PACIFIC JOURNAL OF MATHEMATICS
Vol. 71, No. 2, 1977

MAXIMAL SUBGROUPS AND AUTOMORPHISMS OF CHEVALLEY GROUPS

N. BURGOYNE, R. GRIESS AND R. LYONS

We study outer automorphisms α of a finite Chevalley type group K and show that under certain conditions $C_K(\alpha)$ is a maximal subgroup of K.

1. Introduction.

(1.1) In classification problems for finite simple groups there is often the need for detailed information about known families of groups. A particular question, that can arise in proving generation lemmas, is this:

> If K is a known finite simple group, and α is an automorphism of K of prime order, is $C_K(\alpha)$ a maximal subgroup of K?

The results in this article were motivated mainly by this question.

We consider the case when K is a Chevalley type group. Simple examples show that if α is inner or diagonal, then, in general, $C_K(\alpha)$ is not maximal. However, we find that if α is a field or graph type automorphism then, in general, $C_K(\alpha)$ *is maximal.* There are exceptions, and we also emphasize that our results are not complete for the graph type automorphisms for the families of types A, D, E_6.

In §2 we give a general result about finite subgroups of simple algebraic groups over fields of finite characteristic: let L be a finite Chevalley type group, let $G \supset L$ be a corresponding algebraic group; then, in Theorem 1, we describe all finite groups M such that $L \subseteqq M \subset G$. This allows us to answer the above question in a large number of cases. See 1.3 for details.

In §3, Theorem 2 gives an explicit description of all subgroups lying between $C_K(\alpha)$ and K when K is a twisted Chevalley group and α the automorphism induced by the usual field automorphism of the corresponding algebraic group.

In the remainder of §1 we give notation, some lemmas, and a discussion of automorphisms of Chevalley type groups.

(1.2) *Notation.* We use the approach of Steinberg [23] to describe the finite Chevalley type groups. We let G be a simple algebraic group over the algebraically closed field k of characteristic $p \neq 0$. In particular we suppose G is connected and its centre $Z(G)=1$. Let σ be an endomorphism of G onto itself: thus σ is an automorphism of G as an abstract group and a morphism of G as an algebraic group but, in general, σ^{-1} need not be a morphism. We will be concerned almost exclusively with the case where the group

$$G_\sigma = \{g \in G \mid \sigma g = g\}$$

is finite. In this case the possibilities for σ can be explicitly described, see §11 of [23]. Before summarizing these results we need some notation.

Let B be a Borel subgroup of G and H a maximal torus contained in B. Let Σ, Σ^+ and $\Pi = \{\alpha_1, \cdots, \alpha_l\}$ denote the corresponding sets of roots, positive roots, and fundamental (or simple) roots. Here $l =$ rank of G. We use lower case Greek letters for roots (and also for endomorphisms) and reserve θ for the unique highest root in Σ^+ and θ_s for the unique highest short root in Σ^+ (in case there are short roots). We let Σ^* denote the dual root system to Σ. Let V be the real vector space spanned by Π and (α, β) the usual Euclidean inner product on V and put $\langle \alpha, \beta \rangle = 2(\alpha, \beta)/(\beta, \beta)$.

As usual, for each $\alpha \in \Sigma$, let x_α denote a fixed homomorphisms of k_+ into G satisfying $hx_\alpha(t)h^{-1} = x_\alpha(t\alpha(h))$ for $h \in H$. For convenience we often identify H with $\mathrm{Hom}_Z(\Gamma, k^*)$ via $h(\alpha) = \alpha(h)$ where Γ denotes the lattice spanned by Σ in V. Let $X_\alpha = \langle x_\alpha(t) \mid t \in k \rangle$; then $U = \langle X_\alpha \mid \alpha \in \Pi \rangle$ is the unipotent radical of B and $G = \langle X_\alpha \mid \pm\, \alpha \in \Pi \rangle$.

If $N = N_G(H)$ then $W = N/H$ is the Weyl group. W acts naturally on V and if $n_w H = w \in W$ for some $n_w \in N$ we have $(n_w h n_w^{-1})(\alpha) = h(w^{-1}\alpha)$. For $\alpha \in \Sigma$ and $0 \neq t \in k$ let $n_\alpha(t) = x_\alpha(t)x_{-\alpha}(-t^{-1})x_\alpha(t)$ and $n_\alpha = n_\alpha(1)$. Then $n_\alpha(t) \in N$ and $h_\alpha(t) = n_\alpha(t)n_\alpha^{-1} \in H$ and $h_\alpha(t)(\beta) = t^{\langle \beta, \alpha \rangle}$.

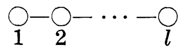
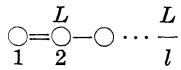
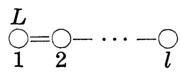
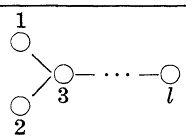
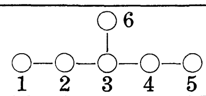
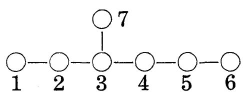
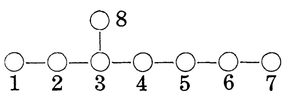
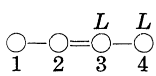
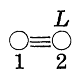
The above facts are all well known and can be found, for example, in [5] and [17].

Now let σ be an endomorphism of G such that G_σ is finite. By results in [23] we may suppose that σ normalizes B and H. Hence σ induces a permutation on Π which (by slight abuse of notation) we also denote by σ. From the explicit calculation in §11 of [23] we may suppose that σ is in "standard form," i.e.,

$$\sigma(x_\alpha(t)) = x_{\sigma(\alpha)}(t^{q_\alpha}) \quad \text{for} \quad \pm\alpha \in \Pi$$

where q_α is a power of p. The above formula uniquely determines the action of σ on G. We list the distinct possibilities for the standard form σ in Table 1. In column 1 we give the type of Σ; in column 2 the Dynkin diagram for Π, here "L" denotes a long root; in column 3 a standard notation for σ, q is always a positive power of p; in column 4 the permutation action of σ on Π; in column 5 the values of $q_i = q_{\alpha_i}$; and in column 6 any restrictions on l, p or q.

TABLE 1

A_l		σ_q	1	q	$l \geqq 1$
		$^2\sigma_q$	$(1,l)(2,l-1)\cdots$	q	$l \geqq 2$
B_l		σ_q	1	q	$l \geqq 3$
C_l		σ_q	1	q	$l \geqq 2$
		$^2\sigma_q$	(1, 2)	$2q_1 = q_2$	$l = 2,\ p = 2,\ q = q_1q_2$
D_l		σ_q	1	q	$l \geqq 4$
		$^2\sigma_q$	(1, 2)	q	
		$^3\sigma_q$	(1, 2, 4)	q	$l = 4$
E_6		σ_q	1	q	
		$^2\sigma_q$	(1, 5)(2, 4)	q	
E_7		σ_q	1	q	
E_8		σ_q	1	q	
F_4		σ_q	1	q	
		$^2\sigma_q$	(1, 4)(2, 3)	$q_1 = q_2 = 2q_3 = 2q_4$	$p = 2,\ q = q_1q_4$
G_2		σ_q	1	q	
		$^2\sigma_q$	(1, 2)	$q_1 = 3q_2$	$p = 3,\ q = q_1q_2$

With σ as above, if r is a positive integer then σ^r is also in standard form (except for $(^3\sigma_q)^2$ in the D_4 case, where the roots must be renumbered). If $\sigma = \sigma_q$ then $\sigma^r = \sigma_{q^r}$. Table 2 gives the connections between σ and σ^r in the twisted cases.

TABLE 2

Type of G	σ	σ^r
$A_l,\ D_l,\ E_6$	$^2\sigma_q$	σ_{q^r} if r=even $^2\sigma_{q^r}$ if r=odd
D_4	$^3\sigma_q$	σ_{q^r} if $r \equiv 0(3)$ $^3\sigma_{q^r}$ if $r \not\equiv 0(3)$(*)
$C_2,\ F_4\ G_2$	$^2\sigma_q$	$\sigma_{q^{r/2}}$ if r = even $^2\sigma_{q^r}$ if r = odd

(*) but if $r \equiv -1(3)$, σ^r acts as (1, 4, 2) on Π.

We put $O^{p'}(G_\sigma) = G_\sigma^s$ and use the usual notation to denote these groups. With 8 exceptions, namely $A_1(2)$, $A_1(3)$, ${}^2A_2(2)$, $C_2(2)$, ${}^2C_2(2)$, ${}^2F_4(2)$, $G_2(2)$, ${}^2G_2(3)$, these groups are simple. Also G_σ is the product of G_σ^s and all its diagonal automorphisms. Note that if $r \geqq 2$ then $|G_{\sigma^r}: G_\sigma|_p = |G_{\sigma^r}^s: G_\sigma^s|_p \neq 1$.

Keeping the above notation we give two elementary lemmas.

LEMMA 1.1. $N_G(U_\sigma) \subseteqq B$.

Proof. If $g \in N_G(U_\sigma)$ then using the Bruhat normal form $g = bn_w u$. Now $U_\sigma^{bn_w} = U_\sigma^{u^{-1}} \subseteqq U$ and also $U_\sigma^b \subseteqq U$. For each $i = 1, \cdots, l$ an $x_{\alpha_i}(t)$ with $t \neq 0$ occurs in some element of U_σ. Now $x_{\alpha_i}(t)^b = x_{\alpha_i}(t')v$ where $t' \neq 0$ and only x_β with β of height $\geqq 2$ occur in v. Hence $w(\alpha_i) \in \Sigma^+$ all i. Hence $w = 1$ and so $g \in B$.

LEMMA 1.2. *Let K be a group, $G_\sigma^s \subseteqq K \subseteqq G_\sigma$. Then $C_G(K) = 1$ and $N_G(K) = G_\sigma$.*

Proof. Let $g \in C_G(K)$. By the above lemma, $g \in B$. Now $[g, N_\sigma] = 1$ implies $g \in H$ and identifying H with $\mathrm{Hom}(\Gamma, k^*)$ gives $g(\alpha_i) = 1$ for $i = 1, \cdots, l$ and so $g = 1$.

Next let $g \in N_G(K)$; then for all $k \in K$, $g^{-1}kg = \sigma(g^{-1}kg)$. Thus $g\sigma(g^{-1}) \in C_G(K) = 1$ and so $g \in G_\sigma$. Since G_σ/G_σ^s is abelian we have $N_G(K) = G_\sigma$.

Finally we mention that our notation from finite group theory is standard, see for example [13]. In particular we use $g^x = x^{-1}gx$.

(1.3) *Automorphisms of G_σ.* Let G and σ be as in (1.2). In

TABLE 3

G	$\sigma(q = p^f)$	Coset representatives	$\mathrm{Aut}(G_\sigma)/\mathrm{Inn}(G_\sigma)$
A_l $l \geqq 2$ D_l $l \geqq 5$ E_6	σ_q	$\sigma_{p^i}, {}^2\sigma_{p^i}$ $1 \leqq i \leqq f$	$Z_2 \times Z_f$
	${}^2\sigma_q$		Z_{2f}
D_4	σ_q	$\sigma_{p^i}, \sigma_{p^i}, {}^3\sigma_{p^i}$ $1 \leqq i \leqq f$	$S_3 \times Z_f$
	${}^2\sigma_q$	$\sigma_{p^i}, {}^2\sigma_{p^i}$ $1 \leqq i \leqq f$	Z_{2f}
	${}^3\sigma_q$	$\sigma_{p^i}, {}^3\sigma_{p^i}$ $1 \leqq i \leqq f$	Z_{3f}
C_2 $p = 2$ F_4 $p = 2$ G_2 $p = 3$	σ_q	$\sigma_{p^i}, {}^2\sigma_{p^i - 1}$ $1 \leqq i \leqq f$	Z_{2f}
	${}^2\sigma_q$	${}^2\sigma_{p^i - 1}$ $1 \leqq i \leqq f$	Z_f
All others	σ_q	σ_{p^i} $1 \leqq i \leqq f$	Z_f

particular we suppose σ is in the standard form given in Table 1 for a fixed choice of B, H and x_α's in G. Hence G_σ is finite.

Let λ be any endomorphism of G satisfying $\lambda\sigma = \sigma\lambda$, then λ induces an element $\bar{\lambda} \in \mathrm{Aut}(G_\sigma)$. The structure of $\mathrm{Aut}(G_\sigma)/\mathrm{Inn}(G_\sigma)$ is described in [5]. Using these results it is straightforward to check that the endomorphisms λ listed in Table 3 give, via $\bar{\lambda}$, a complete set of coset representatives for $\mathrm{Inn}(G_\sigma)$ in $\mathrm{Aut}(G_\sigma)$. Note that G_σ is not, in general, simple.

Now suppose $\bar{\lambda}$ is one of the "coset representatives" given above and let α be any element in the coset $\mathrm{Inn}(G_\sigma)\bar{\lambda}$. Thus $\alpha = i_g\bar{\lambda}$ where $i_g(x) = gxg^{-1}$ for $g, x \in G_\sigma$.

LEMMA 1.3. *Let λ, $\alpha = i_g\bar{\lambda}$ be as above. Suppose $\bar{\lambda}$ and α both have order r and $\lambda^r = \sigma$. Then $\bar{\lambda}$ and α are conjugate under* $\mathrm{Inn}(G_\sigma)$.

Proof. Using $\bar{\lambda}i_g = i_{\lambda(g)}\bar{\lambda}$, and $Z(G_\sigma) = 1$, $\alpha^r = \bar{\lambda}^r = 1$ gives $g\lambda(g)\cdots\lambda^{r-1}(g) = 1$. By Lang's theorem [20] there exists $k \in G$ such that $g = k^{-1}\lambda(k)$. Hence $k = \lambda^r(k) = \sigma(k)$ and so $k \in G_\sigma$ and $\alpha = i_k^{-1}\bar{\lambda}i_k$.

LEMMA 1.4. *Let $\bar{\lambda}$, $\alpha = i_g\bar{\lambda}$ be as above. Suppose $\bar{\lambda}$, α both have order r. Suppose $\lambda^r \neq \sigma$ but that $\lambda_1^r = \sigma$ for some λ_1 such that $\langle\bar{\lambda}_1\rangle = \langle\bar{\lambda}\rangle$. Then $\bar{\lambda}$ and α are conjugate under* $\mathrm{Inn}(G_\sigma)$.

Proof. Suppose $\bar{\lambda}_1 = \bar{\lambda}^m$ for some integer m. Let $\beta = \alpha^m$ then $\beta = i_k\bar{\lambda}_1$ for some $k \in G_\sigma$. Since $\bar{\lambda}_1$ and β both have order r, Lemma 1.3 implies that $\bar{\lambda}_1$ and β are conjugate under $\mathrm{Inn}(G_\sigma)$. Suppose $\bar{\lambda} = \bar{\lambda}_1^d$ for some integer d then, since $\bar{\lambda}$ and α have the same order, we have $\alpha = \beta^d$. Hence $\bar{\lambda}$ and α are conjugate under $\mathrm{Inn}(G_\sigma)$.

Using these two results an inspection of Table 3 immediately yields

PROPOSITION 1.1. *Let λ be as above and suppose $\bar{\lambda}^r = 1$, where r is a prime number. Then, apart from the possible exceptions* (i), (ii) *given below, the coset* $\mathrm{Inn}(G_\sigma)\bar{\lambda}$ *contains a unique class of elements of order r, under conjugation by* $\mathrm{Inn}(G_\sigma)$, *and furthermore there exists an endomorphism λ_1 such that $\lambda_1^r = \sigma$ and $\langle\bar{\lambda}_1\rangle = \langle\bar{\lambda}\rangle$. The possible exceptions are*:

$$\text{(i)}\quad G = A_l(l \geqq 2),\ D_l(l \geqq 4),\ E_6 \ \textit{with} \begin{cases} \sigma = \sigma_q & \textit{with}\ \lambda = {}^2\sigma_q \\ \sigma = {}^2\sigma_q & \textit{with}\ \lambda = \sigma_q\,. \end{cases}$$

$$\text{(ii)}\quad G = D_4 \ \textit{with} \begin{cases} \sigma = \sigma_q & \textit{with}\ \lambda = {}^3\sigma_q \\ \sigma = {}^3\sigma_q & \textit{with}\ \lambda = \sigma_q\,. \end{cases}$$

Note that $r = 2$ in (i) and $r = 3$ in (ii). These exceptions do occur; in fact only for $G = A_l$ with $l =$ even is there a single class for the given λ. For $G = D_l$ the number of classes increases as $l/2$.

We now consider when $C = C_{G^s_\sigma}(\alpha)$ is a maximal sugroup of G^s_σ. Apart from the exceptions (i), (ii) Proposition 1.1 implies first that we may suppose $\alpha = \bar{\lambda}$, and next, since $C_{G^s_\sigma}(\bar{\lambda}) = C_{G^s_\sigma}(\bar{\lambda}_1)$, we may suppose that $\lambda^r = \sigma$. Now an immediate consequence of Theorem 1 is that, if C is nonsolvable, then it is always maximal in G^s_σ.

In the exceptions (i), (ii) we have a more complicated problem, especially when $r = p$. Theorem 2 is one step towards a solution.

2. Theorem 1.

(2.1) *Statement of results.* Let G be a simple algebraic group over an algebraically closed field k of characteristic $p \neq 0$. Let λ be an endomorphism of G onto itself such that the subgroup G_λ of fixed points is finite. As discussed in (1.2) we may suppose λ is in standard form. If r is any positive integer the endomorphism λ^r is also in standard form. The possibilities for λ and the corresponding λ^r are listed in the tables in §1.

Recall that $G^s_\lambda = O^{p'}(G_\lambda)$ and, with eight exceptions, is a simple group. G_λ is the product of G^s_λ and all its diagonal-type outer automorphisms.

If G, λ are such that G^s_λ is one of the three groups $A_1(2)$, $A_1(3)$, ${}^2C_2(2)$ we call this an *exceptional case.*

THEOREM 1. *Let G, λ be as above and not an exceptional case. Let M be a finite subgroups of G containing G^s_λ. Then there exists a positive integer r such that* (with $\mu = \lambda^r$)

$$G^s_\mu \subseteqq M \subseteqq G_\mu \,.$$

An immediate consequence is that if G, λ are as in the statement of the theorem and $\mu = \lambda^r$ where r is a *prime* number then $G_\lambda \cap G^s_\mu$ is a proper maximal subgroup of G^s_μ.

The proof of the theorem is given in (2.3)-(2.5). It was necessary to handle the case $G_\lambda = {}^2G_2(q)$ separately and this occupies (2.5). In the general case the proof falls into two parts. In (2.3) we first describe $N_G(U_\lambda)$ (see Lemma 2.3) then use this to show there exists a (unique) integer r such that, if $\mu = \lambda^r$, $U_\mu \in \mathrm{Syl}_p(M)$. In (2.4) we combine this result with induction on the rank of G and show that either (a) the theorem holds, or (b) M contains a proper strongly 2-embedded subgroup. Using results of H. Bender [2] we easily rule out (b).

(2.2) *The exceptional cases.* If G, λ are an exceptional case there do exist finite subgroups M such that $G_\lambda^s \subset M \subset G$ and which do not satisfy the conclusion of the theorem. We now describe all these 'exceptional' M.

If $G_\lambda^s = A_1(2)$ or $A_1(3)$ we use results of Dickson, see [6]. If $G_\lambda^s = {}^2C_2(2)$ we use Suzuki [25] and the recent work of Flesner [11].

$A_1(2)$: M is a subgroup of a dihedral group of order $2(q \pm 1)$ in $G_{\lambda^r} = A_1(q)$ where $q = 2^r$ and $q \pm 1 \equiv 0 \pmod 3$.

$A_1(3)$: M is a subgroup of $G_{\lambda^2}^s = A_1(9)$ and is isomorphic to the alternating group on 5 letters.

${}^2C_2(2)$: M is either a subgroup of a group of order $4(q \pm \sqrt{2q}+1)$ in $G_{\lambda^r} = {}^2C_2(q)$ where $q = 2^r$ and r is odd, or else M is a subgroup of $G_{\lambda^{2r}} = C_2(2^r)$ and is isomorphic to a subgroup of the four dimensional orthogonal group of index one over $\boldsymbol{F}_{2^r}$.

(2.3) *Proof. First part.* We assume throughout this subsection that G, λ satisfy the hypothesis of the theorem and also that $G_\lambda \neq {}^2G_2(q)$. The main technique in proving the following lemmas is the Chevalley commutator relations together with the known embedding of U_λ in U.

The subgroups B, U, H and sets of roots Σ, Π, etc. are as described in (1.2).

LEMMA 2.1. $C_U(U_\lambda) = Z(U)$.

Proof. We call two roots $\rho, \sigma \in \Sigma$ *fundamentally independent* if $\rho + \sigma \in \Sigma$ and $\{\rho, \sigma\}$ is a fundamental system in the rank 2 system $(\boldsymbol{Z}\rho + \boldsymbol{Z}\sigma) \cap \Sigma$. If ρ and σ are fundamentally independent, then in G we have a commutator relation $[x_\rho(t), x_\sigma(u)] = x_{\rho+\sigma}(\pm tu) \cdots$. Note that $\rho, \sigma \in \Sigma$ and $(\rho, \sigma) < 0$, then ρ and σ are fundamentally independent unless $\Sigma = G_2$ and ρ and σ are short roots inclined at 120°.

Recall that θ is the highest root in Σ^+, and θ_s is the highest short root (in the case of two root lengths). Let $D = \{x \in \boldsymbol{R}\Sigma \mid (x, \sigma) \geqq 0$ for all $\sigma \in \Sigma^+\}$ be the usual fundamental domain for the action of W on $\boldsymbol{R}\Sigma$. Since W is transitive on roots of a given length, D contains exactly one root of each length. Clearly $\theta \in D$; otherwise for some $\sigma \in \Sigma^+$, we would have $(\theta, \sigma) < 0$ and so $\theta + \sigma \in \Sigma$. Since D is also a fundamental domain for the dual root system Σ^*, D contains the highest root of Σ^*, whose dual—which is θ_s-therefore lies in D. Thus, for any $\rho \in \Sigma - \{\theta, \theta_s\}$, there is $\sigma \in \Sigma^+$ such that $(\rho, \sigma) < 0$.

Hence:

(*) If $\rho \in \Sigma^+ - \{\theta, \theta_s\}$, then there exist $\sigma \in \Sigma^+$ such that ρ and

σ are fundamentally independent, unless $\Sigma = G_2$ and ρ is the sum of the fundamental roots.

We also need:

(**) Suppose Σ has two root lengths, $\rho \in \Sigma^+$, and $\theta_s < \rho < \theta$. Then $\theta_s + \rho \notin \Sigma$, and there exists $\sigma \in \Sigma^+$ such that ρ and σ are fundamentally independent and $\theta_s + \sigma \notin \Sigma$.

To prove this, note that if σ is any long root in Σ^+, then $\theta_s + \sigma \notin \Sigma$, since otherwise $\theta_s + \sigma$ would be a short root. In particular, $\theta_s + \rho \notin \Sigma$ since $\rho(>\theta_s)$ is long. Now, using (*), choose $\sigma \in \Sigma^+$ such that ρ and σ are fundamentally independent. Since $\rho + \sigma(>\theta_s)$ is long, σ is long, so $\theta_s + \sigma \notin \Sigma$, as required.

For any $u \in U$, we have $u = \prod_{\rho \in \Sigma^+} x_\rho(t_\rho)$, $t_\rho \in k$. We take all products over Σ^+ to be in increasing order with respect to Σ^+. We set $\operatorname{supp}(u) = \{\rho \in \Sigma^+ \mid t_\rho \neq 0\}$ for $u \in U$.

Now consider the case $\lambda = \sigma_q$, where q is some power of p, so $U_\lambda = \{\prod_\rho x_\rho(t_\rho) \mid t_\rho \in GF(q)\}$. Let $u \in C_U(U_\lambda)$. We shall show $\operatorname{supp}(u) \subseteqq \{\theta_s, \theta\}$. Let ρ_0 be the least element of $\operatorname{supp}(u)$, so

$$u = x_{\rho_0}(t_{\rho_0}) \prod_{\rho > \rho_0} x_\rho(t_\rho),\ t_{\rho_0} \neq 0 .$$

If there exists $\sigma \in \Sigma^+$ such that ρ_0 and σ are fundamentally independent, then we get $1 = [u, x_\sigma(1)] = x_{\rho_0+\sigma}(\pm t_{\rho_0}) \cdots$, contradiction. Thus no such σ is available. By (*), either $\rho_0 \in \{\theta_s, \theta\}$, or $\Sigma = G_2$ and $\rho_0 = \alpha + \beta$, where $\Pi = \{\alpha, \beta\}$, with, say, α long and β short. In this last case, $1 = [u, x_{\alpha+2\beta}(1)] = x_{2\alpha+3\beta}(\pm 3t_{\rho_0})$ and $1 = [u, x_\beta(1)] = x_{\alpha+2\beta}(\pm 2t_{\rho_0})$, so $3t_{\rho_0} = 2t_{\rho_0} = 0$, contradiction. Hence, $\rho_0 \in \{\theta_s, \theta\}$. Suppose $\rho_0 = \theta_s$ and let ρ_1 be the least element of $\operatorname{supp}(u)$ greater than ρ_0 (if $\operatorname{supp}(u) \neq \{\rho_0\}$). If $\rho_1 \neq \theta$, choose σ so that ρ_1 and σ are fundamentally independent and $\rho_0 + \sigma \notin \Sigma$ (by (**)). Then $1 = [u, x_\sigma(1)] = x_{\rho_1+\sigma}(\pm t_{\rho_1}) \cdots$ contradicting $t_{\rho_1} \neq 0$. Therefore $\rho_1 = \theta$, so $\operatorname{supp}(u) \subseteqq \{\theta_s, \theta\}$. If actually $\operatorname{supp}(u) \subseteqq \{\theta\}$ for all $u \in C_U(U_\lambda)$, then $C_U(U_\lambda) \subseteqq X_\theta \subseteqq Z(U)$, as required. So we may assume $\theta_s \in \operatorname{supp}(u)$, i.e., $u = x_{\theta_s}(t)x_\theta(t')$ with $t \neq 0$. There exist a (short) $\sigma \in \Sigma^+$ such that $\theta_s + \sigma \in \Sigma$. We get $1 = [u, x_\sigma(1)] = x_{\theta_s}(\pm mt) \cdots$, where $m = 2$ if G is of type B, C or F_4 and $m = 3$ if of type G_2. Hence $m = p$ and in precisely these case $Z(U) = X_{\theta_s}X_\theta \supseteqq C_U(U_\lambda)$, as required.

Next, suppose Σ has one root length, $\lambda = {}^2\sigma_q$ or ${}^3\sigma_q$, and $\Sigma \neq A_{2n}$. Let $u \in C_U(U_\lambda)$, let ρ_0 be the least element of $\operatorname{supp}(u)$, so

$$u = x_{\rho_0}(t_{\rho_0}) \prod_{\rho > \rho_0} x_\rho(t_\rho)$$

with $t_{\rho_0} \neq 0$. Suppose $\rho_0 \neq \theta$, and choose $\sigma \in \Sigma^+$ such that σ and ρ_0 are fundamentally independent. Let $\bar{x}_\sigma$ be the product of the distinct images of $x_\sigma(1)$ under the powers of λ, so that $\bar{x}_\sigma \in U_\lambda$ and $\bar{x}_\sigma = x_\sigma(1)x_{\lambda(\sigma)}(1)\cdots$. The roots $s, \lambda(s), \cdots$ have the same height, so $1 =$

$[u, \bar{x}_\sigma] = x_{\rho_0+\sigma}(\pm t_{\rho_0}) \cdots$, contradiction. Thus $\rho_0 = \theta$, so $u \in X_\theta \subseteqq Z(U)$.

If $\Sigma = A_{2n}$ and $\lambda = {}^2\sigma_q$, essentially the same argument works, except that if $\sigma + \lambda(\sigma) \in \Sigma$, we define $\bar{x}_\sigma = x_\sigma(1)x_{\lambda(\sigma)}(1)x_{\sigma+\lambda(\sigma)}(b)$, with $b \in GF(q^2)$ chosen to satsfy $b + b^q = 1$; if $\sigma = \lambda(\sigma)$, we define $\bar{x}_\sigma = x_\sigma(b)$ with b chosen to satisfy $b + b^q = 0$. Then $1 = [u, \bar{x}_\sigma] = x_{\rho_0+\sigma}(\pm t_{\rho_0}) \cdots$ or $x_{\rho_0+\sigma}(\pm b t_{\rho_0}) \cdots$, contradiction, unless $\rho_0 = \theta$.

Suppose $\Sigma = C_2$ and $\lambda = {}^2\sigma_q$. Then $q = 2n^2$, $n = 2^f > 1$, by assumption. Let $\Pi = \{\alpha, \beta\}$, with α long. For every $t \in GF(q)$, let $\bar{x}(t) = x_\alpha(t)x_\beta(t^n)x_{\alpha+\beta}(t^{1+n}) \in U_\lambda$. Suppose $u = \prod_\rho x_\rho(t_\rho) \in C_U(U_\lambda)$. Then $1 = [u, \bar{x}(t)] = x_{\alpha+\beta}(tt_\beta + t^n t_\alpha)x_{\alpha+2\beta}(tt_\beta^2 + t^{2n}t_\alpha)$ for all $t \in GF(q)$. Hence $tt_\beta + t^n t_\alpha = tt_\beta^2 + t^{2n}t_\alpha = 0$. With $t = 1$, we conclude $t_\alpha = t_\beta = t_\beta^2$. Now if $t_\alpha = t_\beta = 1$, we get $t^n = t^{2n}$ for all $t \in GF(q)$, so $q = 2$, contradiction. Hence $t_\alpha = t_\beta = 0$, so $u \in X_{\alpha+\beta}X_{\alpha+2\beta} \in Z(U)$.

Suppose $\Sigma = F_4$ and $\lambda = {}^2\sigma_q$. We need:

(***) if $\rho_0 \in \Sigma^+ - \{\theta_s, \theta\}$, then there exist $\sigma, \sigma' \in \Sigma^+$ and an element $\bar{x}_\sigma = x_\sigma(1)x_{\sigma'}(1)\prod_\rho x_\rho(t_\rho)$ of U_λ such that (i) $ht(\sigma) = ht(\sigma')$, and $t_\rho = 0$ unless $ht(\rho) > ht(\sigma)$, (ii) ρ_0 and σ are fundamentally independent, and $\rho_0 + \sigma - \sigma' \notin \Sigma$.

Assuming this, let $u \in C_U(U_\lambda)$ and let ρ_0 be the least element of $\operatorname{supp}(u)$, $u = x_{\rho_0}(t_{\rho_0}) \cdots$. If $\rho_0 \neq \theta_s$ or θ, choose σ, σ', and $\bar{x}_\sigma$ as in (***). Then $1 = [u, \bar{x}_\sigma] = x_{\rho_0+\sigma}(t_{\rho_0}) \cdots$ because the condition $\rho_0 + \sigma - \sigma' \notin \Sigma$ guarantees that the only way to express $\rho_0 + \sigma$ as the sum of an element of $\operatorname{supp}(u)$ and an element of $\operatorname{supp}(\bar{x}_\sigma)$ is as $\rho_0 + \sigma$. But $t_{\rho_0} \neq 0$, so $\rho_0 \in \{\theta_s, \theta\}$. Hence θ_s is the only possible short root in $\operatorname{supp}(u)$. Since $\lambda(u) \in C_U(U_\lambda)$, and $\lambda(\theta_s) = \theta$, the same argument applied to $\lambda(u)$ implies that the only possible long root in $\operatorname{supp}(u)$ is θ. Hence $u \in X_{\theta_s}X_\theta = Z(U)$, and we are done.

To prove (***) we examine Σ in detail. Let $\Pi = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, read from one end of the Dynkin diagram to the other, with α_1 short. We write the root $\sum_{i=1}^4 n_i\alpha_i$ as $n_1n_2n_3n_4$. Thus $\theta_s = 2321$ and $\theta = 2432$. If $\rho_0 \in \{0100, 0110, 0221, 1221, 1321\}$, take $\sigma = 1000$, $\sigma' = 0001$, $\bar{x}_\sigma = x_\sigma(1)x_{\sigma'}(1)$. If $\rho_0 \in \{0010, 0210, 2431\}$, take $\sigma = 0001$, $\sigma' = 1000$, $\bar{x}_\sigma = x_\sigma(1)x_{\sigma'}(1)$. In the remaining cases, take $\bar{x}_\sigma = x_\sigma(1)x_{\sigma'}(1)x_{\sigma+\sigma'}(1)$. If $\rho_0 \in \{1000, 0011, 1110, 1111, 2221\}$, take $\sigma = 0100$, $\sigma' = 0010$. If $\rho_0 \in \{0001, 1100, 0211, 1211, 2211\}$, take $\sigma = 0010$, $\sigma' = 0100$. If $\rho_0 \in \{1210, 2210, 2421\}$, take $\sigma = 0011$, $\sigma' = 1100$. If $\rho_0 = 0111$, take $\sigma = 1100$, $\sigma' = 0011$. Then (***) is easily verified.

LEMMA 2.2. $C_G(U_\lambda) = Z(U)$.

Proof. By Lemma 1.1, $C_G(U_\lambda) \subseteqq B$, so by Lemma 2.1, it suffices to show $C_B(U_\lambda) \subseteqq U$. Let $U' = \langle X_\rho \mid \rho \in \Sigma^+ - \Pi \rangle$, define $\bar{B} = B/U'$, and for any $A \subseteqq B$ write $\bar{A}$ for AU'/U'. It suffices to show $C_{\bar{B}}(\bar{U}_\lambda) \subseteqq \bar{U}$. Now $\bar{U}$ is the direct product of $\bar{X}_\rho$ over all $\rho \in \Pi$, and $\bar{X}_\rho \cong X_\rho$ for

$\rho \in \Pi$. In particular $\bar{U}$ is abelian, so $C_{\bar{B}}(\bar{U}_\lambda) = \bar{U}C_{\bar{H}}(\bar{U}_\lambda)$, as $\bar{B} = \bar{U}\bar{H}$. Thus it suffices to show $C_{\bar{H}}(\bar{U}_\lambda) = 1$. Suppose $h \in H$ and $\bar{h} \in C_{\bar{H}}(\bar{U}_\lambda)$. For any $\rho \in \Pi$, there exists $u \in U_\lambda$ such that $\rho \in \operatorname{supp}(u)$, say $u = \overline{x_\rho(t_\rho) \cdots}, t_\rho \neq 0$. Then, identifying H with $\operatorname{Hom}(\Gamma, k^*)$, $\bar{1} = [\bar{h}, \bar{u}] = \overline{x_\rho(t_\rho(h(\rho) - 1)) \cdots}$, so $h(\rho) = 1$. Thus $h = 1$, as required.

LEMMA 2.3. $N_G(U_\lambda) = \langle B_\lambda, Z(U)\rangle$.

Proof. Let $g \in N_G(U_\lambda)$. Then $g^{-1}\lambda(g) \in C_G(U_\lambda)$. By Lemma 2.2, $g^{-1}\lambda(g) \in Z(U)$. Since $Z(U)(=X_\theta$ or $X_{\theta_s}X_\theta)$ is connected, an elementary version of Lang's theorem [20] implies the existence of $z \in Z(U)$ such that $g^{-1}\lambda(g) = z^{-1}\lambda(z)$. Then $gz^{-1} = \lambda(gz^{-1})$, so $gz^{-1} \in G_\lambda$. By Lemma 1.1, $g \in B$, so $gz^{-1} \in G_\lambda \cap B = B_\lambda$. Hence $g = gz^{-1}z \in \langle B_\lambda, Z(U)\rangle$, so $N_G(U_\lambda) \subseteqq \langle B_\lambda, Z(U)\rangle$. The other inclusion is obvious.

LEMMA 2.4 *Let $z \in Z(U)$ and suppose $\langle G_\lambda^s, z\rangle$ is a finite group. Then there exists a positive integer r such that $\langle G_\lambda^s, z\rangle \subseteqq G_{\lambda^r}$.*

Proof. First suppose $Z(U)$ is one-dimensional. Thus $Z(U) = \langle x_\theta(t) \mid t \in k\rangle$ where θ is the root of maximal height in Σ^+. Choose $n \in N \cap \langle X_\theta, X_{-\theta}\rangle$ so that $nx_\theta(t)n^{-1} = x_{-\theta}(-t)$. Suppose $z = x_\theta(t)$ for some fixed, nonzero, $t \in k$ and put $g = nz$. On the 3-dimensional adjoint module for $\langle X_\theta, X_{-\theta}\rangle$ g is represented by a matrix whose trace is $t^2 - 1$. Since g has finite order this implies that t is algebraic over $GF(p)$. Suppose $t \in GF(p^r)$ then, since we may suppose that $\lambda(x_\theta(t)) = x_\theta(t^q)$, we have $\langle G_\lambda^s, z\rangle \subseteqq G_{\lambda^r}$.

Now suppose $Z(U)$ is two-dimensional. First suppose G is of type C_l or F_4. Hence k has characteristic 2 and there exist roots $\{\delta_1, \delta_2, \delta_1 + \delta_2, \delta_1 + 2\delta_2\} \subseteqq \Sigma^+$ such that $Z(U) = \langle x_{\delta_1+\delta_2}(t), x_{\delta_1+2\delta_2}(t) \mid t \in k\rangle$ (in fact $\delta_1 + \delta_2 = \theta_s$ and $\delta_1 + 2\delta_2 = \theta$). We suppose $z = x_{\delta_1+\delta_2}(t_1)x_{\delta_1+2\delta_2}(t_2)$ for some fixed $t_1, t_2 \in k$. Put $G_1 = \langle x_\gamma(t) \mid \pm\gamma \in \{\delta_1, \delta_2\}, t \in k\rangle$ thus G_1 is of type C_2 and λ fixes G_1. Choose $n \in (G_1)_\lambda$ such that $nx_{\delta_i}(t)n^{-1} = x_{-\delta_i}(t)$ and put $g = nz$. There is a natural 4-dimensional module for G_1 on which

$$n \longrightarrow \begin{pmatrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{pmatrix} \quad \text{and} \quad z \longrightarrow \begin{pmatrix} 1 & 0 & t_1 & t_2 \\ & 1 & 0 & t_1 \\ & & 1 & 0 \\ & & & 1 \end{pmatrix}$$

This gives t_1^2 and t_2 as coefficients in the characteristic polynomial of g. Since g has finite order t_1, t_2 are algebraic over $GF(Z)$ and we are done.

If G is of type G_2, $z = x_{2\alpha_1+\alpha_2}(t_1)x_{3\alpha_1+2\alpha_2}(t_2)$ and choosing $n \in N_\lambda$ such that $nx_{\alpha_i}(t)n^{-1} = x_{-\alpha_i}(-t)$ put $g = nz$. Compute the characteristic polynomial for g as represented in the 7-dimensional module for G. Its coefficients are $(t_1^2 - 1)$ and $(t_2^2 - t_1^2 + 1)$. Hence, as before, we are done.

LEMMA 2.5. *There exists a positive integer r such that, with $\mu = \lambda^r$, we have $G_\mu^s \subseteqq M$ and $U_\mu \in \mathrm{Syl}_p(M)$.*

Proof. Choose the positive integer r to be maximal subject to $G_{\lambda^r}^s \subseteqq M$. Without loss, we may assume $r = 1$, and shall show that $U_\lambda \in \mathrm{Syl}_p(M)$. Suppose $U_\lambda \notin \mathrm{Syl}_p(M)$. By Lemma 2.3 and Sylow's theorem, there exists $z \in Z(U) - U_\lambda$ such that $\langle G_\lambda^s, z\rangle \subseteqq M$. By Lemma 2.4, $\langle G_\lambda^s, z\rangle \subseteqq G_{\lambda^n}$ for some n. Hence the lemma follows from the following statement, which contradicts the maximality of r:

(†) If $z \in Z(U)_{\lambda^n \lambda^n} - U_\lambda$ for some n, then $\langle G_\lambda^s, z\rangle \supseteqq G_{\lambda^m}^s$ for some $m > 1$.

We now establish (†). Let $K = \langle G_\lambda^s, z\rangle$.

Our method is to first study the case A_1 and use this result along with the action of N_λ on the root subgroups of G_λ.

Case 0. $\Sigma = A_1$: If p is odd, (†) is an immediate consequence of a result of Dickson [7]. Suppose $p = 2$. Then $G_\lambda^{(s)} = \langle x_\rho(t), x_{-\rho}(t) \mid t \in GF(q)\rangle$ and $z = x_\rho(t_1)$ for some $t_1 \in GF(q^n) - GF(q)$, where $\Sigma^+ = \{\rho\}$. Define m by $GF(q)(t_1) = GF(q^m)$, so that $K \subseteqq G_\lambda m$ and $m > 1$. Now distinct Sylow 2-subgroups in G_{λ^m} intersect trivially, so distinct Sylow 2-subgroups in K intersect trivially. Since $G_\lambda \subseteqq K$ and G_λ has more than one Sylow 2-subgroup, so does K. It follows that any two involutions in K are conjugate in K, [13]. In particular, $x_\rho(t_1)$ and $x_\rho(1)$ are conjugate in K, hence conjugate in $N_K(U \cap K)$. Hence there are $u \in U$, $h_1 \in H$ such that $uh_1 \in K$ and $x_\rho(1)^{uh_1} = x_\rho(t_1)$. Identifying H with $\mathrm{Hom}(\Gamma, k^*)$, we see that $h_1(\rho) = t_1^{1/2}$. Hence for any positive integer l, and any $t \in GF(q)$, we may choose $h \in K$ such that $x_\rho(1)^h = x_\rho(t)$, and conclude that $x_\rho(tt_1^l) = x_\rho(1)^{h(uh_1)^l} \in K$. Thus $x_\rho(f(t_1)) \in K$ for all $f[X] \in GF(q)[X]$. Hence $x_\rho(t) \in K$ for all $t \in GF(q^m)$, i.e., $U_{\lambda^m} \subseteqq K$. Then $K \supseteqq \langle U_{\lambda^m}, N_\lambda\rangle \supseteqq G_{\lambda^m}^s$ as required.

Case 1. Σ arbitrary, $\lambda = \sigma_q$, and $Z(U) = X_\theta$: Let $G_\theta = \langle X_\theta, X_{-\theta}\rangle$ and $K_\theta = K \cap G_\theta$. Then λ is an endomorphism of G_θ, and $\langle (G_\theta)_\lambda, z\rangle \subseteqq K_\theta \subseteqq (G_\theta)_{\lambda^n}$ since $z \in Z(U) = X_\theta$. By Case 0, $(G_\theta)_{\lambda^m} \subseteqq K_\theta$ for some $m > 1$, so $(X_\theta)_{\lambda^m} \subseteqq K$. Conjugating by elements of N_λ, we get $(X_\rho)_{\lambda^m} \subseteqq K$ for all $\rho \in \Sigma$ of the same length as θ. If there is one root length, this gives immediately $G_{\lambda^m}^s \subseteqq K$. If there are two root lengths, let $\rho \in \Sigma$ be short and choose $\sigma \in \Sigma$ long such that $\rho + \sigma \in \Sigma$. For any $t \in GF(q^m)$, $t \neq 0$, $h_\sigma(t) \in K$, so $x_\rho(t^{-1}) = x_\rho(1)^{h_\sigma(t)} \in K$. Thus $(X_\rho)_{\lambda^m} \subseteqq K$, so $K \supseteqq \langle (X_\rho)_{\lambda^m} \mid \rho \in \Sigma \rangle = G^s_{\lambda^m}$.

Case 2. $\lambda = \sigma_q$, $Z(U) \neq X_\theta$: We have two root length, $Z(U) = \langle X_{\theta_s}, X_\theta \rangle$, and the characteristic of k is the strength of the multiple bond in the Dynkin diagram of Σ. Let $\Sigma^0 = (Z\theta_s + Z\theta) \cap \Sigma$, $G^0 = \langle X_\rho \mid \rho \in \Sigma^0 \rangle$, $K^0 = G^0 \cap K$. Then λ is an endomorphism of G^0, $\langle (G^0)^s_\lambda, z \rangle \subseteqq K^0$. If (†) holds for G^0, then $\langle (G^0)^s_\lambda, z \rangle \supseteqq (G^0)^s_{\lambda^m}$ for some $m > 1$. In particular, $(X_\rho)_{\lambda^m} \subseteqq K$ for $\rho = \theta_s$ and θ, and then for all $\rho \in \Sigma$, by conjugation by elements of N_λ. Hence in proving (†) we may assume $\Sigma = \Sigma^0$. Thus $\Sigma = C_2$ or G_2, with $p = 2$ or 3 respectively.

We take $\Pi = \{\alpha, \beta\}$, with α long and β short. Suppose $\Sigma = C_2$, so $p = 2$. For every $y = x_{\alpha+\beta}(t_1)x_{\alpha+2\beta}(t_2) \in Z(U)$, set $\pi_{\alpha+\beta}(y) = t_1$, $\pi_{\alpha+2\beta}(y) = t_2$. Let $k_1 = \pi_{\alpha+\beta}(K \cap Z(U))$, $k_2 = \pi_{\alpha+2\beta}(K \cap Z(U))$. Thus k_i is an additive group, $GF(q) \subseteqq k_i \subseteqq GF(q^n)$, $i = 1, 2$, and $k_1 \cup k_2 \neq GF(q)$ as $z \notin U_\lambda$. Let $t_1 \in k_1$, $t_2 \in k_2$, and choose $u_1 = x_{\alpha+\beta}(t_1)x_{\alpha+2\beta}(t_1') \in K$ and $u_2 = x_{\alpha+\beta}(t_2')x_{\alpha+2\beta}(t_2) \in K$. Now $n_\alpha(1)$, $n_\beta(1) \in G^s_\lambda \subseteqq K$, so

$$(1) \qquad x_{\alpha+\beta}(t_1t_2)x_{\alpha+2\beta}(t_1^2t_2) = [u_1^{n_\alpha(1)}, u^{n_\beta(1)}] \in K .$$

Thus $t_1t_2 \in k_1$, $t_1^2t_2 \in k_2$, so $\{t^2 \mid t \in k_1\} \subseteqq k_2 \subseteqq k_1$, from the special cases $t_2 = 1$ and $t_1 = 1$. But the map $t \to t^2$ is injective on $GF(q^n)$, so $k_1 = k_2$. From (1), $k_1 \cdot k_2 \subseteqq k_1$, so k_1 is a field. Thus for some $m > 1$, $k_1 = k_2 = GF(q^m)$. For any $t \in GF(q^m)$, we take $t_1 = t$ and $t_2 = t^{-1}$ and t^{-2} in (1) and conclude $\langle (X_{\alpha+\beta})_{\lambda^m}, (X_{\alpha+2\beta})_{\lambda^m} \rangle \subseteqq K$. As usual this gives $G^s_{\lambda^m} \subseteqq K$.

Suppose $\Sigma = G_2$ so $p = 3$. Write $z = u_1u_2$, with $u_1 \in X_{\alpha+2\beta}$ and $u_2 \in X_{2\alpha+3\beta}$. Then $u_2 = [z^{n_\alpha(1)}, x_\alpha(1)]^{\pm 1} \in K$, so $u_1 = zu_2^{-1} \in K$. Since $z \notin G_\lambda$, either u_1 or $u_2 \notin G_\lambda$, so without loss we may assume $z = u_1$ or $z = u_2$.

Since G has a graph automorphism commuting with λ and interchanging θ_s and θ we may assume that $z \in X_{2\alpha+3\beta}$. By Case 0 applied to $\langle X_{2\alpha+3\beta}, X_{-2\alpha-3\beta} \rangle$, there is $m > 1$ such that $(X_\rho)_{\lambda^m} \subseteqq K$ for $\rho = 2\alpha + 3\beta$, and then for all long $\rho \in \Sigma$. For any $t \in GF(q^m)$, K contains $[x_\alpha(t), x_\beta(1), x_\beta(1)] = x_{\alpha+2\beta}(\pm t)x_{\alpha+3\beta}(t')x_{2\alpha+3\beta}(t'')$ with $t', t'' \in GF(q^m)$, so $x_{\alpha+2\beta}(t) \in K$ as $\alpha + 3\beta$ and $2\alpha + 3\beta$ are long. Thus $(X_\rho)_{\lambda^m} \subseteqq K$ for $\rho = \alpha + 2\beta$, hence for all short ρ, whence $G^s_{\lambda^m} \subseteqq K$.

Case 3. $\lambda = {}^2\sigma_q$ or ${}^3\sigma_q$, with G_λ a Steinberg variation, but $\Sigma \neq A_{2n}$ (the cases of twisted F_4, G_2, C_2 are not being considered here): In this case $Z(U) = X_\theta$, so by Case 0, $K \supseteqq (X_\theta)_{\lambda^m}$ for some $m > 1$. Conjugating by N_λ, we get $K \supseteqq (X_\rho)_{\lambda^m}$ for all $\rho \in \Sigma$ fixed by the twist defining G. Choose such a ρ and a σ not fixed by the twist, such that $(\rho, \sigma) < 0$ (these can be found in Π, for example, joined by the multiple bond in the twisted Dynkin diagram). Denote the images of σ under the twist by σ_1 (and also σ_2 if $G_\lambda = {}^3D_4$). Then $x_\sigma(t)x_{\sigma_1}(t^q)(\cdot x_{\sigma_2}(t^{q^2})) \in K$ for all $t \in GF(q^2)(GF(q^3))$. Since $K \supseteqq \langle (X_\rho)_{\lambda m}, (X_{-\rho})_{\lambda m}\rangle$, $h_\rho(t) \in K$ for all $t \in GF(q^m)$, $t \neq 0$.

If $G_\lambda = {}^3D_4$ and $m \equiv 1 \pmod 3$, then for all $t \in GF(q^3)$ and all $0 \neq u \in GF(q^m)$, we have $(x_\sigma(t)x_{\sigma_1}(t^q)x_{\sigma_2}(t^{q^2}))^{h_\rho(u^{-1})} = x_\sigma(tu)x_{\sigma_1}(t^q u)x_{\sigma_2}(t^{q^2}u) = x_\sigma(tu)x_{\sigma_1}((tu)^{q^m})x_{\sigma_2}((tu)^{q^{2m}}) \in K$. Hence $x_\sigma(v)\,x_{\sigma_1}(v^{q^m})\,x_{\sigma_2}(v^{q^{2m}}) \in K$ for all v of the form $\sum_i t_i u_i$ with $t_i \in GF(q^3)$, $u_i \in GF(q^m)$, that is, for all $v \in GF(q^{3m})$. Thus $(X_\sigma X_{\sigma_1} X_{\sigma_2})_{\lambda m} \subseteqq K$, so $G^s_{\lambda m} \subseteqq K$. The case $m \equiv -1 \pmod 3$ is similar, as is the case $\lambda = {}^2\sigma_q$ and m odd.

If $G_\lambda = {}^3D_4$ and $m \equiv 0 \pmod 3$, we may assume $m = 3$, and must prove $x_\sigma(t) \in K$ for all $t \in GF(q^3)$. Now

$$\begin{aligned} x(t, u) &\equiv x_{\sigma_1}((u^q - u)t^q)x_{\sigma_2}((u^{q^2} - u)t^{q^2}) \\ &= (x_\sigma(tu)x_{\sigma_1}((tu)^q)x_{\sigma_2}((tu)^{q^2}))^{-1}(x_\sigma(t)x_{\sigma_1}(t^q)x_{\sigma_2}(t^{q^2}))^{h_\rho(u^{-1})} \in K \end{aligned}$$

for all $t, u \in GF(q^3)$, so for all $t, u, v \in GF(q^3)$ with $u, v \notin GF(q)$, K contains $x(t, u)^{h_\rho((v^q - v)^{-1}(u^q - u))} \cdot x(t, v)^{-1} = x_{\sigma_2}(y(u, v)t^{q^2})$, where $y(u, v) = (u^{q^2} - u)(v^q - v)(u^q - u)^{-1} - (v^{q^2} - v)$.

Clearly there exist $u, v \in GF(q^3) - GF(q)$ such that $y(u, v) \neq 0$; fixing these and letting t vary, we get $x_{\sigma_2}(t) \in K$ for all $t \in GF(q^3)$, as desired. The case $\lambda = {}^2\sigma_q$, m even, is similar but simpler: $x_{\sigma_1}((u^q - u)t^q) \in K$ for $t, u \in GF(q^2)$, and u may be chosen so $u^q - u \neq 0$.

Case 4. $\Sigma = A^2_n$, $\lambda = {}^2\sigma_q$: For each $\rho \in \Sigma$, let ρ_1 be the image of ρ under the twist. If $\rho \in \Sigma$ and $\rho + \rho_1 \in \Sigma$, then G_λ has a nonabelian "root subgroup" $\{x_\rho(t)x_{\rho_1}(t^q)x_{\rho+\rho_1}(u) \mid t, u \in GF(q^2), t^{1+q} + u + u^q = 0\}$. If $\rho \in \Sigma$ and $\rho + \rho_1 \notin \Sigma$, then G_λ has an abelian root subgroup

$$\{x_\rho(t)x_{\rho_1}(t^q) \mid t \in GF(q^2)\} .$$

There exists $\tau \in \Sigma^+$ such that $\tau + \tau_1 = \theta$. Thus $(X_\theta)_\lambda = \{x_\theta(u) \mid u \in GF(q^2), u + u^q = 0\}$. Choose $0 \neq u_0 \in GF(q^2)$ such that $u_0 + u_0^q = 0$. Then for any $u \in GF(q^2)$, $u + u^q = 0$ if and only if $uu_0^{-1} \in GF(q)$, so $(X_\theta)_\lambda = \{x_\theta(u_0u_1) \mid u_1 \in GF(q)\}$. Let $K_\theta = K \cap \langle X, X_{-\theta}\rangle_\lambda$, so that K_θ contains $(X_\theta)_\lambda$, $(X_{-\theta})_\lambda$, and z. Let $h = h_\theta(u_0) \in H$. Then K^h_θ contains $\{x_{\pm\theta}(u_1) \mid u_1 \in GF(q)\}$, canonical generators of $A_1(q)$, and also contains $z^h = x_\theta(t)$ for some $t \notin GF(q)$. By Case 0, there exists $m > 1$ such that K^h_θ contains $\{x_{\pm\theta}(u_1) \mid u_1 \in GF(q^m)\}$. In particular, K_θ contains $x_{\pm\theta}(u_1)^{h^{-1}} = x_{\pm\theta}(u_0u_1)$ for all $u_1 \in GF(q^m) \cdot h_\theta(u_1) \in K^h_\theta$ for all $u_1 \in GF(q^m)$, so $h_\theta(u_1) = h_\theta(u_1)^{h^{-1}} \in K_\theta$ for all $u_1 \in GF(q^m)$, $u_1 \neq 0$. For any $t, u \in GF(q^2)$ satisfying $t^{1+q} + u + u^q = 0$ and any $u_1 \in GF(q^m)^x$, we conjugate $x_\tau(t)x_{\tau_1}(t^q)x_\theta(u)(\in G_\lambda)$ by $h_\theta(u_1)$ and get

$$x(t, u, u_1) = x_\tau(tu_1)x_{\tau_1}(t^q u_1)x_\theta(uu_1^2) \in K .$$

Suppose m is odd. Then $t^q u_1 = (tu_1)^{q^m}$ and $tu_1(tu_1)^{q^m} + uu_1^2 + (uu_1^2)^{q^m} = tu_1 t^q u_1 + uu_1^2 + u^q u_1^2 = (t^{1+q} + u + u^q)u_1^2 = 0$, so $x(t, u, u_1) \in G_{\lambda^m}$. Now every element of $GF(q^{2m})$ is a sum of elements of the form tu_1 with $t \in GF(q^2)$, $u_1 \in GF(q^m)^x$, so for every $t \in GF(q^{2m})$, K contains an element of the form $x_\tau(t)x_{\tau_1}(t^{q^m})x_\theta(u)$ with $t^{1+q^m} + u + u^{q^m} = 0$. Since K contains $x_\theta(u_0 u_1)$ for all $u_1 \in GF(q^m)$, it contains $x_\theta(v)$ for all $v \in GF(q^{2m})$ satisfying $v + v^{q^m} = 0$. Hence K contains $\{x_\rho(t)x_{\rho_1}(t^{q^m})x_\theta(u) \mid t, u \in GF(q^{2m}), t^{1+q^m} + u + u^{q^m} = 0\}$, a nonabelian root subgroup of G_{λ^m}. Conjugating by N_λ, we see that K contains all nonabelian root subgroups of G_{λ^m}. If $n = 1$, we are therefore done. If $n > 1$, there exists $\gamma \in \Sigma$ such that $\gamma + \gamma_1 \notin \Sigma$ while $\gamma + \theta, \gamma_1 + \theta \in \Sigma$ (for example, $-\gamma \in \Pi$, with $-\gamma$ at an end of the Dynkin diagram). Then for all $t \in GF(q^2)$, $u_1 \in GF(q^m)^x$, we have $x_\gamma(tu_1)x_{\gamma_1}((tu_1)^{q^m}) = x_\gamma(tu_1)x_{\gamma_1}(t^q u_1) = (x_\gamma(t)x_{\gamma_1}(t^q))^{h\theta(u_1)} \in K$. It follows that $x_\gamma(v)x_{\gamma_1}(v^q)^m \in K$ for all $v \in GF(q^{2m})$, so K contains an abelian root subgroup of G_{λ^m}. Hence $K \supseteq G^s_{\lambda^m}$, as required.

Suppose m is even. We may assume $m = 2$, and shall prove $G^s_{\lambda^2} \supseteq K$. Let τ, γ be as in the previous paragraph. For any $t \in GF(q^2)$ and $u_1 \in GF(q^2)^x$, we have $x_1 = x_\gamma(tu_1)x_{\gamma_1}(t^q u_1) = (x_\gamma(t)x_{\gamma_1}(t^q))^{h\theta(u_1)} \in K$, and also $x_2 = x_\gamma(tu_1)x_{\gamma_1}(tu_1)^q) \in G_\lambda \subseteq K$. Hence $x_{\gamma_1}(t^q(u_1^q - u_1)) = x_2 x_1^{-1} \in K$. Fix u_1 such that $u_1^q \neq u_1$ and let t vary; we get $(X_{\gamma_1})_{\lambda^2} \subseteq K$. Similarly, $(X_\gamma)_{\lambda^2} \subseteq K$, so conjugating by N_λ, we get $(X_\rho)_{\lambda^2} \subseteq K$ for all $\rho \in \Sigma$ such that $\rho + p_1 \notin \Sigma$. Also, we have $x_\theta(u_0 u_1) \in K$ for all $u_1 \in GF(q^2)$. Since u_0 was chosen in $GF(q^2)$ and $u_0 \neq 0$, $(X_\theta)_{\lambda^2} \subseteq K$. Hence $(X_\theta)_{\lambda^2} \subseteq K$ for all $\rho \in \Sigma$ with $\rho = \rho_1$. For any $t \in GF(q^2)$ there is $u \in GF(q^2)$ such that $x_3 = x_\tau(t)x_{\tau_1}(t^q)x_\theta(u) \in G_\lambda$. Let $u_1 \in GF(q^2)^x$. Let $x_4 = x_3^{h\theta(u_1)} = x_\tau(tu_1)x_{\tau_1}(t^q u_1)x_\theta(\ ) \in K$ and choose $u' \in GF(q^?)$ such that $x_5 = x_\tau(tu_1)x_{\tau_1}((tu_1)^q)x_\theta(u') \in G_\lambda$. Then $x_{\tau_1}(t^q(u_1^q - u_1)) = x_5 x_4^{-1} x_\theta(\ ) \in K$. As above, we get $(X_{\tau_1})_{\lambda^2} \subseteq K$. Conjugating by N_λ, $(X_\rho)_{\lambda^2} \subseteq K$ for all $\rho \in \Sigma$ such that $\rho + \rho_1 \in \Sigma$. Thus $(X_\rho)_{\lambda^2} \subseteq K$ for all $\rho \in \Sigma$, as required.

Case 5. $\Sigma = C_2$, $\lambda = {}^2\sigma_q$, $q > 2$: Thus $q = 2q_0^2$, $q_0 = 2^j > 1$. We take $\Pi = \{\alpha, \beta\}$, with β short. Let $\mathscr{S}$ be the additive group $k \oplus k$. For $(t_1, t_2) \in \mathscr{S}$, set $x(t_1, t_2) = x_{\alpha+\beta}(t_1)x_{\alpha+2\beta}(t_2)$. For any subgroup J of G set $\mathscr{S}_J = \{(t_1, t_2) \mid x(t_1, t_2) \in J\}$, an additive subgroup of $\mathscr{S}$. Thus $\mathscr{S}_{G_\lambda} = \{(t, t^{2q_0}) \mid t \in GF(q)\}$. Since $z \in Z(U_\lambda) - G_\lambda$, $\mathscr{S}_{G_\lambda} \subset \mathscr{S}_K \subseteq \mathscr{S}_{G_{\lambda^n}}$. Also, let $n_0 = (n_\alpha(1)n_\beta(1))^2 \in G_\lambda$, so that $x_\rho(t)^{n_0} = x_{-\rho}(t)$ for all $\rho \in \Sigma$, $t \in k$, and also $n_0^2 = 1$. Finally, for any $t_1, t_2 \in k^x$, let $h(t_1, t_2)$ be the element of H which takes α to $t_1^2 t_2^{-1}$ and β to $t_1^{-1}t_2$. Thus $x(t_1, t_2)^{h(u_1, u_2)} = x(t_1 u_1, t_2 u_2)$.

Suppose $(t_1, t_2) \in \mathscr{S}_K$ and $t_1 t_2 \neq 0$. We show that $h(t_1, t_2) \in K$. First $C_G(x(t_1, t_2)) \subseteq B$, for if $g \in C_G(x(t_1, t_2))$, we write $g = bnu$ in canonical form and get $x(t_1, t_2)^n \in X_{\alpha+\beta}X_{\alpha+2\beta}$, so $n \in H$ and $g \in B$. On the other hand, $C_U(n_0) = 1$ as $U \cap U^{n_0} = 1$. Hence $x(t_1, t_2)$ and n_0 do not centralize any involution of G in common. If follows that $x(t_1, t_2)$ and n_0 are conjugate in the (dihedral) group $\langle x(t_1, t_2), n_0 \rangle$, hence also in K. Similarly, $x(1, 1)$ and n_0 are conjugate in K. Thus $x(t_1, t_2) = x(1, 1)^g$ for some $g \in K$. Writing g in canonical form, we see $g = uh(t_1, t_2)$ for some $u \in U$. However, $B \cap K = (U \cap K)(H \cap K)$. To see this, choose $t \in GF(q)$, $t \neq 0$ or 1, and let $h = h(t, t^{2q_0}) \in G_\lambda \subseteqq K$. Then $C_U(h) = 1$, so $C_B(h) = H$. By the Schur-Zassenhaus theorem, $B \cap K$ has a subgroup H_0 such that $B \cap K = (U \cap K)H_0$, $U \cap K \cap H_0 = 1$, and $h \in H_0$. Then H_0 is abelian, so $H_0 \subseteqq C_B(h) = H$, so $H_0 = H \cap K$. Since $g \in B \cap K$, $h(t_1, t_2) \in H \cap K \subseteqq K$, as claimed.

Thus, if $(t_1, t_2) \in \mathscr{S}_K$, $(u_1, u_2) \in \mathscr{S}_K$, and $u_1 u_2 \neq 0$, then $(t_1, u_1, t_2 u_2) \in \mathscr{S}_K$.

Suppose now that no element of $\mathscr{S}_K$ has the form $(0, t)$ or $(t, 0)$ with $t \neq 0$. Let $\mathscr{S}_1 = \{t \mid (t, u) \in \mathscr{S}_K$ for some $u\}$, and define the function φ on $\mathscr{S}_1$ by the condition $(t, \varphi(t)) \in \mathscr{S}_K$. Since $\mathscr{S}_1$ is an additive subgroup of $GF(q^n)$, and $GF(q) \subset \mathscr{S}_1$, the last paragraph implies that $\mathscr{S}_1$ is a field, so $\mathscr{S}_1 = GF(q^m)$ for some $m > 1$; also, φ preserves multiplication, so is an automorphism of $GF(q^m)$. Thus for some $d = 2^i$, $d \leqq q^m$, $\mathscr{S}_K = \{(t, t^d) \mid t \in GF(q^m)\}$. Since $\mathscr{S}_{G_\lambda} \subseteqq \mathscr{S}_K$, $t^d = t^{2q_0}$ for all $t \in GF(q)$. Let $x_0 = x_\alpha(1)x_\beta(1)x_{\alpha+\beta}(1)(\in G_\lambda)$. For each $t, u \in GF(q^m)^x$, K contains $[x_0^{h(t,t^d)}, x_0^{h(u,u^d)}] = x(w_1, w_2)$ where $w_1 = t^{2-d}u^{d-1} + u^{2-d}t^{d-1}$, $w_2 = t^{2-d}u^{2d-2} + u^{2-d}t^{2d-2}$. By the above $w_2 = w_1^d$. In the special case $u = 1$ this yields $(t^{-d} + t^{-d^2+2d-2})(t^{d^2} + t^2) = 0$. Fix t. We wish to show $t^{d^2} + t^2 = 0$. Suppose $t^{d^2} + t^{3d-2} = 0$. For any $u \in GF(q)$, $u^d = u^{2q_0}$; with the equation $w_2 = w_1^d$, this gives $(t^{2-d} + t^{2d-2})(u^{1-q_0} + u^{2q_0-1})^2 = 0$ for all $u \in GF(q)^x$. Since $q > 2$, also $q - 1 > 3q_0 - 2$, so for suitable u, the right hand factor does not vanish. Thus $t^{2-d} = t^{2d-2}$. Hence $t^2 + t^{d^2} = t^2 + t^{3d-2} = 0$ anyway. So $t^2 = t^{d^2}$ for all $t \in GF(q^m)$. Let $d_0 = 1/2d$; then $t^{2d_0^2} = t$, which implies that m is odd and $H \cap K \supseteqq \{h(t, t^{2d_0}) \mid t \in GF(q^m)\} = H_{\lambda m}$. Conjugating elements of U_λ by those of $H_{\lambda m}$, we find $U_{\lambda m} \subseteqq K$, so $K \supseteqq \langle U_{\lambda m}, n_0 \rangle = G^s_{\lambda m}$.

Finally, suppose $\mathscr{S}_K$ contains an element of the form $(t, 0)$ or $(0, t)$ for some $t \neq 0$. We show that $K \supseteqq G_{\lambda^2}$. This is equivalent to $K^\lambda \supseteqq G_{\lambda^2}$, so without loss we may assume $(0, t) \in \mathscr{S}_K$, i.e., $x_{\alpha+2\beta}(t) \in K$. Then $K \supseteqq \langle x_{\alpha+2\beta}(t), n_0 \rangle$ so $g = n_0(1)x_{\alpha+2\beta}(t) = n_\alpha(1)n_{\alpha+2\beta}(1)x_{\alpha+2\beta}(t) \in K$. A 2×2 matrix calculation shows that $n_{\alpha+2\beta}(1)x_{\alpha+2\beta}(t)$ has odd order e. Since it commutes with $n_\alpha(1)$, $n_\alpha(1) = n_\alpha(1)^e = g^e \in K$. For any $u, v \in GF(q)$, $x(u, u^{2q_0}) \in K$ and $x_0(v) = x_\alpha(v)x_\beta(v^{q_0})x_{\alpha+\beta}(v^{1+q_0}) \in K$, so $x(uv, u^2v) = [x(u, u^{2q_0})^{n_\alpha(1)}, x_0(v)] \in K$. Replacing u by uv and v by 1, we get $x(uv, u^2v^2) \in K$, so $x_{\alpha+2\beta}(u^2(v^2 + v)) \in K$. Since $q > 2$, v exists with $v^2 + v \neq 0$; this gives $(X_{\alpha+2\beta})_{\lambda^2} \subseteqq K$. It follows easily that $(X_{\alpha+\beta})_{\lambda^2} \subseteqq K$. Hence $n_{\alpha+\beta}(1) \in \langle (X_{\alpha+\beta})_{\lambda^2}, n_0 \rangle \subseteqq K$, so $K \supseteqq \langle (X_{\alpha+\beta})_{\lambda^2}, n_\alpha(1), n_{\alpha+\beta}(1), n_0 \rangle = G_{\lambda^2}$.

Case 6. $\Sigma = F_4$, $\lambda = {}^2\sigma_q$: Here $q = 2q_0^2$, $q_0 = 2^j$. We notate elements of Σ as in Lemma 2.1. Then Σ^+ is partitioned into 4 subsets giving root subgroups of U_λ of type ${}^2C_2$ ({0100, 0010, 0110, 0210}, {0011, 1100, 1111, 2211}, {0211, 1110, 1321, 2431}, and {0111, 2210, 2321, 2432}) and 4 subsets giving root subgroups of type A_1 ({1000, 0001}, {1210, 0221}, {1211, 2221}, and {1221, 2421}). $Z(U) = X_{2321}X_{2432}$. Let $\mathscr{S} = k \oplus k$, for each $(t_1, t_2) \in \mathscr{S}$ set $x(t_1, t_2) = x_{2321}(t_1)x_{2432}(t_2)$, and for each subgroup J of G set $\mathscr{S}_J = \{(t_1, t_2) \in \mathscr{S} \mid x(t_1, t_2) \in J\}$. Thus $\mathscr{S}_{G_\lambda} = \{(t, t^{2q_0}) \mid t \in GF(q)\}$, where $q = 2q_0^2$, and $\mathscr{S}_{G_\lambda} \subset \mathscr{S}_K \subseteqq \mathscr{S}_{G_{\lambda^n}}$.

We show that if $(t_1, t_2), (u_1, u_2) \in \mathscr{S}_K$, then $(t_2u_1, t_1^2u_2) \in \mathscr{S}_K$. Namely, conjugating $x(t_1, t_2)$ and $x(u_1, u_2)$ by appropriate elements of N_λ ($\subseteqq K$), we get $x_{0110}(t_1)x_{0210}(t_2), x_{1111}(u_1)x_{2211}(u_2) \in K$, so $x(t_2u_1, t_1^2u_2) = [x_{0110}(t_1)x_{0210}(t_2), x_{1111}(u_1)x_{2211}(u_2), x_{1000}(1)x_{0001}(1)] \in K$. In particular, since $(1, 1) \in \mathscr{S}_K$, the map $\varphi: (t_1, t_2) \rightarrow (t_2, t_1^2)$ is a permutation of $\mathscr{S}_K$. For $(t_1, t_2), (u_1, u_2) \in \mathscr{S}_K$, let $(z_1, z_2) = \varphi^{-1}(t_1, t_2)$. Then $(t_1u_1, t_2u_2) = (z_2u_1, z_1^2u_2) \in \mathscr{S}_K$, so $\mathscr{S}_K$ is closed under multiplication. Since φ maps $\mathscr{S}_K$ to itself, $\mathscr{S}_K \subseteqq GF(q^m) \oplus GF(q^m)$ for some m, and $\mathscr{S}_K$ projects onto both summands.

If $\mathscr{S}_K$ contains no element of the form $(0, t)$ or $(t, 0)$ for $t \neq 0$, then the map $\psi: GF(q^m) \rightarrow GF(q^m)$ defined by $(t, \psi(t)) \in \mathscr{S}_K$ is an automorphism of $GF(q^m)$, so $\mathscr{S}_K = \{(t, t^d) \mid t \in GF(q^m)\}$ for some $d = 2^i$. Since $\mathscr{S}_{G_\lambda} \subset \mathscr{S}_K$, $m > 1$. Since $\varphi(t, t^d) = (t^d, t^2) \in \mathscr{S}_K$, we get $t^{d^2} = t^2$ for all $t \in GF(q^m)$. Hence m is odd and K contains $(Z(U))_{\lambda^m}$. Conjugating by N_λ, we see that K contains$(Z\ (U_\rho))_{\lambda^m}$ for any nonabelian root subgroup U_ρ of U. Hence for all $t \in GF(q^m)$, K contains

$$[x_{0110}(t)x_{0210}(t^d), x_{1111}(1)x_{2211}(1)] ,$$

which, modulo terms in $(Z(U_\rho))_{\lambda^m}$ for various nonabelian U_ρ, equals $x_{1221}(t)x_{2421}(t^d)$. Thus K contains $(U_\rho)_{\lambda^m}$ for all abelian root subgroups U_ρ. Hence $K \supseteqq \langle (X_{1000}X_{0001})_{\lambda^m}, N_\lambda \rangle \supseteqq \{h_{1000}(t)h_{0001}(t^d) \mid t \in GF(q^m)\}$. Conjugating $x_{0100}(1)x_{0010}(1)x_{0110}(1) (\in G_\lambda)$ by these element yields

$$(X_{0100}X_{0010}X_{0110}X_{0210})_{\lambda^m} \subseteqq K .$$

Hence $K \supseteqq U_{\lambda^m}$, so $K \supseteqq G^s_{\lambda^m}$.

If $\mathscr{S}_K$ contains an element of the form $(t, 0)$ or $(0, t)$ with $t \neq 0$, then since φ maps $\mathscr{S}_K$ to $\mathscr{S}_K$, $\mathscr{S}_K \supseteqq GF(q) \oplus GF(q)$. Hence K contains $(Z(U_\rho))_{\lambda^2}$ for all nonabelian root subgroups U_ρ of U. From the commutator $[x_{0110}(t), x_{1111}(1)]$ we see that K contains $(U_\rho)_{\lambda^2}$ for all abelian root subgroups U_ρ of U. If $q > 2$, we apply the argument of case 5 to the group generated by a nonabelian root group and its negative, and conclude that $(U_\rho)_{\lambda^2} \subseteqq K$ for all nonabelian root groups U_ρ, whence $G^s_{\lambda^2} \subseteqq K$. If $q = 2$, a direct examination of $C_2(2) (\cong S_6$, the symmetric group) shows that ${}^2C_2(2)$ and a Sylow 2-center generate $C_2(2)$, whence $(U_\rho)_{\lambda^2} \subseteqq K$ for all nonabelian root groups U_ρ, so again

$G^s_{\lambda^2} \subseteq K$. This completes the proof of Lemma 2.5.

(2.4) *Proof. Second part.* We continue with the assumptions given in (2.3). As a consequence of Lemma 2.5 we have a unique $\mu = \lambda^r$ such that $G^s_\mu \subseteq M$ and $U_\mu \in \mathrm{Syl}_p(M)$. Put $K = G_\mu \cap M$. In this sub-section we will show that $K = M$. Apart from the ${}^2G_2$-case this will complete the proof of the theorem.

We use induction on the rank of G. The first step is when G is of type A_1. Since $\mu \neq \sigma_2, \sigma_3$ we see from [6] that in this case $K = M$.

The induction will be applied to the components of semi-simple groups which occur in parabolic subgroups of G and, when $p \neq 2$, in centralizers of involutions in G. Since such components may have the same rank as G we perform the same rank as G we perform the induction among groups of the same rank in the following order,

$$A < (C, D, G) < (B, E) < F .$$

This partial ordering insures that the induction procedure is valid when the above described subgroups hare the same rank as G.

To begin, we review some elementary facts. Let $\tilde{S}$ be a connected, semi-simple, algebraic group and μ an endomorphism of $\tilde{S}$ onto itself with $\tilde{S}_\mu$ finite. Since μ must permute the components of $\tilde{S}$ we have a unique decomposition $\tilde{S} = \tilde{F}_1\tilde{F}_2 \cdots$ where $\tilde{F}_i \cap \tilde{F}_j \subseteq Z(\tilde{S})$ for $i \neq j$ and each $\tilde{F}_i$ has the form

$$\tilde{S} = \tilde{A}\mu(\tilde{A}) \cdots \mu^{n-1}(\tilde{A})$$

with $\mu^n(\tilde{A}) = \tilde{A}$ and $\tilde{A}$ a component of $\tilde{S}$.

For $\tilde{X}$ one of $\tilde{S}$, $\tilde{F}$, $\tilde{A}$ put $X = \tilde{X}/Z(\tilde{X})$ and note that μ is naturally defined on S and F and μ^n on A. It is easily seen that $F^s_\mu \cong A^s_{\mu^n}$ and that the images of $\tilde{S}^s_\mu$ and $N_{\tilde{S}}(\tilde{S}^s_\mu)$ in S are, using an obvious extension of Lemma 1.2, respectively S^s_μ and S_μ.

The purpose of the next lemma is to extend the conclusion of Theorem 1 to the case where G is replaced by a semi-simple group $\tilde{S}$. This lemma is used in the proofs of Lemmas 2.8 and 2.9. In the situations there the assumption (i) below will hold because of our induction hypothesis.

LEMMA 2.6. *Let $\tilde{S}$ be a connected, semi-simple, algebraic group and μ an endomorphism of $\tilde{S}$ onto itself with $\tilde{S}_\mu$ finite. For a component $\tilde{A}$ of $\tilde{S}$ put $A = \tilde{A}/Z(\tilde{A})$. Assume that*

(i) *For each component $\tilde{A}$ of $\tilde{S}$ the conclusion of Theorem 1 holds with G replaced by A and λ replaced by μ^n, where n is the length of the μ-orbit containing $\tilde{A}$.*

(ii) *$\tilde{L}$ is a finite subgroup of $\tilde{S}$ satisfying $\tilde{S}^s_\mu \subseteq \tilde{L}$ and $|\tilde{L}: \tilde{S}^s_\mu|_p = 1$.*

Then $\tilde{L}$ normalizes $\tilde{S}^s_\mu$.

Proof. Put $S = \tilde{S}/Z(\tilde{S})$ and $L = \tilde{L}Z(\tilde{S})/Z(\tilde{S})$ then since $N_{\tilde{S}}(\tilde{S}^s_\mu)Z(\tilde{S})/Z(\tilde{S}) = S_\mu$ it suffices to show that $L \subseteq S_\mu$.

Suppose first that the components of S form a single μ-orbit. Thus $S = A \times B$ where A is a component and $B = \mu(A) \times \cdots \times \mu^{n-1}(A)$ and $\mu^n(A) = A$. If $n = 1$ then $B = 1$. Now $BL \cap A$ is finite and $BS^s_\mu \cap A = A^s_{\mu^n}$ and hence $|BL \cap A: A^s_{\mu^n}|_p = 1$. By assumption (i) we have $BL \cap A \subseteq A_{\mu^n}$. Hence L normalizes S^s_μ and so $L \subseteq S_\mu$.

We now use induction on the number of μ-orbits of components in S. Suppose $S = E \times F$ where E, F are nontrivial products of μ-orbits. Then $S_\mu = E_\mu \times F_\mu$ and $S^s_\mu = E^s_\mu \times F^s_\mu$. Again we have $EL \cap F$ finite and $ES^s_\mu \cap F = F^s_\mu$ and hence $|EL \cap F: F^s_\mu|_p = 1$. By induction $EL \cap F \subseteq F_\mu$. Similarly $FL \cap E \subseteq E_\mu$. Hence $L \subseteq (EL \cap F) \times (FL \cap E) \subseteq F_\mu \times F_\mu = S_\mu$.

NOTE. In the two situations where the above lemma is used assumption (i) fails to hold only if A, μ^n are one of the 3 exceptional cases described in (2.1). Furthermore $n = 1$ except in one special occurrence in Lemma 2.8 with $G^s_\mu = {}^2F_4(2)$ and $\tilde{S}$ of type $A_1 \times A_1$. If $\tilde{S}$ has an orbit $\tilde{E}$ containing a component $\tilde{A}$ such that A, μ^n do not satisfy assumption (i) we call this an *exceptional orbit* (and $\tilde{E} = \tilde{A}$ except for one case). From the last step of the above proof we see that if $\tilde{E}$ is an exceptional orbit the conclusion of the lemma still holds provided $FL \cap E$ normalizes E^s_μ. Now $L \cap E \trianglelefteq FL \cap E$ and by inspection of the cases in (2.2) we conclude that if $L \cap E$ normalizes E^s_μ then $FL \cap E$ must also normalize E^s_μ. We may conclude that if $\tilde{E}$ is an exceptional orbit of $\tilde{S}$ then the conclusion of the lemma still holds provided $\tilde{L} \cap \tilde{E}$ normalizes $\tilde{E}^s_\mu$.

LEMMA 2.7. *$M \cap B = K \cap B$.*

Proof. Since $U_\mu \in \mathrm{Syl}_p(M)$ we have $M \cap U = K \cap U$ and hence $M \cap B = N_M(U_\mu)$, using Lemma 2.3. Let $g \in M \cap B$, since $B_\mu = H_\mu U_\mu$ we may suppose that $g = hz$ where $h \in H_\mu$ and $z \in Z(U)$. If $h \in M$ then $z \in Z(U) \cap M \subseteq U_\mu$ and so $g \in K$.

If $h \notin M$ we argue as follows. First suppose $Z(U)$ is 2-dimensional. In such a case it is is always true that $G_\mu = G^s_\mu$ and hence $H_\mu \subseteq M$. Thus we may suppose that $Z(U)$ is one-dimensional. Thus $Z(U) = \langle x_\theta(t) | t \in k \rangle$ where θ is the root of maximal height in Σ^+. If G is not of type A_1 or C_l, $l \geqq 2$, then θ is either a fundamental weight or for A_l, $l \geqq 2$, the sum of two distinct fundamental weights. This implies that there exists $h_1 \in H \cap G_\mu^s$ such that $h_1(\theta) = h(\theta)$ and hence $[h_1^{-1}h, z] = 1$ (here we identify H with Hom (Γ, k^*)). Since $H \cap G_\mu^s \subseteqq H_\mu \cap M$, $h_1^{-1}hz \in M \cap B$ and since $h_1^{-1}h$ and z have coprime orders $z \in M \cap B$. Hence $z \in U_\mu$ and again $g \in K$.

If G is of type A_1 we quote L. Dickson [6].

If G is of type C_l let $z = x_\theta(t)$ for some fixed $t \in k$, where $\theta = \alpha_1 + 2\alpha_2 + \cdots + 2\alpha_l$. We may choose $h_1 \in H \cap G_\mu^s$ such that if $h_2 = h_1 h$ then, for some $s \in k^*$,

$$h_2(\alpha_1) = s \quad h_2(\alpha_2) = \cdots = h_2(\alpha_l) = 1 .$$

Let $w_i \in W$ denote the reflection corresponding to $\alpha_i \in \Pi$. Put $n_i = n_{w_i} \in N$ and $n = n_2 \cdots n_l$. It is easily checked that $nh_2zn^{-1} = h_2x_{\alpha_1}(\pm t) \in M \cap B$. Now $h_2x_{\alpha_1}(\pm t)h_2x_\theta(t) = h_2^2x_{\alpha_1}(\pm s^{-1}t)x_\theta(t)$ and since $h_2^2 \in M$ therefore $x_{\alpha_1}(\pm s^{-1}t)x_\theta(t) \in M$. Since $M \cap U = U_\mu$ we have $z = x_\theta(t) \in U_\mu$ and so $g \in K$.

Let X be a subgroup of the finite group Y. Recall that X is said to be *strongly p-embedded* in Y if $|X \cap X^y|_p = 1$ for all $y \in Y - X$. Using Sylow's theorems we see that X is strongly p-embedded in Y if and only if $N_Y(T) \subseteqq X$ for all $1 \neq T \subseteqq S$ where $S \in \mathrm{Syl}_p(X)$. The 'only if' part is clear. Conversely, take $y \in Y - X$ and assume $p \mid |X \cap X^y|$. Let $P \in \mathrm{Syl}_p(X \cap X^y)$. Then $N_Y(P) \subseteqq X$, so that $P \in \mathrm{Syl}_p(X^y)$. Therefore $P, P^{y^{-1}} \in \mathrm{Syl}_p(X) \subseteqq \mathrm{Syl}_p(Y)$ as well. Choose $x \in X$ with $P = P^{yx}$. Thus $yx \in N_Y(P) \subseteqq X$, so that $y \in X$, as required.

LEMMA 2.8. *K is strongly p-embedded in M.*

Proof. Let $1 \neq T_\mu$ then a theorem of A. Borel and J. Tits [4] implies the existence of a parabolic subgroup $P \subset G$ such that P is fixed by μ and $N_G(T) \subseteqq P$. Without restriction we may suppose $B \subseteqq P$. If $P \subseteqq B$ by Lemma 2.7 we have $N_\mu(T) \subseteqq K$. If $P \neq B$ let $R =$ radical of P and put $\tilde{S} = P/R$. $\tilde{S}$ is a connected, semi-simple, algebraic group and μ acts naturally on it. Put $\tilde{M} = (M \cap P)R/R$, $\tilde{K} = (K \cap P)R/R$ then $\tilde{S}_\mu^s \subseteqq \tilde{K} \subseteqq N_{\tilde{S}}(\tilde{S}_\mu^s)$. If $\tilde{S}$ has no exceptional orbits Lemma 2.6 says that $\tilde{M}$ normalizes $\tilde{K}$. By Lemma 2.7, since $R \subseteqq B$, we have $M \cap R = K \cap R$. Hence $M \cap P$ normalizes $K \cap P$ and so, again using Lemma 2.7, $M \cap P = (K \cap P)N_{M \cap P}(U_\mu) = K \cap P$. Hence K is strongly p-embedded in M.

Suppose next that $\tilde{A}$ is an exceptional orbit in $\tilde{S}$. By the note following Lemma 2.6 we must show that $\tilde{M} \cap \tilde{A}$ normalizes $\tilde{K} \cap \tilde{A}$.

Let V be the unipotent radical of P and put $W = V/V'$. Let W_μ be the image V_μ in W. Since V' is closed and connected an argument similar to that in Lemma 2.3 shows that W_μ is just the fixed points of the endomorphism $vV' \to \mu(v)V'$, $v \in V$, of W.

Now $V_\mu = K \cap V = M \cap V$ so $\tilde{M} \cap \tilde{A}$ normalizes W_μ. Hence for all $k \in \tilde{M} \cap \tilde{A}$, $k^{-1}\mu(k)$ centralizes W_μ. Our aim is to show that $C_{\tilde{A}}(W_\mu) \subseteq Z(\tilde{A})$. This will immediately give $\tilde{M} \cap \tilde{A} \subseteq N_{\tilde{A}}(\tilde{A}_\mu)$ and since $N_{\tilde{A}}(\tilde{A}_\mu) = N_{\tilde{A}}(\tilde{K} \cap \tilde{A})$ we are done.

To compute $C_{\tilde{A}}(W_\mu)$ we may suppose P is maximal, subject to $\mu(P) = P$. Let Δ be a proper subset of Π such that $\Pi - \Delta$ contains no proper μ-invariant subset (note that μ permutes Π) then

$$P = \langle x_\gamma(t) \mid \gamma \in \Sigma^+ \text{ or } -\gamma \in \Delta,\, t \in k \rangle$$

and the choice of Δ is further restricted by requiring $\tilde{A}$ to be a component of $\tilde{S} = P/R$. The possible cases are easily listed: except when G_μ^s is ${}^2A_l(l = \text{odd})$, ${}^3D_4$, ${}^2F_4$. $\Pi - \Delta$ is a single root, say α, and $\tilde{A}$ is the image modulo R of $\langle x_\beta(t), x_{-\beta}(t) \mid t \in k \rangle$ some $\beta \in \Delta$. In this case an $\tilde{A}$-invariant, μ-invariant submodule W_1 of W has basis

$$\{x_\gamma(1) \mid \gamma = \alpha, \alpha + \beta, \alpha + 2\beta, \cdots\} \bmod V' .$$

It is easily seen that $C_{\tilde{A}}((W_1)_\mu) \subseteq Z(\tilde{A})$.

When $|\Pi - \Delta| \geqq 2$, $\tilde{A}$ is again of type A_1 except for the ${}^2F_4$ case when $\tilde{A}$ is either of types $A_1 \times A_1$ or C_2. Again a suitable $\tilde{A}$- and μ-invariant sub-module $W_1 \subseteq W$ is easily found such that $C_{\tilde{A}}((W_1)_\mu) \subseteq Z(\tilde{A})$. For example in the ${}^2F_4$ case with $\tilde{A}$ the image modulo R of $\langle x_\beta(t) \mid \beta = \pm\alpha_1, \pm\alpha_4, t \in k \rangle$ let W_1 have basis

$$\{x_\gamma(1) \mid \gamma = \alpha_2, \alpha_3, \alpha_1 + \alpha_2, \alpha_3 + \alpha_4\}$$

then $(W_1)_\mu$ has basis $\{x_{\alpha_2}(1)x_{\alpha_3}(1), x_{\alpha_1+\alpha_2}(1)x_{\alpha_3+\alpha_4}(1)\}$.

LEMMA 2.9. *K is strongly 2-embedded in M.*

Proof. By Lemma 2.8 we may suppose $p \neq 2$. If the lemma is false then there exists a $t \in \operatorname{Inv}(K \cap K^m)$ for some $m \in M - K$. Now $C_G(t)$ contains a unique, maximal, semi-simple, connected algebraic $\tilde{S}$, [18]. Since we may suppose G is not of type A_1, $\tilde{S} \neq 1$. Since $\mu(t) = t$, μ normalizes $\tilde{S}$ and hence $\tilde{S}_\mu^s \subseteq \tilde{S} \cap K \subseteq \tilde{S} \cap M$.

Since all p-elements of $C_G(t)$ lie in $\tilde{S}$ we have $|\tilde{S} \cap K^m|_p \neq 1$. By Lemma 2.8 $|K \cap K^m|_p = 1$ and hence $O^{p'}(\tilde{S} \cap M) \not\subseteq \tilde{S} \cap K$. However if $\tilde{S}$ contains no exceptional orbits Lemma 2.6 implies $O^{p'}(\tilde{S} \cap M) \subseteq \tilde{S} \cap K$, contradiction.

If $\tilde{A}$ is an exceptional orbit of $\tilde{S}$ then $\tilde{A}$ is of type A_1 and $p = 3$. If $\tilde{A} \cap M$ does not normalize $\tilde{A} \cap K$ then from the list of exceptional cases in (2.2) we see that $\tilde{A} \cap K$ is not strongly 3-embedded in $\tilde{A} \cap M$. But then K is not strongly 3-embedded in M, contradicting Lemma 2.8.

LEMMA 2.10. $K = M$.

Proof. Suppose $K \neq M$, by Lemma 2.9 and a theorem of H. Bender [2] either the Sylow 2-subgroup of K is cyclic or quaternion or K is solvable. Using ref. [8], [12] and a theorem of Burnside we see that K has no non-abelian simple subgroups. Since K contains $[G_\mu^s, G_\mu^s]$ it follows that G_μ is ${}^2A_2(2)$.

Let $t \in \operatorname{Inv} K$ then $K = O_{2'}(K)C_K(t)$ and $O_{2'}(C_K(t)) = 1$. By Lemma 2.9 $C_K(t) = C_M(t)$ and so by [12], $M = O_{2'}(M)C_K(t)$. Then $O_{2'}(K) \subseteqq O_{2'}(M)$ and $C_{O_{2'}(M)}(t) \subseteqq O_{2'}(C_K(t)) = 1$ so $O_{2'}(M)$ is abelian. Hence $M \subseteqq N_G(O_{2'}(K))$ and now a direct calculation yields $N_G(O_{2'}(K)) = G_\mu$. So $K = M$, a contradiction.

(2.5) *Proof.* ${}^2G_2$*-case.* In this subsection G is of type G_2 and $\lambda = {}^2\sigma_q$ where $q = 3q_0^2$, $q_0 = 3^f$. For this case we give a direct proof of the theorem by analyzing the structure of $C_M(j)$ where j is an involution in G_λ.

Proof. We let μ be the highest power of λ such that $G_\mu \subseteqq M$, and show that $M = G_\mu$. Without loss, we may assume $\mu = \lambda$, since the various powers of λ are ${}^2\sigma_{qm}$ and σ_{qm}, and the σ_{qm}-case has already been done.

We take $\Pi = \{\alpha, \beta\}$, with α long and choose notation so the commutator formulas are as in [15]. Let j be the element of H such that $j(\alpha) = j(\beta) = -1$ and let $C = C_G(j)$. Thus $\ker j \cap \Sigma^+ = \{\alpha + \beta, \alpha + 3\beta\}$, so $C = L_1L_2$, where $L_1 = \langle X_{\alpha+\beta}, X_{-\alpha-\beta}\rangle$, $L_2 = \langle X_{\alpha+3\beta}, X_{-\alpha-3\beta}\rangle$, $[L_1, L_2] = 1$, $L_1 \cap L_2 = Z(C) = \langle j\rangle$, and each L_i is isomorphic to $SL_2(k)$. Clearly $j \in G_\lambda$. For any subgroup J of G let $C_J = C_J(j)$.

Put $x_+^*(t) = x_{\alpha+\beta}(t)x_{\alpha+3\beta}(t^{3q_0})$ and define $x_-^*(t)$ similarly, and let $L = \langle x_+^*(t), x_-^*(t) \mid t \in GF(q)\rangle$. Then $L \cong PSL_2(q)$ and $C_{G_\lambda} = L \times \langle j\rangle$.

Suppose $C_M \subseteqq N_C(C_{G_\lambda})$. Let T_{G_λ}, T_M, and T_N be Sylow 2-subgroups of C_{G_λ}, C_M, and $N_C(C_{G_\lambda})$, respectively, such that $T_{G_\lambda} \subseteqq T_M \subseteqq T_N$. An easy computation shows $N_C(C_{G_\lambda}) = T_NC_{G_\lambda}, T_N$ is nonabelian of order 16, T_{G_λ} is elementary abelian of order 8, and $|N_{G_\lambda}(T_{G_\lambda})/C_{G_\lambda}(T_{G_\lambda})| = 21$. If $T_M = T_N$, then $|N_M(T_{G_\lambda})/C_M(T_{G_\lambda})| = 42$, which is absurd since $GL(3, 2)$ has no subgroups of order 42. Thus $T_M \subset T_N$, so $C_M = T_MC_{G_\lambda} = C_{G_\lambda}$. By a theorem of Walter [28], $|M| = |G_\lambda|$, so $M = G_\lambda$, as required. Thus, we may assume $C_M \not\subseteqq N_C(C_{G_\lambda})$.

Let $\bar{C} = C/\langle j\rangle$, and for any $A \subseteqq C$ write $\bar{A}$ for $A\langle j\rangle/\langle j\rangle$. Then $\bar{C} = \bar{L}_1 \times \bar{L}_2$, $\bar{L}_i$ isomorphic to $PSL_2(k)$. Let π_i, $i = 1, 2$, be the projection $\bar{C}$ on $\bar{L}_i$.

Suppose $\pi_1(\bar{L}) \subseteqq \bar{C}_M$. Since $\bar{L} \subseteqq \bar{C}_M$, also $\pi_2(\bar{L}) \subseteqq \bar{C}_M$. Since $j \in C_M$, we get $x_\rho(t) \in M$ for $\rho = \pm(\alpha + \beta)$, $\pm(\alpha + 3\beta)$, and all $t \in GF(q)$. In particular, $n_{\alpha+\beta}(1) \in M$. Now U_λ contains an element

$$x = x_\alpha(1)x_\beta(1)\cdots,$$

so M contains $[x, x_{\alpha+3\beta}(t)] = x_{2\alpha+3\beta}(\pm t)$ for all $t \in GF(q)$. Conjugating by N_λ, we find $x_{-2\alpha-3\beta}(t) \in M$ for all $t \in GF(q)$. Hence M contains $n_{2\alpha+3\beta}(1)$. Since $W = \langle w_{\alpha+\beta}, w_{2\alpha+3\beta}\rangle$, M covers N/H. As $\langle (X_{\alpha+\beta})_{\lambda^2}, (X_{\alpha+3\beta})_{\lambda^2}\rangle \subseteqq M$, it follows that $G_{\lambda^2} \subseteqq M$. Thus, we may assume $\pi_1(\bar{L}) \not\subseteqq \bar{C}_M$, and similarly, $\pi_2(\bar{L}) \not\subseteqq \bar{C}_M$.

Suppose next that $\pi_1(\bar{C}_M)$ is not solvable. Now $\pi_1(\bar{L}) = (\bar{L}_1)^s_\lambda 2$, so either $\pi_1(\bar{C}_M)^s = (\bar{L}_1)^s_{\lambda 2m}$ for some m, or else $q = 3$ and $\pi_1(\bar{C}_M) \cong A_5$, the alternating group. To see this observe that since $\pi_1(\bar{C}_M)$ is finite its inverse image in L_1 is a finite subgroup of $SL_2(k)$ and so is conjugate in $GL_2(k)$ to a subgroup of $SL_2(3^f)$ for some f. Hence for purposes of identifying $\pi_1(\bar{C}_M)$ up to isomorphism, we may assume it lies in $SL_2(3^f)$. If $3^2 \nmid |\pi_1(\bar{C}_M)|$, the argument of Lemma 2.4 shows that $\pi_1(\bar{C}_M) \subseteqq (\bar{L}_1)_{\lambda 2n}$ for some n and Dickson's results [6] may be used. While if $3^2 \nmid |\pi_1(\bar{C}_M)|$, these results imply $\pi_1(\bar{C}_M) \cong A_5$.

If $\pi_1(\bar{C}_M) \cong A_5$, then $\bar{C}M \cap \bar{L}_1 \lhd \pi_1(\bar{C}_M)$ and $\pi_1(\bar{L}) \not\subseteqq \bar{C}_M$ imply $\bar{C}_M \cap \bar{L}_1 = 1$. Hence $\pi_2(\bar{C}_M)/\bar{C}_M \cap \bar{L}_2 \cong A_5$, so $\pi_2(\bar{C}_M)$ is nonsolvable. Applying the above argument to $\pi_2(\bar{C}_M)$ yields $\pi_2(\bar{C}_M) \cong A_5$, hence $\bar{C}_M \cong A_5$, so $C_M \cong Z_2 \times A_5$. Since M contains $G_\lambda \cong {}^2G_2(3)$, all involutions in C_M are M-conjugate in this case, so by a theorem of Janko [19], $3^2 \nmid |M|$, which is absurd as $G_\lambda \subseteqq M$.

Hence, $\pi_1(\bar{C}_M)^s = (\bar{L}_1)^s_{\lambda 2m}$. Since we are assuming that $\pi_1(\bar{C}_M)$ is not solvable this group is simple, so as in the A_5 case we get $\pi_2(\bar{C}_M)^s = (\bar{L}_2)^s_\lambda 2m$, $\bar{C}^s_M \cap \bar{L}_1 = \bar{C}^s_M \cap \bar{L}_2 = 1$. If $m = 1$, then $\bar{L} \subseteqq \bar{C}_M$ implies $\bar{L} = \bar{C}^s_M$, so $\bar{C}_M \subseteqq N_G(\bar{L})$, contrary to what was shown above. Hence $m > 1$. Now $\bar{C}^s_M$ is defined by an isomorphism between the $\pi_i(\bar{C}_M)^s$, which restricts on $\pi_i(\bar{L})$ to $x_{\pm(\alpha+\beta)}(t) \leftrightarrow x_{\pm(\alpha+3\beta)}(t^{3q_0})$. From the well-known classification of automorphisms of PSL_2 there exists $d = 3^i$ such that $\bar{C}^s_M = \langle \bar{x}^*_\pm(t) \mid t \in GF(q^m)\rangle$, where we define $x^*_+(t) = x_{(\alpha+\beta)}(t)x_{(\alpha+3\beta)}(t^d)$ and x^*_- is defined similarly. (This extends previous notation; $t^d = t^{3q_0}$ for $t \in GF(q)$.) Hence $C^s_M = \langle x^*_\pm(t) \mid t \in GF(q^m)\rangle$. Set $h^*(t) = h_{\alpha+\beta}(t)h_{\alpha+3\beta}(t^d)$. Since $[L_1, L_2] = 1$, C^s_M contains $h^*(t)$ for all $t \in GF(q^m)$.

Let x, y and z be elements of G_λ of the form $x = x_\alpha(1)x_\beta(1)\cdots$, $y = x_{\alpha+\beta}(1)x_{\alpha+3\beta}(1)\cdots$, $z = x_{\alpha+2\beta}(1)x_{2\alpha+3\beta}(1)$, then for any $t, u \in GF(q^m)^x$, M contains the following elements:

(1) $$x^{h^*(t)} = x_\alpha(t^{3-d})x_\beta(t^{d-1})\cdots,\ y^{h^*(u)} = x_{\alpha+\beta}(u^2)x_{\alpha+3\beta}(u^{2d})\cdots$$

(2) $$[x^{h^*(t)}, y^{h^*(u)}] = x_{\alpha+2\beta}(t^{d-1}u^2)x_{2\alpha+3\beta}(t^{3-d}u^{2d}).$$

Since every element of $GF(q^m)$ is a sum of square, M contains

(3) $$x_{\alpha+2\beta}(t^{d-1}u)x_{2\alpha+3\beta}(t^{3-d}u^d).$$

Replacing u by ut^{d-1} and t by 1 in (3), and multiplying the resulting element by the inverse of (3), we get

$$(4)\qquad x_{2\alpha+3\beta}((t^{3-d} - t^{d^2-d})u^d) \in M .$$

Also, M contains

$$(5)\qquad [x^{h^*(t)}, x] = x_{\alpha+\beta}(t^{3-d} - t^{d-1})x_{\alpha+3\beta}(t^{3d-3} - t^{3-d}) \cdots .$$

Suppose $t_0^{d^2} \neq t_0^3$ for some $t_0 \in GF(q^m)$. From (4), $x_{2\alpha+3\beta}(t) \in M$ for all $t \in GF(q^m)$, and then from (3), $x_{\alpha+2\beta}(t) \in M$ for all t. By (1),

$$x_{\alpha+\beta}(u)x_{\alpha+3\beta}(u^d) \in M ,$$

and by (5), $x_{\alpha+\beta}(t^{3-d} - t^{d-1})x_{\alpha+3\beta}(t^{3d-3} - t^{3-d}) \in M$. Substituting $t^{3-d} - t^{d-1}$ for u and multiplying by the inverse of this last element,

$$x_{\alpha+3\beta}(t^{3d-d^2} - t^{d^2-d} - t^{3d-3} + t^{3-d}) \in M$$

for all $t \in GF(q^m)$. Since $\bar{C}_M^s \cap \bar{L}_2 = 1$, the expression in parentheses vanishes identically. This yields

$$(6)\qquad (t^3 - t^{d^2})(t^{-d^2-3+3d} + t^{-d}) = 0$$

for all $t \in GF(q^m)^x$. On the other hand, since M contains $(X_{\alpha+2\beta})_{\lambda^2 m}$, $(X_{2\alpha+3\beta})_{\lambda^2 m}$, and an elment of $N_G(H)$ taking all roots to their negatives, M contains $\hat{h}(t, u) = h_{\alpha+2\beta}(t)h_{2\alpha+\beta}(u)$ for all $t, u \in GF(q^m)^x$, so contains $y^{\hat{h}(t,u)} = x_{\alpha+\beta}(t^3u)x_{\alpha+3\beta}(tu^3) \cdots$, hence contains $x_{\alpha+\beta}(t^3u)x_{\alpha+3\beta}(tu^3)$. Since $\bar{C}_M^s \cap \bar{L}_i = 1$, $i = 1, 2$, it follows that $tu^3 = (t^3u)^d$ for all $t, u \in GF(q^m)$. Hence $u^d = u^3$ (take $t = 1$) and $t^{3d} = t$ (take $u = 1$). Therefore $t^d = t^3$ and $t^9 = t$ for all $t \in GF(q^m)$, so $q = 3$ and $m = 2$. For any $t \in GF(9) - GF(3)$, we get $t^{d^2} \neq t^3$, and so by (6), $t^{d^2-4d+3} = -1$. But the left side is $t^{9-12+3} = 1$, contradiction.

Hence $t^{d^2} = t^3$ for all $t \in GF(q^m)$. This implies that m is odd, and $C_M^s = C_{\lambda^2 m}$. Hence $M \cap G_{\lambda^2 m} \supseteqq \langle C_{\lambda^2 m}, G_\lambda \rangle \supset C_{\lambda^2 m}$. It follows from Walter's theorem [28] (applied to $M \cap G_{\lambda^2 m}$) that $|M \cap G_{\lambda^2 m}| = |G_{\lambda^2 m}|$, i.e., $M \supseteqq G_{\lambda^2 m}$, as required. Hence we may assume $\pi_1(\bar{C}_M)$ is solvable, and similarly that $\pi_2(\bar{C}_M)$ is solvable. In particular, $q = 3$.

It follows from Dickson's results [6] that $\pi_i(\bar{C}_M) \subseteqq N_{\bar{L}_i}(\bar{L}) \cong S_4$, the symmetric group for $i = 1, 2$. If $9 \mid |\bar{C}_M|$, it follows easily that $\pi_1(\bar{L}) \times \pi_2(\bar{L}) \subseteqq \bar{C}_M$, contrary to what was shown above. Thus $\bar{C}_M$ has Sylow 3-subgroups of order 3. Since $\bar{C}_M \not\subseteqq N_{\bar{G}}(\bar{C}_{G_\lambda})$, C_M must be an extension of the central product $Q_8 * Q_8$ by either a group of order 3 or the symmetric group S_3. Let by a Sylow 2-subgroup of C_M. It is easily verified that $Z(T) = \langle j \rangle$. Hence T is a Sylow 2-subgroup of M. Since $\langle j^M \rangle \supseteqq (G_\lambda)'$, which is perfect, $O_2(M) = 1$. Now T_λ is elementary of order 8, and all its nonidentity elements are conjugate in M (indeed in G_λ). Since $j \in T_\lambda$ and $O_{2'}(C_M(j)) = 1$, it follows that $O_{2'}(M) \subseteqq \langle O_{2'}(C_M(i)) \mid i \in T_\lambda^\sharp \rangle = 1$. Let M_0 be a minimal normal subgroup of M. Thus M_0 is the direct product of isomorphic nonabelian simple groups. By [8], [12] and and a theorem of Burnside, each simple factor has 2-rank at least 2. However, one sees easily that T has 2-rank 3. Hence, M_0 is simple. From the structure of T, we see that $T_\lambda = C_T(T_\lambda)$, and $|N_T(T_\lambda)/T_\lambda| \geqq 4$. On the other hand, since $\langle j \rangle = Z(T)$, $j \in M_0$, and so $(G_\lambda)' = \langle j^M \rangle \subseteqq M_0$, so $|N_{M_0}(T_\lambda)/T_\lambda|$ is divisible by 7. Since $N_{M_0}(T_\lambda)/T_\lambda \lhd N_M(T_\lambda)/T_\lambda$, a subgroup of $GL_3(2)$, it follows that $N_{M_0}(T_\lambda)/T_\lambda = N_M(T_\lambda)/T_\lambda \cong GL_3(2)$. In particular, $|T| \geqq 2^6$, so $|T| = 2^6$, and also $T \subseteqq M_0$. Hence $M_0 \supseteqq T[T, C_M] = C_M$. By the the Frattini argument, $M = M_0 N_M(T) \subseteqq M_0 C_M = M_0$, so $M = M_0$ is simple.

Quoting the classification of finite simple groups in which the centralizer of an involution (in the centre of Sylow 2-subgroups) is isomorphic to C_M, we find that the only such group which in addition has a subgroup isomorphic to G_λ is the alternating group A_9 (see, for example [14]). Hence $M \cong A_9$.

Let S be a Sylow 3-subgroup of M containg U_λ. Then $|S| = 3^4$, so $U_\lambda \lhd S$, i.e., $S \subseteqq N_G(U_\lambda)$. By Lemma 1.1, $S \subseteqq B$, so $S \subseteqq U$. Let $U' = X_{\alpha+\beta} X_{\alpha+3\beta} X_{\alpha+2\beta} X_{2\alpha+3\beta}$. Now S is the wreath product $Z_3 \wr Z_3$. It follows easily that $S' = U_\lambda \cap U' = \langle x_{\alpha+\beta}(1) x_{\alpha+3\beta}(1), x_{\alpha+2\beta}(1) x_{2\alpha+3\beta}(1) \rangle$, and also that S is generated by U_λ and an element $z \in C_U(S')$ of order 3. The only such z lie in U', so $S = U_\lambda(S \cap U')$. Hence $|S: S \cap U'| = 3$. Let $U^2 = Z(U) = X_{\alpha+2\beta} X_{2\alpha+3\beta}$. Then $U'/U^2 = Z(U/U^2)$, so $S \cap U'/S \cap U^2 \subseteqq Z(S/S \cap U^2)$, so $S/S \cap U^2$ is abelian. Hence $S' \subseteqq S \cap U^2 \subseteqq Z(S)$, contradiction. This completes the proof.

3. Theorem 2.

(3.1) *Statement of results.* As in previous sections G denotes a simple algebraic group over an algebraically closed field k of characteristic $p \neq 0$.

We wish to examine certain $\eta \in \mathrm{Aut}\,(G_\mu)$ and determine the subgroups of G_μ lying above $C_{G_\mu}(\eta)$. We cannot restrict ourselves to η induced on G_μ by an element of the form $g \cdot \lambda$, where $\lambda^n = \mu$, $0 < n \in Z$, $g \in G_\mu$. For example, let $G = A_l(k)$, $l \geqq 2$, $\mu = {}^2\sigma_q$. The "field" (or "graph") automorphism η of $O^{p'}(G_\mu) = {}^2A_l(q) \cong PSU(l+1, q)$ does not have the above shape. Indeed, it is induced on G_μ by $\lambda \in \mathrm{Aut}\,(G)$, $\lambda = \sigma_q$. Thus, to examine questions of this type, we must consider pairs of commuting endomorphisms λ, μ of G with G_λ and G_μ finite. Then some power of λ centralizes G_μ. We may suppose that μ, λ are in standard form (see 1.2) and put $G_{\mu,\lambda} = G_\mu \cap G_\lambda$.

THEOREM 2. *Let G be as described above. Let $r > 1$ be an integer and $\lambda = \sigma_q$, $\mu = {}^s\sigma_{q^{r/s}}$ where G possesses a graph automorphism of order $s \in \{2, 3\}$ and s divides r.*

Let M be a group, $O^{p'}(G_{\lambda,\mu}) \leqq M \leqq G_\mu$. Then precisely one of the following holds if r is a prime (i.e., $r = s$)

(1) $G_{\lambda,\mu} \cong C_n(2^m)$, $G_\mu \cong {}^2A_{2n}(2^m)$, $O^{2'}(M) \cong {}^2A_{2n-1}(2^m)$, $M/O^{2'}(M)$ *is cyclic of order dividing* $2^m + 1$, $n \geqq 2$.

(2) $M \leqq G_{\lambda,\mu}$

(3) $O^{p'}(G_\mu) \leqq M$

(4) $p = 2$, $G_{\lambda,\mu} \cong {}^2C_2(2)$, $G_\mu \cong {}^2C_2(2^r)$; *M lies in a a unique maximal subgroup M_0 which is a Frobenius group of order* $4(2^r \pm 2^{(r+1)/2} + 1)$ *and* $G_\mu \cong {}^2C_2(2^r)$ *for odd* $r \geqq 5$.

(5) $p = 3$, $G_{\lambda,\mu} \cong PGL(2, 3)$, $G_\mu \cong {}^2A_2(3) \cong U_3(3)$, $G_{\lambda,\mu} < M < G_\mu$, $M \cong PSL(2, 7)$,

(6) $p = 5$, $G_{\lambda,\mu} \cong PGL(2, 5)$, $O^{5'}(G_\mu) \cong {}^2A_2(5) \cong U_3(5)$, $G_{\lambda,\mu} < M_i < O^{5'}(G_\mu)$, $i = 1, 2$, $M_1 \cong A_7$, $M_2 \cong M_{10}$.

Furthermore, if r is not assumed to be prime, but $|M|_p = |G_{\lambda,\mu}|_p$, *then* ($x$) *holds, for some* $2 \leqq x \leqq 6$.

We wish to emphasize the point that we have not fully examined the question: if G_μ is a finite group of Lie type and η is a noninner automorphism, what are the subgroups of G_μ lying above $C_{G_\nu}(\eta)$? We have examined only the case where η is induced on G_μ by λ, an endomorphism of G with $\lambda^r = \mu$ or $\lambda = \sigma_q r$ and $\mu = {}^s\sigma_{q^{r/s}}$. For instance, letting λ^* be the image of one of the above λ in $\mathrm{Aut}(G_\mu)$, there may be an η in the coset $\mathrm{Inn}(G_\mu)\cdot\lambda^*$ such that $|\eta| = |\lambda^*|$, yet η and λ^* are not conjugate in $\mathrm{Aut}(G_\mu)$ or even $(G_\mu)_\eta \not\cong (G_\mu)_{\lambda^*}$.

In proving the above result we may apply Theorem 1 wherever $\langle\lambda, \mu\rangle$ is a cyclic group; for then λ may be replaced by a generator of $\langle\lambda, \mu\rangle$.

(3.2) *An example.* As an illustration of where our results do not apply we give the following example, for which we thank J. E. McLaughlin.

Take G to have type A_3, $\mu = {}^2\sigma_3$, $\lambda = \sigma_3$. Then $L = O^{3'}(G_\mu) \cong {}^2A_3(3) \cong U_4(3)$ satisfies $L_\lambda \cong B_3(3)$. However, L has an automorphism η of order 2, $\eta \equiv \lambda \pmod{\mathrm{Inn}(L)}$, such that $L_\eta \cong {}^2D_2(3) \cong A_6$. There is a subgroup $M < L$ containing L_η, $M \cong PSL(3, 4)$. The existence of this M is not easily predicted by a study of the Lie structure. Indeed, its existence led J. E. McLaughlin to construct a sporadic simple group [21]. Looking at this example in more detail, we see that ${}^2A_3(3) = {}^2D_3(3)$, so that L may be regarded as $K/Z(K)$, where $K = \Omega^-(6, 3)$, the commutator subgroup of the orthogonal group $O^-(6, 3)$. In terms of matrices, let B be any symmetric 4×4 nonsingular matrix of determinant -1 with entries from $\boldsymbol{F}_3$ and let $^-$ be the result of applying the field automorphism $x \mapsto x^3$ to a 4×4

matrix with entries from $\boldsymbol{F}_9$. Then $SU(4, 3)$ may be identified with $\{A \mid {}^t\bar{A}BA = B, \det A = 1\}$ and it has a "natural" field automorphism $\varphi: A \rightarrow \bar{A}$. However, φ is not the "standard field automorphism" of $SU(4, 3)$, as we have defined the term above. In fact, the fixed points of φ is the special orthogonal group associated with B. See Artin [1], p. 210.

A variation of our situation is the following: M is a group lying between $O^{p'}(G_{\lambda,\mu})'$ and $O^{p'}(G_\mu)$. The problem (still not fully solved) is to show that $O^{p'}(G_{\lambda,\mu})' \lhd M$ or identify M.

Of course, any "interesting" exceptions will be ones not already described by our main theorem. That is, we will be dealing with a Chevalley or twisted group $O^{p'}(G_{\lambda,\mu})$ which is not perfect (i.e., is not equal to its commutator subgroup). The possibilities for $O^{p'}(G_{\lambda,\mu})$ are then the solvable groups $A_1(2)'$, $A_1(3)'$, ${}^2A_2(2)$, and ${}^2C_2(2)$, plus the nonsolvable groups $B_2(2) \cong \Sigma_6$, $G_2(2) \cong \operatorname{Aut}(U_3(3))$, ${}^2G_2(3) \cong \operatorname{Aut}(L_2(8))$ and ${}^2F_4(2)'$. The only exception known to the authors, for $O^{p'}(G_{\lambda,\mu})$ nonsolvable, is

$$G_2(2)' < M < G_2(4) , \quad M \cong J_2, \text{ Janko simple group}$$

group of order 604,800; there are two conjugacy classes of such M, see Wales [27].

We mention that [27] does not determine all maximal subgroups of $G_2(4)$ containing $G_2(2)'$.

Another example we mention is the containment

$${}^2F_4(2)' < M < {}^2E_6(2) ,$$

where $M \cong M(22)$, the Fischer group of order $2^{17}3^9 5^2 \cdot 7 \cdot 11 \cdot 13$ [9], [10]. This does not quite fit in the above situation, because ${}^2F_4(2)$ cannot be realized as $G_{\lambda,\mu}$, where $G = E_6(k)$, char $k = 2$. However, the questions to be asked here are obvious: find finite groups M (if any) for which ${}^2F_4(2)' < M < X$, where $X \cong {}^2F_4(q)$, $F_4(q)$, ${}^2E_6(q)$ and $E_6(q)$, for q even, and where ${}^2F_4(2)' < {}^2F_4(2)$ is embedded in the natural fashion in X. We point out that in the above case where $M \cong M(22)$, it is not known for certain that the ${}^2F_4(2)'$ subgroup of M is conjugate to the one embedded in the "natural" way in ${}^2E_6(2)$.

(3.3) *Proof of Theorem* 2. We proceed by a series of lemmas. Some important intermediate results are given in Propositions 3.1 and 3.2.

LEMMA 3.1. *Suppose G has a root system Σ having one root length. Let $\mu = {}^s\sigma_q$, $s \in \{2, 3\}$, and let $\lambda = \sigma_q$. Suppose M is a subgroup of G such that $G^s_{\lambda,\mu} \subsetneqq M \subset G^s_\mu$. Then one of the following holds:*

(a) $p \nmid |M: G^s_{\lambda,\mu}|$
(b) $p = 2$, $\Sigma = A_{2n}$, *and either* $O^{2'}(M) \cong {}^2A_{2n-1}(q)$, *or* $G_\mu = {}^2A_2(2)$.

Proof. Let $\bar{\Sigma}$ be the twisted "root system" of G_μ and $\bar{W}$ the corresponding Weyl group. Thus $N_\mu/H_\mu \cong N_{\lambda,\mu}/H_{\lambda,\mu} \cong \bar{W}$. Also, $U_\mu = \prod_{\rho \in \bar{\Sigma}} x_\rho$. If $\Sigma \neq A_{2n}$, then $\bar{\Sigma}$ is a bona fide root system, and X_ρ is parametrized by $GF(q)$ for long p, by $GF(q^s)$ for short ρ. If $\Sigma = A_{2n}$, then $s = 2$, and $\bar{\Sigma} = \{\pm(a_i, 2a_i), \pm a_i \pm a_j \mid 1 \leqq i < j \leqq n\}$ is of type "BC_n", with $X_{\pm a_i \pm a_j}$ parametrized by $GF(q^2)$ and $X_{\pm(a_i, 2a_i)}$ of type ${}^2A_2$. The parametrizations by $GF(q^s)$ are not quite canonical: if τ is the Frobenius automorphism of $GF(q^s)/GF(q)$ there are s canonical parametrizations of X_ρ, in which the same element is represented as $x_\rho(t)$, or $x_\rho(t^\tau)$ (or $X_\rho(t^{\tau^2})$ if $s = 3$). We shall ignore this ambiguity since it does not affect the validity of our arguments. Note that if X_ρ is parametrized by $GF(q)$, then $(X_\rho)_\mu = X_\rho$; while if by $GF(q^s)$, then $(X_\rho)_\mu = \{x_\rho(t) \mid t \in GF(q)\}$.

We show first that $N_{G_\mu}(U_{\lambda,\mu}) \subseteq B_\mu$. Let $g \in N_{G_\mu}(U_{\lambda,\mu})$, and write $g = bn_w u$ in canonical form ($w \in \bar{W}$). For every fundamental $\rho \in \bar{\Sigma}$, let $U^\rho = \prod_{\substack{\sigma \neq \rho \\ \sigma > 0}} X_\sigma$, so that $U_\rho \lhd U$, $U = U^\rho X_\rho$, and $X_\rho \cap U_\rho = 1$. (In case $\Sigma = BC_n$ we take $\{(a_1, 2a_1), a_2 - a_1, \cdots, a_n - a_{n-1}\}$ as the fundamental system.) Now $U_{\lambda,\mu} \cap X_\rho \neq 1$ for each such ρ, so $(U_{\lambda,\mu})^b$ contains an element of the form $x_\rho u_\rho$ with $1 \neq x_\rho \in X_\rho$, $u_\rho \in U^\rho$. Since $(x_\rho u_\rho)^{n_w} \in (U_{\lambda,\mu})^{u^{-1}} \subseteq U$, $w(\rho) \in \bar{\Sigma}^+$. Hence $w = 1$, so $g \in B_\mu$.

Now suppose (a) fails. Let $U^* = N_{M \cap U_\mu}(U_{\lambda,\mu})$. Since $U_{\lambda,\mu}$ is not one of $N_M(U_{\lambda,\mu})$ which equals $N_{M \cap B_\lambda}(U_{\lambda,\mu})$ by the above. Since U_μ is the Sylow p-subgroup of B_μ, $U^* \supsetneqq U_{\lambda,\mu}$.

Suppose $\Sigma \neq A_{2n}$. Put a partial order $\leqq$on $\bar{\Sigma}$ refining the order given by heights. Write each $u \in U_\mu$ as $u = \prod_{\bar{\Sigma}^+} x_\rho(t_\rho)$ in order, and set $\operatorname{supp}(u) = \{\rho \mid t_\rho \neq 0\}$. Among all elements of $U^* - U_{\lambda,\mu}$, choose x to have the greatest support, in the lexicographic ordering. Write $x = x_{\rho_0}(t_{\rho_0}) \prod_{\rho > \rho_p} x_\rho(t_\rho)$ with $t_{\rho_0} \neq 0$. Then in fact $x_{\rho_0}(t_{\rho_0}) \notin U_{\lambda,\mu}$, otherwise $x' = x_{\rho_0}(-t_{\rho_0})x \in U^* - U_{\lambda,\mu}$, and $\operatorname{supp}(x') > \operatorname{supp}(x)$, contrary to choice of x. In particular, $t_{\rho_0} \notin GF(q)$, so ρ_0 is short. Suppose there is $\sigma \in \bar{\Sigma}^+$ such that ρ_0 and σ are fundamentally independent. Let $x^* = [x_\sigma(1), x] = x_{\rho_0+\sigma}(\pm t_{\rho_0}) \cdots$, (for a complete description of the commutator formula in Steinberg variations, see [15]). Then $x_\sigma(1) \in U_{\lambda,\mu}$ and $x \in U^*$ imply $x^* \in U_{\lambda,\mu}$, so $t_{\rho_0} \in GF(q)$, contradiction. Hence no such σ is available. Suppose $\bar{\Sigma} = G_2$, with fundamental system $\{\alpha, \beta\}$, β short, and $\rho_0 = \alpha + \beta$. Then $x_\beta(1)$, $x_{\alpha+2\beta}(1) \in U_{\lambda,\mu}$, so $U_{\lambda,\mu}$ contains both $[x_\alpha(1), x] = x_{\alpha+2\beta}(\pm(t^\tau_{\rho_0} + t^{\tau^2}_{\rho_0}))$ and

$$[x_{\alpha+2\beta}(1), x] = x_{2\alpha+3\beta}(\pm(t_{\rho_0} + t^\tau_{\rho_0} + t^{\tau^2}_{\rho_0})) .$$

Hence $GF(q)$ contains both coefficients, so contains t_{ρ_0}, contradiction.

We conclude from (*) (see Lemma 2.1) that $\rho_0=\theta_s$. In the factorization of x, all terms $x_\rho(t_\rho)$ after the first are for long ρ, hence lie in $U_{\lambda,\mu}$. Hence $x_{\rho_0}(t_{\rho_0})^{-1}x \in U_{\lambda,\mu}$, so $x_{\rho_0}(t_{\rho_0}) \in U^*$. Hence $X_{\rho_0} \cap M \supset (X_{\rho_0})_\lambda$. Now $\langle X_{\rho_0}, X_{-\rho_0}\rangle \cong A_1(q^s)$, and λ induces a field automorphism σ_q on this group, so by Theorem 1 (more precisely Lemma 2.5, which holds even for $q = 2$), $\langle X_{\rho_0}, X_{-\rho_0}\rangle \subseteqq M$, as s is prime. Conjugating by $N_{\lambda,\mu}$, we get $X_\rho \subseteqq M$ for all short ρ; since $X_\rho = (X_\rho)_\lambda \subseteqq M$ for long ρ, $M = G^s_\mu$, contrary to hypothesis. Therefore, $\Sigma = A_{2n}$.

If $n = 1$, then (b) is immediate from work of Mitchell [22] and Hartley [16]. Suppose then $n > 1$. For a root $\rho = \pm a_i \pm a_j$, $X_\rho = \{x_\rho(t) \mid t \in GF(q^2)\}$ and $(X_\rho)_\lambda = \{x_\rho(t) \mid t \in GF(q)\}$. For each $i = 1, \cdots, n$, there is a root subgroup $X_i = \{x_i(t, u) \mid t^{1+q} + u + u^q = 0,\ t, u \in GF(q^2)\}$ corresponding to the "root" $(a_i, 2a_i)$. The opposite root subgroup is denoted by X_{-i}. We separate X_i into parts X_{a_i} and X_{2a_i} as follows: let $X_{2a_i} = Z(X_i) = \{x_i(0, u) \mid u \in GF(q^2),\ u + u^q = 0\}$, and write $x_{2a_i}(u)$ for $x_i(0, u)$. Let X_{a_i} be a transversal to X_{2a_i} in X_i. If q is odd, we may choose X_{a_i} to be μ-invariant, so that if a coset C of X_{2a_i} in X_i is fixed by λ, then the representative of C in X_{a_i} is fixed by λ. The element of X_{a_i} representing the coset $x_i(t, u)X_{2a_i}$ will be written $x_i(t)(t \in GF(q^2))$. Thus X_i is parametrized by $GF(q^2)$. We choose $x_i(0) = 1$, without loss.

Let $\tilde{\Sigma} = \{\pm a_i, \pm 2a_i, \pm a_i \pm a_j \mid 1 \leqq i < \leqq n\}$. Define a height function on $\tilde{\Sigma}$ by setting $ht(a_i) = i$ and extending linearly. Then for $\rho, \sigma \in \tilde{\Sigma}^+$, $[X_\rho, X_\sigma] \subseteqq \langle X_\alpha \mid \alpha \in \tilde{\Sigma},\ ht(\alpha) \geqq ht(\rho) + ht(\sigma)\rangle$. Let $\leqq$ be a partial order on $\tilde{\Sigma}$ refining the height order. Since $X_{\pm a_i \pm a_j}$, X_{2a_i}, and $X_i = X_{a_i}X_{2a_i}$ are subgroups of G_μ, and since $a_i < 2a_i$, every $u \in U_\mu$ is uniquely expressable as $\Pi x_\rho(t_\rho)$, the product over $\rho \in \tilde{\Sigma}^+$ in increasing order, with t_ρ in the appropriate field. Set $\operatorname{supp}(u) = \{\rho \mid t_\rho \neq 0\}$. Again, among all $x \in U^* - U_{\lambda,\mu}$ choose x maximal in the lexicographic ordering. Say $x = x_{\rho_0}(t_{\rho_0}) \prod_{\rho > \rho_0} x_\rho(t_\rho)$, with $t_{\rho_0} \neq 0$. Then as before, $x_{\rho_0}(t_{\rho_0}) \notin U_{\lambda,\mu}$.

Suppose q is odd. Then $(X_i)_\lambda = (X_{a_i})_\lambda = \{x_{a_i}(t) \mid t \in GF(q)\}$ for each i. So $x_{a_i}(1) \in U_{\lambda,\mu}$ for all i. Suppose $\rho_0 = a_j - a_i$ for some $j > i$. Then $[x, x_{a_i}(1)] = x_{a_j}(\pm t_{\rho_0}) \cdots$ lies in $U_{\lambda,\mu}$ so $t_{\rho_0} \in GF(q)$, whence $x_{\rho_0}(t_{\rho_0}) \in U_{\lambda,\mu}$, contradiction. If $\rho_0 = a_i$, then for $j = 1$ or 2, $U_{\lambda,\mu}$ contains $[x, x_{a_j}(1)] = x_{a_i + a_j}(\pm t_{\rho_0}) \cdots$, so $t_{\rho_0} \in GF(q)$ and $x_{\rho_0}(t_{\rho_0}) \in U_{\lambda,\mu}$, contradiction. If $\rho_0 = a_i + a_j$, $j > i$, then $U_{\lambda,\mu}$ contains $[x, x_{a_j - a_i}(1)] = x_{2a_j}(\pm(t_{\rho_0} - t^q_{\rho_0})) \cdots$. Since $(X_{2a_j})_\mu = 1$, $t_{\rho_0} - t^q_{\rho_0} = 0$, so $t_{\rho_0} \in GF(q)$, again giving a contradiction. Suppose $\rho_0 = 2a_i$, $1 \leqq i < l$. Write $x = x_{2a_i}(t_{\rho_0}) \cdots x_{a_i + a_{i+1}}(t) \cdots$. Then

$$[x, x_{a_{i+1} - a_i}(1)] = x_{a_i + a_{i+1}}(\pm t_{\rho_0}) \cdots x_{2a_{i+1}}(\pm(t - t^q) \pm t_{\rho_0}) \cdots$$

lies in $U_{\lambda,\mu}$, so $t_{\rho_0} \in GF(q)$ and $t - t^q \pm t_{\rho_0} = 0$. Hence $t - t^q \in GF(q)$. Since q is odd, this implies $t - t^q = 0$. Hence $t_{\rho_0} = 0$, contradiction.

We conclude that $\rho_0 = 2a_n$. Hence $M \cap X_n \supset (X_n)_\lambda (=1)$. Applying the case $n = 1$ to $\langle X_n, X_{-n}\rangle$, we get $\langle X_n, X_{-n}\rangle \subseteqq M$. Conjugating by $N_{\lambda,\mu}$, we get $X_i \subseteqq M$ for all i. Hence M contains $[x_{a_1}(t), x_{a_2}(t')] = x_{a_1+a_2}(\pm tt')$ for all $t, t' \in GF(q^2)$, so $X_{a_1+a_2} \subseteqq M$. This easily yields $G^s_\mu = M$, contradiction. Therefore, q is even, i.e., $p = 2$.

In this case, we have $(X_i)_\lambda = X_{2a_i}$, and X_{a_i} is not λ-invariant. Let x, ρ_0, and t_{ρ_0} be as before. If $\rho_0 = a_j - a_i$ for some $j > i$, then $U_{\lambda,\mu}$ contains $[x, x_{2a_i}(1)] = x_{a_j+a_i}(t_{\rho_0}) \cdots$, so $t_{\rho_0} \in GF(q)$, contradiction. If $\rho_0 = 2a_i$, then $x_{\rho_0}(t_{\rho_0}) \in X_{2a_i} \subseteqq U_{\lambda,\mu}$, contradiction. If $\rho_0 = a_i + a_j \neq a_{n-1} + a_n$, then there exists $\sigma = a_{j'} - a_{i'}$, $j' > i'$, such that $\rho_0 + \sigma$ is of the form $a_k + a_l$, and so $U_{\lambda,\mu}$ contains $[x, x_\sigma(1)] = x_{\rho_0} + \sigma(t_{\rho_0}) \cdots$, contradiction. If $\rho_0 = a_i$, $1 \leqq i < n$, then $U_{\lambda,\mu}$ contains $[x, x_{a_{i+1}-a_i}(1)] = x_{a_{i+1}}(t_{\rho_0}) \cdots$, contradiction. Suppose $\rho_0 = a_n$, and write $x = x_{a_n}(t_{\rho_0}) \cdots x_{2a_n}(t')$, $x_{a_n}(t_{\rho_0}) = x_n(t_{\rho_0}, u)$. Then $u + u^q = t^{1+q}_{\rho_0} \neq 0$, so $u \in GF(q^2) - GF(q)$. Let $n_0 = n_{a_n-a_{n-1}}(1)$, and set $x' = x^{n_0} = x_{a_{n-1}}(t_{\rho_0}) \cdots x_{2a_{n-1}}(t')$ (with other nontrivial terms coming only from roots of the form $a_i + a_j$ or $2a_i$). Let $x^{(2)} = [x', x_{a_n-a_{n-1}}(1)]$. Then $x^{(2)} \in M$, and $x^{(2)} = x_{a_n}(t_{\rho_0}) \cdots x_{a_n+a_{n-1}}(t'^q + u^q)x_{2a_n}(\ )$, with inside nontrivial terms coming only from roots of the form $a_n + a_j$ Let $u' = t'^q + u^q$. Since $t' \in GF(q)$ and $u \notin GF(q)$, $u' \notin GF(q)$. Now set $n_1 = n_{a_{n-1}}(1)$, and $x^{(3)} = [x', (x^{(2)})^{n_1}]$. Then $x^{(3)} \in M$, and $x^{(3)} = x_{a_n}(t_{\rho_0}u') \cdots$. Since $u' \notin GF(q)$, we may assume that $t_{\rho_0} \notin GF(q)$, by replacing x by $x^{(3)}$ at the outset if necessary. But then $[x, x^{n_0}] = x_{a_n+a_{n-1}}(t^2_{\rho_0})$ and $t^2_{\rho_0} \in GF(q)$, so the maximality of x is violated. Thus $\rho_0 \neq a_n$, so $\rho_0 = a_n + a_{n-1}$. Hence $x_{\rho_0}(t_{\rho_0}) = x \cdot x_{2a_n}(\ ) \in U^* - U_{\lambda,\mu}$. Applying Theorem 1 (Lemma 2.5) to $\langle X_{a_n+a_{n-1}}, X_{-a_n-a_{n-1}}\rangle$, we see that $X_{a_n+a_{n-1}} \subseteqq M$. Thus $X_\rho \subseteqq M$ if $\rho = \pm a_i \pm a_j$. Let $\tilde{G} = \langle X_\rho \mid \rho = \pm a_i \pm a_j \text{ or } 2a_i\rangle$, so that $\tilde{G} \subseteqq M$, and $\tilde{G}$ is (canonically generated) ${}^2A_{2n-1}(q)$. It is easily verified that $N_{G_\mu}(\tilde{G})$ is the unique maximal subgroup of G_μ containing $\tilde{G}$. One considers the permutation group induced by $SU(2n + 1, q)$ on anisotropic vectors of a given length in the natural $2n + 1$-dimensional module over $GF(q^2)$, and shows that the only sets of imprimitivity have the property that every block is a subset of one-dimensional subspace. Hence $\tilde{G} \subseteqq M \subseteqq N_{G_\mu}(\tilde{G})$. Since $N_{G_\mu}(\tilde{G})/\tilde{G} \cong Z_{q+1}$ is of odd order, $\tilde{G} = O^{2'}(M)$, completing the proof.

We are now entitled to work under the following conditions:

(A) $r > 1$ is an integer

(B) λ, μ are commuting endomorphisms of G with G_λ and G_μ finite and λ induces an automorphism of order r on G_μ

(C) Either (i) $\lambda^r = \mu$ and $\lambda = \sigma_q$ or $\lambda = {}^s\sigma_q$ where $r \nmid s$ and the Dynkin diagram for G has period $s \in \{2, 3\}$; or (ii) $\lambda = \sigma_q$ and $\mu = {}^s\sigma_{q^{r/s}}$, where $r \mid s$ and the Dynkin diagram for G has period $s \in \{2, 3\}$.

(D) $O^{p'}(G_{\lambda,\mu}) \leqq M \leqq G_\mu$

(E) $|M|_p = |G_{\lambda,\mu}|_p$ i.e., $U_{\lambda,\mu} \in \mathrm{Syl}_p(M)$.

First a few observations. Namely, $G_{\lambda,\mu}$ and G_μ have the same rank and consequently, if P is a $\langle \lambda, \mu \rangle$-invariant parabolic subgroup of G, λ leaves invariant every component of $P_\mu/O_p(P_\mu)$ (see 2.4 for a discussion of components). We do not assume r is a prime. Here, the critical assumption is that $M_{\lambda,\mu} = M \cap G_{\lambda,\mu}$ contains a Sylow p-group of M. Also, even though Theorem 1 deals with the above case (C. i), none of the following arguments, except Lemma 3.9 and Proposition 3.2 are simplified by quoting Theorem 1.

LEMMA 3.2. *Let P_μ be a proper parabolic subgroup of G_μ containing B_μ. Write $P_\mu = O_p(P_\mu)\cdot L_\mu$, where L_μ is generated by H_μ and standard root groups from G_μ. Let Σ_μ be a root system for G_μ. Let $\Sigma_0 = \{r \in \Sigma_\mu \mid X_r \leqq O_p(P_\mu)\}$, where X_r denotes a root group for G_μ* (rather than for G). *Set $P_\mu^- = \langle X_r, H_\mu \mid X_{-r} \leqq P_\mu \rangle$. Then $G_\mu = \langle O_p(P_\mu), O_p(P_\mu^-)\rangle$.*

Proof. Let $S = \langle O_p(P_\mu), O_p(P_\mu^-)\rangle$. Then L_μ normalizes S, whence SL_μ is a group containing B_μ, i.e., SL_μ is a standard parabolic subgroup. If SL_μ were proper, then $O_p(SL_\mu)$ would meet X_α nontrivially, for some $\alpha \in \Sigma_0$. But $X_{-\alpha} \leqq S$ implies that $O_p(\langle X_\alpha, X_{-\alpha}\rangle) = 1$, contradiction. Thus $SL_\mu = G$. Since $S \lhd SL_\mu$, $S = G_\mu$, as required.

LEMMA 3.3. *Let P be proper parabolic subgroup of G containg B. Then $C_{G_\mu}(O_p(P_\mu)) \leqq O_p(P_\mu)$, i.e., $O_{p'}(P_\mu) = 1$ and P_μ is p-constrained.*

Proof. If necessary, we shall replace μ by $\nu = \mu^j$, where $j > 1$ is an integer such that (i) if μ involves a graph automorphism of period $s > 1$, $(j, s) = 1$ (ii) in G_ν, two opposite root groups generate a quasisimple group, i.e., we are avoiding small fields. Note that G_ν and G_μ have the same Weyl group and $G_\mu \leqq G_\nu$. We claim that this change affects neither hypothesis nor conclusion. Namely, set $C_\tau = C_{G_\tau}(O_p(P_\tau)) \lhd P_\tau$ for $\tau \in \{\mu, \nu\}$. By the fact that if X_μ is a root group for G_ν and $X_\mu = (X_\nu)_\mu$, $C_{G_\nu}(X_\mu) = C_{G_\nu}(X_\nu)$ (a straightforward exercise) and the fact that $O_p(P_\tau)$ is a product of root groups in G_τ, $\tau \in \{\mu, \nu\}$, we get $C_\mu = C_\nu \cap G_\mu$. Thus, it suffices to prove $C_\nu \leqq O_p(P_\nu)$, because then C_μ is a normal p-group in P_μ, whence $C_\mu \leqq O_p(P_\mu)$. So, we make the replacement.

Let r be a root in the root system Σ_μ and X_r the corresponding root group in G_μ. An element of H_μ centralizes X_r if and only if it centralizes X_{-r}. Therefore, by Lemma 3.2, $C \cap H_\mu \leqq Z(G) = 1$. Letting $^-$ denote the quotient $P_\mu \to \bar{P}_\mu = P_\mu/O_p(P_\mu)$, we claim that $\bar{C} \cap \bar{H}_\mu = 1$. If not, let $H_0 \leqq H_\mu$ satisfy $\bar{H}_0 = \bar{C} \cap \bar{H}_\mu$. Now, C is a normal subgroup of p-power index in $C \cdot O_p(P_\mu)$, whence $H_0 \leqq C$, and so $C \cap H_\mu \neq 1$, absurd. Thus $\bar{C} \cap \bar{H}_\mu = 1$. It follows that $\bar{C} \cap O^{p'}(\bar{P}_\mu) = 1$, because our replacement of μ guarantees that any normal subgroup of $O^{p'}(\bar{P}_\mu)$ lies in $\bar{H}_\mu$. Therefore, $[\bar{C}, \bar{U}_\mu] = 1$. This means $C \leqq B_\mu$. Since B_μ has a normal Sylow p-subgroup and $O_p(\bar{C}) = 1$, it follows that $\bar{C}$ is a normal p'-subgroup of $\bar{B}_\mu$, whence $1 \neq \bar{C} \leqq \bar{H}_\mu$, in conflict with above statements. The lemma follows.

LEMMA 3.4. (i) *For any* μ, U *is the unique conjugate of* U *which contains* U_μ. (ii) *Also* U *is the unique conjugate of* U *which contains* $U_{\lambda,\mu}$, *unless* q *is even*, $\lambda = \sigma_q$, $\mu = {}^2\sigma_{q^{r/s}}$ *and* G *has type* A_{2n}, *in which case* $\{g \in G \mid U_{\lambda,\mu} \leqq U^g\} = B \cup Bn_{w_r}B \cup n_{w_s}B$, *where* $\{1, w_r, w_s\} = \{w \in \langle w_r, w_s\rangle \mid X^w_{r+s} \leqq \langle X_r, X_s\rangle\}$ *where* r, s *are the* nth *and* $(n+1)$st *roots in the Dynkin diagram for* G. (iii) *However, in all cases*, U_μ *is the unique* G_μ*-conjugate of* U_μ *containing* $U_{\lambda,\mu}$.

Let $P(\lambda, \mu)$ *be a parabolic subgroup for* $G_{\lambda,\mu}$. (iv) *Then there is a unique parabolic subgroup* $P(\mu)$ *of* G_μ *which contains* $P(\lambda, \mu)$, *and satisfies* $P(\mu)_\lambda = P(\lambda, \mu)$. (v) *Also there is a unique* $\langle\lambda, \mu\rangle$*-invariant parabolic subgroup* P *of* G *for which* $P_{\lambda,\mu} = P(\lambda, \mu)$ *and* $P = \langle P(\lambda, \mu), B\rangle$, *unless we have the above exceptional* q, G, λ, μ (see (ii)) *and the* $P(\lambda, \mu)$ *is the one containing* $B_{\lambda,\mu}$ *which is associated with the subset of the Dynkin diagram for* G *consisting of all short roots. In the exceptional case, there is a* $\langle\lambda, \mu\rangle$*-invariant parabolic subgroup of* G *for which* $P_{\lambda,\mu} = P(\lambda, \mu)$, *e.g.*, $P = \langle P(\lambda, \mu), B^g\rangle$, *where* $g \in G_{\lambda,\mu}$ *satisfies* $B^g_{\lambda,\mu} \leqq P$.

Proof. (ii) Let $U_\mu < V = U^g$, $g \in G$. Let Σ be a root system for G. Write $g = bn_w u$, where $b \in B$, $n_w \in N_G(H)$ represents the element w of the Weyl group, and $u \in U(w) = \langle X_\alpha \mid \alpha \in \Sigma^+, \alpha^{w^{-1}} \in \Sigma^-\rangle$. Let $U^{(w)} = \langle X_\alpha \mid \alpha \in \Sigma^+, \alpha^{w^{-1}}\Sigma^+\rangle$. Then $U^g = U^{n_w u}$ and so $U_\mu \leqq U^{(w)u}$. Suppose $g \notin B$. Then there is such a g for which w is a fundamental reflection, $w = w_\alpha$ (see the appendix of Steinberg's notes [24]) so that $U^{(w)} \lhd U$. Thus to get a contradiction, it suffices to show $U_{\lambda,\mu} \nleqq U^{(w)}$.

Write $X_r = U_{(w)}$. If $\langle\lambda, \mu\rangle$ leave X_r invariant, we are done, as $(X_r)_\lambda \neq 1$. Therefore $\mu = {}^s\sigma_{q'}$ where q' is some power of p and $s = 2$ or 3. But now, we see that $R = \langle X_r^{\mu^i} \mid 0 \leqq i \leqq -1\rangle$ satisfies $R_{\lambda,\mu} \nleqq U^{(w)}$ by checking the possibilities, unless $G = A_{2n}(k)$, $n \geqq 1$, $\mu = {}^2\sigma_q r/2$ and $\lambda = \sigma_q$ and r is the nth or $(n+1)$st node in the Dynkin diagram for A_{2n}. The verification of the rest of (i) and (ii) is an exercise.

The proof of (iii) is obtained by a similar argument, and (iv) and (v) are straightforward.

LEMMA 3.5. *There does not exist a proper parabolic subgroup of* G_μ *containing* G_λ.

Proof. Assume false, and take a parabolic subgroup R, $G_\lambda \leqq R < G_\mu$. Embed U_λ in a Sylow p-subgroup of R. By Lemma 3.4, $U_\lambda < U_\mu < R$. Since R is a proper parabolic subgroup, it is p-constrained (by Lemma 3.3) whence $Z(U) \leqq O_p(R)$. Thus $1 \neq Z(U)_\lambda \leqq O_p(R) \cap G_\lambda \lhd G_\lambda$, whereas $O_p(G_\lambda) = 1$, contradiction.

LEMMA 3.6. *Let P be a parabolic subgroup of G which is $\langle\lambda, \mu\rangle$-invariant. Then $O_p(P_\lambda) = O_p(P)_\lambda$, $O_p(P_\mu) = O_p(P)_\mu$, $O_p(P_{\lambda,\mu}) = O_p(P)_{\lambda,\mu}$.*

Proof. Clearly $O_p(P)_\lambda \leqq O_p(P_\lambda)$. Suppose the containment is proper. Let $^-$ denote the quotient map $P \to P/O_p(P)$. Then $\overline{O_p(P_\lambda)} \neq 1$ is a normal p-subgroup of $\bar{P}$. However, $\langle\lambda, \mu\rangle$ leaves invariant a complement L to $O_p(P)$ in P. The structure of L implies that $O_p(L_\lambda) = 1$, contradiction. So $O_p(P_\lambda) = O_p(P)_\lambda$. The other assertions are proven similarly.

LEMMA 3.7. *Let $V \leqq H_\mu$ be a group of order prime to p for which $[U_{\lambda,\mu}, V] = 1$. Then $V = 1$ unless $p = 2$, $\mu = {}^2\sigma_{q^{r/2}}$, $\lambda = \sigma_q$, $G = A_n(k)$, n even, and $|V| \mid q+1$ and $O^{p'}(C_{G_\mu}(V))/Z(O^{p'}(C_{G_\mu}(V))) \cong {}^2A_{n-1}(q)$.*

Proof. If G_μ has rank 1, i.e., $G_\mu \cong A_1(q)$, ${}^2A_2(q)$, ${}^2C_2(q)$ or ${}^2G_2(q)$, the lemma is well-known to be true.

Let G be a counterexample of minimal rank. Letting Π be the set of fundamental roots, we may apply induction to $\bar{P} = P/O_p(P)$, P any parabolic subgroup. Then $\bar{V} \leqq Z(\bar{P})$ unless $\bar{P}/Z(\bar{P})$ has a component of type A_l, l even. If $\bar{V} \leqq Z(\bar{P})$, the Frattini argument shows $C_G(V)$ covers $P/O_p(P)$. Since $V \neq 1$, $C_G(V)$ cannot cover all such $P/O_p(P)$, whence G has type A_n, n even. On the other hand, letting P be associated with various subsets of Π, we see that V centralizes all root groups, for short roots in Σ_μ, and on any root group for a long root in Σ_μ, V centralizes precisely the center. The remaining statements now follow.

LEMMA 3.8. *Let P be a proper parabolic subgroup of G containing B. Assume P is $\langle\lambda, \mu\rangle$-invariant. Then $C_{P_\mu}(O_p(P_{\lambda,\mu})) \leqq O_p(P_\mu)\cdot K$ where $K = 1$ unless $G_\mu = {}^2A_n(q)$, n, q even and $K \leqq H$ is a cyclic group of order dividing $q+1$ and centralizing $G_{\lambda,\mu}$. In particular, $C_{G_\mu}(G_{\lambda,\mu}) = 1$ unless $G_\mu = {}^2A_n(q)$, n, q* even, and *$G_{\lambda,\mu} \cong C_{n/2}(q)$, in which case $C_{G_\mu}(G_{\lambda,\mu}) \cong Z_{q+1}$.*

Proof. The last sentence follows from the first statement of the lemma whose proof we now begin. We may assume r is a prime and that $r = s$ if there is a graph automorphism involved in μ. Let

$C = C_P(O_p(P_{\lambda,\mu}))$ and let $^-$ be the quotient map $P \to \bar{P} = P/O_p(P)$. We may assume $\bar{C} \neq 1$. Since $\bar{C} \neq 1$, $P \neq B$, and so G_μ has rank at least 2. Let L be the standard $\langle \lambda, \mu \rangle$-invariant complemet to $O_p(P)$ in P (i.e., $L = \langle H, X_\alpha | \alpha$ runs over a subset of $\Sigma \rangle$). Then $\bar{P} \cong L$ as $\langle \lambda, \mu \rangle$-groups. Since $L_{\lambda,\mu}$ normalizes $O_q(P_{\lambda,\mu})$, $L_{\lambda,\mu}$ normalizes $D = C \cap L \cong \bar{C}$.

Assume that $D_0 = C_D(O^{p'}(L_{\lambda,\mu})) = C_D(O^{p'}(P_{\lambda,\mu})) \neq 1$. A Frattini argument then shows D_0 centralizes $O_p(P_{\lambda,\mu})(U \cap L_{\lambda,\mu}) = U_{\lambda,\mu}$. By Lemma 3.7 $G_\mu \cong {}^2A_n(q)$, n, q even, and $1 \neq D_0 \leqq K$ in the notation of Lemma 3.7. Then, as $D_0 \leqq D$, $D \leqq N_{G_\mu}(K)$ and the lemma is verified by inspection.

We may now assume $D_0 = 1$. This will eventually lead to a contradiction. Now $D_\lambda \leqq C_{P_\lambda}(O_p(P_\lambda)) \leqq O_p(P_\lambda)$, by Lemma 2. So, $D_\lambda = 1$. We may assume $D_\mu \neq 1$. Since r is prime, D_μ is nilpotent by Thompson's theorem [13]. Let $1 \neq V \leqq D_\mu$ be minimal normal in $D_\mu L_{\lambda,\mu}\langle \lambda \rangle$. Then V is an elementary abelian t-group, for some prime $t \neq r$.

Assume that $t = p$. Let $L_1, \cdots, L_n$ be the components of $O^{p'}(L_\mu)$ and let $\pi_i: O^{p'}(L_\mu) \to \bar{L}_i = L_i/Z(L_i)$ be the "projections." Our hypotheses on λ, μ imply that λ stabilizes each L_i. Since $V \neq 1$ is a p-group, and $Z(L_i)$ is a p'-group for all i, $V^{\pi_i} \neq 1$ for some i. Then $V^{\pi_i}(\bar{L}_i)_\lambda$ lies in a proper parabolic subgroup of $\bar{L}_i$, which is impossible by Lemma 3.5. Thus $t \neq p$.

Take $S \leqq O_p(P_\mu)$ such that $S > O_p(P_{\lambda,\mu}) = S_{\lambda,\mu}$, $S_\lambda \leqq C_S(V) \lhd S$ and $S/C_S(V)$ is an irreducible $V\langle \lambda \rangle$-module for which $C_V(S) < V$ (such a choice is possible because $O_p(P_\mu) > O_p(P_{\lambda,\mu})$, $t \neq p$, $V \leqq P_\mu$ and $O_p(P_\mu) \geqq C_{P_\mu}(O_p(P_\mu)))$.

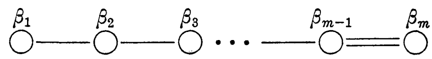
We claim that $r = p$. If $r \neq p$, then $(S/C_S(V))_\lambda = 1$, which implies $SV/C_S(V)$ is nilpotent, whence $[S, V] \leqq C_S(V)$, $[S, V] = [S, V, V] = 1$ and so $S \leqq C_S(V)$, which is false. Therefore $r = p$.

We next argue that $p = 2$. In S, take a minimal $V\langle \lambda \rangle$-invariant subgroup T which covers $S/C_S(V)$. Then T is special or elementary abelian, $T = [T, V]$ and $C_T(V) = T'$. Since $V\langle \lambda \rangle/\langle \lambda^p \rangle$ is a Frobenius group, $S/C_S(V) \cong T/C_T(V)$ is a free $\Lambda = \boldsymbol{F}_p(\langle \lambda \rangle/\langle \lambda^p \rangle)$-module. Choose $T_1 \leqq T$ so that $T_1 \geqq C_T(V)$, $T_1/C_T(V)$ has order p^p and is a free Λ-module. Observe that T_1 cannot be elementary, or else $t \neq p$ implies that $T_1 \cong C_T(V) \times T_1/C_T(V)$ as $\langle \lambda \rangle$-groups, and freeness of the right factor over Λ contradicts $(T_1)_\lambda \leqq C_T(V)$. Take any hyperplane A of $C_T(V)$ which is λ-invariant. Then $T_1(\langle \lambda \rangle/\langle \lambda^p \rangle)$ is a "maximal group of maximal class," so by one of [26], [7], [3] we get, for odd p, $Z(T_1(\langle \lambda \rangle/\langle \lambda^p \rangle))/A > C_T(V)/A$. So assume p odd. Since $T/C_T(V)$ is an irreducible $V\langle \lambda \rangle$-module, and since $Z(T/A) > C_T(V)/A$, it follows that T/A is abelian, hence $T = [T, V] \times C_T(A) = [T, V]$ is elementary, which is impossible as noted above. Therefore, $p = 2$ and we also get $O_2(P_\mu)$ nonabelian.

Next consider the action of involutions in $L_{\lambda,\mu}$ on V. Suppose there is an involution w in $L_{\lambda,\mu}$ with $C_V(w) \neq 1$. Then $C_{L_{\lambda,\mu}}(w) \leqq Q$, a proper parabolic subgroup of $L_{\lambda,\mu}$. Let $Q_1 = O_2(Q)$, $Q_0 = C_{Q_1}(w)$. Then we get $[C_V(w), Q_0] \leqq Q_0 \cap C_V(w) = 1$ (because $L_{\lambda,\mu}$ normalizes V). So, $[C_V(w), Q_1] = 1$, by the $P \times Q$ lemma. By induction and $t \neq 2$, we get that $V \cap L_i \leqq Z(L_i)$ whenever L_i is a component of L_μ such that $w \notin C(L_i)$.

If $[L_i, w] = 1$, we claim that $V^{\pi_i} = 1$. Suppose i is an index for which $[L_i, w] = 1$ and $V^{\pi_i} \neq 1$. Set $Y = L_i$. Then V^{π_i} is normalized by Y_λ. If, for some involution x in the center of a Sylow group of Y_λ, $C_{V^{\pi_i}}(x) \neq 1$, we apply induction to get a contradiction. Therefore, by easy calculation, one concludes that there is no four-group W in Y_λ. Therefore $Y_\lambda \cong A_1(2)$, ${}^2A_2(2)$, ${}^2B_2(2)$.

We eliminate these cases. First assume $Y_\lambda \cong A_1(2)$. Then $Y \cong A_1(4)$ or ${}^2A_2(2)$. But $Y \cong A_1(4)$ is out because the only possibility for V^{π_i} is $O_3(Y_\lambda)$, whence $V^{\pi_i} \cong [V, Y_\lambda] \leqq V$. The $P \times Q$ lemma applied to the action of $(\langle\lambda\rangle/\langle\lambda^2\rangle) \times [V, Y_\lambda]$ on $O_2(P_\mu)$ tells us that $[V, Y_\lambda]$ centralizes $O_2(P_\mu)$, against Lemma 3.3. Thus $Y \cong {}^2A_2(2)$ and $Y_\lambda \cong A_1(2)$. Also, $G_\mu \cong {}^2A_{2m}(2)$, and $m \geqq 3$, since $w \in L$ centralizes Y_λ. The only possiblity is $|V^{\pi_i}| = 3$. Since V is an irreducible $\langle\lambda\rangle$-module, $V^{\pi_i} \cong [V, Y_\lambda]$. We have $V_\lambda^{\pi_i} = 1$ because $D_\lambda = 1$. Thus, as $[V, Y_\lambda]$ is cyclic and is normalized by Y_λ, the structure of $PSU(3, 2)$ implies $Z(Y) = 1$. Now it is clear that the parabolic subgroup P we are considering is associated with a subset of the Dynkin diagram



for G_μ (type C_m, $m \geqq 3$) which contains the rightmost (long) root, β_m, but not β_{m-1}. Let Q be the parabolic subgroup associated with $\{\beta_2, \beta_3, \cdots, \beta_m\}$. Then $O^{2'}(Q)/O_2(Q) \cong SU(2m-1, 2)$ and $O_2(Q)$ is the "standard module" for $SU(2m-1, 2)$. In particular, as Y is the group generated by the root groups associated with $\pm\beta_m$, $Y \cong SU(3, 2)$. But this contradicts $Z(Y) = 1$. Thus, $Y_\lambda \cong A_1(2)$ is impossible.

Suppose $Y_\lambda \cong {}^2A_2(2)$. Since $r = 2$ one sees that λ cannot induce a field automorphism on Y by inspecting the possibilities. Thus $\lambda = {}^s\sigma_q$, $s \in \{2, 3\}$. If $\mu = \lambda^2$ were not a field automorphism, $s = 3$ and λ would induce a field automorphism on Y, which is impossible. Thus $s = 2$ and $\mu = \lambda^2$ is a field automorphism; in fact $\lambda = {}^2\sigma_2$, $\mu = \sigma_4$, $Y \cong A_2(4)$. Then, the structure of $A_2(4)$ and $[V, Y_\lambda] \neq 1$ implies that $[V, Y_\lambda] = Z(Y) \cong Z_3$. But then $V = [V, Y_\lambda]$ cannot satisfy $V^{\pi_i} \neq 1$, contradiction.

Suppose $Y_\lambda \cong {}^2B_2(2)$. Then $r = 2$ implies that Y is not of type

${}^2B_2$. Thus, $Y \cong B_2(2)$. Clearly, $V^{\pi_i} \cong 1$ and $V_\lambda = 1$ are impossible in this case.

We conclude that each $V^{\pi_i} = 1$, i.e., that $V \cap O^{2'}(L_\mu) \leqq Z(O^{2'}(L_\mu)) \leqq H_\mu$. Therefore, $[V, L \cap U_{\lambda,\mu}] \leqq H_\mu \cap V$. Since $t \neq p$, $[V, L \cap U_{\lambda,\mu}] = [V, L \cap U_{\lambda,\mu}, L \cap U_{\lambda,\mu}] \leqq [H_\mu, U_{\lambda,\mu}] \leqq U$. Therefore $[V, L \cap U_{\lambda,\mu}] = 1$. Since $[O_2(P)_{\lambda,\mu}, V] = 1$, this gives $[V, U_{\lambda,\mu}] = 1$. We new quote Lemma 3.7 to see that our lemma holds.

It therefore remains to treat the case that $C_V(w) = 1$ for every involution w in $L_{\lambda,\mu}$. Assume this. If $W \leqq L_{\lambda,\mu}$ is elementary of order 4, $V = \langle C_V(x) \mid x \in W^\#\rangle$. So, no such W exist, i.e., $L_{\lambda,\mu}$ has cyclic or quaternion Sylow 2-groups. Thus $r = 2$ implies that $L_\mu \cong A_1(4)$ or ${}^2A_2(2)$ if $L_\mu > L_{\lambda,\mu}$ and $L_\mu = A_1(2)$ or ${}^2A_2(2)$ if $L_\mu = L_{\lambda,\mu}$.

At this point we may enlarge P if necessary to assume that P_μ is a maximal parabolic subgroup of G_μ. Thus, G_μ has rank 2. If $L_\mu \cong A_1(4)$, then $G_\mu \cong A_2(4)$, $B_2(4)$, ${}^2A_3(2)$, ${}^2A_3(4)$ or ${}^2A_4(2)$. If $L_\mu \cong {}^2A_2(2)$, then $G_\mu \cong {}^2A_4(2)$. If $L_\mu \cong A_1(2)$, then $G_\mu \cong {}^2A_3(2)$. By inspection, each of these groups satisfies the conclusion of the lemma, so that the proof is complete.

PROPOSITION 3.1. *Let M be a group such that $O^{p'}(G_{\lambda,\mu}) \leqq M < G_\mu$, $M \not\leqq G_{\lambda,\mu}$ and $U_{\lambda,\mu} \in \mathrm{Syl}_p(M)$. Then $\tilde{M}_{\lambda,\mu} = N_M(O^{p'}(G_{\lambda,\mu}))$ is strongly p-embedded in M.*

(Note that $G_{\lambda,\mu} = N_G(G_{\lambda,\mu})$ unless $G = A_n(k)$, n, q even, $\mu = {}^2\sigma_{q^{r/s}}$, $\lambda = \sigma_q$.)

Proof. Let $R \neq 1$ be a p-group in $G_{\lambda,\mu}$ and, as in Lemma 3.4 embed $N_{G_{\lambda,\mu}}(R)$ in $P(\lambda, \mu)$, a parabolic subgroup of $G_{\lambda,\mu}$. We may assume that $P(\lambda, \mu) \geqq U_{\lambda,\mu}$ by replacing R with a conjugate by an element of $O^{p'}(G_{\lambda,\mu})$ if necessary. Using Lemma 3.4(iv), we have that $P(\lambda, \mu)$ lies in a unique parabolic subgroup $P(\mu)$ of G_μ with $P(\mu)_\lambda = P(\lambda, \mu)$. By Lemma 3.4(v), we may take P, a $\langle\lambda, \mu\rangle$-invariant parabolic subgroup of G with $P_\mu = P(\mu)$ and we may assume $U \leqq P$, by Lemma 3.4(i).

It suffices to prove $M \cap P = M \cap P_\mu \leqq P_{\lambda,\mu} \cdot K$, where K is as in Lemma 3.8. Set $C = C_{P_\mu}(O_p(P_{\lambda,\mu}))$ and take $g \in M \cap P_\mu$. Then $U_{\lambda,\mu} \in \mathrm{Syl}_p(M)$ implies that $M \cap P_\mu$ normalizes $O_p(P_{\lambda,\mu})$, whence $[g, O_p(P_{\lambda,\mu}), \lambda] = 1$. Clearly $[O_p(P_{\lambda,\mu}), \lambda, g] = 1$, and so $[\lambda, g, O_p(P_{\lambda,\mu})] = 1$ by the three subgroups lemma, Thus $[\lambda, g] \in C$. By Lemma 3.8 $C \leqq O_p(P_\mu) \cdot K$, where $K \leqq H_\mu$, $|K| \mid q + 1$. Letting $\bar{\ }$ be the quotient $P \to \bar{P} = P/O_p(P)$, we get $[\overline{P \cap M}, \lambda] \leqq \bar{C} = \bar{K}$. Thus $\overline{P \cap M} \leqq \bar{P}_{\lambda,\mu}$ or if $\bar{K} \neq 1$, $\overline{P \cap M} \leqq N_{\bar{P}_\mu}([\overline{P \cap M}, \lambda]) \leqq N_{\bar{P}_\mu}(\bar{K}) = C_{\bar{P}_\mu}(\bar{K})$ and $\bar{P}$ has a component of type $A_n(k)$, n, q even. Also, we may enlarge P, if necessary, to assume that $\bar{P}_\mu$ has one component.

Suppose $\overline{P \cap M} \leqq \bar{P}_{\lambda,\mu}$. Then $O^{2'}(P_{\lambda,\mu}) \leqq P \cap M \leqq O_2(P_\mu) \cdot L_{\lambda,\mu}$, where

L is a $\langle\lambda, \mu\rangle$-invariant complement to $O_2(P)$ in P. Then $(|M: G_{\lambda,\mu}|, 2) = 1$ implies that $P \cap M = O^{2'}(P_{\lambda,\mu})$, as required. Thus, we may suppose $\overline{P \cap M} \not\leq \bar{P}_{\lambda,\mu}$. Let K, L be as above. We have $1 \neq [\overline{P \cap M}, \lambda] \leqq \bar{K}$, q is even and $G = A_n(k)$, n even, $\mu = 2_{\sigma_q r/2}$, $\lambda = \sigma_q$. From Lemma 3.8, we know that $O^{2'}(C_{\bar{P}_\mu}(\bar{K}))/Z(O^{2'}C_{\bar{P}_\mu}(\bar{K}))) \cong {}^2A_{n-1}(q)$. Thus $\bar{Y} = O^{2'}(C_{\bar{P}_\mu}(\bar{K}))$ satisfies: $\overline{P \cap M} \cap \bar{Y}$ contains a Sylow 2-group of $\overline{P \cap M}$. Since $\bar{U}_{\mu,\lambda} \leqq O^{2'}(\bar{Y}_\lambda) \leqq O^{2'}(\overline{P \cap M})$, we may apply induction to $\bar{P}$ to get $O^{2'}(\bar{Y}_\lambda) \cong C_{n/2}(q)$. The structure of $\bar{P}_\mu$ implies that $N_{\bar{P}_\mu}(\bar{Y}_\lambda) = \bar{K} \times \bar{Y}_\lambda$, whence $\overline{P \cap M} = (\overline{P \cap M} \cap \bar{K}) \times \bar{Y}_\lambda$.

As in the case $\overline{P \cap M} \leqq \bar{P}_{\lambda,\mu}$, we argue that $O^{2'}(P_{\lambda,\mu}) = O^{2'}(P \cap M)$. Write $(O_2(P_\mu)\cdot K) \cap M = O_2(P_{\lambda,\mu})\cdot K_1$, where K_1 is a cyclic $2'$-group. Now, K_1 is trivial on the Frattini factor group of $O_2(P_{\lambda,\mu})$, because K is, whence K_1 centralizes $O_2(P_{\lambda,\mu})$. But also, $[U_{\lambda,\mu}, K_1] \leqq O_2(P_{\lambda,\mu})$. Since K_1 then stabilizes the chain $U_{\lambda,\mu} \geqq O_2(P_{\lambda,\mu}) \geqq 1$, we get $K_1 \leqq C(U_{\lambda,\mu})$. The Frattini argument on $O_2(P_{\lambda,\mu})K_1 \lhd P \cap M$ implies that $C_{P\cap M}(K_1)$ covers $\overline{P \cap M}$, whence $K_1 \leqq Z(P \cap M)$. Since K contains a Hall $2'$-subgroup of $Z(P \cap M)$, it follows that $K_1 \leqq K$, whence $K_1 = K \cap M$. Therefore, $M \leqq P_{\lambda,\mu}\cdot K$, as required.

COROLLARY. *If $p = 2$, $|M|_2 = |U_{\lambda,\mu}|$, $M \geqq O^{2'}(G_{\lambda,\mu})$ and $M \not\leq G_{\lambda,\mu}$, then $\mu \in \langle\lambda\rangle$ and M lies in a unique maximal subgroup M_0 of G_μ, and we are in one of the following situations.*

(a) *$G_\lambda \cong A_1(2)$, $M_0 \cong D_{2^r+1}$, and r is odd, $r \geqq 3$; $G_\mu \cong A_1(2^r)$*

(b) *$G_\lambda \cong {}^2B_2(2) \cong Sz(2)$, r is odd, $r \geqq 5$, and M_0 is a Frobenius group of order*

$$4(2^r \pm 2^{(r+1)/2} + 1);\ G_\mu \cong {}^2B_2(2^r)\,.$$

Proof. Let $L = O^{2'}(G_{\lambda,\mu})$ then $\tilde{M}_{\lambda,\mu} = N_M(O^{2'}(G_{\lambda,\mu}))$ is strongly embedded in M and $L = O_{2',2}(L)$, which implies $L \cong A_1(2)$, ${}^2B_2(2)$ or ${}^2A_2(2)$. We claim that $L \cong {}^2A_2(2)$ is impossible. So, assume $L \cong {}^2A_2(2)$. Then G_μ must be isomorphic to ${}^2A_2(2^r)$ for odd $r \geqq 3$. Let t be an involution of L. Then t inverts $O(M)$ because $C_{G_\mu}(t) = U_\mu$. Thus, $O(L) = [O(L), t] \leqq O(M)$. An easy calculation (which we omit) shows that $O(L) \cong Z_3 \times Z_3$ is self centralizing in G_μ. This means $O(L) = O(M)$ and so $M \leqq N_{G_\mu}(O(L)) = G_{\lambda,\mu} \cong PGU(3, 2)$, i.e., we have no exception in this case. Therefore, M has cyclic Sylow 2-groups, whence $M = O_{2',2}(M)$. A survey of the possibilities produces (a) and (b) as the precise list of exceptions to $M \not\leq G_{\lambda,\mu}$.

REMARK. We henceforth assume that p is odd. Thus, $\tilde{M}_{\lambda,\mu} = M_{\lambda,\mu} = M \cap G_{\lambda,\mu}$ (see Lemma 3.8 and use $G_{\lambda,\mu} = N_{G_\mu}(O^{p'}(G_{\lambda,u}))$ if $G_\mu \not\cong {}^2A_n(q)$, n, q even).

LEMMA 3.9. *If t is an involution of $M_{\lambda,\mu}$, then $C_M(t) \leqq M_{\lambda,\mu}$*

unless either $\lambda^r = \mu$ (i.e., Theorem 1 applies to G) *or one of* (2), (3), (5), (6) *holds.*

Proof. Let t be an involution of $M_{\lambda,\mu}$. Set $C = C_G(t)$. Then $C = \tilde{H}L$, where $\tilde{H}$ is a conjugate of H and $L = O^{p'}(C)$.

We assume that $C \cap M \nleqq M_{\lambda,\mu}$.

Case 1. $L = 1$. Then, letting t' be a conjugate of t in H, have that t' inverts every X_α, $\alpha \in \Sigma$. This implies that U is abelian, so that $G = A_1(k)$. Thus, $\mu = \lambda^r$ and Theorem 1 applies.

We observe that, if L contains some $\tilde{L} \lhd C$ with $p \mid |\tilde{L}_{\lambda,\mu}|$ and $\tilde{L} \cap M = \tilde{L}_{\lambda,\mu}$, we are done; for then, letting $R \in \mathrm{Syl}_p(\tilde{L} \cap M)$ we have $M = (\tilde{L} \cap M)\cdot N_M(R) \leqq M_{\lambda,\mu}$, a contradiction.

Case 2. $L \neq 1$ and quasisimple of rank at least 2. Then by induction, $C \cap M \leqq M_{\lambda,\mu}$ unless $L_\mu/Z(L_\mu) \cong {}^2A_2(p)$, $p = 3$ or 5. In the latter case, $L/Z(L) \cong A_2(k)$. Let t' be a conjugate of t in H and let X_α, X_β, $X_{\alpha+\beta}$ be the root groups centralized by t'. The shape of L_μ forces $G = A_n(k)$, $n \geqq 4$ and $\mu = {}^2\sigma_p$. Since $n \geqq 4$, we may choose roots γ and δ so that $\{\alpha, \beta, \gamma, \delta\}$ is a linearly independent set such that $\gamma + \delta$ is a root. Then, as t' inverts X_γ and X_γ, t' centralizes $X_{\gamma+\delta} = [X_\gamma, X_\delta]$. Since $\gamma + \delta$ is not in the span of α and β, this is a contradiction. Thus, Case 2 does not hold.

Case 3. $L \neq 1$ and quasisimple of rank 1, i.e., $L/Z(L) \cong A_1(k)$. Let t' be a conjugate of t in H. Then t' inverts X_β for all $\beta \neq \alpha$, α a fixed root in Σ^+ (as in Case 1, we know U is nonabelian). It follows that $C_G(X_\alpha)/X_\alpha$ has abelian Sylow p-subgroups. Also, if $O^{p'}(C_G(X_\alpha)/X_\alpha$ were strictly larger then $O_p(C_G(X_\alpha)/X_\alpha)$, a Frattini argument would show that t' centralize some X_β, $\beta \neq \alpha$. Since this is false, $O^{p'}(C_G(X_\alpha)/X_\alpha) = O_p(C_G(X_\alpha)/X_\alpha)$. Therefore, if α is long, $G = A_2(k)$ and if α is short, the fact that there are no long roots orthogonal to α implies $G = B_2(k)$.

Assume $G = B_2(k)$. Then $\langle\lambda, \mu\rangle$ is a cyclic group and Theorem 1 applies since $G_{\lambda,\mu}$ is not an exceptional case.

Thus $G = A_2(k)$. If $\langle\lambda, \mu\rangle$ is cyclic, then Theorem 1 applies since $G_{\lambda,\mu}$ cannot be an exceptional case. So we may assume $\langle\lambda, \mu\rangle$ is not cyclic. We then have $\mu = {}^2\sigma_q r/2$ and $\lambda = \sigma_q$. Then $G_{\lambda,\mu} \cong PGL(2, q)$ and we quote [22] to get that (2), (3), (5) or (6) holds.

Case 4. $L \neq 1$ is not quasisimple. Let $\tilde{L} \nleqq Z(L)$ be any $\langle\lambda, \mu\rangle$-invariant normal subgroup of L. By Lemma 3.2 we have that $|\tilde{L}_{\lambda,\mu}| \equiv 0 \pmod p$. Thus, if $\langle\lambda, \mu\rangle$ had more than one orbit on the set of components of L, Lemma 3.8 applied to an $\tilde{L}$ as above, $\tilde{L} \neq L$ dan to $C_L(\tilde{L}) \neq 1$, shows that $L \cap M = M_{\lambda,\mu}$, a contradiction. Therefore, $\langle \lambda, \mu \rangle$ has one orbit on the set of components of L. So, L has $s \in \{2, 3\}$ components, $\langle \mu \rangle$ is transitive on them and λ normalizes each one.

Since $L \cap M > L_{\lambda,\mu}$, induction implies that $O^{p'}(L_{\lambda,\mu})/Z(L_{\lambda,\mu}) \cong A_1(3)$, $A_1(5)$, or $A_1(5)$ and $L \cap M \cong A_5$, A_7 or M_{10} respectively. But then $L_\mu/Z(L_\mu)$ must be isomorphic to, respectively, $A_1(9)$, ${}^2A_2(5)$ or ${}^2A_2(5)$. No μ of the form ${}^s\sigma_q r/s$ will give $L_\mu/Z(L_\mu)$ isomorphic to any of these possibilities. This final contradiction proves the lemma.

PROPOSITION 3.2. *Suppose* $M_{\lambda,\mu} < M$. *Then* $M_{\lambda,\mu}$ *is strongly embedded in* M, *or else* (6) *or an exceptional case listed in* (2.2) *holds.*

Proof. By Lemma 3.9, it suffices to prove that $N_M(S) \leqq M_{\lambda,\mu}$, for $S \in \mathrm{Syl}_2(M_{\lambda,\mu})$. Supposing this to be false, take an element $g \in N_M(S) - M_{\lambda,\mu}$ of odd order such that $\langle g \rangle$ causes fusion among elements of $Z \leqq \Omega_1(Z(S))$ which are not fused in M. Let z_1, z_2 be two such elements. Assume that $|C_{M_{\lambda,\mu}}(z_1)| \equiv 0 \pmod p$, $i=1, 2$. Then, as $O^{p'}(C_{M_{\lambda,\mu}}(z_1))$ and $O^{p'}(C_{M_{\lambda,\mu}}(z_2))$ are fused under g, $|M_{\lambda,\mu} \cap M^g_{\lambda,\mu}| \equiv 0 \pmod p$. By Proposition 3.1, this forces $g \in M_{\lambda,\mu}$, contradiction. Hence we must show that $|C_{M_{\lambda,\mu}}(z_i)| \equiv 0 \pmod p$.

The arguments in the proof of Lemma 3.9 show that if $O^{p'}(C_G(z_i)) \neq 1$, then $O^{p'}C_{G_{\lambda,\mu}}(z_i)) \neq 1$, so that we may assume $O^{p'}(C_G(z_i)) = 1$. Then, as in Case 1 in the proof of Lemma 3.9, we get that $G = A_1(k)$. But then $\langle \lambda, \mu \rangle$ is cyclic, and Theorem 1 tells us that $p = 3$, $G_\mu \cong A_1(9)$ and $M \cong \Sigma_5$ as in (2.2).

LEMMA 3.10. *G, μ, λ and M satisfy one of the conclusions of Theorem* 2.

Proof. If false, Proposition 3.2 tells us that $M_{\lambda,\mu}$ is strongly embedded in M. By Bender's theorem [2] and Theorem 1, as $\langle \lambda, \mu \rangle$ is not cyclic, $M_{\lambda,\mu}$ is a solvable Steinberg variation. The only possibility is ${}^2A_2(2)$, where $p = 2$ and and the Corollary to Proposition 3.1 tells us that no such M exists, contradiction.

This completes the proof of Theorem 2.

REFERENCES

1. E. Artin, *Geometric Algebra*, Interscience, N. Y. (1957).

2. H. Bender, *Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festläßt*, J. Algebra, **17** (1971), 527-554.

3. N. Blackburn, *On a special class of p-groups*, Acta Math., **100** (1958), 45-93.

4. A. Borel and J. Tits, *Éléments unipotents et sous-groupes paraboliques de groupes*

réductifs. I, Inv. Math., **12** (1971), 95-105.
5. R. Carter, *Simple Groups of Lie Type*, J. Wiley & Sons, N. Y. (1972).
6. L. Dickson, *Linear Groups*, Dover, N. Y. (1958).
7. L. Evans, *On a theorem of Thompson on fixed points of p-groups acting on p-groups*, Math. Z., **93** (1966), 105-8.
8. W. Feit and J. Thompson, *Solvability of groups of odd order*, Pacific J. Math., **13** (1963), 775-1029.
9. B. Fischer, *Finite groups generated by 3-transpositions*. I, Inv. Math., **13** (1971), 232-246.
10. ———, *Subgroups of* $^2E_6(2)$ *generated by 3-transpositions*, (to appear).
11. D. E. Flesner, *Maximal subgroups of* $PSp_4(2^n)$ *containing central elations or noncentered skew elations*, Illinois J. Math., **19** (1975), 247-268.
12. G. Glauberman, *Central elements in core free groups*, J. Algebra, **4** (1966), 403-420.
13. D. Gorenstein, *Finite Groups*, Harper & Row, N. Y. (1968).
14. D. Gorenstein and K. Harada, *Finite groups whose 2-subgroups are generated by at most 4 elements*, Mem. Amer. Math. Soc., No. **147** (1974).
15. R. Griess, *Schur multipliers of finite simple groups of Lie type*, Trans. Amer. Math. Soc., **183** (1973), 355-421.
16. R. W. Hartley, *Determination of the ternary collineation groups whose coefficients Lie in the* $GF(2^n)$, Ann. Math., **27** (1925), 140-158.
17. J. Humphreys, *Linear Algebraic Groups*, Springer-Verlag, N. Y. (1975).
18. N. Iwahori, *Centralizers of involutions in finite Chevalley group*, Lecture Notes in Math. No. **131**, Springer-Verlag (1970).
19. Z. Janko, *A new finite simple group with abelian Sylow 2-subgroups and its characterization*, J. Algebra, **4** (1966), 147-186.
20. S. Lang, *Algebraic groups over finite fields*, Amer. J. Math., **78** (1956), 555-563.
21. J. McLaughlin, *A simple group of order* 898,128,000, From R. Brauer & H. Sah, 'Theory of Finite Groups', Benjamin, N. Y. (1969).
22. H. N. Mitchell, *Determination of the ordinary and modular ternary linear groups*, Trans. Amer. Math. Soc., **12** (1911), 207-242.
23. R. Steinberg, *Endomorphisms of linear algebraic groups*, Mem. Amer. Math. Soc., no. **80** (1968).
24. ———, *Lectures on Chevalley Groups*, Yale Univ. (1967).
25. M. Suzuki, *On a class of doubly transitive groups*, Ann. Math., **75** (1962), 105-145.
26. J. Thompson, *Fixed points of p-groups acting on p-groups*, Math. Z., **86** (1964), 12-13.
27. D. Wales, *Generators of the Hall-Janko group as a subgroup of* $G_2(4)$, J. Algebra, **13** (1969), 513-516.
28. J. Walter, *The characterization of finite groups with abelian Sylow 2-subgroups*, Ann. Math., **89** (1969), 405-514.

Received April 14, 1976 and in revised form December 14, 1976. This research was supported by NSF Grants, MPS 74-07807, MPS 71-03070, and MPS 75-07512.

University of California
Santa Cruz, CA 95064