x_i \in \mathbf{T}_i(k)$ $(i = 1, 2)$, (these have orders 1093 (a prime) and 4 respectively), and let $x = x_1x_2$. We claim that $C_{\mathbf{G}}(x) = \mathbf{T}$. Indeed, let $C_{\mathbf{G}}(x) = \mathbf{T}' \cdot \mathbf{D}$; then $x \in \mathbf{T}' \cdot Z(\mathbf{D})$. This implies that $\mathbf{T}'(k)$ contains an element of order 1093. Then the projection of $\mathbf{T}'$ on $\mathbf{R}_{l_1/k}(\mathbb{G}_m)$ must contain $\mathbf{T}_1$. It follows that the semisimple rank of $C_{\mathbf{G}}(x_1)$ is ≤ 2. On the other hand, $C_{\mathbf{G}}(x_1)$ contains a unipotent element which does not commute with x_2, implying that $\mathrm{rank}\mathbf{D} \leq 1$. Then the projection of $\mathbf{T}'$ on $\mathbf{R}_{l_2/k}(\mathbb{G}_m)$ must contain $\mathbf{T}_2$, and eventually, $\mathbf{T}' \supset \mathbf{T}_3$, i.e. $C_{\mathbf{G}}(x) = \mathbf{T}$ and $\#C_G(x) = 8744$.

Next, let $y_1 \in \mathbf{SL}_7(k)$, $y_2 \in \mathbf{SL}_2(k)$ be the elements which induce on l_1 and l_2 the automorphisms of orders 7 and 2 respectively, and $y = \mathrm{diag}(y_1, y_2)$.

Lemma 5.10 *For any* $z \in yC_G(x)$, $\#C_G(z) \leq 2912 \cdot 3^{55}$.

Proof. Let $z = yt$, $t = \mathrm{diag}(t_1, t_2)$. Write t_1 as $t_1 = \varepsilon t_1'$ where $t_1' \in \mathbf{T}_1$, $\varepsilon = \pm 1$, and put $t_2' = \mathrm{diag}(\varepsilon, t_2)$. Then $z = z_1 z_2$ where $z_i = y_i t_i$, and

$$C_{\mathbf{G}}(z) = C_{\mathbf{G}}(z_1) \cap C_{\mathbf{G}}(z_2).$$

We claim that the semisimple rank of $C_{\mathbf{G}}(z)$ is ≤ 5. Since $C_{\mathbf{G}}(z_1)$ obviously contains an unipotent element which does not commute with z_2, it suffices to show that the semisimple rank of $C_{\mathbf{G}}(z_1)$ is ≤ 6. Assume that the latter is 7. Then $z_1 \in \mathbf{S}' \cdot \mathbf{Z}$ where $\mathbf{S}'$ is a one-dimensional torus and $\mathbf{Z}$ is the center of a semisimple group of rank 6. However, since $\#\mathbf{S}'(k) \leq 4$ and none of possible k-defined factors of $\mathbf{Z}$ contains a k-element of order 7, this is impossible. Thus, $C_{\mathbf{G}}(z) = \mathbf{S}'' \cdot \mathbf{D}$ where $\mathrm{rank}\mathbf{D} \leq 5$. Clearly, z is contained in a maximal k-torus $\mathbf{S} \subset \mathbf{G}_1$ of the form $\mathbf{S} = (\mathbb{G}_m \times \mathbf{R}_{m_1/k}(\mathbb{G}_m) \times \mathbf{B}) \cap \mathbf{SL}_9$ where $\mathbf{B}$ is either $(\mathbb{G}_m)^2$ or $\mathbf{R}_{m_2/k}(\mathbb{G}_m)$, $[m_2 : k] = 2$. Then

$$\#C_G(z) = (\#\mathbf{S}''(k)) \cdot (\#\mathbf{D}(k)) \leq (\#\mathbf{S}(k)) \cdot (\#\mathbf{D}(k)) \leq 2912 \cdot 3^{55}.$$

The lemma is proved. ■

It follows that

$$\#E(x,y) \leq (8744)^3 \cdot (2912 \cdot 3^{55})^2 < 10^{19} \cdot 3^{110}.$$

On the other hand, $\#G > (1/2^8) \cdot 3^{248}$, and $\#E(x,y) < \#G$.

The group $F_4(3)$. Let $\mathbf{G}_1$ (resp. $\mathbf{G}_2$) be the subgroup in $\mathbf{G}$ of type F_4 over $k = \mathbf{F}_3$ generated by the root subgroups $\mathbf{G}_\alpha$ for $\alpha \in \{\tilde{\alpha}, \alpha_1, \alpha_2\}$ where $\tilde{\alpha}$ is the highest root (resp. for $\alpha = \alpha_4$). Then $\mathbf{G}_1 \simeq \mathbf{SL}_4$, $\mathbf{G}_2 \simeq \mathbf{SL}_2$ and $\mathbf{G}_1$ and $\mathbf{G}_2$ commute. Let $\mathbf{T}_1 = \mathbf{R}^{(1)}_{l/k}(\mathbb{G}_m)$ be the maximal torus in $\mathbf{G}_1$ corresponding to the extension l/k of degree 4. Obviously, $\mathbf{T}_1$ is the maximal central torus in its centralizer $C_{\mathbf{G}}(\mathbf{T}_1)$. Let x_1 be a generator of $\mathbf{T}_1(k)$; x_1 has order 40. We claim that $C_{\mathbf{G}}(x_1) = C_{\mathbf{G}}(\mathbf{T}_1)$. Indeed, otherwise x_1 would be a k-element in a group of the form $\mathbf{T}' \cdot \mathbf{Z}$ where $\mathbf{T}' \subset \mathbf{T}$ is a k-subtorus of co-dimension $r \geq 1$ and $\mathbf{Z}$ is the center of a certain semisimple group of rank $\leq r+1$. If $r = 1$ then $\mathbf{Z}$ has exponent 2 or 3 implying that $\mathbf{T}'$ should contain an element of order at least 20, which is impossible. If $r = 2$ then $\#\mathbf{T}'(k) = 4$ and $\#\mathbf{Z} \leq 8$, and again x_1 cannot belong to $(\mathbf{T}' \cdot \mathbf{Z})(k)$. Now, let x_2 be a non-trivial unipotent element in $\mathbf{G}_2(k)$, and $x = x_1 x_2$. Then the above argument shows that $C_G(x) = \mathbf{T}_1(k) \times \langle x_2 \rangle$; therefore $\#C_G(x) = 120$. Next, let $y \in \mathbf{G}_1(k) = SL_4(3)$ be the element which induces on l an automorphism of order 4. The characteristic polynomial of y is $\lambda^4 + 1$, i.e. y has order 8.

Lemma 5.11 *For any $z \in yC_G(x)$, we have: $\#C_G(z) \leq 8 \cdot 3^{14}$.*

Proof. We have $z = ytx^{\varepsilon}$ where $t \in \mathbf{T}_1(k)$, $\varepsilon = 0$, 1 or 2. Since $C_G(z) \subset C_G(yt)$, in estimating the order of $C_G(z)$ we may assume that $z = yt \in \mathbf{G}_1$. Obviously z also has order 8. Since $\mathbf{G}$ is simply connected, $\mathbf{R} = C_{\mathbf{G}}(z)$ is connected, and therefore $\mathbf{R} = \mathbf{S}_1\mathbf{D}$, almost direct product of the maximal central torus $\mathbf{S}_1$ and a semisimple group $\mathbf{D}$. First, we show that $\mathbf{D}$ cannot belong to either of types A_3, B_3 or C_3. Indeed, if $\mathbf{D}$ were of type B_3 or C_3, the center of $\mathbf{D}$ would not be bigger than $\{\pm 1\}$, and $\dim \mathbf{S}_1 = 1$. Then either $\mathbf{S}_1$ or $\mathbf{S}_1 \times \{\pm 1\}$ would contain an element of order 8, which is impossible. To show that $\mathbf{D}$ cannot be of type A_3, notice that the semi-simple part of the centralizer of z^2 in $\mathbf{G}_1$ is of type $(A_1)^2$, implying that $C_{\mathbf{G}}(z^2)$ should contain $(A_1)^3$. So, if $\mathbf{D}$ were of type A_3, there would be an embedding $(A_1)^3 \hookrightarrow A_3$ which is impossible. As follows from Table 5, in all other cases of rank three groups $\#D(k) \leq 2 \cdot 3^{14}$ and since $\#\mathbf{S}_1(k) \leq 4$, we obtain our estimation. If D is of rank ≤ 2 then $\#D(k) \leq 2 \cdot 3^{11}$, and since $\#\mathbf{S}_1(k) \leq 40$, we again have our estimation. The lemma is proved. ■

Using our estimations, we get

$$\#E(x,y) \leq (120)^3 \cdot (8 \cdot 3^{14})^2 < 3 \cdot 10^{21}$$

while $\#G > 5 \cdot 10^{24}$.

Table 6:

G	ord(x)	ord(y)	m	$f(x,y)$	$\#G$
M_{11}	5	4	8	2,000	7,920
M_{12}	11	5	10	26,620	95,040
M_{22}	11	5	5	33,275	443,520
M_{23}	11	5	15	299,475	10,200,960
M_{24}	11	10	20	532,400	244,823,040
J_1	7	6	6	12,348	175,560
J_2	7	6	24	197,568	604,800
J_3	17	8	8	314,432	50,232,960
J_4	23	22	264	847,991,232	$> 8.6 \cdot 10^{19}$
·1	23	11	66	52,999,452	$> 4,1 \cdot 10^{18}$
·2	23	11	11	1,472,207	$> 4.2 \cdot 10^{13}$
·3	23	11	22	5,888,828	495,766,656,000
Hs	7	6	36	444,528	44,352,000
Mc	11	5	750	748,687,500	898,128,000
Sz	11	5	40	26,240,827,392	448,345,497,600
He	17	8	16	1,257,728	4,030,387,200
Ly	37	18	18	16,411,572	$> 5.1 \cdot 10^{16}$
Ru	29	14	28	19,120,976	145,926,144,000
$O'N$	11	10	20	532,400	460,815,505,920
Fi_{22}	13	6	155520	$< 5.4 \cdot 10^{13}$	$> 6.4 \cdot 10^{13}$
Fi_{23}	17	16	32	5,030,912	$> 4.0 \cdot 10^{18}$
Fi_{24}	17	16	32	5,030,912	$> 1.2 \cdot 10^{24}$
F_5	19	9	27	5,000,211	$> 2.7 \cdot 10^{14}$
F_3	19	18	72	35,557,056	$> 9 \cdot 10^{16}$
F_2	31	15	3600	386,091,360,000	$> 4.1 \cdot 10^{33}$
F_1	41	40	400	11,027,360,000	$> 8 \cdot 10^{53}$

6. Proof of Theorem 3.5 for sporadic groups.

All the sporadic groups are considered with the help of Lemma 5.1 and information from [Atlas]. The results of computations are arranged in Table 6, which for every sporadic group G contains: the orders of x and y, the maximum of orders of centralizers of elements of the order equal to that of y (denoted as y), the corresponding value of the function $f(x, y)$ which is the upper bound for the number of elements in $E(x, y)$ (*cf.* Lemma 5.1) and, finally, the order of G.

7. Conjecture (FSQ) and the additive properties of normal subgroups in D^*.

Thinking about the possibility of generalizing the given proof Theorem 2.6 to somewhat more general cases, one cannot help noticing that the only spot in the argument where D itself was used, is Proposition 3.4 which establishes property (C) for D^* if D is of degree 3. However, in further argument this fact is employed in a much weaker form, viz. as property (C) for the finite quotients D^*/M which probably can be proved in a more general set-up. (Just to compare: the centralizer of $x \in D$ is basically the maximal subfield $K(x)$, while the centralizer of the coset xN in D^*/N contains the image of $K(x)$ as well as the image of the following set: $N + xN$ which may be quite big.) A suggestive surprisingly general result in this direction was proved in [BS], [Tu]: if D is an infinite division ring then for any subgroup $N \subset D^*$ of finite index we have $N - N = D$ (so-called property $N - N$). Obviously, the quotient $F = D^*/N$ cannot be a simple group if for some $x \in D^* \setminus N$ we have $N + xN = D$ since then the coset xN belongs to the center of F. Unfortunately, this property $(N + xN)$ which is apparently very much like $(N - N)$, does not always hold true, even for p-adic division algebras. So, the real issue now is to find (say, using technique of [BS], [Tu]) some additive property of normal subgroups $N \subset D^*$ of finite index that would enable us to establish property (C) or its modification in general case. At the present stage it is difficult to predict the form of such a property, so we limit ourself to standing the following rather straightforward consequence of the above.

Proposition 7.1 *Let D be a division ring, $N \subset D^*$ be a normal subgroup of finite index such that for any $x, y \in D^*$ we have*

$$D^* = (N + yN + yxN)(N + xN)(X + yN + yxN) \tag{19}$$

Then the quotient $F = D^*/N$ cannot be a simple group.

Proof. As we mentioned above, the image of $N + xN$ in F is contained in the centralizer $C(\overline{x}) = C_F(\overline{x})$ of $\overline{x} = xN$ (indeed, if $g = n_1 + xn_2$ then $gn_1^{-1} = 1 + x(n_2n_1^{-1})$ commutes with $x(n_2n_1^{-1})$ in D^*, and therefore, $\overline{g} = \overline{gn_1}^{-1}$ commutes with $\overline{x} = \overline{x}(\overline{n}_2\overline{n}_1^{-1})$ in F). Repeating this argument, we obtain that the image of $N + yN + yxN$ in F is contained in $C_F(\overline{x}, \overline{y})$. In other words, (19) for any $x, y \in D^*$ implies property (C) for F. But then, according to Theorem 3.5, F cannot be a simple group. ∎

References

[Atlas] J. Conway, R. Curtis, S. Norton, R. Parker, and R. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985

[Bo] N. Bourbaki, *Groupes et Algèbres de Lie*, Hermann, Paris, 1968

[BS] V. Bergelson and D. Shapiro, *Multiplicative subgroups of finite index in a ring*, Proc. AMS, **116** (4), 1992, pp. 885-896

[FT] W. Feit and J.G. Thompson, *Solvability of groups of odd order,* Pacific J. Math, **13**, 1963, pp. 755-1029

[H] M. Hall, *The Theory of Groups,* The Macmillan Company, New York, 1959

[K] M. Kneser, *Orthogonale Gruppen über algebraicshen Zahlköpern*, J. reine und agew. Math., **196** (3-4), 1956, pp. 213-220

[M1] G.A. Margulis, *Finiteness of quotient groups of discrete subgroups*, Funct. Anal. i ego Prilozhenia, **13** (3), 1979, pp. 28-39 (English translation: Funct. Anal. Appl., **13**, 1979, pp. 178-187)

[M2] G.A. Margulis, *On the multiplicative group of a quaternion algebra over a global field*. Dokl. Akad. Nauk SSSR, **252** (3), 1980, pp. 542-546 (English translation: Soviet Math. Dokl., **21** (3), 1980, pp. 780-784)

[PR1] V.P. Platonov and A.S. Rapinchuk, *On the group of rational points of three-dimensional groups*. Dokl. Akad. Sci. USSR, **247** (2), 1979, pp. 279-282 (English translation: Soviet Math. Dokl., **20** (4), 1979, pp. 693-697)

[PR2] V.P. Platonov and A.S. Rapinchuk, *The multiplicative structure of division algebras over number fields and the Hasse norm principle*. Trudy Math. In-ta Acad. Sci. USSR, **165**, 1984, pp. 171-187 (English translation: Proc. Steklov Inst. Math., **165**, 1985, pp. 187-205)

[PR3] V.P. Platonov and A.S. Rapinchuk, *Algebraic Groups and Number Theory*, “Nauka” Publishers, Moscow, 1991 (English translation: “Pure and Applied Mathematics” series, N139, “Academic Press”, 1993)

[Ra] M.S. Raghunathan, *On the group of norm 1 elements in a division algebra*, Math. Ann. **279**, 1988, pp. 457-484

[RBC] A.S. Rapinchuk, V.V Benyash-Krivetz, V.I. Chernousov, *Representation varieties of the fundamental groups of compact orientable surfaces*, Preprint 94-030, SFB 343, Universität Bielefeld, 1994

[Ri] C. Riehm, *The norm 1 group of p-adic division algebra*, Amer. J. Math., **92** (2), 1970, pp. 499-523

[SpSt] T.A. Springer and R. Steinberg, *Conjugacy classes* in *"Seminar on Algebraic Groups and Related Finite Groups"*, Lect. Notes in Math, Berlin, Heidelberg, N. Y. Springer, **131**, 1970, pp. 167-266

[St] R. Steinberg, *Lectures on Chevalley groups*, Yale Univ. Lecture Notes, 1967

[To] G. Tomanov, *On the reduced norm 1 group of a division algebra over a global field*, Izv. Acad. Sci. USSR, Ser. Math., **55** (4), 1991 (English translation: Math. USSR Izvestiya **39** (1), 1992, pp. 895-904)

[Tu] G. Turnwald, *Multiplicative subgroups of finite index in a division ring*, Proc. AMS, **120** (2), 1994, pp. 377-381