JOURNAL OF ALGEBRA **106**, 15–45 (1987)

Primitive Permutation Groups of Odd Degree, and an Application to Finite Projective Planes

WILLIAM M. KANTOR*

Department of Mathematics, University of Oregon,
Eugene, Oregon 97403

Communicated by Marshall Hall, Jr.

Received April 1, 1984

INTRODUCTION

One of the most beautiful and important results concerning finite projective planes is the Ostrom–Wagner Theorem [26]: such a plane admitting a 2-transitive collineation group must be desarguesian. It has long been conjectured that the same conclusion must hold if it is only assumed that there is a collineation group transitive on incident point-line pairs [11, pp. 208–214; 17]. The starting point for this paper was a proof of this conjecture, modulo a degenerate situation:

THEOREM A. *Let π be a projective plane of order n, and let F be a collineation group transitive on incident point-line pairs. Then either*

(i) *π is desarguesian and $F \geqslant PSL(3, n)$, or*

(ii) *F is a Frobenius group of odd order $(n^2+n+1)(n+1)$, and n^2+n+1 is prime.*

It is well known that the group F in Theorem A must act primitively on the points of π [17; 11, p. 79]. It turns out that this weaker condition is more useful than the transitivity assumed in Theorem A:

THEOREM B. *Let π be a projective plane of order n, and let F be a collineation group permuting the points primitively. Then either*

(i) *π is desarguesian and $F \geqslant PSL(3, n)$, or*

(ii) *F is a regular or Frobenius group of order dividing $(n^2+n+1)(n+1)$ or $(n^2+n+1)\,n$, and n^2+n+1 is prime.*

* This research was supported in part by NSF Grant MCS 7903130–82.

0021-8693/87 $3.00

Theorems A and B, part (ii), involve possibilities that have been studied with only limited success for 35 years. These are arithmetic situations, rather than group-theoretic ones (cf. [11, pp. 87–90; 208–213]).

The proof of the Ostrom–Wagner Theorem is both elegant and informative. By contrast, our proof of Theorem B uses a sledgehammer approach, involving detailed properties of all finite simple groups. In fact, the proof uses relatively little concerning projective planes. The plane in Theorem B has n^2+n+1 points, and this number is odd. The classification of finite simple groups[1] provides fairly good insight into the structure of primitive permutation groups of odd degree, as can be seen from (2.1) and the following result.

THEOREM C. *Let F be a primitive permutation group on a set of odd size, and let x be a point. If F has a nonabelian simple normal subgroup G, then one of the following holds.*

(C.1) *F is A_d or S_d, and F_x is the stabilizer of a subset of the relevant d-set Y, or F_x is the stabilizer of a partition of Y into l subsets of size k, where $d=kl$; or G is A_7 and G_x is $PSL(3, 2)$.*

(C.2) *G is a group of Lie type of characteristic 2, and G_x is a parabolic subgroup.*

(C.3) *G is a group of Lie type of odd characteristic, and $G_x = N_G(C_G(\sigma))$ for a field automorphism σ of prime order.*

(C.4) *G is $PSL(d, q)$ with q odd and G_x is either the stabilizer of a subspace or the stabilizer of a pair of incident subspaces interchanged by a graph automorphism lying in $F_x - G_x$; or G is $E_6(q)$ with q odd and G_x is a parabolic subgroup of type $P\Omega^+(10, q)$.*

(C.5) *G is a classical group of odd characteristic and G_x is the stabilizer of a direct sum decomposition into two subspaces, which are perpendicular to one another if G is not of the form $PSL(d, q)$ and are interchanged by a graph automorphism lying in $F_x - G_x$ if G is of the form $PSL(d, q)$.*

(C.6) *G is a classical group of odd characteristic, and G_x is the stabilizer of a direct sum decomposition into subspaces of equal dimension, which are all isometric and pairwise orthogonal if G is not of the form $PSL(d, q)$.*

(C.7) *G is $G_2(q)$, ${}^3D_4(q)$, or $E_7(q)$ with q odd, and G_x is the normalizer of a fundamental subgroup; or G is $E_7(q)$ or $E_8(q)$ with q odd, and G_x is the*

[1] At the time of this writing (January, 1984), this classification is not quite complete: the uniqueness of the Monster has not been proved. However, this does not cause any difficulties with our use of the classification.

stabilizer of a family of k pairwise commuting fundamental subgroups, where $k=3$ or 7 when G is $E_7(q)$ and $k=8$ when G is $E_8(q)$.

(C.8) *G is ${}^3D_4(q)$ and $G_x = G_2(q)$; or G is $G_2(q)$ or ${}^3D_4(q)$, and G_x is the normalizer of a subgroup $SL(3, q)\cdot 2$ or $SU(3, q)\cdot 2$ depending on whether $q \equiv 1$ or $-1 \pmod 4$.*

(C.9) (i) *G is $F_4(q)$, ${}^2E_6(q)$, or $E_6(q)$ with q odd, and F_x is the normalizer of a subgroup $2^2 \cdot P\Omega(8, q)$; or* (ii) *G is $F_4(q)$, ${}^2E_6(q)$, $E_6(q)$, $E_8(q)$, or $E_8(q)$ with q odd, and G_x is the normalizer of a subgroup $2\cdot P\Omega(9, q)$, $(4, q+1)\cdot P\Omega^-(10, q)$, $(4, q-1)\cdot P\Omega^+(10, q)$, $2\cdot P\Omega^+(16, q)$* or *$2^2\cdot(P\Omega^+(8, q)\times P\Omega^+(8, q))$, respectively.*

(C.10) *G is $G_2(q)$, $G_2(q)$, $P\Omega(7, q)$, $P\Omega^+(8, q)$, or $P\Omega^+(8, q)$ for a prime $q \equiv \pm 3 \pmod 8$, and G_x is $2^3PSL(3, 2)$, $G_2(2)$, $\Omega(7, 2)$, $\Omega^+(8, 2)$,* or *$2^6\cdot 2^3PSL(3, 2)$, respectively; and in the latter case $F_x - G_x$ contains a triality automorphism.*

(C.11) *G is $E_8(q)$, $E_7(q)$, $E_6(q)$, ${}^2E_6(q)$, or $G_2(q)$, q is odd, and F_x is the normalizer of an abelian subgroup of order $(q\pm 1)^8$, $(q\pm 1)^7/2$, $(q-1)^6/d$, $(q+1)^6/d$, or $(q\pm 1)^2$, respectively, where $d\in\{1, 3\}$ and $q\pm 1\equiv 0 \pmod 4$; and, if $G=G_2(q)$, then q is a power of 3 and $F_x - G_x$ contains a graph automorphism. (See* (3.6) *for an explicit construction of these abelian groups.)*

(C.12) *G is $PSU(3, 5)$ and G_x is $A_6\cdot 2$.*

(C.13) *G is $PSL(2, q)$ or ${}^2G_2(q)$ with q odd, $q>3$, and either G_x is the centralizer of an involution or G is $PSL(2, q)$ and G_x is A_4, S_4, or A_5.*

(C.14) *G is sporadic.*

We have not been precise in (C.1) and (C.3)–(C.6): the exact conditions on dimensions are purely arithmetic and do not seem interesting. In (C.5) and (C.6) we have dealt with the groups $P\Omega(5, q)$ and $P\Omega^\pm(6, q)$ but have not described G_x in the case of their isomorphic copies $PSp(4, q)$, $PSL(4, q)$ and $PSU(4, q)$. The "fundamental subgroups" in (C.7) are isomorphic to $SL(2, q)$, and will be defined in Section 3. For further informaton concerning (C.7), (C.9), and (C.11), see Table II, [18] and [2, Theorem 3], respectively. In each case appearing in (C.7)–(C.13), the group G_x is uniquely determined up to conjugacy in Aut G but not necessarily in G. (See [21] for discussions and applications of the examples in (C.10), and especially of the $P\Omega^+(8, q)$-classes of subgroups $\Omega^+(8, 2)$.) Finally, the possibilities in (C.14) are mostly known, and obviously involve a case-by-case analysis.

Theorem C is almost implicit in Aschbacher's papers [1] and [2]. In effect, our proof is just a fairly straightforward exercise in the use of his classical involution theorem and other results in [1], with some assistance from the work in [8, 10] and [19] on groups generated by long root elements. Theorem C constains as a special case Theorem A of [2], which was proved using [1] but not [8, 10, 19]. Theorem C should also be compared to the classification of all primitive permutation representations of prime power degree of simple groups [23, 20, 16].

This paper has been divided into two parts. Part I contains a proof of Theorem C. Part II contains the deduction of Theorem B from Theorem C. Since we are proving Theorem B instead of Theorem A, none of the known results concerning flag-transitive collineation groups are relevant. Instead, we require the result of Wagner [31] stating that a finite projective plane is desarguesian if its collineation group is transitive on points and contains a nontrivial perspectivity. Beyond this, the proof involves the tedious elimination of each of the various possibilities in Theorem C using properties of G, elementary counting arguments, and properties of integers of the form m^2+m+1. It does not seem as if the stronger hypothesis of Theorem A would have significantly simplified or shortened this obnoxious case analysis.

Our group theoretic and geometric notation is standard. For the required background concerning root groups and fundamental subgroups, see [8, 10, 19] and, of course, [7]. If k is an integer and p is a prime then k_p denotes the largest power of p dividing k.

If G is a group then $n \cdot G$ denotes an extension of a group of order n by G, while $G \cdot n$ denotes an extension of G by a group of order n. If Σ is a family of subsets of G, and $H \leqslant G$, then $H \cap \Sigma$ denotes $\{S \in \Sigma \mid S \subseteq H\}$.

PART I. THEOREM C

1. Notes on Aschbacher's Classical Involution Theorem

In [1], Aschbacher considered a group X, and an X-invariant collection Ω of subgroups of X, such that the following hold for all A, $B \in \Omega$, $A \neq B$:

(Ω.1) A has a unique involution $z(A)$ and nonabelian Sylow 2-subgroups;

(Ω.2) Either $A = O^{2'}(A)$ or $A/O(A) \cong SL(2, 3)$;

(Ω.3) $A/O(A) \cong B/O(B)$;

(Ω.4) $|A \cap B|_2 \leqslant 2$, and $[A, B] = 1$ if $|A \cap B|_2 = 2$;

(Ω.5) If v is any 2-element in $B - Z(B)$ centralizing $z(A)$ then v normalizes A.

Throughout this section we will assume that (Ω.1)–(Ω.5) hold. The following result is an easy consequence of the results in [1].

Theorem 1.1. *Assume that $X=\langle\Omega\rangle$ and $O(X)=O_2(X)=1$. Then there are subgroups $Y_1,\dots,Y_\alpha$ of X such that, for each β,*

(i) $Y_\beta=\langle Y_\beta\cap\Omega\rangle$;

(ii) *If Y_β is simple it is M_{11}, M_{12}, $Sp(6,2)$, $\Omega^+(8,2)$, or a Chevalley group over a field of odd characteristic (and, in the latter case, each A in $Y_\beta\cap\Omega$ is normal either in a fundamental subgroup of Y_β or, for $Y_\beta=G_2(q)$ or ${}^3D_4(q)$, possibly in a short fundamental subgroup of Y_β);*

(iii) *If Y_β is not simple then Y_β is $PSL(2,s^2)\cdot 2$, $PSL(3,s)\cdot 2$ or $PSU(3,s)\cdot 2$ for some odd prime power s;*

(iv) $X=Y_1\times\cdots\times Y_\alpha$; *and*

(v) $\Omega=\bigcup_\beta(Y_\beta\cap\Omega)$.

Proof. In [1, pp. 356–357], Aschbacher defined sets $A(K)\subseteq A^*(K)\subseteq\Omega$ for each $K\in\Omega$ so that [1, Theorems 3 and 4]

(1.2) (a) If $A(K)\neq\varnothing$ for some $K\in\Omega$ then $[A^*(K),\Omega-A^*(K)]=1$ and $\langle A^*(K)\rangle\cong M_{12}$ or $G_2(q)$ with $q=2$ or q odd, and

(b) If $A(K)=\varnothing$ for all $K\in\Omega$ then distinct orbits of X on Ω commute.

It follows that (i) and (v) hold for suitable groups Y_β, and either Y_β is M_{12} or $G_2(q)$ as in (1.2)(a), or Y_β is transitive on $Y_\beta\cap\Omega$. In the latter case [1, Theorem 1] states that (ii) or (iii) holds. Now (iv) is clear. ▮

Remark. We have not defined $A(K)$. However, we note that, if $Y_\beta=\langle A^*(K)\rangle$ is as in (1.2)(a), then Y_β has two orbits on $Y_\beta\cap\Omega$ and $Y_\beta\cap\Omega$ contains two members sharing an involution.

Lemma 1.3. *If $X=\langle\Omega\rangle$, $O(X)=1$, $A\in\Omega$, $Q\in\mathrm{Syl}_2(A)$ and $Z(Q)\not\leq O_2(X)$, then $O_2(X)$ centralizes Q.*

Proof. Since $Q\cap O_2(X)=1$, Q centralizes $O_2(X)$ by [1, (6.13)]. ▮

2. Preliminary reductions

Let F be a primitive permutation group on a set X, where $|X|=n$ is *odd*. Let $x\in X$. According to the O'Nan–Scott Theorem [28, 3], there are three possible situations:

(2.1) (i) F has a regular normal elementary abelian p-subgroup V, and F_x is an irreducible subgroup of Aut V.

(ii) $F \rhd T_1 \times \cdots \times T_k$ with T_i simple, $k > 1$, F transitive on $\{T_1, ..., T_k\}$, and $F \leqslant F_1 wr S_k$ for a primitive group F_1 of degree n_1, where $F_1 \trianglerighteq T_1$ and $n = n_1^k$.

(iii) $F \trianglerighteq G$ with G simple and nonabelian, and $C_F(G) = 1$.

Clearly, (2.1)(i) is impossible to classify, while (2.1)(ii) more or less reduces to (2.1)(iii)—except, of course, that any transitive group of degree k may be induced on $\{T_1, ..., T_k\}$. Therefore, we will focus on (2.1)(iii), which is the situaton in Theorem C.

The remainder of Part I is concerned with the proof of Theorem C. First, we will introduce slightly more convenient notation:

$$M^* = F_x \quad \text{and} \quad M = G_x,$$

$$T^* \in \mathrm{Syl}_2(M^*) \quad \text{and} \quad T = T^* \cap M.$$

PROPOSITION 2.2. *If $G = A_m$, $m \neq 6$, then* (C.1) *holds.*

Proof. Here, $F = A_m$ or S_m, and T contains the product of two disjoint transpositions. If M^* is intransitive on the relevant m-set then it is the stabilizer of a subset. Otherwise, since M^* contains a product of two disjoint 2-cycles it is imprimitive for $m \geqslant 8$. Finally, the possibilities for $m \leqslant 7$ are easy to enumerate, and show that (C.1) holds in all cases. ▌

LEMMA 2.3. *If G is of Lie type and characteristic p, and if either M contains a Sylow p-subgroup of G or if $O_p(M) \neq 1$, then M is a parabolic subgroup of G. Moreover, if p is odd then* (C.4) *holds, while if $p = 2$ then* (C.2) *holds.*

Proof. Let $U \in \mathrm{Syl}_p(G)$. If $U \leqslant M$ then, by [29, (1.6)], $\langle U^M \rangle$ is contained in a uniquely determined parabolic subgroup P of G. Then M^* normalizes P, so that $M^* = N_F(P)$. Thus, $M = M^* \cap G = P$.

Similarly, if $O_p(M) \neq 1$ then, by [4], M is in a canonically defined parabolic subgroup P. As above, $M = P$.

If p is odd it is straightforward to check that only the possibilities in (C.4) can occur. This is especially easy when G is a classical group. When G is exceptional, it follows from Table 1 in Section 3 in view of the fact that G and $M/O_p(M)$ do not have the same rank. ▌

LEMMA 2.4. *If $G = PSL(2, q)$ or ${}^2G_2(q)$ with q odd and $q > 3$, then* (C.3) *or* (C.1)(3) *holds.*

Proof. This follows readily from [12, Chap. 12; 32; 33]. ▌

LEMMA 2.5. *If $G = PSL(3, q)$ or $PSU(3, q)$ with q odd then one of* (C.3), (C.4), (C.6), *or* (C.12) *holds.*

Proof. This follows from an examination of the lists in [25]. ∎

3. FUNDAMENTAL SUBGROUPS

In Sections 3–6, G will be a group of Lie type over $GF(q)$, where q is odd (cf. (2.3)) and G is not as in (2.4) or (2.5). Let p be the prime dividing q.

Pairs of opposite long root groups generate subgroups $SL(2, q)$, called *fundamental subgroups.* Let $\tilde{\Omega}$ be the set of all fundamental subgroups. Then G is transitive on $\tilde{\Omega}$, and $\tilde{\Omega}$ satisfies (Ω.1)–(Ω.5).

Let T be as in Section 2 and let $Q \leqslant T$ be a Sylow 2-subgroup of a member of $\tilde{\Omega}$. We will be concerned with the conjugacy class Q^G of subgroups of G.

Let $\Delta = T \cap Q^G$. The members of Δ commute in pairs [1, (6.2); 2, (1.3)].

If $H \leqslant G$ and $T \cap H \in \mathrm{Syl}_2(H)$, write $m(H) = |T \cap H \cap Q^G|$. In [2, Theorem 2], both $m(G)$ and $N_G(\Delta)^{\Delta}$ are determined. These are listed in Table I (where $k = m(G)/2$).

If $R \in Q^G$ then R is in a unique member $\tilde{R}$ of $\tilde{\Omega}$. Note that

(3.1) *If* $[Q, R] = 1$ *then* $[\tilde{Q}, \tilde{R}] = 1$.

In general, if $H = \langle H \cap Q^G \rangle$ write $\tilde{H} = \langle \tilde{R} \mid R \in H \cap Q^G \rangle$.

In the next two results we will not assume the hypotheses of Theorem C. For the first one, cf. [9, (3.4)].

TABLE I

G	$m(G)$	$N_G(\Delta)^{\Delta}$
$PSL(n, q)$	$[n/2]$	$S_{m(G)}$
$PSp(2n, q)$	n	S_n
$PSU(n, q)$	$[n/2]$	$S_{m(G)}$
$P\Omega^+(2n, q)$	$2[n/2]$	$2^{k+1-(2,n)} \cdot S_k$
$P\Omega(2n+1, q)$	$2[n/2]$	$2^k \cdot S_k$
$P\Omega^-(2n, q)$	$2[(n-1)/2]$	$2^k \cdot S_k$
$G_2(q)$	1	1
${}^3D_4(q)$	1	1
$F_4(q)$	4	S_4
${}^2E_6(q)$	4	S_4
$E_6(q)$	4	S_4
$E_7(q)$	7	$PSL(3, 2)$
$E_8(q)$	8	$2^3 \cdot PSL(3, 2)$

PROPOSITION 3.2. *Let $\tilde{A}$, $\tilde{B} \in \tilde{\Omega}$ and $J = \langle \tilde{A}, \tilde{B} \rangle$. Then J has a homomorphic image $PSL(3, q)$, $PSU(3, q)$, $G_2(q)$, ${}^3D_4(q)$, or $P\Omega^{\pm}(d, q)$, $d \leqslant 8$, such that $\tilde{A}$ and $\tilde{B}$ project onto fundamental subgroups.*

Proof. If G is an orthogonal group acting projectively on its natural d-dimensional module V then $\dim C_V(\tilde{A}) = d - 4$. When $d \leqslant 8$ use [19]. If $d > 8$ then $C_V(J) \neq 0$, and the result follows easily by induction. The case of the remaining classical groups is handled in exactly the same manner (recalling that $PSp(4, q)$, $PSL(4, q)$ and $PSU(4, q)$ can all be viewed as orthogonal groups). If G is $G_2(q)$ or ${}^3D_4(q)$ then [19] again applies.

In the case of the remaining exceptional groups of Lie type a similar approach works using the following triples (G, d, f), where d is the dimension of a suitable basic module V for G and $f = \dim C_V(\tilde{A})$:

$$(E_8(q), 248, 133); \qquad (E_7(q), 56, 32); \qquad (E_6(q), 27, 15);$$
$$({}^2E_6(q), 27, 15); \qquad (F_4(q), 26, 14).$$

In each of these cases, the weights for V easily produce the indicated value of f.

Since $f > d/2$, in each case $C_V(J) \neq 0$. If $0 \neq v \in C_V(J)$ then $G_v/O_p(G_v)$ is a group of Lie type by [4, 8]. Thus, by successively replacing G by smaller groups we eventually embed a homomorphic image of J into a classical group, thereby reverting to the first paragraph of the proof. ▮

The only interesting parts of the proof of Theorem C are the following curious fact and its subsequent use in (3.7).

PROPOSITION 3.3. *Let Y be an elementary abelian r-subgroup of G normalized by some element $f \in Q$ of order 4, where r is a prime other than 2 and p. Then one of the following holds* (*where $t = f^2$*):

(i) *t centralizes Y, or*

(ii) *$|Y| = 9$, $G = PSL(3, q)$ or $PSU(3, q)$, and the preimage of Y in $SL(3, q)$ or $SU(3, q)$ is extraspecial of order 27.*

Proof. Let Y and G produce a counterexample with $|G| + |Y|$ minimal. Let $1 \neq y \in Y$ with $y^t = y^{-1}$.

We claim that $Y = \langle y^{\langle f \rangle} \rangle$. For otherwise, since (i) does not hold for the pair G, $\langle y^{\langle f \rangle} \rangle$, we must have $G = PSL(3, q)$ or $PSU(3, q)$ as in (ii). However, it is easy to check that the only abelian 3-group normalized by f but not centralized by t has order 9 (cf. [25, pp. 240–241]). Thus, $Y = \langle y^{\langle f \rangle} \rangle$.

Set $J = \langle \tilde{Q}, \tilde{Q}^y \rangle$. Then $\langle y \rangle = \langle tt^y \rangle$ is in J, so that $Y \leqslant J$.

First, suppose that $O_p(J) \neq 1$. By [4] there is a parabolic subgroup P of

G such that $J \leqslant P$ and $O_p(J) \leqslant O_p(P)$. Let φ denote the natural homomorphism $P \rightarrow P/O_p(P)$. Then $J^\varphi \cong J/O_p(J)$ is contained in $P^\varphi = (\prod_i X_i)\, H$, where the X_i are pairwise commuting groups of Lie type and H is a torus. Moreover, $\tilde{Q}^\varphi$ is a fundamental subgroup of P^φ, and hence lies in some X_i. Since $[\tilde{Q}, \tilde{Q}^\varphi] \neq 1$, also $(\tilde{Q}^y)^\varphi \leqslant X_i$. Thus, $J^\varphi \leqslant X_i$. In view of the minimality of $|G| + |Y|$, $X_i/Z(X_i)$ is $PSL(3, q)$ or $PSU(3, q)$. By [8, 19], G has a unique class of subgroups S generated by long root groups such that $S/Z(S) \cong X_i/Z(X_i)$. Since Y^φ is elementary abelian it can lie in $PSL(3, q)$ or $PSU(3, q)$ but not in $SL(3, q)$ or $SU(3, q)$. Thus, $Z(X_i) = 1$. However, since $G \neq X_i$, a glance at the groups G shows that $S = SL(3, q)$ or $SU(3, q)$. This contradicts the fact that $X_i \neq SL(3, q)$, $SU(3, q)$.

Consequently, $O_p(J) = 1$. By (3.2) and [19], $J/Z(J)$ is $PSL(3, q)$, $PSU(3, q)$, $G_2(q)$, ${}^3D_4(q)$, or $P\Omega^+(d, q)$ for some $d \leqslant 8$.

Let V be the natural projective module for $J/Z(J)$ over the algebraic closure K of $GF(q)$. Then $\dim V \leqslant 8$. Assume that the Frobenius group $Y\langle f \rangle$ acts linearly on V—which is certainly the case when $\dim V > 4$. Then V contains a copy of the regular representation of $\langle f \rangle$. But then $C_V(f) \neq C_V(f^2)$, which contradicts the fact that Q is contained in a fundamental subgroup of J.

Thus, $Y\langle f \rangle$ pulls back to a subgroup $D\langle f \rangle$ of $GL(V)$, where we may assume that $D = [D, f]$, D is an r-group, and $Z(D) \neq 1$ consists of scalars.

Let $\dim V = 3$. Then $J/Z(J) = PSL(3, q)$ or $PSU(3, q)$, and $D\langle f \rangle$ has the form $3^{1+2}\langle f \rangle$ by [25]. Moreover, J only acts projectively on V, since $Z(D) \neq 1$. Thus, $Z(J) = 1$ and $J \neq SL(3, q)$, $SU(3, q)$. Consequently, $G = J$ (using S as above) and (ii) holds.

This leaves the case $\dim V = 4$. However, $r \nmid |Z(SL(4, K))|$ so that this case cannot occur. ▮

Now consider the groups F, M^*, M and T^* of Section 2, so that $Q \leqslant T \leqslant M$. From now on *we will assume that G is not as in* (2.4) *or* (2.5).

Write $A = \tilde{Q} \cap M$, $Z(A) = \langle z(A) \rangle$ and

$$\Omega = A^{M^*}, X = \langle \Omega \rangle.$$

Then A contains a Sylow 2-subgroup Q of $\tilde{Q}$, and is known by [12, Ch. 12]. A staightforward check yields:

LEMMA 3.4. (i) *Ω satisfies* (Ω.1)–(Ω.5), *and*

(ii) $X = \langle Q^{M^*} \rangle$.

Note that the case $G = G_2(3^e)$ is different from all others: there, $\operatorname{Aut} G$ does not act on $\tilde{\Omega}$. In other words, in that case some members B of Ω may not be contained in members of $\tilde{\Omega}$. Nevertheless, $\tilde{B}$ continues to be well defined: $\tilde{B}$ is a short fundamental subgroup (generated by short root groups).

LEMMA 3.5. (i) *$\tilde{X}=X$ or G.*

(ii) *If $\tilde{X}=G$ then Ω is not the union of two nonempty commuting subsets.*

Proof. (i) Since M^* normalizes X it acts on $\langle \tilde{R} \mid R \in Q^{M^*}\rangle$, which equals $\tilde{X}$ by Sylow's theorem. If $M^*\tilde{X}=M^*$ then $\tilde{X} \leqslant M^* \cap G=M$, so that $\tilde{X}=X$. The only other possibility is that $M^*\tilde{X}=F$, in which case $\tilde{X}$ cannot be proper in G.

(ii) Assume that $\Omega=\Omega_1 \cup \Omega_2$ with $\Omega_i \neq 0$ and $[\Omega_1, \Omega_2]=1$. If $Q_i \in \Omega_i$ then $[\tilde{Q}_1, \tilde{Q}_2]=1$. Thus, $X=\langle \tilde{\Omega}_1, \tilde{\Omega}_2\rangle=\langle\tilde{\Omega}_1\rangle\langle\tilde{\Omega}_2\rangle \neq G$. ▌

EXAMPLE 3.6. Let η be a set of subgroups of T such that (i) each $R \in \eta$ is a maximal cyclic subgroup of some member of Q^G, (ii) $\eta^T=\eta$, (iii) $W=\langle\eta\rangle$ is abelian, and (iv) $|\eta|$ is maximal subject to (i)–(iii). Then η and W are uniquely determined up to conjugacy [2, (1.4)]. Moreover, $N_1/O(N_1)\, W$ is described in [2, Theorem 3], where $N_1=\langle Q_1 \mid Q_1 \in Q^G$ and $Q_1 \leqslant N_G(W)\rangle$.

If G is a classical group then $N_G(W)$ is either reducible or imprimitive on the natural projective module for G.

If G is $F_4(q)$ then $N_G(W)$ lies in the normalizer of a subgroup $2^2 \cdot P\Omega^+(8, q)$. If G is $E_6(q)$ with $q \equiv -1 \pmod 4$, or ${}^2E_6(q)$ with $q \equiv 1 \pmod 4$, then $N_G(W)$ is again contained in the normalizer of a subgroup $2^2 \cdot P\Omega^+(8, q)$ [2, Theorem 6]. In all remaining situations in which G is $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$ or $E_8(q)$, [1, Theorem 3] and the remainder of the list in Theorem C show that the group $N_G(W)$ in (C.11) is maximal in G. When G is $E_6(q)$, $E_7(q)$, or $E_8(q)$ and $q \equiv 1 \pmod 4$, $N_G(W)$ is just the group "N" of BN-fame. The orders given in (C.11) follow easily. (N.B. When $G=E_m(q)$, $m=7$ or 8, let $\tilde{\Delta}$ be a family of m pairwise commuting fundamental subgroups. Then $W<\langle\tilde{\Delta}\rangle$, which makes it very easy to handle $N_G(W)$ both in these cases and in the closely related cases $E_6(q)$ and ${}^2E_6(q)$.)

If G is $G_2(q)$ or ${}^3D_4(q)$ then $N_G(W)$ normalizes a subgroup $S=SL(3, q)$ or $SU(3, q)$ generated by long root groups. However, if G is $G_2(q)$ and q is a power of 3 then there is a graph automorphism interchanging $Q \cap W$ and $C_W(Q)$ but not normalizing S, as required in (C.11).

LEMMA 3.7. *If M contains no fundamental subgroups, and if $O(M^*) \neq 1$, then* (C.6) *or* (C.11) *holds.*

Proof. Let Y be a minimal normal elementary abelian r-subgroup of M^* contained in M, where $r \neq 2$, p (recall that we are assuming that $O_p(M) = 1$). Define η as in (3.6), let $R \in \eta$, and let t be the involution in R. Since (3.3)(ii) does not hold for G, t centralizes Y. Then Y acts on the set of 1, 2, or 4 subnormal fundamental subgroups of $C_G(t)$. There are 4 such subgroups only when G is $P\Omega^+(8, q)$, in which case G has no 3-element permuting them nontrivially (although Aut G does). Consequently, Y normalizes $\tilde{R} \cap M$ (where $\tilde{R}$ is the fundamental subgroup containing R).

Write $R^+ = \tilde{R} \cap M$. Clearly, $[R^+, Y] \leqslant R^+ \cap Y$. If $[R^+, Y] = 1$ then $M^* = N_F(Y) \geqslant \tilde{R}$, contrary to our hypothesis.

Thus, $1 \neq R^+ \cap Y \lhd R^+$, and R^+ has a unique maximal cyclic subgroup R_0. Since $N_G(\tilde{R})$ does not induce nontrivial field automorphisms on $\tilde{R}$, it follows that Y and $R^+ \cap Y$ act the same on R^+. Thus, $R_0 = C_{R^+}(Y)$.

Similarly, if D is in some member of η^{M^*} we can define D^+ and D_0 as above. Then $D_0 \cap Y$ centralizes R_0, so that R_0 acts on the only fundamental subgroup $\tilde{D}$ containing $D_0 \cap Y$. It follows that R_0 acts on D^+ and hence on D_0. Write $R_2 = O_2(R_0)$ and $D_2 = O_2(D_0)$. Then $[R_2, D_2] \leqslant R_2 \cap D_2$, and consequently $[R_2, D_2] = 1$. (For, by (Ω.4) the only other possibility is that $R_2 \cap D_2 = \langle t \rangle$, in which case $\tilde{R}$ and $\tilde{D}$ commute since $R_2 \neq D_2$.)

This shows that the set η_2 of all the groups D_2 generates an abelian normal subgroup W_2 of M^*. Moreover, $|\eta_2| \geqslant |\eta|$. Then $\eta_2 \in \eta^G$ [2, (1.4)], and (3.6) applies. ∎

The preceding proof depended upon (3.3) and Aschbacher's results concerning η^G. The case $O_2(M) \neq 1$ is even easier, since it is implicit in [1]:

LEMMA 3.8. *If* $\tilde{X} = G$, $O(M) = 1$, *and* $O_2(M) \neq 1$ *then* (C.5), (C.6), (C.10), *or* (C.11) *holds.*

Proof. Let Y be a minimal normal 2-subgroup of M^* contained in M. Then $z(A) \in Y$ (since otherwise by (1.3) Q centralizes Y and $M^* = N_F(Y) \geqslant \langle \tilde{Q}^{M^*} \rangle = \tilde{X}$, which is not the case). Consequently, $Y = \langle z(A)^{M^*} \rangle \leqslant X$.

In view of (3.5)(ii), [1, Theorems D and 3] provide an $O(X) = 1 \neq O_2(X)$ version of (1.2), stating that one of the following holds: (i) $W \lhd X$ (cf. (3.6)); (ii) $X \cong \mathbb{Z}_2^{n-d} \rtimes A_n$ for some $n \geqslant 5$, where $d = (2, n)$; (iii) $X \cong \mathbb{Z}_2^6 \rtimes PSL(3, 2)$; (iv) X is isomorphic to a parabolic subgroup of $\Omega^+(8, 2)$ of the form $\mathbb{Z}_2^6 \rtimes (\mathbb{Z}_2^3 \rtimes PSL(3, 2))$; or (v) X is a nonsplit extension $2^3 PSL(3, 2)$.

If (i) holds we are finished (by (3.6)).

In (ii)–(iv) there are two conjugate members of Ω having the same center (cf. [1, (11.5) and p. 413]), so that G is orthogonal. Let V be the natural projective module for G, and assume for the moment that $G \neq P\Omega^+(8, q)$. If

Y pulls back to an abelian subgroup of $\Omega(V)$ then either M^* is reducible on V or (C.6) holds. If Y pulls back to an extraspecial group then, since $M = N_G(Y)$, M/Y must be an orthogonal group over $GF(2)$, and (as $|G: N_G(X)|$ is odd) the only possibility for X is $\mathbb{Z}_2^6 \rtimes A_8$. In that case X has four members with the same center, whereas $G \neq P\Omega^+(8, q)$.

This leaves the case $G = P\Omega^+(8, q)$. The preceding paragraph applies almost verbatim, unless $M^* - M$ contains a triality automorphism. In view of $|T|$, $X \cong 2^6 A_8$ or $2^6 \cdot 2^3 PSL(3, 2)$. By conjugating within Aut $P\Omega^+(8, q)$ we can replace M by another group in order to guarantee that the normal subgroup of X of order 2^6 pulls back to an elementary abelian subgroup of $\Omega^+(8, q)$. Then M is monomial with respect to an orthogonal basis and is invariant under a triality automorphism. It follows easily that $X \cong 2^6 \cdot 2^3 PSL(3, 2)$ and that X is uniquely determined up to conjugacy in Aut $P\Omega^+(8, q)$ (cf. [21]). Thus, (C.10) holds.

Finally, consider case (v). Here, X has two classes of quaternion groups either or both of which might be in Ω; moreover, there is a unique member of each class lying in T, and these have the same center. Since Aut $X \cong X$ we have $X = N_G(X)$, and then the structure of T forces G to be $G_2(q)$ or ${}^3D_4(q)$. It is easy to see that $G_2(q)$ has a unique conjugacy class of subgroups (v) (e.g., argue as in [21, Sect. 8]). If G is ${}^3D_4(q)$ let V be its natural 8-dimensional module over $GF(q^3)$ [30]. Then it is straightforward to see that X must fix a nonzero vector in V; and then $N_G(X)$ lies in a group $G_2(q)$ by [30]. (N.B. See the proof of (3.11) for a further discussion of ${}^3D_4(q)$ that makes this inclusion in $G_2(q)$ apparent.) ▮

In view of (2.3), (3.5), (3.7) and (3.8), *throughout the remainder of the proof of Theorem* C *we may assume that* $O_p(M) = 1$, *and that either* $\tilde{X} = X$ *or else* $O(M) = O_2(M) = 1$.

Lemma 3.9. *If* $G \neq G_2(q)$, ${}^3D_4(q)$, *and if* X *contains no nontrivial long root elements, then* (C.10) *holds.*

Proof. Since A has no nontrivial long root element, while $\tilde{A} = SL(2, q)$, $p \nmid |A|$. Thus, either A is metacyclic or is $SL(2, r)$ or $SL(2, r) \cdot 2$, where $r = 3$ or 5 and $r \neq p$ [12, Chap. 12].

By (3.5)(ii) and (1.1), X is one of the following (where s is an odd prime power): (i) M_{11}, (ii) M_{12}, (iii) $PSL(2, s^2) \cdot 2$, (iv) $PSL(3, s) \cdot 2$ or $PSU(3, s) \cdot 2$, (v) $Sp(6, 2)$, (vi) $\Omega^+(8, 2)$, or (vii) a group of Lie type over $GF(r)$.

In (i) there are Frobenius groups of order $9 \cdot 4$ and $5 \cdot 4$ whose Sylow 2-subgroups fix 3 of the 11 points and hence lie in conjugates of Q. By (3.3) this eliminates (i). Similarly, groups of order $9 \cdot 4$ and $5 \cdot 4$ eliminate (ii) as well.

Note that M^* acts on X, and $C=C_{M^*}(X)$ is 1: otherwise, $M^*=N_F(C)\geqslant \tilde{X}$. A further restriction is provided by the fact that X contains $m(X)=m(G)$ pairwise commuting members of Q^G.

Case (iii). Since $m(G)>1$ by Table I, this case cannot occur.

Case (iv). By Table I, $m(G)=m(X)=2$ and T is transitive on Δ. However, only one member of Δ lies in X'.

Case (v). Since $m(G)=m(X)=2$, Table 1 shows that G is $PSL(4, q)$, $PSL(5, q)$, $PSp(4, q)$, $PSU(4, q)$, $PSU(5, q)$, $P\Omega(7, q)$, or $P\Omega^-(8, q)$. By [22], $G=P\Omega(7, q)$ or $P\Omega^-(8, q)$. Moreover, $Sp(6, 2)=W(E_7)'<P\Omega(7, q)$ for each q, and $Sp(6, 2)$ contains a Sylow 2-subgroup of G when $q\equiv \pm 3 \pmod 8$. Thus, $X=Sp(6, 2)<P\Omega(7, q)$ occurs in (C.10). It remains to show that $X=Sp(6, 2)<P\Omega^-(8, q)$ does not.

Assume that $G=P\Omega^-(8, q)$. Then $G\cong\Omega^-(8, q)$, and G acts on an 8-space V. Let P_1 and P_3 be the parabolic subgroups of X containing T and having the form $2^5\cdot\Omega(5, 2)$ and $2^6\cdot SL(3, 2)$, respectively. It is easy to see that P_3 acts monomially with respect to an orthogonal basis of V, and $\dim C_V(P_3)=\dim C_V(T)=1$. Also, $P_1'=2^5\cdot A_6$ and $\dim C_V(P_1')=2$. Consequently, $C_V(T)=C_V(P_1)$, and $X=\langle P_1, P_3\rangle$ fixes $C_V(T)$. This contradicts the fact that $N_F(X)$ is maximal in F.

Case (vi). This time, $m(G)=m(X)=4$. Also, $C=1$. Thus, $|T|$ divides $|\mathrm{Aut}\, X|$, so that $|T|\leqslant 2^{12}\cdot 2^3$. Only $G=P\Omega^+(8, q)$ is allowed by these conditions, and $W(E_8)'<\Omega^+(8, q)$ shows that $\Omega^+(8, 2)$ lies in $P\Omega^+(8, q)$. Once again this case occurs in (C.10).

Case (vii). Recall that $r\neq p$. Since $O_2(X)=1$, $X\neq SL(2, r)$, $SL(2, r)\cdot 2$. If X has a subgroup $PSL(3, r)$ or $SL(3, r)$ containing Q, then X has a subgroup of order r^2 normalized by Q and inverted by $z(Q)$, contradicting (3.3). Consequently, X cannot be an exceptional group of Lie type, $PSL(k, r)$ or an orthogonal group of dimension $\geqslant 7$.

Also note that $m(X)$, as defined for the group X of Lie type, must coincide with $m(G)$. Moreover, $N_X(\Delta)^\Delta$ must lie in $N_G(\Delta)^\Delta$. By Table I, and [22], X is not an exceptional group of Lie type.

Consequently, G and X are both classical groups. By Table I, G acts projectively on a $2m(G)+4$-dimensional $GF(q)$-space V. Then X also acts projectively on the $2m(X)+4$-dimensional space V. By [22], X is $P\Omega(5, 3)$ or $P\Omega^-(6, 3)$. Moreover, by Table I, $\dim V\leqslant 8$.

If $X=P\Omega(5, 3)$ then $|M|_2=2^6$ or 2^7. This can only happen when $G=P\Omega(5, q)$ or $P\Omega^\pm(6, q)$. Since $X\cong W(E_6)'$, it is easy to deduce that $|G: N_G(X)|$ is even.

Finally, if $X=P\Omega^-(6, 3)$ then by [22, (4, 4a), (5.7)] we have $\dim V\geqslant 6$

and a perfect subgroup of $SL(V)$ projecting onto X has a center of order divisible by 3. Thus, G is not orthogonal or symplectic. Now $\dim V \geqslant 6$ shows that $m(G) \geqslant 3$, whereas $m(X) = 2$. ▮

The method used at the end of *Case* (v) can be used in a situation excluded in (3.9) (cf. (3.10)), and also to give an elementary proof of the uniqueness in Aut G of the conjugacy classes of subgroups $\Omega(7,2) < \Omega(7,q)$ or $\Omega^+(8,2) < P\Omega^+(8,q)$. For example, suppose that X is $\Omega^+(8,2)$. By [22], X pulls back to a nonsplit extension $2\Omega^+(8,2) < \Omega^+(8,q)$. Let $Y = \mathbb{Z}_2 \times \Omega(7,2) < 2\Omega^+(8,2)$. Then Y fixes a 1-space, just as in the proof in *Case* (v). Now X has an orbit of 120 nonsingular 1-spaces. Also, $2\Omega^+(8,2)$ has a subgroup $2^7 \cdot A_8$, and this group leaves invariant exactly two sets of 120 nonsingular 1-spaces. The stabilizer of either set in $O^+(8,q)$ is just the Weyl group $W(E_8)$ embedded in the natural way. Thus, X is uniquely determined up to conjugacy in Aut G. Incidentally, it then follows that q is a prime (since M^* is a maximal subgroup of F).

LEMMA 3.10. *If $G = G_2(q)$ or ${}^3D_4(q)$, and if X contains no nontrivial long root elements, then* (C.8) *or* (C.10) *holds.*

Proof. The first five paragraphs of the proof of (3.9) are valid without change.

This time, $m(G) = 1$, while T contains the central product of two quaternion groups. This leaves the following cases: (iv) $PSL(3,s) \cdot 2$ or $PSU(3,s) \cdot 2$, and (vii) $PSL(3,r)$, $PSU(3,r)$, $G_2(r)$ and ${}^3D_4(r)$ with $r \neq p$ and $r = 3$ or 5. By [22], X is $PSL(3,s) \cdot 2$ or $PSU(3,s) \cdot 2$ with $p \mid s$, $PSU(3,3) \cdot 2 = G_2(2)$, or $PSU(3,3)$.

Let $Z(Q) = \langle t \rangle$. Then $C_G(t) = (S\tilde{Q}) \cdot 2$, where the first product is a central product and $S = SL(2,q')$, $q' = q$ or q^3, is a short fundamental subgroup. On the other hand, $C_X(t)$ has the form $(SL(2,s)\,D) \cdot 2$, where the first product is again central, $s = r = 3$ in (vii), and D is metacyclic except when $X \cong PSU(3,3)$ and D is cyclic of order 4. Then the $SL(2,s)$ lies in S or in $\tilde{Q}$, and the former occurs if $p \mid s$ (since X contains no nontrivial long root elements).

Assume that $G = G_2(q)$. If $p = 3$ we can apply a graph automorphism to M^* to obtain a new group "X" containing nontrivial long root elements, so that [19] applies and (C.8) holds. If $p \neq 3$ and $p \mid s$ then the proof of [14, (4B)] shows that X fixes a 1-space $\langle w \rangle$ in the standard 7-dimensional module V for G; then $\langle w \rangle$ is uniquely determined, and M^* normalizes a group $SL(3,q)$ or $SU(3,q)$ generated by long root elements (by [30] or (3.11)). Thus, X must be $G_2(2)$ or $PSU(3,3)$, and $p \neq 3$. We must eliminate the latter case. There, the $SL(2,3)$ in $C_X(t)$ contains Q, so that $A = \tilde{Q} \cap M = C_X(D) = SL(2,3)$. Let $B \in A^X - \{A\}$ with $\langle Z(A), Z(B) \rangle < T$. Then $\dim C_V(-z(A)) = 4$ and $\dim C_V(-z(A)) \cap C_V(-z(B)) = 2$, so that

$\langle A, B\rangle$ acts on the 6-space $\langle C_V(z(A)), c_V(z(B))\rangle$, and $X = \langle A, B\rangle$ fixes its orthogonal complement. By [30] (or (3.11)), M^* normalizes a group $SL(3, q)$ or $SU(3, q)$ generated by long root groups, and this contradicts one of our hypotheses.

This leaves the case $G = {}^3D_4(q)$. Here, we will show that M^* normalizes a nontrivial subgroup of a suitable $G_2(q)$. We begin by studying the action of T on the natural $\Omega^+(8, q^3)$ module V for G.

Since T lies in some subgroup $G_2(q)$, T fixes some vector $v \neq 0$. We claim that

(3.11) $C_V(T) = \langle v\rangle$, *and T fixes a unique* 1-*space* $\langle w\rangle \neq \langle v\rangle$.

For, $T > \langle Z(Q), Z(R)\rangle$ for some $R \in Q^G - \{Q\}$. Extending the ground field shows that $\langle \tilde{Q}, \tilde{R}\rangle$ lies in the monomial group of a subgroup $SL(3, q^2)$ of $G_2(q^2)$, acting on $v^\perp \otimes_{GF(q)} GF(q^2)$ by fixing two totally singular 3-spaces [30, pp. 23, 38]. Moreover, T lies in $SL(3, q^2)\cdot 2$, and hence interchanges these 3-spaces. Since $G_2(q^2) < \Omega(7, q^2)$ it follows that $\langle Q, R\rangle\, T$ fixes a nonsingular 6-space of $v^\perp$ and induces ± 1 on its orthogonal complement $\langle w\rangle$ in $v^\perp$. This proves (3.11).

In particular, we see that T lies in a uniquely determined subgroup $G_2(q)$ of G—namely, G_v—and a uniquely determined subgroup $SL(3, q)\cdot 2$ or $SU(3, q)\cdot 2$—namely, $G_{\langle w\rangle}$.

Now consider $X \cong PSL(3, s)\cdot 2$, $PSU(3, s)\cdot 2$, $G_2(2)$, or $PSU(3, 3)$. In the last two cases $C_{XT}(t)$ lies in a group $(SL(2, q)\, SL(2, q))\cdot 2$ which in turn lies in some $G_2(q)$; by (3.11), $C_{XT}(t)$ fixes $\langle v\rangle$. Also, R fixes $\langle v\rangle$. Thus, $XT = \langle C_{XT}(t), R\rangle$ fixes $\langle v\rangle$, so that $C_V(X)$ is $\langle v\rangle$ or $\langle v, w\rangle$. In the first case M^* normalizes our $G_2(q)$, while in the second M^* normalizes $G_{vw} = SL(3, q)$ or $SU(3, q)$.

Finally, if $X \cong PSL(3, s)\cdot 2$ or $PSU(3, s)\cdot 2$ then $C_X(t) = (SL(2, s)\, D)\cdot 2$ where $SL(2, s) \leqslant S = SL(2, q^3)$, so that $GF(s) \subseteq GF(q^3)$. Also, $s^3 \pm 1$ divides $|G|$ and hence divides $(q^{12} - 1)(q^6 - 1)(q^2 - 1)$. Thus, by [34], both q^4 and q^3 are powers of s, and hence $GF(s) \subseteq GF(q)$. Now $C_{XT}(t)$ lies in some $(SL(2, q)\, SL(2, q))\cdot 2$. As before it follows that M^* fixes $\langle v\rangle$ or $\langle v, w\rangle$, and hence contains long root groups, which is not the case. ▮

Once again, the only case $X = G_2(2) < G = G_2(q)$ occurring in (3.10) is uniquely determined up to conjugacy in Aut G—and hence, q is prime since M^* is maximal. To see this, note that the case $p = 3$ was handled in the above proof (in view of [19]), so let $p \neq 3$. Let E be a Sylow 3-subgroup of $C_G(t)$. Then $|N_X(E)| = 27\cdot 8$. It follows that $C_G(E) = SL(3, q)\cdot 2$ or $SU(3, q)\cdot 2$ (depending on whether $q \equiv 1$ or $-1 \pmod 3$), and $C_V(E)$ is a 1-space $\langle v\rangle$. Thus, $|\langle v\rangle^X| = 28$. Let J be a Sylow 2-subgroup of $N_X(E)$. Then J induces ± 1 on $\langle v\rangle$, and fixes a unique second member $\langle u\rangle$ of $\langle v\rangle^X$, inducing ± 1 on $\langle u\rangle$ as well. This uniquely determines $\langle u\rangle$, and hence also the orbit of $\langle u \rangle$ under $N_X(E)$. Consequently, $N_X(E)$ uniquely determines $\langle v \rangle^X$, so that X is determined up to conjugacy in G, as asserted.

4. Classical Groups

In this section G will be a classical group defined by a vector space V equipped either with no form or with an alternating, quadratic or hermitian form.

Lemma 4.1. *If M is reducible then* (C.4) *or* (C.5) *holds.*

Proof. Let W be a minimal M-invariant subspace. Assume that $G \neq PSL(V)$. Then W is either nonsingular or else totally isotropic or totally singular. In view of (C.5), we may assume that W is totally isotropic or totally singular. However, $|G: N_G(W)|$ is never odd for such a W.

Now let $G = PSL(V)$. If $M^* = N_F(W)$ then (C.4) holds, so assume that F contains a graph automorphism. Then M has a second invariant subspace W' of codimension dim W, and M^* fixes $\{W, W'\}$. Since $W \cap W'$ and $\langle W, W' \rangle$ are M^*-invariant, it follows that (C.4) or (C.5) holds. ▮

Let X be as in Section 3.

Lemma 4.2. *If M is irreducible but X is reducible then* (C.6) *holds.*

Proof. By [19], M preserves a decomposition $V = V_1 \oplus \cdots \oplus V_l$ of V into X-irreducible subspaces V_i permuted transitively by M. In view of (C.6), we may assume that $G \neq PSL(V)$. Then all V_i are nonsingular, or all are totally isotropic or totally singular. In the latter case $|G: M|$ would be even. Thus, all V_i are nonsingular, and (C.6) follows easily. ▮

Lemma 4.3. *If X is irreducible then* (C.3) *or* (C.10) *holds.*

Proof. If X contains no nontrivial long root elements then (3.9) states that (C.10) holds. Assume that X contains a nontrivial long root element. Theorems I and II and Section 11 of [19] list all of the candidates for X. If $\tilde{X} = X$ then nothing on those lists has $|G: N_G(X)|$ odd. If $\tilde{X} \neq X$, those lists imply that (C.3) holds. ▮

5. Exceptional Groups of Lie Type

In this section we will complete the proof of Theorem C by settling the case of exceptional groups of Lie type. Let F, G, M^*, M, T, Δ, X, $\tilde{X}$, $m(G)$, and $m(X)$ be as in Section 3. Since Δ is contained in X, $m(X)=m(G)$. As in the proof of (3.9) this greatly restricts the possibilities for X.

LEMMA 5.1. *If* $\tilde{X}=G$ *then* (C.3) *or* (C.10) *holds.*

Proof. By (3.9) and (3.10) we may assume that X contains a nontrivial long root element. By (1.1), (3.5)(ii) and [10], $X=C_G(\sigma)$ for a field automorphism σ, unless X is ${}^2E_6(q')$ in $G=E_6(q)$, $q=q'^{2e}$, e odd, embedded naturally. In the first case (C.3) holds. In the second case $|G: N_G(X)|$ is even. ▌

In view of (3.4) we may now assume that $\tilde{X}=X$. Recall that $O_p(X)=1$.

LEMMA 5.2. *One of* (C.7)–(C.9) *holds.*

Proof. The possibilities for X are more or less listed in [10]. After correcting a few statements concerning centralizers in that paper, and then using Table I (in Sect. 3) and the fact that $m(G)=m(X)$, we obtain the list of candidates in Table II. (For brevity we have omitted q throughout the table, and used Lie notation.)

If G is $G_2(q)$ or ${}^3D_4(q)$ then all possibilities in the table can occur, and appear in (C.7) and (C.8).

Now consider $G=F_4(q)$, ${}^2E_6(q)$ or $E_6(q)$. By Table I, T is transitive on Δ. However, T acts on X. This leaves only the possibilities $X/Z(X)=A_1^4$, $C_2\times C_2$, D_4, B_4, D_5, ${}^2D_5$, C_4, or F_4. Note that G has a subgroup $X=2^2\cdot P\Omega^+(8,q)$ such that $|G: N_G(X))$ is odd and $N_G(X)\geqslant N_G(\Delta)$ (cf. [2, Theorem 6]). Also, ${}^2E_6(q)$ and $E_6(q)$ have subgroups $X=N_G(X)=F_4(q)$ with $|G: X|$ even.

If $G=F_4(q)$ then there is a subgroup $2\cdot\Omega(9,q)$ whose center is $Z(T)$.

TABLE II

G	$X/Z(X)$
G_2	$A_1, A_2\,{}^2A_2$
${}^3D_4$	$A_1, A_2, {}^2A_2, G_2$
F_4	$A_1\times C_3, A_1^2\times C_2, A_1^4, D_4, B_4$
${}^2E_6$	$A_1\times C_3, A_1^2\times C_2, A_1^4, D_4, B_4,$ $A_1\times{}^2A_5, A_1^2\times{}^2A_3, {}^2D_5, C_2\times C_2, C_4, F_4$
E_6	$A_1\times A_5, A_1\times C_5, A_1^2\times A_3, A_1^2\times C_3, A_1^4,$ $C_2\times C_2, C_4, D_4, B_4, D_5, F_4$
E_7	$A_1\times D_6, A_1^3\times D_4, A_1^7$
E_8	$A_1\times E_7, A_1^2\times D_6, A_1^4\times D_4, A_1^8, D_4^2, D_8$

Similar statements hold for all the remaining cases in (C. 9)(ii) (cf. [18] for $Z(X)$). Moreover, this takes care of all possibilities for $F_4(q)$.

If $G={}^2E_6(q)$ then we must still eliminate the cases $X/Z(X)=B_4$, $C_2\times C_2$, or C_4. By [8] there is just one class of subgroups of type B_4, all of the form $2\cdot\Omega(9,q)<(4,q+1)\cdot P\Omega^-(10,q)$, so that their normalizers are not maximal. If $X/Z(X)=C_2\times C_2$ or C_4 then a simple calculation shows that $|{}^2E_6(q)|/|X/Z(X)|$ is divisible by 32 or 8, respectively. Thus, $C_G(X)$ has even order and hence meets $Z(T)$ nontrivially. Since $C_G(Z(T))\geqslant(4,q+1)\cdot P\Omega^-(10,q)$, $X/Z(X)\neq C_4$. Moreover, if $X/Z(X)=C_2\times C_2$ then $N_G(X)<C_G(Z(T))$.

The case $G=E_6(q)$ is handled similarly.

Next, let $G=E_8(q)$. Again T is transitive on Δ. This time, Table II leaves only three possibilities: A_1^8, D_8, and D_4^2. The first two of these are included in (C.7) and (C.9). If $X/Z(X)=D_4^2$ then X lies in $2\cdot P\Omega^+(16,q)$, so that $|Z(X)|=4$. Since $2^2\cdot P\Omega^+(8,q)\cdot S_4$ is contained in $E_6(q)$, $N_G(Z(X))$ induces S_3 on $Z(X)$ and hence does not lie in $2\cdot P\Omega^+(16,q)$. This case is also in (C.9).

Finally, let $G=E_7(q)$. This time, T has orbit lengths 1, 2, and 4 on Δ. Each candidate in Table II has $|G:N_G(X)|$ odd, and appears in (C.7) or (C.9). ∎

This completes the proof of Theorem C.

PART II. THEOREM B

6. Preliminaries

Let π be a projective plane of order n. If Q is any nonempty set of collineations of π then $\pi(Q)$ will denote the set of points fixed by Q. When Q is planar, we will identify $\pi(Q)$ with the fixed point plane of Q.

If t is an involutory collineation other than a perspectivity then $|\pi(t)|=m^2+m+1$ where $n=m^2$ [11, p. 172]. Consequently, we will be especially interested in properties of integers of the form u^2+u+1, where u is an integer.

Lemma 6.1. *If $n=m^2$ then $n^2+n+1=(m^2+m+1)(m^2-m+1)$, where $(m^2+m+1, m^2-m+1)=1$.*

Lemma 6.2. *If $u^2+u+1=p^a$ for a prime p, then either $p^a=p$ or $p^a=7^3$.*

Proof. [24, p. 11]. ∎

Lemma 6.3. *If $n=m^2$ and $n^2+n+1=q^ab$ for a power $q^a>p$ of a prime p, then either $b>8q^a$ or $q^a=m^2\pm m+1=7^3$.*

Proof. By (6.1), $m^2 \pm m + 1 = q^a c$ and $m^2 \mp m + 1 = b/c$ for some odd integer c and some choice of signs. If $c = 1$ then $m^2 \pm m + 1 = 7^3$ by (6.2). If $c \geqslant 3$ then $b/q^a c^2 \geqslant (m^2 - m + 1)/(m^2 + m + 1) > \frac{8}{9}$, since $m^2 \pm m + 1$ is not square-free (as $q^a \geqslant p^2$) and hence $m > 16$ (as is seen by checking all $m \leqslant 16$). ▮

LEMMA 6.4. *If p is a prime divisor of $n^2 + n + 1$ then either*

(i) $p = 3$ *and* $9 \nmid n^2 + n + 1$, *or*

(ii) $p \equiv 1 \pmod 3$.

Proof. If $p = 3$ then (i) is easy to check. Let $p \neq 3$. Clearly, $n^3 - 1 \equiv 0 \pmod p$ and $p \nmid (n^2 + n + 1, n - 1)$, so that n has order 3 in $GF(p)^*$. ▮

LEMMA 6.5. *Assume that G is a collineation group having a proper normal elementary abelian subgroup of order $n^2 + n + 1$. Then $n^2 + n + 1$ is a prime and G is a Frobenius group of odd order dividing $(n^2 + n + 1)(n + 1)$ or $(n^2 + n + 1)\, n$.*

Proof. If $n^2 + n + 1$ is not prime then it is 7^3 by (6.2). This possibility is eliminated in [5, p. 470; 27]. Thus, $n^2 + n + 1$ is prime, G acts on points as a Frobenius group, and G_x is cyclic for each point x. Clearly, $G_x = G_L$ for some line L, and this group acts semiregularly on L or $L - \{x\}$. Moreover, $|G|$ is odd, since an involution would fix more than one point. ▮

LEMMA 6.6. *Assume that G is a point-transitive collineation group of π. Let $Q \subseteq G$ with $\pi(Q)$ a subplane of order u, and let $x \in \pi(Q)$. Then*

(i) $(n^2 + n + 1)|Q^G \cap G_x| = (u^2 + u + 1)|Q^G|$;

(ii) *If G_x is transitive on $Q^G \cap G_x$ then $N_G(\langle Q \rangle)$ is transitive on $\pi(Q)$ and $|\pi(Q)| = |N_G(\langle Q \rangle) : N_G(\langle Q \rangle)_x|$; and*

(iii) *If $Q = \{t\}$, $|t| = 2$ and $u \neq 2$ then $2|G : G_x| > |C_G(t) : C_G(t)_x|^2$.*

Proof. (i) Count the pairs (y, Q^g) with $g \in G$ and $y \in \pi(Q^g)$.

(ii) G is transitive on the above pairs.

(iii) $|C_G(t) : C_G(t)_x|^2 \leqslant (u^2 + u + 1)^2 < 2(n^2 + n + 1)$ *since* $n = u^2$ *here.* ▮

7. START OF PROOF

Let π be the plane in Theorem B. We may assume that conclusion (ii) does not hold. By the result of Wagner [31] stated in the Introduction, we may also assume that *all involutions in F fix m^2+m+1 points, where $n=m^2$*. Thus, the remainder of this paper will be directed towards obtaining a contradiction.

LEMMA 7.1. *$F \trianglerighteq G$ with G simple and nonabelian.*

Proof. By (6.5), F has no nontrivial elementary abelian normal subgroup. Thus, if (7.1) fails then, by (2.1), $F \triangleright T_1 \times \cdots \times T_k$ for $k>1$ simple groups T_i permuted transitively by F, and $F \leqslant F_1 wr S_k$ with the natural action on Y^k for some Y, where F_1 acts primitively on Y and $F_1 \trianglerighteq T_1$. In particular, $n^2+n+1=b^k$ where $b=|Y|$.

Let t be an involution in T_1. Let f be the number of points of Y fixed by t. Then t fixes fb^{k-1} points of π. Thus, $m^2+m+1=fb^{k-1} \geqslant b^{k-1}$. If $k \geqslant 3$ then $m^2+m+1 \geqslant (n^2+n+1)^{2/3}$, whereas $n=m^2$. Consequently, $k=2$ and $m^2+m+1=fb$ while $m^4+m^2+1=b^2$. In particular, $m^2<b$, so that $f=1$ and $b=m^2+m+1$, which is impossible. ▌

Now we are in the situation of Theorem C. Of course, G is transitive on points (and hence also on lines). Moreover, G_x is known by Theorem C. This allows us to ignore F most of the time.

The various possibilities in Theorem C are dealt with in the following places:

(C.1)	(8.3), (8.4)
(C.2)	(10.6)
(C.3)	(8.1), (8.2), (9.4)
(C.4)	(8.4)
(C.5)	(9.1), (9.3)
(C.6)	(9.2), (9.3)
(C.7)	(9.3)
(C.8)	(9.2), (9.3)
(C.9)	(9.3)
(C.10)	(9.2)
(C.11)	(9.2)
(C.12)	(8.3)
(C.13)	(8.1), (8.2)
(C.14)	(11.1).

Note that each possibility produces a diophantine equation $|G:G_x|=n^2+n+1$. While we do not handle all of these equations simultaneously, many are dealt with in large batches, using (6.1), (6.3), and (6.4) (see (9.2)–(9.4) and (10.6) for examples of this). There are many alternative approaches. For example, one could estimate the number of fixed points of a carefully chosen involution in order to contradict (6.6)(iii), but the calculations involved seem worse than those we have used.

However, it seems likely that anyone reading this paper will find better arguments for several of the cases (C.1)–(C.14).

8. Miscellaneous Cases

This section eliminates some of the possibilites in Theorem C.

LEMMA 8.1. *$G \neq {}^2G_2(q)$, $q > 3$.*

Proof. If $G = {}^2G_2(q)$ let $U \in \mathrm{Syl}_3(G)$. By (6.4i), $|U : U_x| = 1$ or 3 for some point x. Then $|G : G_x|$ cannot be odd by (C.3) and (C.13). ▮

LEMMA 8.2. *$G \neq PSL(2, q)$, q odd, $q > 3$.*

Proof. Assume that G is $PSL(2, q)$. By (C.3) and (C.13) one of the following holds: (i) G_x is dihedral of order $q \pm 1$; (ii) G_x is $PSL(2, q')$ or $PGL(2, q')$, where $GF(q') \subset GF(q)$; or (iii) G_x is A_4, S_4 or A_5. Let t be an involution in G.

Case (i). By (6.6)(i),

$$(n^2+n+1)\{1+(q \pm 1)/2\} = (m^2+m+1)|t^G|,$$

where $|t^G| = n^2+n+1$. Now $m^4+m^2+1 = q(q \mp 1)/2$ and $m^2+m+1 = 1+(q \pm 1)/2$. It follows first that $m^2+m+1 = (q+1)/2$ and $m^4+m^2+1 = q(q+1)/2$, and then that $m^2-m+1 = q > m^2+m+1$. Thus, (i) cannot hold.

Case (ii). If $G_x = PSL(2, q')$ then $q = q'^e$ with e odd, and (by (6.6i) with Q an involution)

$$(n^2+n+1)\, q'(q' \pm 1)/2 = (m^2+m+1)\, q(q \pm 1)/2$$
$$n^2+n+1 = q(q^2-1)/q'(q'^2-1).$$

Then $m^2+m+1 = (q \mp 1)/(q' \mp 1)$ and $m^2-m+1 = q(q \pm 1)/q'(q' \pm 1)$, which is impossible.

Thus, $G_x = PGL(2, q')$, and then $q = q'^2$ since F_x is maximal in F. Now

$$(n^2+n+1)\, q'^2 = (m^2+m+1)\, q(q+1)/2$$
$$n^2+n+1 = q(q^2-1)/2q'(q'^2-1) = q'(q+1)/2,$$

so that $m^2+m+1 = q'$ and $m^2-m+1 = (q'^2+1)/2$, which is impossible.

Case (iii). Since G_x contains a Sylow 2-subgroup of G it must be self-normalizing. There are three subcases, which yield the conditions

(a) $q(q^2-1)/24 = n^2+n+1 = (m^2+m+1)\{q(q\pm 1)/2\}/3$,

(b) $q(q^2-1)/48 = n^2+n+1 = (m^2+m+1)\{q(q\pm 1)/2\}/9$, or

(c) $q(q^2-1)/120 = n^2+n+1 = (m^2+m+1)\{q(q\pm 1)/2\}/15$.

Simple calculations eliminate all three possibilities. ▮

Lemma 8.3. *Neither* (C.12) *nor the last case in* (C.1) *can occur.*

Proof. Since $|G: G_x| = 175$ or 15, (6.4) applies. ▮

Lemma 8.4. $G \neq A_d$.

Proof. Assume that $G = A_d$. By (8.2), $d \geqslant 7$, so that $F = A_d$ or S_d. Let Y be the corresponding d-set. By (C.1) and (8.3), F_x is either (i) the stabilizer of a k-set, $1 \leqslant k \leqslant d/2$, or (ii) the stabilizer of a partition of Y into l sets of size k, where $d = kl$. In each case we will show F_x also fixes a line. (N.B. Although F is certainly line-transitive, we do not know that F is line-primitive.)

(i) Since G is not 3-transitive, $k > 1$. Consider $D = (S_{k-1} \times S_{d-k-1} \times S_2) \cap G$. There is a line L fixed by D. Since F_L contains D and a Sylow 2-subgroup of F, while $|F: F_L| = |F: F_x|$, this is impossible.

(ii) Since F_x contains a 5-cycle by (6.4), $k \geqslant 5$. Let D be the pointwise stabilizer or a partition of Y into $l-2$ sets of size k, 2 of size $k-1$ and 2 of size 1. Then D fixes exactly 2 points, and these are interchanged by $N_F(D)$. Thus, $N_F(D)$ fixes a line L.

Let D_1 be the subgroup of D inducing the identity on one of the $k-1$ - sets. Then D_1 fixes exactly $k+1$ points on which $N_F(D_1)$ induces A_{k+1}. Thus, D_1 cannot be planar and $A_{k+1} \times D_1$ must fix a line, which can only be L. Then G_L contains $(S_{2k} \times (S_k wr S_{l-2})) \cap G$. Since $|G_L| = |G_x|$, it follows that $l(l-1) \geqslant \binom{2k}{k}$, so that $l > 3$.

Let E be a subgroup $A_{k-1} wr S_l$ of G_x. Then E fixes exactly $l!$ points, permuted by an A_l in $N_G(E)$. It follows that $N_G(E)$ fixes some line. Now G_L must also contain $N_G(E)^g$ for some $g \in G$. It follows readily that $|G_L| > |G_x|$. ▮

Lemma 8.5. *Case* (C.4) *cannot occur.*

Proof. Assume that (C.4) holds with $G = PSL(d, q)$. Let V be the relevant vector space. Then either (i) G_x is the stabilizer of a k-space, where we may assume that $k \leqslant d/2$, or (ii) G_x is the stabilizer of a flag $V_k \subset V_{d-k}$ with dim $V_i = i$ (where $k < d/2$).

(i) Certainly $k \neq 1$. Choose k-spaces X and Y such that $\dim X \cap Y = 0$. Then $G_{\{X,Y\}}$ fixes no proper subspace of dimension $\neq 2k$. Next choose X' and Y' so that $\dim X' \cap Y' = k-1$, and note that $G_{\{X',Y'\}}$ fixes no subspace of dimension $2k$. Since $G_{\{X,Y\}}$ and $G_{\{X',Y'\}}$ are both conjugate to subgroups of G_L for a line L, it follows that G_L is irreducible. However, $|G: G_L| = |G: G_x| \equiv 1 \pmod{p}$, so that G_L contains a Sylow p-subgroup of G. By (2.3), $G_L = G$, which is not the case.

(ii) Use V_k, $V'_k \subset V_{d-k}$ with $\dim V_k \cap V'_k = k-1$ as above in order to see that G_L is reducible and can fix no subspace of dimension $\neq d-k$, $k-1$, $k+1$. Since $|G_L| = |G_x|$ (or since $F-G$ contains a graph automorphism), this is impossible.

Finally, assume that $G = E_6(q)$ in (C.4). Then G acts on the points of π as a rank 3 permutation group of degree $n^2+n+1 = (q^9-1)(q^{12}-1)/(q-1)(q^4-1) > q^{16}$ and subdegrees 1, $q(q^3+1)(q^8-1)/(q-1)$, $q^8(q^4+1)(q^5-1)(q^5-1)/(q-1)$. Each line L through x meets each suborbit of G_x (as otherwise G_L would be 2-transitive on L). Thus, G is flag-transitive on π, and the lines through x determine partitions of each suborbit of G_x into $n+1$ sets of equal size. It follows that $n+1$ divides both nontrivial subdegrees, and hence divides $q(q^4+1)$. Since $n > q^7$, this is impossible. ▌

9. Odd Characteristic

In this section G will be a group of Lie type over $GF(q)$, where q is a power of an odd prime p. We will show that none of the cases (C.3), (C.5)–(C.11) can occur. (Recall that (C.4), (C.12), and (C.13) were dealt with in (8.5), (8.3), (8.1), and (8.2).) Most of these cases will be eliminated using simple calculations (cf. (9.2)–(9.4)). However, some situations involving orthogonal groups seem to require more care.

Most of the cases can be eliminated in several different ways, although we have not indicated more than a few instances of this (compare the remarks at the end of Sect. 7).

LEMMA 9.1. *If G is orthogonal then G_x is not the stabilizer of a nonsingular subspace.*

Proof. Assume that (C.5) holds with G_x the stabilizer of a nonsingular k-space U of the underlying vector space V, where $2k \leqslant d = \dim V$. Write $U = U_{k-1} \perp U_1$ for a 1-space U_1. Let $U'_1 \in U_1^G \cap U_{k-1}^{\perp}$, where either ($\alpha$) $U'_1 \subseteq U_1^{\perp}$ or (β)$\langle U_1, U'_1 \rangle$ has a radical $R \neq 0$. In either case, $U_{k-1} + U_1$

and $U_{k-1}+U'_1$ produce points of π interchanged by an element of $G_{U_{k-1}}$. Thus, we get two lines L_α and L_β, say, whose stabilizers contain the stabilizers in G of $\{U_{k-1}, \{U_1, U'_1\}\}$. Clearly, G_{L_α} can fix at most two nonzero subspaces of dimension $\leqslant d/2$, and both are nonsingular (of dimension $k-1$ and 2). On the other hand, G_{L_β} can fix at most one nonsingular subspace of dimension $\leqslant d/2$, namely U_{k-1}. Since G_{L_α} and G_{L_β} are conjugate in G, it follows that either both are irreducible or both fix a nonsingular $k-1$-space. (If $k=1$ then both must be irreducible.)

Since $|G_L|=|G_x|$, while $|G_{U_{k-1}}|<|G_U|$ when $k>1$, G_L must be irreducible for any line L. By [19], G_L cannot contain any long root groups. Using G_{L_β} we see that $d-k+1\leqslant 4$, so that $k\leqslant d-k\leqslant 3$ and hence $d=5$ or 6 and $k=d-3$ (since $d>4$ by (8.2)). However, in either case we can choose U_{k-1} so that $U_{k-1}^\perp$ is of type $\Omega^+(4, q)$, and then G_{L_β} will contain a long root group. ▌

Lemma 9.2. *The following cases cannot occur*: (C.10), (C.11), (C.6) *with G orthogonal, and* (C.8) *with $G_x=G_2(q)$.*

Proof. Let Q be as in Section 3. In each case, $Q^G\cap G_x=Q^{G_x}$. (For (C.11) this follows from Sylow's theorem and the description in (3.6) and [2, Theorem 3].) We claim that, in general, (α) $|G:G_x|_p>|N_G(Q):N_G(Q)_x|_p>1$, and ($\beta$) $|N_G(Q)|_p>|G_x|_p$. In view of (6.6)(ii) and (6.1), (α) asserts that Q cannot be planar; while (β) implies that $N_G(Q)$ cannot fix a line L (since $|G_x|=|G_L|$). Since $\pi(Q)$ cannot be a triangle by (α) and (6.4)(i), it follows that (α) and (β) are sufficient to eliminate each of the cases of the lemma for which they hold.

Case $G=G_2(q)$, $G_x=2^3PSL(3,2)$ or $G_2(2)$. Note that $q^2\mid|G:G_x|$, so that $p\neq 3$ by (6.4)(i). Also, $p\neq 7$ since $q\equiv\pm 3 \pmod 8$ in (C.10). Thus, $|G|_p=q^6$, $|G_x|_p=1=|N_G(Q)_x|_p$, and $|N(Q)|_p=q$, so that (α) and (β) hold.

Case $G=P\Omega(7,q)$, $G_x=\Omega(7,2)$. This time $|G|_p=q^9$, $|G_x|_p=1$ and $|N_G(Q)|_p=q^2$.

Case $G=P\Omega^+(8,q)$, $G_x=\Omega^+(8,2)$. Here $|G|_p=q^{12}$, $|G_x|_p=1$ and $|N_G(Q)|_p=q^3$.

Case $G=P\Omega^\pm(d,q)$ and G_x preserves a decomposition of the underlying vector space V as $V=V_1\perp\cdots\perp V_l$ with all V_i isometric of dimension $k=d/l$. We will distinguish several subcases, depending upon the parity of d and k as well as the size of k. Note that $d\geqslant 5$ by (8.2).

Subcase $d=2r+1$, $k=2s+1\geqslant 5$. $|G|_p=q^{r^2}$, $|N_G(Q)|_p=q^{1+(r-2)^2}$, $|G_x|_p=q^{s^2l}l!_p$, $|N_G(Q)_x|_p=q^{1+(s-2)^2}q^{s^2(l-1)}(l-1)!_p$. Note that $p\neq 3$, 5 by (6.4), so that $\log_p(l!_p)=\sum_1^\infty [l/p^i]\leqslant l/(p-1)\leqslant l/6$. Then ($\alpha$) holds since

$|G\colon N_G(Q)|_p = q^{4r-5} > q^{4s-5+l} > q^{4s-5}l_p = |G_x\colon N_G(Q)_x|_p$, and ($\beta$) holds since

$$1+(r-2)^2 \geqslant 1+(sl-1)^2 > 1+s^2l+2sl(s-1) > s^2l+l/6.$$

Subcase $d=2r+1$, $k=2s+1\leqslant 3$. Then $|G|_p$, $|N_G(Q)|_p$ and $|G_x|_p$ are as above, and $q^{4r-5} > q^{7(2r+1)/18} > q^{s^2l}l!_p$ while $|N_G(Q)|_p > q^{7(2r+1)/18} > |G_x|_p$.

Subcase $d=2r$, $k=2s\geqslant 6$. $|G|_p = q^{r(r-1)}$, $|N_G(Q)|_p = q^{1+(r-2)(r-3)}$, $|G_x|_p = q^{s(s-1)l}l!_p$, $|N_G(Q)_x|_p = q^{1+(s-2)(s-3)}q^{s(s-1)(l-1)}(l-1)!_p$, and ($\alpha$) and ($\beta$) are easy to check.

Subcase $d=2r$, $k=2s\leqslant 4$, $G\neq P\Omega^+(8,q)$. $|G|_p$, $|N_G(Q)|_p$ and $|G_x|_p$ are as above, and $|G\colon N_G(Q)|_p = q^{4r-7} > q^{s(s-1)l+l/6} > |G_x|_p$ while $|N_G(Q)|_p > q^{s(s-1)l+l/6} > |G_x|_p$.

Subcase $G=P\Omega^+(8,q)$, $k=2s$. $|G|_p = q^{12}$, $|N_G(Q)|_p = q^3$, $|G_x|_p = q^{s(s-1)l}l!_p = q^{s(s-1)l}$, and ($\alpha$) and ($\beta$) hold.

(N.B. When $k=2s$, (6.3) also yields a contradiction.)

Subcase $d=2r$, $k=1$. $|G|_p = q^{r(r-1)}$, $|N_G(Q)| = q^{1+(r-2)(r-3)}$, $|G_x|_p = d!_p$, $q^{4r-7} \geqslant q^{d/6} > d!_p$ and $q^{1+(r-2)(r-3)} \geqslant q^{d/6} > d!_p$.

Subcase $d=2r$, $k=2s+1\geqslant 3$. Since $|G\colon G_x|$ is odd, a calculation yields that $l=2$ and $r=2s+1$. Now $|G|_p = q^{r(r-1)}$, $|N_G(Q)|_p = q^{1+(r-2)(r-3)}$, and $|G_x|_p = q^{s^22}$.

Assume that $r\geqslant 5$. Then $|N_G(Q)_x|_p = q^{1+(s-2)^2+s^2}$ and (α) holds. Also, (β) holds except when $r=5$. So let $r=5$. Then $\pi(Q)$ cannot be a subplane or a triangle (as (α) holds), so that $N_G(Q)$ fixes a line L. Now $|N_G(Q)|$ divides $|G_L| = |G_x|$. However, $|\Omega^{\pm}(6,q)|$ divides $|N_G(Q)|$ but cannot divide $2\,|O(5,q)|^2$.

Thus, $r=3$ and $G=P\Omega^-(6,q)$. Once again (α) holds but (β) does not. Let $N_G(Q)\leqslant G_L$, and let X be a long root group in $N_G(Q)$. Since $|N_G(X)|_p = q^6$, $N_G(X)$ moves L. Thus, X fixes at least two lines, whereas G_x contains no conjugate of X.

Case (C.11). The description (3.6), together with [2, Theorem 3], show first that $q^2 \mid |G\colon G_x|$—so that $p\neq 3$ by (6.4)—and then that $|G_x|_p \leqslant p$. Consequently, (α) and (β) hold trivially.

Case $G_x = G_2(q) < {}^3D_4(q) = G$. Here $|G|_p = q^{12}$, $|G_x|_p = q^6$, $|N_G(Q)|_p = q^3$ and $|N_G(Q)_x|_p = q$. Then (α) holds but (β) does not. By (α), $N_G(Q)$ fixes a line L. However, by Theorem C there is no subgroup G_L of G containing $N_G(Q)$ and having order divisible by $|G_x|_p = q^6$. ▌

PROPOSITION 9.3. *None of* (C.5)–(C.9) *can occur.*

Proof. In each case (6.3) applies. Instead of going through all of the possible cases, we will list the cases, write $|G\colon G_x| = q^ab$ with $(q,b)=1$, and

TABLE III

G	Case	a	$b/q^a \leqslant$
$PSL(d, q)$	(C.5), $d=k+l$	$\binom{d}{2}-\binom{k}{2}-\binom{l}{2}$	4
$PSU(d, q)$	(C.5), $d=k+l$	$\binom{d}{2}-\binom{k}{2}-\binom{l}{2}$	8
$PSp(2r, q)$	(C.5), $k=2s$, $l=2t$, $r=s+t$	$r^2-s^2-t^2$	4
$PSL(d, q)$	(C.6), $d=kl$	$\binom{d}{2}-l\binom{k}{2}-\lambda$	4
$PSU(d, q)$	(C.6), $d=kl$	$\binom{d}{2}-l\binom{k}{2}-\lambda$	8
$PSp(2r, q)$	(C.6), $k=2s$ $2r=2sl$	$r^2-ls^2-\lambda$	4
$G_2(q)$	(C.7)	4	2
${}^3D_4(q)$	(C.7)	8	2
$E_7(q)$	(C.7), $k=1, 3, 7$	32, 48, 56	8, 6, 1
$E_8(q)$	(C.7)	112	1
$G_2(q)$	(C.8)	3	1
${}^3D_4(q)$	(C.8)	9	2
$F_4(q)$	(C.9)(i)	12	2
$E_6(q)$	(C.9)(i)	24	4
${}^2E_6(q)$	(C.9)(i)	24	4
$F_4(q)$	(C.9)(ii)	12	1
$E_6(q)$	(C.9)(ii)	16	4
${}^2E_6(q)$	(C.9)(ii)	16	4
$E_8(q)$	(C.9)(ii)	64, 96	4, 4

give both a and an upper bound on b/q^a (Table III). (Note that to use (6.3) we do not need a precise value for b/q^a: a rough estimate suffices, namely, $b/q^a \leqslant 8$. Also note that we have to consider the possibility $q^a = m^2 \pm m + 1 = 7^3$ each time; but this presents no serious difficulty.) Moreover, we will give some examples of these calculations.

In (C.5) let k and l be the dimensions of the two subspaces, where $k \leqslant l$. In (C.6) let l be the number of subspaces, let each subspace have dimension k, and write $p^\lambda = l!_p$.

EXAMPLE. $G = G_2(q)$, (C.8). $|(G\colon G_x| = q^3(q^3 \pm 1)/2$. By (6.3), $q^3 = 7^3$, but then $m = 18$ and $|G\colon G_x| \neq 18^4 + 18 + 1$.

EXAMPLE. $G = E_6(q)$, (C.9)(i). The group $X = 2^2 \cdot P\Omega^+(8, q)$ is generated by root groups corresponding to a subroot system, and hence is normalized by a Cartan subgroup. Thus, $G_x = N_G(X)$ has order divisible by $|X|(q-1)^2/(q-1, 3)$. Then $a = 36 - 12$ and $|G: G_x|_{p'}$ is at most

$$\frac{(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1)/(3, q-1)}{(q^4-1)(q^6-1)(q^4-1)(q^2-1)\cdot(q-1)^2/(3, q-1)} < 4q^{24}.$$

Similarly, if $G = {}^2E_6(q)$ in (C.9i) then $|G_x|$ is divisible by $|X|(q+1)^2/(q+1, 3)$.

EXAMPLE. $G = PSU(d, q)$, (C.5). Here $a = \binom{d}{2} - \binom{k}{2} - \binom{l}{2}$ and

$$|G: G_x|_{p'} = \frac{\prod_i^d (q^i - (-1)^i)}{\prod_1^k (q^i - (-1)^i) \prod_1^l (q^i - (-1)^i)} < q^a \frac{2}{(1/2)\cdot(1/2)}$$

since $\prod_1^d (1 + 1/q^i) < 2$ and $\prod_1^k (1 - 1/q^i) > \frac{1}{2}$. (These are proved by noting that $ln(1 + 1/q^i) < 1/q^i$ and $ln(1 - 1/q^i) > -1/q^i$.)

EXAMPLE. $G = PSU(d, q)$, (C.6). This time $a = \binom{d}{2} - l\binom{k}{2} - \lambda$ and $|G: G_x|_{p'}/q^a < 2l!_p/(\frac{1}{2})^l\, l!_{p'}$. Thus, Table III asserts that $2^{l+1}(l!_p)^2 \leqslant 8l!$. This is certainly true if $l!_p = 1$. Since $l!_p < p^{l/(p-1)}$, we cannot have $q^a = 1$ or 3, so that $p \geqslant 7$ by (6.4). If $l \leqslant 12$ then we may assume that $p = 7$, in which case $2^{l+1}7 \leqslant 8l!$ holds. Finally, if $l \geqslant 13$ then

$$2^{l+1}(l!_p)^2 < 2^{l+1}p^{2l/(p-1)} \leqslant 2^{l+1}7^{2l/6} \leqslant 8l!.$$

The remainder of Table III is checked in a similar manner. ▌

We note that there are other simple ways to eliminate various cases. For exaple, when $G = E_7(q)$ or $E_8(q)$ in (C.9), $|G: G_x| \equiv 0 \pmod 9$ and (6.4)(i) applies.

LEMMA 9.4. (C.3) cannot occur.

Proof. Let A be as in Section 3, and let $t = z(A)$. Then $t^G \cap G_x$ is a conjugacy class of G_x (e.g., by [6]).

By (6.6)(ii), $|\pi(t)| = |C_G(t): C_G(t)_x|$. However, it is very easy to check that $|G: G_x|_p > |C_G(t): C_G(t)_x|_p > 1$ in each case. This contradicts (6.1). ▌

Note that the argument in (9.2) also works.

10. CHARACTERISTIC 2

In this section we will show that (C.2) cannot occur. Here G_x will be a parabolic subgroup. It would be nice to handle this situation by using the geometry of groups of Lie type, or by showing that root involutions cannot fix the required numbers of points. Unfortunately, there seem to be too many different cases for such uniform approaches. Instead, we will use elementary properties of the classical groups (10.4), (10.5) and numerical methods (10.1) in order to obtain contradictions.

LEMMA 10.1. (i) *If* $q^i+1 \mid |G:G_x|$ *for some* $i>0$, *then* i *is odd and* $q+1\equiv 0 \pmod 3$.

(ii) *For all* $i, j>0$, $(q^i+1)(q^j+1) \nmid |G:G_x|$.

Proof. (i) If $q^i+1\equiv 2 \pmod 3$ then some prime divisor of $|G:G_x|$ contradicts (6.4)(ii). Thus, i is odd and $q=2^e$ is not a square, so that e is odd. Then $3 \mid q+1$.

(ii) Use (i) and (6.4)(i). ▌

LEMMA 10.2. (i) *The Dynkin diagram of* G_x *is obtained from that of* G *by removing an orbit of graph automorphisms* (*namely, automorphisms lying in* F).

(ii) *There is a line* L *such that* G_L *is contained in a proper parabolic subgroup of* G. (*In particular, if* G *is a classical group then* G_L *acts reducibly on the underlying vector space.*)

Proof. (i) F_x is a maximal subgroup of F.

(ii) [29, (1.6)]. ▌

LEMMA 10.3. (i) G *has BN-rank* $l\geqslant 2$.

(ii) $G\neq PSp(4, q)$.

(iii) G_x *is obtained by removing at most* 2 *nodes from the Dynkin diagram of* G.

(iv) $G\neq G_2(q)$, ${}^3D_4(q)$.

Proof. (i) Since G is not 2-transitive on points, $l>1$.

(ii) Since q^2+1 divides the index of every parabolic subgroup of $PSp(4, q)$, (10.1)(i) applies.

(iii) Otherwise $q^2+1 \mid |G:G_x|$.

(iv) By (10.2i), if $G=G_2(q)$ or ${}^3D_4(q)$ then $|\pi|=(q^6-1)/(q-1)$, $(q^3+1)(q^8+q^4+1)$, or $(q+1)(q^8+q^4+1)$. In the first case, $G=G_2(q)$, the points of π can be identified with the points or the lines of the generalized hexagon for G, and it is easy to check that a long root involution fixes $q+1+(q+1)\cdot q\cdot q$ or $1+(q+1)\,q$ points of π. The remaining possibilities can be eliminated in the same manner, or by noting that $q+1\equiv 0 \pmod 3$ by (10.1)(i), and hence that $|\pi|\equiv 0 \pmod 9$, contradicting (6.4)(i). ▌

LEMMA 10.4. *$G \neq PSL(d, q)$.*

Proof. See the proof of (8.5). ▌

LEMMA 10.5. *G is not a classical group.*

Proof. By (10.3)(ii) and (10.4), we must consider the case in which G acts projectively on a vector space V as a symplectic, orthogonal or unitary group, and G_x is the stabilizer of a totally isotropic or totally singular k-space X. Let $Y \in X^G$ with $X \cap Y^{\perp} = 0$. Then $G_{\{X,Y\}}$ is contained in a parabolic subgroup by (10.2)(ii). However, it is easy to check that $G_{\{X,Y\}}$ fixes a totally isotropic or totally singular subspace only if one of the following holds: (i) $G = PSp(2r, 2)$ or $PSU(d, 2)$, $k = 1$, or (ii) $G = P\Omega^{\pm}(2r, 2)$, $k = 2$, and G_L fixes a totally singular 2-space but no 1-space.

In (i), a transvection fixes too many points of π. In (ii), choose X' and Y' in X^G so that $\dim X' \cap Y' = 1$ and $Y' \not\leq X'^{\perp}$. Then the only totally singular subspace fixed by $G_{\{X',Y'\}}$ is $X' \cap Y'$, of dimension 1. ▌

PROPOSITION 10.6. *Case* (C.2) *cannot occur.*

Proof. We must eliminate the possibilities $G = F_4(q)$, ${}^2E_6(q)$, $E_6(q)$, $E_7(q)$ and $E_8(q)$. By (10.1)(i), $q^4 + 1 \nmid |G : G_x|$. However, a glance at $|G|$ and the possibilities for the orders of parabolics quickly shows that there only five cases to consider: (i) $G = E_7(q)$, G_x of type E_6; (ii) $G = E_7(q)$, G_x of type D_6; (iii) $G = E_7(q)$, G_x of type $D_5 \times A_1$; (iv) $G = {}^2E_6(q)$, G_x of type ${}^2D_4$; and (v) $G = E_6(q)$, G_x of type D_5.

In (ii) and (iii), $q^6 + 1 \mid |G : G_x|$, and this is impossible as above. In (i) and (iv), $(q^5 + 1)(q^9 + 1) \mid |G : G_x|$, which contradicts (10.1)(ii).

In (v), G induces a rank 3 permutation group on the points of π, and this produces the same contradiction as in (8.5). ▌

11. SPORADIC GROUPS

The following Lemma will complete the proof of Theorem B.

LEMMA 11.1. *G is not sporadic.*

There are several approaches to this lemma. For many sporadic groups, all maximal subgroups are known, and hence (6.4) can be applied. However, this method fails for the largest groups.

Alternatively, the method on p. 44 of [13] can be applied, almost verbatim, because $|G_x|$ is divisible by so many prime divisors of $|G|$ (by

(6.4)). However, we will use the most mindless approach, based primarily on elementary arithmetic.

Proof. By (6.4), $|G: G_x|$ is a factor of the product of 3 and all powers p^i of primes $p \equiv 1 \pmod 3$ such that $p^i \| |G|$. Moreover, $|G: G_x| = (m^2+m+1)(m^2-m+1)$ by (6.1). These two conditions produce a very small number of possibilities for m, in view of the possible orders $|G|$ (cf. [15]).

For example, suppose that G is a section of the Monster. Then $(m^2+m+1)(m^2-m+1) | 3 \cdot 7^6 \cdot 13^3 \cdot 19 \cdot 31$. Since $m > 2$, arithmetic produces a unique possibility: $n = m^2 = 5^2$. Then $C_G(t)^{\pi(t)}$ is isomorphic to a subgroup of $PGL(3, 5)$, for each involution t of G; while the pointwise stabilizer of $\pi(t)$ has order dividing $n - m = 20$. When t is a 2-central involution, inspection of the various cases produces a contradiction. (Alternatively, no group G here has a subgroup of index $31 \cdot 21$.)

Similarly, when $G = J_1, J_3, J_4, LyS, Ru$, or ON, $|G: G_x|$ divides $3 \cdot 7 \cdot 19$, $3 \cdot 19$, $3 \cdot 7 \cdot 31 \cdot 37 \cdot 43$, $3 \cdot 7 \cdot 31 \cdot 37 \cdot 67$, $3 \cdot 7 \cdot 13$, or $3 \cdot 7^3 \cdot 19 \cdot 31$, respectively. As above, only $n = 5^2$ is numerically feasible, and this again produces a contradiction. ∎

Note added June 4, 1985. Since this manuscript was submitted, two relevant preprints have circulated. (i) M. Aschbacher, "Overgroups of Sylow subgroups in sporadic groups." This paper contains, among many other things, the completion of the list in Theorem C for the case of all sporadic groups. (ii) M. Liebeck and J. Saxl, "The primitive permutation groups of odd degree." This paper consists of Theorem C and a slightly different proof of it. While Aschbacher's main theorem in [1] still plays a central role in that proof, algebraic group and modular representation theoretic properties of groups of Lie type are used instead of the many subsidiary results in [1] employed in the present approach.

References

1. M. Aschbacher, A characterization of Chevalley groups over fields of odd order, *Ann. of Math.* **106** (1977) 353–398; Correction **111** (1980), 411–414.
2. M. Aschbacher, On finite groups of Lie type of odd characteristic. *J. Algebra* **66** (1980), 400–424.
3. M. Aschbacher and L. L. Scott, Maximal subgroups of finite groups, *J. Algebra* **92** (1985), 44–80.
4. A. Borel and J. Tits, Éléments unipotents et sousgroupes paraboliques des groupes réductifs I, *Invent. Math.* **12** (1971), 97–104.
5. R. H. Bruck, Difference sets in a finite group, *Trans. Amer. Math. Soc.* **78** (1955), 464–481.
6. N. Burgoyne, R. Griess, and R. Lyons, Maximal subgroups and automorphisms of Chevalley groups, *Pacific J. Math.* **71** (1977), 365–403.
7. R. W. Carter, "Simple Groups of Lie Type," Wiley, New York, 1972.
8. B. N. Cooperstein, The geometry of root subgroups in exceptional groups, I, *Geom. Dedicata* **8** (1979), 317–381.

9. B. N. Cooperstein, The geometry of root subgroups in exceptional groups, II, *Geom. Dedicata* **15** (1983), 1–45.
10. B. N. Cooperstein, Subgroups of exceptional groups of Lie type generated by long root elements. I. Odd characteristic. *J. Algebra* **70** (1981), 270–282.
11. P. Dembowski,"Finite geometries," Springer, Berlin/Heidelberg/New York, 1968.
12. L. E. Dickson, "Linear Groups, with an Exposition of the Galois Field Theory," Teubner, Leipzig 1901; reprint, Dover, New York, 1958.
13. B. Fein, W. M. Kantor, and M. Schacher, Relative Brauer groups, II, *J. reine angew. Math.* **328** (1981), 39–57.
14. P. Fong and G. M. Seitz, Groups with a (B, N)-pair of rank 2, I, *Invent. Math.* **21** (1973), 1–57.
15. D. Gorenstein, "Finite Simple Groups: An Introduction to Their Classification, Plenum, New York, 1982.
16. R. Guralnick, Subgroups of prime power index in a simple groups, *J. Algebra* **81** (1983), 304–311.
17. D. G. Higman and J. E. McLaughlin, Geometric ABA-groups. *Illinois J. Math.* **5** (1961), 382–397.
18. N. Iwahori, Centralizers of involutions in finite Chevalley groups, pp. 268–295 in Springer Lecture Notes, No. 131, Springer-Verlag, New York, 1970.
19. W. M. Kantor, Subgroups of classical groups generated by long root elements, *Trans. Amer. Math. Soc.* **248** (1979), 347–379.
20. W. M. Kantor, Some applications of the classification of finite simple groups, *in* "Finite Groups—Coming of Age" (J. McKay, Ed.), Contemporary Math., 45, pp. 159–173, AMS, 1985.
21. W. M. Kantor, Some exceptional 2-adic buildings, *J. Algebra* **92** (1985), 208–223.
22. V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra* **32** (1974), 418–443.
23. R. A. Liebler and J. E. Yellen, In search of nonsolvable groups of central type, *Pacific J. Math.* **82** (1979), 485–492.
24. W. Ljundggren, Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante. *Acta Math.* **74** (1942), 1–21.
25. H. H. Mitchell, Determination of the ordinary and modular ternary linear groups, *Trans. Amer. Math. Soc.* **12** (1911), 207–242.
26. T. G. Ostrom and A. Wagner, On projective and affine planes with transitive collineation groups, *Math. Z.* **71** (1959), 186–199.
27. R. Roth, Correction to a paper of R. H. Bruck, *Trans. Amer. Math. Soc.* **119** (1965), 454–456.
28. L. L. Scott, Representations in characteristic p, *Proc. Sympos. Pure Math.* **37** (1980), 319–331.
29. G. M. Seitz, Flag-transitive subgroups of Chevalley groups. *Ann. of Math.* **97** (1973), 27–56.
30. J. Tits, Sur la trialité et certains groupes qui s'en déduisent, *Publ. Math. I.H.E.S.* **2** (1959), 14–60.
31. A. Wagner, On perspectivities of finite projective planes, *Math. Z.* **71** (1959), 113–123.
32. J. Walter, Finite groups with abelian Sylow 2-subgroups of order 8, *Invent. Math.* **2** (1967), 332–376.
33. H. N. Ward, On Ree's series of simple groups, *Trans. Amer. Math. Soc.* **121** (1966), 62–89.
34. K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math.* **3** (1892), 265–284.