PACIFIC JOURNAL OF MATHEMATICS
Vol. 47, No. 1, 1973

A CHARACTERIZATION OF THE UNITARY AND SYMPLECTIC GROUPS OVER FINITE FIELDS OF CHARACTERISTIC AT LEAST 5

MICHAEL ASCHBACHER

The following characterization is obtained:

THEOREM. Let G be a finite group generated by a conjugacy class D of subgroups of prime order $p \geqq 5$, such that for any choice of distinct A and B in D, the subgroup generated by A and B is isomorphic to $Z_p \times Z_p$, $L_2(p^m)$ or $SL_2(p^m)$, where m depends on A and B. Assume G has no nontrivial solvable normal subgroup. Then G is isomorphic to $Sp_n(q)$ or $U_n(q)$ for some power q of p.

A much larger class of groups satisfies the analogous property for $p = 2$ or 3, including many of the sporatic simple groups. The classification for $p = 2$ appears in [3]. The classification for $p = 3$ is incomplete, but a partial solution appears in [4].

For the most part the proof here mimics that in the papers mentioned above. The exception comes in handling certain degenerate cases. This is accomplished in § 4 by first showing a minimal counter example possesses a doubly transitive permutation representation, and then utilizing numerous results on doubly transitive groups.

1. Notation.

In general G is a finite group and D a G invariant collection of subgroups generating G. G acts on D by conjugation with this representation denoted by G^D. If $\alpha \subseteqq D$ is a set of imprimitivity for this action we define

$$\begin{aligned} D_\alpha &= \{\beta \in \alpha^G : [\alpha, \beta] = 1, \alpha \neq \beta\} \\ \alpha^\perp &= \{\alpha\} \cup D_\alpha \\ A_\alpha &= \alpha^G - \alpha^\perp \\ V_\alpha &= \{\beta \in \alpha^G : \alpha^\perp = \beta^\perp\} \\ W_\alpha &= \{\beta \in \alpha^G : D_\alpha = D_\beta\} \\ D_\alpha^* &= \{B : B \in \beta \in D_\alpha\} . \end{aligned}$$

For $\Omega \subseteqq \alpha^G$, $\mathscr{D}(\Omega)$ is the graph with point set Ω and edges (α^g, α^h) where $\alpha^g \in D_{\alpha^h}$. $\mathscr{B}(\Omega)$ is the geometry with point set Ω and block set $\{\beta^\perp \cap \Omega : \beta \in \Omega\}$. For $\alpha, \beta \in \Omega$ the *line* through α and β in $\mathscr{B}(\Omega)$ is

$$\alpha * \beta = \bigcap_{\gamma \in \alpha^\perp \cap \beta^\perp \cap \Omega} (\gamma^\perp \cap \Omega)$$

$\alpha * \beta$ is *singular* if $\beta \in D_\alpha$ and *hyperbolic* otherwise.

A *triangle* is a triple (A, B, C) with $A \in D$, $C \in D_A$, and $B \in A_A \cap A_C$.

If G is a permutation group on a set Ω, $\Delta \subseteq \Omega$ and $X \subseteq G$, then X_Δ, $X(\Delta)$ is the pointwise, global stabilizer of Δ in X respectively. $X^\Delta = X(\Delta)/X_\Delta$ with induced permutation representation. $F(X)$ is the set of fixed points of X.

$O_\infty(G)$ is the largest normal solvable subgroup of G.

All groups are finite.

2. Locally D-simple groups. Let G be a finite group and D a collection of subgroups of G such that $D^G = D$. Represent G as a permutation group on G by conjugation. G is said to be *D-simple* if G is generated by any G invariant subset of D. G is *locally D-simple* if D generates G and for any A and B in D either $[A, B] = 1$ or $\langle A, B\rangle$ is generated by $A^{\langle A, B\rangle}$. α is a *set of imprimitivity* for G^D if $\alpha \cap \alpha^G = \varnothing$ for $g \in G - N_G(\alpha)$, and $\varnothing \neq \alpha = \langle\alpha\rangle \cap D \neq D$.

LEMMA 2.1. *Let G be locally D-simple and Δ a G invariant subset of D. Then*

(1) *If H is a D-subgroup of G then H is locally $(H \cap D)$-simple.*

(2) *If α is a homomorphism of G then $G\alpha$ is locally $D\alpha$-simple.*

(3) *Let $\Gamma = \langle\Delta\rangle \cap D$. Then $[\Gamma, D - \Gamma] = 1$.*

(4) *If G^Δ is transitive then $\langle\Delta\rangle^\Delta$ is transitive.*

(5) *If $D \cap Z(G)$ is empty and $G = \langle\Delta\rangle$ for some orbit Δ of G^D, then G is D-simple.*

Proof. (1) and (2) are straightforward. Let $H = \langle\Delta\rangle$. Then $H \trianglelefteq G$. Let $A \in \Gamma$, $B \in D - \Gamma$ and assume $[A, B] \neq 1$. Let $X = \langle A, B\rangle$. Then $X = \langle A^X\rangle \leqq H$ so $B \in \Gamma$, contradicting the choice of B. Therefore, (3) holds.

Assume G^Δ is transitive. Let $K = \langle D - \Gamma\rangle$. Then by (3) G is the central product of H and K so for $A \in \Delta$, $\Delta = A^G = A^{KH} = A^H$. Thus (4) holds.

Finally assume G^Δ is transitive, $G = \langle\Delta\rangle$ and $Z(G) \cap D$ is empty. Suppose Ω is an orbit of G^D with $K = \langle\Omega\rangle \neq G$. Then as $G = \langle\Delta\rangle$, $\Delta \cap K$ is empty, so by (3), $[\Delta, \Omega] = 1$. Thus Ω is centralized by G, a contradiction. Thus (5) holds.

LEMMA 2.2. *Let G be locally D-simple and α a set of imprimitivity for G^D. Then*

(1) *If $A \in \alpha$, $B \in \alpha^g \neq \alpha$ and $[A, B] = 1$, then $]\alpha, \alpha^g] = 1$.*

(2) *$\langle\alpha^G\rangle$ is locally $\langle\alpha\rangle^G$-simple.*

Proof. (1) $A = A^B \in \alpha^B$, so $\alpha^B = \alpha$. Thus 2.1.3 applied to $\langle\alpha, B\rangle$ implies $[\alpha, B] = 1$. But now the same argument shows $[\alpha^g, C] = 1$ for each C in α. (2) Let $H = \langle\alpha\rangle \neq K = \langle\alpha^g\rangle$, and $X = \langle H, K\rangle$. Assume

$[H, K] \neq 1$ and let $A \in \alpha, B \in \alpha^g$. Then by (1), $[A, B] \neq 1$ so $B \in \langle A^{\langle A,B\rangle}\rangle \leqq \langle H^X\rangle$. Thus $X = \langle H^X\rangle$.

LEMMA 2.3. *Let G be locally D-simple with G^D transitive, and A abelian. Then*

(1) *Either V_A or W_A equals $\{A\}$.*

(2) *V_A and W_A are sets of imprimitivity for G^D.*

(3) *$V_{V_A} = \{V_A\}$ and $W_{W_A} = \{W_A\}$.*

Proof. Straightforward.

LEMMA 2.4. *Let G be locally D-simple with G^D transitive and $\mathscr{D}(D)$ connected. Let $A \in D$. Then A is contained in a unique maximal set of imprimitivity α of G and $\langle D_\alpha^*\rangle$ is D_α^*-simple.*

Proof. Let $H = \langle D_A\rangle, \pi$ an orbit of H of maximal length on D_A, $\Delta = (\langle\pi\rangle - Z(\langle\pi\rangle)) \cap D, \Gamma = N_D(\Delta)$ and $\alpha = \langle\Gamma - \Delta\rangle \cap D$. As $\mathscr{D}(D)$ is connected, $|\pi| > 1$, so Δ is nonempty. We will show α has the properties claimed in the conclusion of the lemma.

By 2.1.3, $[\alpha, \Delta] = 1$. By 2.1.4 $\langle\pi\rangle$ is transitive on π. Thus transitivity of G^D and maximality of $|\pi|$ imply π is an orbit of $\langle D_B\rangle$ on D_B, for $B \in \alpha$. Therefore $B^\perp \subseteqq \Gamma$.

Suppose $B \in \alpha \cap \alpha^g \neq \alpha$. Then $\Delta \subseteqq B^\perp \subseteqq \Gamma^g = \alpha^g \cup \Delta^g$. Now $\langle\pi\rangle$ is transitive on π so either $\pi \subseteqq \Delta^g$ or $\pi \subseteqq \alpha^g$. If $\pi \subseteqq \Delta^g$ then $\Delta \subseteqq \langle\pi\rangle \subseteqq \langle\Delta^g\rangle$, so $\Delta = \Delta^g$ and therefore $\alpha = \alpha^g$, a contradiction. Thus $\pi \subseteqq \alpha^g$, so $\Delta \subseteqq \langle\pi\rangle \subseteqq \langle\alpha^g\rangle$ and therefore $\Delta \subseteqq \alpha^g$.

So $\Gamma \subseteqq \alpha \cup \alpha^g$. Further $\Delta^g \subseteqq \alpha$, so $\alpha^g \subseteqq C^\perp \subseteqq \Gamma$ for $C \in \Delta^g$. Thus $\Gamma = \alpha \cup \alpha^g$. From the last remark of the second paragraph it follows that Γ is a component of $\mathscr{D}(D)$, contradicting the hypothesis that $\mathscr{D}(D)$ is connected.

It follows that α is a set of imprimitivity for G^D. By 2.2.1, $D_\alpha^* = D_A - \alpha = \Delta - \alpha$. By construction, $Z(\langle\Delta\rangle) \cap \Delta$ is empty, so $D_\alpha^* = \Delta$ and by 2.1.5, $\langle\Delta\rangle$ is Δ-simple.

Finally let β be a set of imprimitivity for G containing A. Δ centralizes A, so Δ normalizes β. If $B \in \beta \cap \Delta$ then as $K = \langle\Delta\rangle$ is Δ-simple, $\Delta \subseteqq \langle B^K\rangle \leqq \langle\beta^K\rangle = \langle\beta\rangle$. Thus $\Delta \subseteqq \beta$. As $N_G(\beta)$ is transitive on $\beta, \alpha \subseteqq D_{\alpha^g} \subseteqq \beta$ for $\alpha^g \in D_\alpha$. Thus $A^\perp \subseteqq \beta$, and transitivity of $N_G(\beta)^\beta$ implies β is a component of $\mathscr{D}(D)$, contradicting the hypothesis that $\mathscr{D}(D)$ is connected.

So $\beta \cap \Delta$ is empty and by 2.1.3, $[\beta, \Delta] = 1$. Thus $\beta \subseteqq N_D(\Delta) - \Delta = \alpha$. Thus α is maximal as claimed.

Lemmas 2.6 and 2.7 are from §2 of [4]. 2.6 is a slight generalization of its counterpart, but the same proof goes through.

LEMMA 2.6. *Let G be locally Ω-simple, let $\Lambda \subseteqq \Omega$, and let H be a Ω-subgroup of G. Assume*

(i) *H takes the edge set of $\mathscr{D}(\Lambda)$ onto the edge set of $\mathscr{D}(\Omega)$ under conjugation.*

(ii) *There exists a partition $\Lambda = \Sigma\Lambda_i$ of Λ such that if $\alpha^h \in \Lambda$ for some $\alpha \in \Lambda_i$, $h \in H$, then there exists $r \in N_H(\Lambda_i)$ with $\alpha^h = \alpha^r$.*

Let $\bar{G}$ be a second group satisfying the hypothesis of G for which there exists a permutation isomorphism *T of H^Ω $\bar{H}^{\bar{\Omega}}$ and an isomorphism S of $\mathscr{D}(\Lambda)$ and $\mathscr{D}(\bar{\Lambda})$ such that*

(iii) *T restricted to $N_H(\Lambda_i)$ commutes with S and $N_H(\alpha)T = N_{\bar{H}}(\alpha S)$ for each $\alpha \in \Lambda$.*

Then S extends to an isomorphism of $\mathscr{D}(D)$ and $\mathscr{D}(\bar{D})$.

A *triangle* in D is a triple (A, B, C) with $A \in D$, $C \in D_A$, and $B \in A_A \cap A_C$. D is *locally conjugate* in G if for $A, B \in D$, A is conjugate to B in $\langle A, B\rangle$, or $[A, B] = \perp$.

LEMMA 2.7. *Let Ω be locally conjugate in G with G^Ω primitive and $\mathscr{D}(\Omega)$ connected. Assume*

(*) *If (α, β, γ) is a triangle and $X = \langle \alpha, \beta, \gamma\rangle$, then $\beta^\perp \cap X \subseteqq \beta^{\langle \alpha^\perp \cap X\rangle}$ and $\beta^\gamma \subseteqq (\beta^\perp \cap X)^\alpha$.*

Then $\langle \alpha^\perp \rangle$ is transitive on A_α and G^Ω is rank 3.

3. p-transvections. Let G be a finite group, p a prime. A set of *p-transvections* of G is a G invariant collection D of subgroups generating G such that for any $A, B \in D$, $|A| = p$ and $\langle A, B\rangle$ is the homomorphic image of a subgroup of $SL_2(p^n)$, with n and the image depending on A and B.

If $p = 2$ then D is a set of odd transpositions. Groups generated by odd transpositions have been classified [3]; they include the sporatic simple groups discovered by Fischer plus many infinite classes of simple groups. Conway's sporatic simple group $\cdot 1$ is generated by 3-transvections, as is the Hall-Janko group and Suzuki's sporatic simple group.

LEMMA 3.1. *Let D be a set of p-transvections of $G, p > 2$, and let $M = O_\infty(G)$. Then*

(1) *G is locally D-simple*

(2) *If G is a p-group then G is abelian*

(3) *If $G = M$ is not a p-group then $p = 3$ and G is a $\{2, 3\}$ group*

(4) *If $p > 3$ then $M/O_p(G) = Z(G/O_p(G))$.*

(5) *Let $M = 1$. Then G is a simple unless $p = 3$ and $G \cong PGU_{3n}(2)$.*

Proof. Let $A, B \in D, [A, B] \neq 1$. Set $X = \langle A, B\rangle$. Then X is isomorphic to $SL_2(p^n)$ or $L_2(p^n)$ unless $p = 3$ and $X \cong SL_2(5)$ or $L_2(5)$.

This implies (1) and (2). If $G = M$ then as $L_2(q)$ is simple for $q > 3$, X must be isomorphic to $SL_2(3)$ or A_4. Therefore, 4.1 of [4] yields (3).

Assume $p > 3$. To prove (4) we may assume $O_p(G) = 1$. Let Q be a minimal normal subgroup of G contained in M. Then Q is a q-subgroup for some prime $q \neq p$. If A centralizes Q then Q is in the center of $G = \langle D \rangle$, so we can assume $[A, Q] \neq 1$. But then $\langle A^Q \rangle \leqq AQ$ is a solvable D-subgroup whose order is divisible by q, contradicting (3).

Finally assume $M = 1$ and let H be a minimal normal subgroup of G. If $A \not\leq H$ and $x \in H$ then $\langle A, A^x \rangle$ has a normal subgroup of index p, so either $A^x \in A^{\perp}$ or $\langle A, A^x \rangle \cong SL_2(3)$ or A_4. If $A^H \subseteqq A^{\perp}$ then $[H, A]$ is a normal abelian subgroup of H, so $[H, A] = 1$. Thus H is centralized by $G = \langle D \rangle$, a contradiction. Therefore, if $A \not\leq H$, then [4] implies $AH \cong PGU_{3n}(2)$. $PGU_m(2)$ is normal in $\mathrm{Aut}\, U_m(2)$ so $G = C_G(H)HA$. By induction on $|G|$, $G/H \cong C_G(H)A \cong Z_p$ or $PGU_{3m}(2)$. But now [4] implies the latter case does not occur.

So we can take $A \leqq H$. So $G = \langle D \rangle = H$ is simple.

The proof of the following lemma is due to David Wales.

LEMMA 3.2. *Let $G \cong L_2(q)$ or $SL_2(q)$, $q = p^m$ odd, with Sylow p-subgroup P. Assume G acts irreducibly on a n-dimensional vector space over $GF(p)$, such that $n = 2 \dim C_V(P)$ and P acts semiregularly on $V - C_V(P)$. Then $G \cong SL_2(q)$, $n = 2m$, and G acts in its natural representation on V.*

Proof. Let B be a basis of V, and $GF(r)$ the splitting field for the representation of G on V. Extend the action of G to a vector space W over $GF(r)$ with basis B. W is the sum of k absolutely irreducible G-invariant subspaces W_i of W. By inspection of the irreducible representations of $SL_2(q)$ (e.g. §30, [7]), $\dim C_{W_i}(P) = 1$ for all i. Thus as $n = 2 \dim C_V(P)$ and P acts semiregularly on $V - C_V(P)$, $\dim C_{W_i}(P) = 2$. Again by inspection of the representations of $SL_2(q)$, $q = r$, $G \cong SL_2(q)$, and G acts in its natural fashion on W_1. Further G^{W_i}, $1 \leqq i \leqq k$, are the m equivalent representations obtained from G^{W_i} by $\mathrm{Aut}\, GF(q)$. Thus $n = 2m$ and G acts in its natural fashion on V.

LEMMA 3.3. *Let D be a class of p-transvections of G, p odd, with $G/O_\infty(G) \cong L_2(q)$. Let $M = O_p(G)$, $A \in D$, $m = |A^M|$ and $Z = Z(G)$. Assume $O_\infty(G)/M = Z(G/M)$. Then for some $B \in D$, $G = MX$ where $X = \langle A, B \rangle \cong SL_2(q)$, $Z = [A^{\perp}, M] \cap [B^{\perp}, M]$, $M = [A, M][B, M]$, $|M/Z| = m^2$ where $m = |A^M|$, $Z = C_M(x)$ for any p'-element of X, and $[M, \beta]$ is transitive on A^M.*

Proof. As $G/O_\infty(G) \cong L_2(q)$ there exists $B \in D$ with $X = \langle A, B \rangle \cong L_2(q)$ or $SL_2(q)$. Let $\alpha = A^{\perp} \cap X$, and $\Omega = \alpha^X$. Let $K = \prod_\Omega [M, \beta]$.

By 3.1, $[M, \alpha]$ is elementary abelian, $G = \langle [M, \alpha], X\rangle$ normalizes K and $[A, M/K] = 1$. So $M = K$. As X^{Ω} is doubly transitive, $Z_0 = [M, \alpha] \cap [M, \beta] = [M, \gamma] \cap [M, \delta]$ for all pairs $(\alpha, \beta), (\lambda, \delta)$ from Ω. So as $[M, \alpha]$ is abelian, $Z_0 \leqq Z$. Thus we can assume $Z_0 = 1$. Therefore, M is elementary abelian. A is in m groups $\langle A, C\rangle, C \in B^M$, so there are m^2 total D-subgroups isomorphic to $L_2(q)$ or $SL_2(q)$. Set $\bar{G} = G/Z$. $Z = C_M(X)$, so $m^2 \geqq |\bar{X}^{\bar{G}}| = |\bar{M}| \geqq |[\bar{M}, \alpha][\bar{M}, \beta]|$. On the other hand $m = |A^{\bar{M}}| \leqq |[\bar{M}, \alpha]|$, so $m = |[\bar{M}, \alpha]|$, $\bar{M} = [\bar{M}, \alpha][\bar{M}, \beta]$, and $A^{\bar{M}} = A^{[\bar{M}, \beta]}$. Lemma 3.2 implies $\bar{X} \cong SL_2(q)$ and $C_{\bar{M}}(x) = 1$ for all p'-elements $x \in X$. So it suffices to show $Z = 1$. Let $\langle u\rangle = Z(X)$. Then $M = Z[M, u]$, so $D \subsetneqq X[M, u] \trianglelefteq G$. Thus $Z = 1$.

LEMMA 3.4. *Let D be a class of p-transvections of G, p odd, with $M = O_p(G)$, X a D-subgroup with $X/Z(X) \cong U_3(q)$, and $G = MX$. Let $Z = Z(G)$, $A \in M$ and $m = |AM|$. Then $Z \leqq [A^{\perp}, M]$ and $|M/Z| = m^3$.*

Proof. Let $X = \langle A_i, 1 \leqq i \leqq 3\rangle$, $A = A_1$, let $\alpha_i = A_i^{\perp} \cap X$ and $\Omega = \alpha^X$. Set $Z_0 = [\alpha, M] \cap [\alpha_2, M]$. As X^{Ω} is doubly transitive $Z_0 = [\beta, M] \cap [\gamma, M]$ for $\beta, \gamma \in \Omega$. $[\alpha, M]$ is abelian so $G = \langle X, A^M\rangle$ centralizes Z_0. Thus we can assume $Z_0 = 1$.

Set $N = \prod_{i=1}^{3} [M, \alpha_i]$. By 3.3, $[M, \alpha_i]^{\alpha_j} \leqq [M\alpha_i][M, \alpha_j]$, so N is normalized by $G = \langle \alpha_1, \alpha_2, \alpha_3, M\rangle$. A centralizes M/N, so $M = N$. As $Z_0 = 1$, M is abelian. Let u be the involution in $\langle \alpha_1, \alpha_2\rangle$ and v the involution in $\langle \alpha_2, \alpha_3\rangle$. We may assume $[u, v] = 1$. $M = C_M(u) \times [M, u]$ and by 3.3, $C_M(u) = C_M(\alpha_1) \cap C_M(\alpha_2)$ and $[M, u] = [M, \alpha_1][M, \alpha_2]$. Therefore, $C_M(u) \cap C_M(v) = Z$ and as X has one class of involutions, $|C_M(u)/Z|^3 = |M/Z| = |C_M(u)/Z|m^2$. So $|M/Z| = m^3$, and as $|M| \leqq m^3$, $Z = 1$. That is $Z = Z_0 \leqq [A, M]$.

4. Groups with $\mathscr{D}(D)$ disconnected. This section consists of a proof of the following theorem:

THEOREM 4.1. *Let D be a conjugacy class of p-transvections, $p \geqq 5$, of the group G. Assume $\mathscr{D}(D)$ is disconnected and $O_\infty(G) = 1$. Then $G \cong L_2(q)$ or $U_3(q)$ for some power q of p.*

Throughout § 4, G is a counterexample of minimal order to Theorem 4.1. For $A \in D$ let $\bar{A}$ be the component of $\mathscr{D}(D)$ containing A. Let $\bar{D}$ be the set of components. Write $A \sim B$ if $A, B \in D$ and $\langle A, B\rangle$ is isomorphic to $L_2(p)$ or $SL_2(p)$. For $\bar{A} \neq \bar{B}$ define

$$\Gamma_{A\bar{B}} = \{C \in \bar{A}\colon A \sim E \sim C \text{ for some } E \in \bar{B}\} .$$

Now for $\bar{A} \neq \bar{B}$, $A \sim B$ if and only if $\bar{A} \cup \bar{B}^A = \bar{B} \cup \bar{A}^B$. Thus if $A \sim$

B then $X = \langle \Gamma_{A\bar{B}}, \Gamma_{B\bar{A}} \rangle$ acts on $\Gamma = \bar{A} \cup \bar{B}^A$ of order $p+1$, so $Y = \langle \Gamma_{A\bar{B}} \rangle = AY_\Gamma$ and $X = \langle Y, B \rangle = \langle A, B \rangle X_\Gamma$. By 3.1, $X_\Gamma = 0_\infty(X)$ and Y is a p-group. Further for fixed $\bar{B} \neq \bar{A}$, the sets $\Gamma_{C\bar{B}}$, $C \in \bar{A}$, partition $\bar{A}$.

Let $m = |\Gamma_{A\bar{B}}|$, and let n be the number of classes $\Gamma_{C\bar{B}}$ in $\bar{A}$. If $m > 1$ then applying 3.3 to X we have that $\langle A, B \rangle$ contains a central involution $u = u(A, B)$, and u centralizes only A in $\Gamma_{A\bar{B}}$.

Let $C \in \bar{A}$. $\langle C, B \rangle$ contains $E \in \Gamma_{A\bar{B}}$ and $v = u(E, B)$ is in the center of $\langle C, B \rangle$. Indeed $v = u(C, F)$ where $C \sim F \in \bar{B} \cap \langle C, B \rangle$. As v centralizes a unique member of $\Gamma_{A\bar{B}}$ and $\Gamma_{C\bar{B}}$, each member C_1 of $\Gamma_{C\bar{B}}$ determines a distinct member E_1 of $\Gamma_{A\bar{B}} \cap \langle C_1, B \rangle$. Thus $m = |\Gamma_{C\bar{B}}|$ for all $C \in \bar{A}$. Further $u = u(C_1, F_1)$ for some $C_1 \in \Gamma_{C\bar{B}}$, $F_1 \in \Gamma_{F\bar{A}}$. So $C_D(u)$ intersects each $\Gamma_{C\bar{B}}$ in $\bar{A}$ in a unique member. Set $K = \langle C_D(u) \rangle$ and $H = \langle K, \bar{A} \rangle$. Minimality of G implies $K \cong SL_2(q)$ for some power q of p. So the set Δ of components of $\mathscr{D}(D)$ containing an element of $C_D(u)$ has order $q+1$ and $Q = \langle C_{\bar{A}}(u) \rangle$ acts regularly on $\Delta - \{\bar{A}\}$.

Now there are m^2 involutions $u(A_1, B_1)$, $A_1 \in \Gamma_{A\bar{B}}$, $B_1 \in \Gamma_{B\bar{A}}$, and m^2 pairs (A_1, C_1), $C_1 \in \Gamma_{C\bar{B}}$, with $u(A_1, B_1)$ centralizing at most one pair. It follows there exists u with $A, C \in Q$. So as Q is abelian, $\langle \bar{A} \rangle$ is abelian. Notice that if $m = 1$ then $A = \Gamma_{A\bar{B}} \cap \langle C, B \rangle$, so again $[A, C] = 1$, and $\langle \bar{A} \rangle$ is abelian. Therefore:

LEMMA 4.2. *$\langle \bar{A} \rangle$ is abelian.*

Let $\langle c \rangle = C \in \bar{A}$. We have shown there is an $\langle e \rangle = E \in C_{\bar{A}}(u) \cap \Gamma_{C\bar{B}}$, and we can choose e such that $\bar{B}^c = \bar{B}^e$. Thus as $\langle \bar{A} \rangle$ is abelian, $\bar{B}^{Qc} = \bar{B}^{cQ} = \bar{B}^{eQ} = \bar{B}^Q$, so H acts on $\Delta = \bar{A} \cup \bar{B}^Q$, and $H = KH_\Delta = KO_p(H)$ by 3.1. Summarizing:

LEMMA 4.3. (1) *If $m > 1$ then $\langle A, B \rangle$ contains a central involution u.* (2) *If $\langle A, B \rangle$ contains a central involution u then $\langle \bar{A}, \bar{B} \rangle = H = \langle C_D(u) \rangle 0_p(H)$ with $\langle C_D(u) \rangle \cong SL_2(q)$ for some power q of p.*

Let $J = N_G(\bar{A})$, $I = C_G(\bar{A})$. For $X \subseteq G$ let $F(X)$ be the set of points in $\bar{D}$ fixed by X.

LEMMA 4.4. *Assume u is an involution in the center of $\langle A, B \rangle$. Then*

(i) *If v is an involution in the center of $\langle A, C \rangle$ with $[u, v] = 1$, then $u = v$.*

(ii) $J = O(J)C_J(u)$.

Proof. Set $H = \langle C_D(u) \rangle$. Let v be as in (i). Then v acts on H and fixes $\bar{A}$. There are $q+1$ members of $\bar{D}$ intersecting H, and $q+1$ is even, by 4.3. Thus v fixes a second member $\bar{E} \neq \bar{A}$ of $\bar{D}$

with $\bar{E} \cap H \neq \varnothing$. As $H \cong SL_2(q)$, v centralizes an element E of $\bar{E}$. Thus $\langle u \rangle = Z(\langle A, E \rangle) = \langle v \rangle$, yielding (i). (i) and Glauberman's Z^*-theorem imply (ii).

LEMMA 4.5. *Assume* $m(\bar{A}, \bar{B}) = 1$ *with* $A \sim B$. *Let* $x \in \langle A, B \rangle$ *fix* $\bar{A}$ and $\bar{B}$. *Then*

(1) $B = \bar{B}(A)$ *is the unique element of* $\bar{B}$ *with* $A \sim B$.

(2) x *acts as scalar multiplication in* $GF(p)$ *on* $Q = \langle \bar{A} \rangle$.

(3) *Assume* $y \in J$ *has scalar action on* Q *and fixes* $\bar{B}$. *Then* y *has the same action on* $\langle \bar{B} \rangle$ *and if* $|xI/I| > 2$ *then* $F(x) = \{\bar{A}, \bar{B}\}$.

(4) *If* $\langle A, C \rangle \cong L_2(p^n)$ *or* $SL_2(p^n)$, n *odd, for all* $C \in \bar{B}$, *then* $\langle \bar{A}, \bar{B} \rangle \cong L_2(q)$ *or* $SL_2(q)$.

(5) *If* $p = 5$ *and* $\langle A, C \rangle \cong L_2(p^n)$ *or* $SL_2(p^n)$, n *even, for some* $C \in \bar{B}$ *then there exists* y *with* $|Iy/I| = 4$ *inducing scalar action on* Q *and* $\langle \bar{B} \rangle$.

(6) $m(\bar{A}, \bar{C}) = 1$ *for all* $\bar{C} \neq \bar{A}$.

Proof. (1) is just a restatement of $m(\bar{A}, \bar{B}) = 1$. Let $C \in \bar{A}$. $\langle C, B \rangle$ contains an element A_1 of D centralizing C with $A_1 \sim B$. Thus by (1), $A_1 = \bar{A}(B) = A$. So $x \in \langle A, B \rangle \leqq \langle C, B \rangle$ and thus has the same action on C as on A. This yields (2). Notice that (2) implies $J = IC_J(x)$.

Assume $y \in J$ is as in the hypothesis of (3). Then for $C \in \bar{A}$, y fixes C and therefore $\bar{B}(C)$. So y acts on $\langle C, B \rangle$ with scalar action on $\bar{B} \cap \langle C, B \rangle$. So y acts on $\bar{B}$ as on $\bar{A}$.

Assume y has order r^n for some prime r, r dividing $p - 1$, and $\bar{C} \in F(y) - \{\bar{A}, \bar{B}\}$. Suppose first that $m(\bar{A}, \bar{C}) > 1$. Then by 4.3, $K = \langle \bar{A}, \bar{C} \rangle = HM$ where $H = \langle C_D(u) \rangle$, $u = u(A, C)$, and $M = O_p(K)$. y fixes A so y fixes $\Gamma_{C\bar{A}}$ for $A \sim C$. As $|\Gamma_{C\bar{A}}|$ is a power of p and $p \equiv 1 \bmod r$, x fixes a point C of $\Gamma_{C\bar{A}}$. As this holds for each $A \in \bar{A}$, we can assume x normalizes H. Thus with 4.3, $F(yu) = \{\bar{A}, \bar{C}\}$ and $[y, u] = 1$. Now $J = IC_J(y)$, so $[M, y] \leqq M \cap I = [A, M]$ by 3.3. So if y acts by scalar multiplication on $\bar{C}$, then $[M, y] \leqq [A, M] \cap [C, M] = Z(K)$ by 3.3, so that y centralizes $M/Z(K)$. But y does not even centralize $[A, M]/Z(K)$. So y does not have scalar action on $\bar{C}$.

Set $\bar{E} = \bar{B}^u$. y has scalar action on $\bar{E}$ and $\bar{B}$, so as above $m(\bar{E}, \bar{B}) = 1$. $\langle E, B \rangle \cong SL_2(q)$ or $L_2(q)$ so there exists an involution t with cycle $(\bar{E}, \bar{B})$ inverting y mod $C(\bar{B})$. Thus $ut \in N(\bar{B})$ inverts y mod $C(\bar{B})$, while $N(\bar{B}) = C(\bar{B})C(y)$. So $|yC(\bar{B})/C(\bar{B})| = |yI/y| \leqq 2$.

Assume $|yI/y| > 2$. Then as above $m(\bar{E}, \bar{F}) = 1$ for all $\bar{E}, \bar{F} \in F(y)$ and $C_G(y)$ fixes $F(y)$ pointwise. Now if z is an element centralizing $\bar{A}$, $\bar{B}$, and y then $F(z) = \langle C_D(z) \rangle \cap \bar{D}$ and minimality of G implies $F(z) \cap F(y) = \{\bar{A}, \bar{B}\}$. Thus z moves $\bar{C}$, so $z = 1$. Now there exists an involution t with cycle $(\bar{A}, \bar{B})$ inverting y modulo $C(\bar{A}) \cap C(\bar{B})$. Thus $y^t = y^{-1}$. Similarly there exists s with cycle $(\bar{B}, \bar{C})$ inverting y. So ts

moves $\bar{A}$ to $\bar{C}$ and centralizes y, a contradiction. Thus we have shown (3).

Assume the hypothesis of (4). Let $E \in \bar{A}$, and $C = \bar{B}(E)$. Then for $\alpha \in Q^{\#} \cap \langle A, C\rangle$, $\langle a\rangle \in \bar{A}$. So $\bar{A} = \{\langle a\rangle : a \in Q^{\#}\}$. Let $\Delta = \bar{A} \cup \bar{B}^Q$. Clearly Q normalizes Δ. Further for $E = \langle e\rangle \in \bar{A}$, $\bar{B}^{eB} \subseteqq \bar{A} \cup \bar{B}^{(\langle E,B\rangle \cap Q)}$, so as $\bar{A} = \{\langle a\rangle : a \in Q^{\#}\}$, B normalizes Δ. Thus $X = \langle \bar{A}, \bar{B}\rangle$ normalizes Δ. Further X^Δ is 2-transitive with $Q^\Delta \trianglelefteq X^\Delta_{\bar{A}}$ and regular on $\Delta - \{\bar{A}\}$. Therefore, a result [11] of Kantor and Seitz implies $X^\Delta \cong L_2(q)$. This yields (4).

Assume the hypothesis of (5). Then there exists $y \in \langle A, C\rangle$ with $|yI/I| = 4$ inducing scalar action on $Q \cap \langle A, C\rangle$ and $\langle \bar{B}\rangle \cap \langle A, C\rangle$. By (2), $x = y^2$ inverts Q and $\langle \bar{B}\rangle$, so orbits of x on $\bar{A}$ have order at most two. Suppose (A_1, A_2) is such an orbit. Let $B_2 = \bar{B}(A_2)$ and set $X = \langle A_1, B_2\rangle$. Then y normalizes X with x inverting $Q \cap X$, so y induces scalar action on $Q \cap X$ and fixes A_1, a contradiction. Thus y fixes $\bar{A}$ pointwise and induces scalar action on Q. This yields (5).

It remains to show (6). Assume $m(\bar{A}, \bar{C}) > 1$ and let $u = u(A, C)$. By 4.4, $J = 0(J)C_J(u)$. As $J = IC_J(y)$, $[u, y] \leqq 0(I)$. Thus some conjugate v of u centralizes y. Now if $p > 5$ or $p = 5$ and $\langle A, E\rangle \cong L_2(5^n)$ or $SL_2(5^n)$, n even, for some $E \in \bar{B}$, then we can choose y with $|Iy/I| > 2$. So by (3), $F(y) = \{\bar{A}, \bar{B}\}$. As $[v, y] = 1$ and v fixes $\bar{A}$, v fixes $\bar{B}$. So v centralizes some $B \in \bar{B}$, and by 4.3, as $m(\bar{A}, \bar{B}) = 1$, $v \in I$. But this is impossible as $u \notin I$.

It follows from (4) that $\langle \bar{A}, \bar{B}\rangle \cong L_2(q)$ or $SL_2(q)$ with $q = p^n$, n odd. So $\bar{A} = \{\langle a\rangle : a \in Q^{\#}\}$. But by 4.3, $\langle \bar{A}, \bar{C}\rangle = H = \langle C_D(u)\rangle O_p(H)$ with $O_p(H) \neq Z(H)$. Thus there exists $a \in Q^{\#} \cap O_p(H)$ with $\langle a\rangle \notin \bar{A}$, a contradiction.

LEMMA 4.6. *$m(\bar{A}, \bar{B}) = 1$ for all $\bar{B} \neq \bar{A}$.*

Proof. Assume not. Then by 4.5.6, $m(\bar{A}, \bar{B}) > 1$ for all $\bar{B} \neq \bar{A}$. Let $u = u(A, B)$, $v = u(A, C)$. By 4.4, u is conjugate to v under J, so J takes $\bar{C}$ to a point of $F(u)$. But by 4.3 and 4.4, $C_G(u)^{F(u)}$ is 2-transitive. Thus J is transitive on $\bar{D} - \{\bar{A}\}$. Let $K = \langle \bar{A}, \bar{B}\rangle$, $H = \langle C_D(u)\rangle$ and $M = O_p(K)$. Let $\Omega = \bigcup_{K \cap J} C_Q(u^k)$. Suppose $w \in u^J$ inverts $1 \neq x \in \Omega$. Then wu^k inverts x while by 4.4, wu^k has odd order. So $X = [Q, u^J] \leqq \langle Q - \Omega\rangle \leqq M \cap Q$ by 3.3. But $X \trianglelefteq J$, J is transitive on $\bar{D} - \{\bar{A}\}$ and $M \cap Q$ fixes $\bar{B}$, so X fixes $\bar{D}$ pointwise, contradicting 3.1.5.

LEMMA 4.7. (1) *There exists a prime r such that for all $\bar{B} \neq \bar{A}$, $J = IN_L(R)$ for some r-group with $F(R) = \{\bar{A}, \bar{B}\}$.*

(2) *$G^{\bar{D}}$ is doubly transitive.*

Proof. (1) implies that there exists a prime r such that for any $\bar{B} \neq \bar{A}$, a Sylow r-subgroup of $G_{\bar{A}\bar{B}}$ fixes only two points. This implies $G^{\bar{D}}$ is doubly transitive. So it suffices to proof (1). But unless $p = 5$ there exists a prime r dividing $p - 1$ and an r-element $y \in \langle A, B\rangle$ fixing $\bar{A}$ and $\bar{B}$ with $|Iy/I| > 2$. So 4.5 implies (1) unless $p = 5$ and $\langle \bar{A}, \bar{B}\rangle = H \cong L_2(5^n)$ or $SL_2(5^n)$, n odd. As $5^n = |Q| = |\langle \bar{A}\rangle|$, this holds for all $\bar{B} \neq \bar{A}$.

Suppose u is an involution in I and let $(\bar{C}, \bar{E})$ be a cycle in u and $X = \langle \bar{C}, \bar{E}\rangle$. As u does not centralize X, u acts fixed point free on $X \cap \bar{D}$, so as n is odd, u induces an outer automorphism in $PGL_2(5^n)$ on X, and thus there exists a 2-element $y \in X$ inducing scalar action in $GF(5)$ on $\langle \bar{C}\rangle$ and $\langle \bar{E}\rangle$ with y^2 not centralizing $\langle \bar{C}\rangle$. Thus by 4.5, $|F(y)| = 2$, so $|\bar{D}| = m$ is even.

Assume m is odd. Then I has odd order. Let x be the involution in $\langle A, B\rangle \cap J$. By 4.5, $J = IC_J(x)$. But as m is odd J contains a Sylow 2-subgroup of G, so the Z^*-theorem contradicts $O_\infty(G) = 1$. Therefore, m is even.

If a Sylow 2-subgroup of $G_{\bar{A}\bar{B}}$ fixes exactly two points for every $\bar{B} \neq \bar{A}$, then G^D is doubly transitive. So choose $\bar{B}$ such that a Sylow group of $G_{\bar{A}\bar{B}}$ fixes more than two points. Then $H = \langle \bar{A}, \bar{B}\rangle \cong L_2(5^n)$, $C_J(H)$ has odd order and the involution $x \in H_{\bar{A}\bar{B}}$ fixes three or more points. Suppose $y^2 = x$ for some $y \in G$. If $(\bar{C}, \bar{E})$ is a cycle of y in $F(x)$ then y normalizes $X = \langle \bar{C}, \bar{E}\rangle$ so as $y^2 = x$ and n is odd, y fixes two points in $X \cap \bar{D}$, which must be $\bar{C}$ and $\bar{E}$. This is a contradiction, so x is not rooted in this manner.

Suppose I has odd order. Then by 4.5, $J = IC_J(y)$ for any involution $y \in \langle \bar{A}, \bar{C}\rangle$ and any $\bar{C} \neq \bar{A}$. So $y \in x^I$. Let u be an involution. We may assume u has cycle $(\bar{A}, \bar{B})$. So u normalizes H, and as I has odd order and x is not rooted in $\langle u, H\rangle$, $u \in H$. Thus $u \in x^G$. Thus G has one class of involutions, so as x is not rooted, a Sylow 2-subgroup of G is elementary abelian. Walter's classification of such groups [13] implies $G \cong L_2(5^n)$, a contradiction. So I has even order. Thus x centralizes some involution $u \in I$; as $|\bar{D}|$ is even, there exists $\bar{R} \in F(x) \cap F(u) - \{\bar{A}\}$; minimality of G implies $\langle C_{\bar{D}}(u)\rangle \cong L_2(5^n), SL_2(5^n)$ or $U_3(5^n)$, so $F(x) \cap F(u) = \{\bar{A}, \bar{R}\}$.

Consider $C_G(x)^{F(x)}$. Arguments such as in 4.5.3 and in the last paragraph show that nontrivial elements of $C(x)^{F(x)}$ fix at most two points. Let $(\bar{C}, \bar{E})$ be a cycle of u in $F(x)$. We have shown x is rooted modulo $C(\bar{C}) \cap C(\bar{E})$, while x is not rooted. So $C(\bar{C}) \cap C(\bar{E})$ has even order and there exists an involution $v \in C(x)^{F(x)}$, fixing $\bar{C}$ and $\bar{E}$, and centralizing u. v acts on $F(x) \cap F(u) = \{\bar{A}, \bar{R}\}$. Let $L = C_{\bar{A}\bar{R}}^{F(x)}$. L acts semiregularly on $F(x) - \{\bar{A}, \bar{R}\}$ and $C_L(v)$ acts on $F(v) \cap F(x) = \{\bar{C}, \bar{E}\}$, so $\langle v\rangle = C_L(u)$. So a Sylow 2-subgroup S of $\langle L, v\rangle = L^*$ is semidihedral or dihedral, and there are one or two classes of involutions in $L^* - L$, respectively. But if $\bar{T} \in F(x) - \{\bar{A}, \bar{R}\}$ let t be the involution in $C(x)^{F(x)}$ fixing $\bar{T}$ and $\bar{T}^u$ and centralizing u. Then $t \in v_i^L$, $i = 1$ or 2, one of the (at most) two classes of involutions in $L^* - L$. So L takes $F(t) \cap F(x) = \{\bar{T}, T^u\}$ to $F(x) \cap F(v_i)$. Thus L has one orbit, or two orbits of equal length, on $F(x) - \{\bar{A}, \bar{R}\}$, for S semidihedral or dihedral, respectively. It now follows easily that $C(x)^{F(x)}$ is 2-transitive. But J and therefore $C_J(x)$ cannot take $\bar{B}$ to $\bar{R}$ as there is no involution in I fixing $\bar{B}$. This last contradiction completes the proof of 4.7.

Set $L = G_{\bar{A}\bar{B}}$, $H = \langle \bar{A}, \bar{B} \rangle$, $K = C_G(H)$, and $Q = \langle \bar{A} \rangle$.

LEMMA 4.8. (1) *$J = IL$ and $K \neq 1$.*
(2) *$H \cong L_2(q)$ or $SL_2(q)$.*

Proof. By 4.7.1 there exists a prime r such that a Sylow r-subgroup R of L fixes only $\bar{A}$ and $\bar{B}$, and $J = IN_J(R)$. $N_J(R)$ acts on $F(R) = \{\bar{A}, \bar{B}\}$; so $N_J(R) \leqq L$. If $K = I \cap L = 1$ then I is regular on $\bar{D} - \{\bar{A}\}$ by 4.7.2, so [11] implies $G \cong L_2(q)$ or $U_3(q)$. Thus $K \neq 1$. Minimality of G implies $H = \langle C_D(K) \rangle \cong SL_2(q)$ or $L_2(q)$.

LEMMA 4.9. *Suppose $x \in L^\#$ with $|C_Q(x)| = q_0 > 1$. Then $\langle C_D(x) \rangle \cong L_2(q_0)$, $SL_2(q_0)$ or $U_3(q_0)$ and $|F(x)| = q_0 + 1$ or $q_0^3 + 1$.*

Proof. Minimality of G yields the desired form for $\langle C_D(x) \rangle$. If $\bar{C} \in F(x)$ then $[x, C] = 1$ where $C = \bar{C}(A)$, $A \in C_{\bar{A}}(x)$. Thus $|F(x)| = q_0 + 1$ or $q_0^3 + 1$.

LEMMA 4.10. *Set $n = |\bar{D}|$. Then $(n - 1, |K|)$ is a power of p.*

Proof. Let r be a prime divisor of $|K|$, and R a Sylow r-subgroup of K. By 4.9, $F(R) = q + 1$ or $q^3 + 1$, so if $r \neq p$ then a Sylow r-subgroup R_1 of $N_I(R)$ fixes a second point $\bar{B}$ of $F(R)$; that is $R_1 = R$. So R is Sylow in I and r does not divide $n - 1 = |I : K|$.

LEMMA 4.11. *$|\bar{D}| = n$ is even. If u is an involution then $n \equiv |F(u)| \bmod 4$. $|L|$ is even.*

Proof. Results of Bender on doubly transitive groups [5.6] imply L has even order. By 3.1, G is simple, so any involution u must act as an even permutation on $\bar{D}$. Thus $n \equiv |F(u)| \bmod 4$. If n is odd, 2-elements fix an odd number of points. So by 4.8 and 4.9, $|K|$ and $|L/HK|$ are odd. And by 4.5.3, $|H \cap L| \not\equiv 0 \bmod 4$. As L has even order, $|H \cap L| \equiv |L| \equiv 2 \bmod 4$. Thus $p \equiv q \equiv 5 \bmod 8$. Let u be the involution in $H \cap L$, and S a u-invariant Sylow 2-subgroup of I. As

n is odd and $J = IL$, $S\langle u\rangle$ is Sylow in G. As G has no subgroup of index two, $S \neq 1$. Let s be an involution in S, and $(\bar{B}, \bar{C})$ a cycle in s. Then s normalizes $X = \langle \bar{B}, \bar{C}\rangle$ and as $|F(s)| = 1$, s acts fixed point free on $\bar{D} \cap X$. So as $p \equiv q \equiv 5 \bmod 8$, $\langle s, X\rangle \cong PGL_2(q)$ and there exists $y \in \langle s, X\rangle$ of order 4 inducing scalar multiplication on $\langle \bar{B}\rangle$ and fixing $\bar{B}$ and $\bar{C}$. By 4.5.3, $|F(y)| = 2$, contradicting n odd.

LEMMA 4.12. *If $J = O(I)L$ then $J = O_\pi(I)L$, where π is the set of primes dividing $n - 1$. Also $O_p(K) \neq 1$, and $O_\pi(I)$ is not nilpotent.*

Proof. Set $P = O_\pi(I)$. If $P \neq O(I)$ let R/P be minimal normal in J/P, $R < O(I)$. R/P is an r-group for some prime r and by a Frattini argument, $J = PN_J(R_1)$ where R_1 is a Sylow r-subgroup of R contained in K. By 4.9, $N_J(R_1) = LP_1$ where $|P_1| = q$ or q^3, and $P_1 \trianglelefteq N_J(R_1)$. Thus $PP_1 \trianglelefteq J$, so $P_1 \leqq P$ and $J = PL$. Results of Kantor and Seitz on doubly transitive groups [11, 12] imply P is not nilpotent or regular on $\bar{D} - \{\bar{A}\}$. Thus $1 \neq P \cap L = P \cap K = O_p(K)$ by 4.10.

LEMMA 4.13. *Let $X \subseteqq L$ fix 3 or more points of $\bar{D}$. Then $C_G(X)^{F(X)}$ is doubly transitive.*

Proof. It suffices to show there exists a prime r such that a Sylow r-subgroup of $C_L(X)$ fixes only $\bar{A}$ and $\bar{B}$. Thus with 4.5 we can assume $q = 5^m$ with $m > 1$ odd. Thus there is an r-element $1 \neq y \in H \cap L$, $r > 2$, and as m is odd y is not inverted in J/I by 4.8. Thus arguing as in 4.5, $F(y) = \langle \bar{A}, \bar{B}\rangle$. $[y, X] = 1$ unless $C_Q(X) \neq 1$, in which case 4.9 implies $C_G(X)^{F(X)}$ is doubly transitive.

LEMMA 4.14. *Assume $q \equiv -1 \bmod 4$ and x is an involution in L inverting Q with $|F(x)| > 2$. Then $|F(x)| = q + 1$.*

Proof. As $q \equiv -1 \bmod 4$, q is an odd power of p, so no element in $H \cap L$ is inverted in J/I. Thus if $y \in H \cap L$ with $|y| > 2$ then $|F(y)| = 2$. Therefore, with 4.9 and 4.13, $C_G(x)^{F(x)}$ is a Zaussenhaus group. So $C_G(x)^{F(x)}$ has a normal subgroup isomorphic to $L_2(m)$, of index at most two, with $|F(x)| = m + 1$. Now if $m \equiv 1 \bmod 4$ then by 4.9 and 4.11, K has odd order, and $\langle x\rangle$ is Sylow in L, so that $|C_L(x)^{F(x)}|$ is odd, contradicting $m \equiv 1 \bmod 4$. So $m \equiv -1 \bmod 4$. Thus $C_L(x)^{F(x)}$ is cyclic and inverted by any $t \in C_G(x)$ with cycle $(\bar{A}, \bar{B})$. As we can choose $t \in H$, and $[K, t] = 1$, it follows that $|C_K(x)| = \varepsilon \leqq 2$. Further $\varepsilon(m - 1)/2 = |C_L(x)^{F(x)}| = \varepsilon|H \cap L| = \varepsilon(q - 1)/2$, so $m = q$.

LEMMA 4.15. *Suppose u is an involution in $Z^*(L)$ fixing 3 or more points. Then $u \in Z^*(J)$.*

Proof. $u \in Z^*(L)$ so $u^L \cap C_L(u) = \{u\}$. Now 4.13 implies $u^G \cap L = u^L$. Further as $|\bar{D}|$ is even, if v is a conjugate of u in J centralizing u then we can assume $v \in L$, so $v \in u^G \cap C_L(u) = u^L \cap C_L(u) = \{u\}$. Thus by the Z^*-theorem, $u \in Z^*(J)$.

LEMMA 4.16. *If $H \cong L_2(q)$ then $H \cap \bar{D} = F(X)$ for any $1 \neq X \leqq K$.*

Proof. If $F(X) \neq H \cap \bar{D}$ then by 4.9, $H \leqq \langle C_D(X) \rangle \cong U_3(q)$, so $H \cong SL_2(q)$.

LEMMA 4.17. *Assume u is an involution in L fixing $m + 1 \geqq 3$ points, let $c = |L: C_L(u)|$ and let e be the number of conjugates of u with cycle $(\bar{A}, \bar{B})$. Then $|D| - 1 = m(m + 1)e/c + m$.*

Proof. Let Ω be the set of pairs (v, α) where $v \in u^G$ and α is a cycle in v. Then $|u^G|(n - m - 1)/2 = |\Omega| = n(n - 1)e/2$ where $n = |\bar{D}|$. Further by 4.13, $|u^G| = n(n - 1)c/m(m + 1)$.

LEMMA 4.18. (1) *Let S be a 2-group such that $C_Q(S) \neq 1$. Then S has rank at most one.*

(2) *$J = O(I)L$.*

Proof. Suppose $1 \neq \langle u \rangle = H \cap L$. Then by 4.15, $u \in Z^*(I)$, so $J = O(I)L$. Define $P = O_\pi(I)$ as in 4.12, and assume S has 2-rank at least two. Then $P = \prod_{S^\#} C_P(s)$, while by 4.9, $C_P(s)$ is a p-group for $s \in S^\#$. Thus P is a p-group, contradicting 4.12.

So $H \cap L = 1$ and by 4.16, $N_I(H) = QK$ is strongly embedded in I. As $Q \leqq O(I)$ and $[K, H \cap L] = 1$, Bender's classification of groups with a strongly embedded subgroup [6] implies $J = O(I)N_J(H \cap L)$. By 4.5, augmented by arguments such as in 4.13 for the case $q = 5^m$, m odd, $N_J(H \cap L) = L$. Now arguing as above, S has 2-rank at most one.

Define $P = O_\pi(I)$ as in 4.12. Set $P_0 = O_p(K)$. $P_0 \neq 1$ by 4.12 and 4.18.

LEMMA 4.19. (1) *$F(X) = H \cap \bar{D}$ for $1 \neq X \leqq P_0$.*

(2) *$H \cap K = 1$.*

(3) *Assume u is an involution in K and let $v \in u^G$ have cycle $(\bar{A}, \bar{B})$. Let P_1 be a $\langle u, v \rangle$ invariant Sylow p-group of $O(K)$. Then $[v, P_1] = P_1$ and $[u, P_1] \neq 1$.*

Proof. Assume $1 \neq X \leqq P_0$ with $F(X) \neq H \cap D$. Then $Y = \langle C_D(X) \rangle \cong U_3(q)$ by 4.9. So $H \cap K = \langle u \rangle \neq 1$. Further as $N_K(X)^{F(X)}$ is a p'-group, $X = P_0$. Let $(\bar{C}, \bar{E})$ be a cycle in u and $v \in u^G$ fix $\bar{C}$ and $\bar{E}$. Then $[u, v] = 1$ so v acts on $\langle C_D(u) \rangle = H$ and thus also on P_0.

v induces an automorphism on $Y \cong U_3(q)$ and therefore fixes points $\bar{A}_i \in F(P_0)$. So $\bar{C} \in \langle \bar{A}_1, \bar{A}_2 \rangle \leqq Y$ and therefore $F(P_0) = \bar{D}$, a contradiction. This yields (1).

Assume $1 \neq \langle u \rangle = H \cap K$. Then in particular $[u, P_0] = 1$. Let $v \in u^G$ have cycle $(\bar{A}, \bar{B})$. v acts on P_0 and $F(v) \cap F(x) = F(v) \cap F(u) = \varnothing$ for $x \in P_0^{\#}$. Thus $C_{P_0}(v)$ acts fixed point free on $F(v)$ of order $q + 1$, so $C_{P_0}(v) = 1$. Define e and c as in 4.17. It follows that $c = 1$ and $e \equiv 0 \bmod p$. So by 4.17, $|\bar{D}| - 1 = q[(q + 1)e/c + 1] \equiv q \bmod pq$. So P_0Q is Sylow in P and u centralizes P_0Q, and inverts a Hall p'-group P_1 of P. Thus $P = P_1 \times (P_0Q)$ is nilpotent, contradicting 4.12. This yields (2).

Assume the hypothesis of (3) and define c and e as in 4.17. Arguing as above, $[v, P_1] = P_1$, so p divides e. By 4.18, $L = O(K)C_L(u)$, so if $[P_1, u] = 1$, then p does not divide c. But then arguing as above we have a contradiction.

LEMMA 4.20. $q \equiv 1 \bmod 4$.

Proof. Assume $q \equiv -1 \bmod 4$. By 4.9, 4.10, and 4.14, $C_P(x)$ is a p-group for any involution $x \in L$, while by 4.12, P is not a p-group. Thus L has 2-rank one. Suppose K has odd order. By 4.11, L has even order so there exists an involution $x \in L$ and $\langle x \rangle$ is Sylow in J. If $|F(x)| = 2$, then by 4.11, $n = |\bar{D}| \equiv 2 \bmod 4$, and [2] implies $G \cong L_2(q)$. Thus by 4.14, $|F(x)| = q + 1$. Let v be a conjugate of x with cycle $(\bar{A}, \bar{B})$. We may choose $v = t$ or tx where $t \in H$. By 4.16, $F(P_0) = H \cap \bar{D}$, so $|F(P_0) \cap F(v)| = 0$ or 2. Thus if $C_{P_0}(v) \neq 1$ then $1 \equiv q + 1 = |F(x)| \equiv 0$ or $2 \bmod p$, so v inverts P_0. Thus $v = tx$, and x inverts P_0. Define e and c as in 4.17. Then $e = (q - 1)c/2$, so by 4.17, $n - 1 = q(q^2 + 1)/2$. In particular QP_0 is Sylow in P and inverted by x. As $|F(x)| = q + 1$, x inverts an x-invariant Sylow r-subgroup of P for $r \neq P$, with 4.10. Thus x inverts P, and P is abelian, contradicting 4.12.

So K contains an involution u. Let $v \in u^G$ have cycle $(\bar{A}, \bar{B})$, with $[v, u] = 1$. As $H \cap K = 1$ and v acts fixed point free on $F(u) = H \cap \bar{D}$, $v = t$ or ut where $t \in H$. By 4.19 $[v, P_0] \neq 1$, so $v = ut$. Thus defining e and c as in 4.17, $e = (q - 1)c/2$, so by 4.17, $n - 1 = q[(q + 1)e/c + 1] = q(q^2 + 1)/2$. Let R be a $\langle u \rangle(H \cap L)$ invariant r-Sylow group of P, where $r \neq p$. Then $\langle u \rangle(H \cap L)$ acts semiregularly on R, $|R| > q$. As a p'-Hall group of P has order $(q^2 + 1)/2$, $(q^2 + 1)/2$ is a prime power. Thus q is a prime (e.g. Lemma 3.1, [1]). P_0 acts semiregularly on $\bar{D} - F(P_0)$ of order $q(q^2 + 1)/2 - q = q(q^2 - 1)2$, so $|P_0| = q$. Thus $Q = C_P(u) \leqq Z(P)$, or $[P, u]$ is a Hall p'-group of P. In either event P is nilpotent, contradicting 4.12.

LEMMA 4.21. *$|K|$ is odd.*

Proof. Assume K has even order and let u be an involution in K and v a conjugate of u, centralizing u, with cycle $(\bar{A}, \bar{B})$. By 4.1, $[v, P_1] = P_1$ and $[u, P_1] \neq 1$. So $C_{P_1}(uv) \neq 1$, $|F(uv)| \equiv 0 \bmod p$ and $uv \notin u^G$. So by 4.11 and 4.18, $uv \in x^G$ or $(ux)^G$ where $x \in H$. Now $[x, P_0] = 1$ so $|F(x)| \equiv 2 \bmod p$. Thus $uv \in (ux)^G$ and as $|F(uv)| \equiv 0 \bmod p$ and $|F(P_0) \cap F(ux)| = 2$, $C_{P_0}(ux) = C_{P_0}(u) = 1$. So $Q = C_P(u)$, yielding a contradiction as in 4.20.

LEMMA 4.22. *L has 2-rank one.*

Proof. Assume not. Then as $|K|$ is odd by 4.21, there exists an involution $x \in H \cap L$ and an involution $u \in L$ with $|C_Q(u)| = r$, $q = r^2$, and $Q = C_Q(u) \times C_Q(ux)$. Notice $P = C_P(x)C_P(u)C_P(ux) = C_P(x)Q$. Set $m + 1 = |F(x)|$. As P_0 acts semi-regularly on $F(x) - \{\bar{A}, \bar{B}\}$, $m \equiv 1 \bmod p$. Let P_2 be a subgroup of $C_P(x)$ maximal with respect to being normal in $C_J(x)$ and semiregular on $F(x) - \{\bar{A}\}$. Let M/P_2 be a minimal subgroup of $C_J(x)/P_2$ contained in $C_P(x)$. By 4.10, M/P_2 is a p-group and as P_2 is semi-regular on $F(x) - \{\bar{A}\}$ of order $m \equiv 1 \bmod p$, P_2 is a p'-group. Thus $M = P_2(P_0 \cap M) = P_2M_0$ and $C_J(x) = P_2(N(M_0) \cap C_J(x)) = P_2C_L(x)$ as $F(x) \cap F(M_0) = \{\bar{A}, \bar{B}\}$. So $|P_2| = m$ and $P_2 \leqq QC_P(x) = P$. Thus P_2Q is regular on $\bar{D} - \{\bar{A}\}$. As u inverts P_2, P_2Q is nilpotent and thus contained in Fit (P), the Fitting subgroup of P. So Fit (P) is transitive on $\bar{D} - \{\bar{A}\}$ and nilpotent, contradicting 4.12.

LEMMA 4.23. *$|\bar{D}| \equiv 2 \bmod 4$.*

Proof. Assume not. Let x be the involution in $H \cap L$. By 4.11, $|F(x)| \equiv 0 \bmod 4$. As in 4.14, $C_G(x)^{F(x)}$ is a Zassenhaus group and t inverts $L^{F(x)}$ where $t \in H$ has cycle $(\bar{A}, \bar{B})$. But $[t, P_0] = 1$ and $P_0 \cong P_0^{F(x)}$, a contradiction.

4.22 and 4.23 together with [2] imply $G \cong L_2(q)$ or $U_3(q)$. Thus the proof of Theorem 4.1 is complete.

5. Examples.

Hypothesis 5.1. *Let V be a $2m$ dimensional space over $GF(q)$, q a power of the odd prime p, with nondegenerate skew symmetric bilinear form $(,)$. For $u \in V^\#$ the transvection u^* determined by u is the map*

$$u^*\colon \langle x\rangle \longrightarrow \langle x + (x, u)u\rangle$$

considered as a projective transformation of V. Let $D = \{\langle u^* \rangle : u \in V^\#\}$ and $G = \langle D \rangle$.

G is the $2m$ dimensional projective *symplectic* group $SP_{2m}(q)$ over $GF(q)$.

LEMMA 5.2. *Assume hypothesis* 5.1. *Let $A = \langle a^* \rangle$ and $B = \langle b^* \rangle$ lie in D with $[A, B] \neq 1$. Set $L = \langle D_A \cap D_B \rangle$. Then*

(1) *D is a class of p-transvections of G.*

(2) *$L/Z(L) \cong SP_{2m-2}(q)$ for $m > 1$.*

Proof. Let $\langle c^* \rangle = C \in D$. Then $[A, C] = 1$ if and only if $(a, c) = 0$. So (,) restricted to $\langle a, b \rangle$ is a nondegenerate skew symmetric bilinear form and therefore $\langle A, B \rangle$ is a homomorphic image of a subgroup of $SL_2(q)$. This yields (1). Similarly L acts as a symplectic group on $\langle a, b \rangle^\perp$ yielding (2).

Hypothesis 5.3. *Let V be a n-dimensional vector space over $GF(q^2)$ with nondegenerate semibilinear form (,). For nonsingular vector u let u^* be the transvection determined by u considered as a projective transformation of V. Let $D = \{u^* : (u, u) = 0\}$, and $G = \langle D \rangle$.*

G is the n dimensional projective special *unitary* groups, $U_n(q)$.

LEMMA 5.4. *Assume hypothesis* 5.3. *Let $A = \langle a^* \rangle$ and $B = \langle b^* \rangle$ lie in D with $[A, B] \neq 1$. Set $L = \langle D_A \cap D_B \rangle$ then*

(1) *D is a class of p-transvections of G.*

(2) *$L/Z(L) \cong U_{n-2}(q)$* for *$n \geqq 4$.*

(3) *G contains a unique class of D-subgroups K^G with $K/Z(K) \cong U_{n-1}(q)$.*

Proof. The proofs of (1) and (2) are as in 5.2. Assume K is a D-subgroup of G with $K/Z(K) \cong U_{n-1}(q)$. As $[a^*, c^*] = 1$ if and only if $(a, c) = 0$, $\langle u : \langle u^* \rangle \in K \cap D \rangle$ is a nonsingular hyperplane of V preserved by K. As G is transitive on such hyperplanes, (3) follows.

6. Proof of main theorem.

For the remainder of this paper G is a counter example of minimal order to the main theorem. Lemma 3.1 implies:

LEMMA 6.1. *G is simple.*

Theorem 4.1 implies:

LEMMA 6.2. *$\mathscr{D}(D)$ is connected.*

Let $A \in D$. By 2.4, A is contained in a unique maximal set of imprimitivity α of G^D. Set $H = \langle D_\alpha \rangle$, $M = O_\infty(H)$, and $\Omega = \alpha^G$. By 2.4, H is D_α^*-simple. Minimality of G implies $H/M \cong Sp_n(q)$ or $U_n(q)$, for some power q of p.

LEMMA 6.3. *Let $\beta \in D_\alpha, \gamma \in D_\beta \cap A_\alpha$. Set $\Gamma = D_\alpha \cap D_\gamma$ and $L = \langle \Gamma \rangle$. Then $LM = H$, $M \neq Z(H)$ and $\alpha * \beta = \{\alpha\} \cup \beta^M$.*

Proof. Let $B \in \beta$. $H/M \cong Sp_n(q)$ or $U_n(q)$ has $V_{BM/M}$ as a set of imprimitivity on $D_\alpha^* M/M$, so $\langle \beta \rangle$ is abelian. Set $K = \langle D_\beta \cap \Gamma \rangle$, $H_1 = \langle D_\beta \rangle$, and $M_1 = O_\infty(H_1)$.

Assume $n \geqq 4$. Then by 5.2 and 5.4, $KM_1/M_1 \cong U_{n-2}(q)$ or $Sp_{n-2}(q)$. Suppose L is not D-simple. Then by 2.1, L is the central product of two D-subgroups L_i. Let $B \in L_1$. K is D-simple, so $K = L_2$. Thus $\beta = B^\perp \cap L_1$, so $\mathscr{D}(L_i \cap D)$ is disconnected. Thus $L/O_\infty(L) \cong L_2(q) \times L_2(q)$ or $U_3(q) \times U_3(q)$. As $U_5(q)$ contains no D-subgroup of the latter type, that case is eliminated. As $\beta = B^\perp \cap L_1$, $\beta = B^\perp \cap D_\alpha^*$. Now let $C \in \gamma$ with $X = \langle A, C \rangle \cong SL_2(q)$, and $x \in X$ fix α and γ with $|x| \geqq 4$. x centralizes L and normalizes H. Suppose $L \neq \langle C_{D_\alpha^*}(x) \rangle = Y$. Then there exists $\delta \in A_\gamma \cap Y$. Minimality of G implies $\mathscr{D}(Y \cap D)$ is connected so we can choose $\delta \in D_\sigma$ for some $\sigma \subseteqq L$. Let $Z = \langle \lambda, \delta \rangle$. As $\gamma, \delta \in D_\sigma$, $Z/O_p(Z) \cong SL_2(q)$. So as $[x, \delta] = 1$, we get $[x, \lambda] = 1$, a contradiction. So $L = Y$ and as x induces an automorphism on $H/M \cong Sp_4(q)$ or $U_4(q)$ with $Y/O_\infty(Y) \cong L_2(q) \times L_2(q)$, this automorphism has order two. As $|x| > 2$, $1 \neq x^2$ centralizes H/M. As $[x^2, B^\perp \cap D_\alpha^*] = 1$, $[H, x^2]$, so $\langle x^2 \rangle = Z(X)$ and $X \cong SL_2(5)$. But now $C_D(x^2)$ is a component of $\mathscr{D}(D)$, contradicting 6.2.

So L is D-simple. Therefore, minimality of G implies $L/O_\infty(L) \cong H/M$ and $O_\infty(K) = M_1 \cap K \neq Z(K)$. As $D_\gamma \cap (\alpha^* \beta) = \{\beta\}$, $\alpha^* \beta = \{\alpha\} \cup \beta^M$.

Thus we may assume $n \leqq 3$. Suppose $X = \langle A, E \rangle \cong SL_2(q)$ for $E \in D_\beta^*$. Then we may choose $C \in \gamma \cap X$. Let $\langle u \rangle = Z(X)$. Then $u \in \langle A, C \rangle$, so $[u, L] = 1$. u acts on H/M and centralizes β, so $J = \langle C_{D_\alpha^*}(u) \rangle$ contains a D-subgroup isomorphic to $SL_2(q_0)$ for some q_0 dividing q. Let $\langle v \rangle$ be the center of that subgroup. If $J \neq L$ then considering $\langle J, X \rangle$, minimality of G yields a contradiction. So $J = L$ and $[v, X] = 1$. $\langle C_{D_\alpha^*}(v) \rangle = X_0 \cong SL_2(q)$, so arguing on v in place of u we get $X_0 = L$ and $q_0 = q$. If $H = LM$ then as $D_\alpha \neq D_\gamma$, $M \neq Z(H)$, and as above $\alpha^* \beta = \{\alpha\} \cup \beta^M$. So we may assume $H/M \cong U_3(q)$. Define x as above with $u \in \langle x \rangle$. $[x, L] = 1$ and x acts on $H/M \cong U_3(q)$, so as $2 < |x|$ divides $q - 1$, $u \in \langle x \rangle$ centralizes H/M, contradicting $LM \neq H$.

So X does not exist. Thus $H \cong L_2(q)$. Claim $\beta = B^\perp \cap D_\alpha^* = \alpha^* \beta - \{\alpha\}$. For if not $\beta \subseteqq \langle \alpha^* \beta - \{\alpha, \beta\} \rangle$ whereas $\alpha \not\subseteqq \langle \alpha^* \beta - \{\alpha, \beta\} \rangle$.

Choose $1 \neq x \in H_1$ fixing α and λ. x acts on H and centralizes β, so $[x, H] = 1$. Let $E \in D_\alpha^* - L$ and $C \in \gamma$. The action of x on $\langle C, E\rangle$ yields a contradiction.

LEMMA 6.4. *Let (α, γ, β) be a triangle in Ω. Then there exists σ with α, β, and γ in D_σ.*

Proof. Claim $\mathscr{D}(\Omega)$ has diameter two. For if not $\alpha\beta\gamma\delta$ be a chain with $d(\alpha, \delta) = 3$. Let $H_1 = \langle D_\gamma\rangle$, $M_1 = O_\infty(H_1)$, $\Gamma = D_\alpha \cap D_\gamma$ and $L = \langle \Gamma\rangle$. Then by 6.3, $H_1 = LM_1$, so $\delta M_1 = \sigma M_1$ for some $\sigma \in \Gamma$. Thus $\sigma \in D_\alpha \cap D_\delta$, contradicting $d(\alpha, \delta) = 3$. Thus $\mathscr{D}(\Omega)$ has diameter two, so if (α, γ, β) is a triangle, by 6.3, $LM = H$. So again there exists $\sigma \in \Gamma$ with $\sigma M = \beta M$. α, β, and γ are in D_σ.

LEMMA 6.5. *Let $\gamma \in A_\alpha$. Then $\langle \alpha, \gamma\rangle \cong SL_2(q)$ and $|\langle \alpha\rangle| = q$.*

Proof. Set $X = \langle \alpha, \gamma\rangle$. By 6.4, there exists $\beta \in D_\alpha \cap D_\gamma$. Let $H_1 = \langle D_\beta\rangle$, $M_1 = O_\infty(H)$. Suppose $A \neq E \in \alpha$ with $A \equiv E \bmod M_1$. Then $A = \langle a\rangle$, $E = \langle e\rangle$ with $x = ae^{-1} \in M_1$. Thus x fixes every singular line $\beta^*\delta = \{\beta\} \cup \delta^{M_1}$ through β. As $H \leqq C_G(x)$ is transitive on D_α, x fixes all singular lines through any $\beta \in D_\alpha$. Let $\sigma \in A_\alpha$. By 6.3, there are distinct singular lines $\beta_i^*\sigma$, $i = 1, 2$, with $\beta_i \in D_\alpha$. Then x fixes $(\beta_1^*\sigma) \cap (\beta_2^*\sigma) = \{\sigma\}$. Thus x fixes Ω pointwise. But this contradicts 6.1.

So $|\langle \alpha\rangle| = |\langle \alpha\rangle M/M| = q$ by 6.3. By 6.3, $X/O_p(X) \cong SL_2(q)$, so $|\langle \alpha\rangle| = q$, $O_p(X) = 1$.

LEMMA 6.6. *Ω is locally conjugate in G, $\langle \alpha^\perp\rangle$ is transitive on A_α, and G^Ω is rank 3.*

Proof. By 6.5, Ω is locally conjugate in G. Therefore, to show $\langle \alpha^\perp\rangle$ is transitive on A_α and thus that G^Ω is rank 3, it suffices to show (*) of 2.7. But if (α, γ, β) is a triangle in Ω, set $X = \langle \alpha, \gamma, \beta\rangle$. Then by 6.3, $X/O_p(X) \cong SL_2(q)$ with $\alpha^\perp \cap X = \alpha^{O_p(X)}$. So 3.3 yields (*).

Following the notation of D. Higman let $k = |D_\alpha|$, $l = |A_\alpha|$, $\lambda = |D_\alpha \cap D_\beta|$ for $\beta \in D_\alpha$, and $\mu = |D_\alpha \cap D_\gamma|$ for $\gamma \in A_\alpha$. Let $m = |\beta^M|$. [10] implies:

LEMMA 6.7. *$l = k(k - \lambda - 1)/\mu$ and either*

(1) *$k = l$ and $\mu = (\lambda + 1)/2 = k/2$ or*

(2) *$d^2 = (\lambda - \mu)^2 + 4(k - \mu)$ is a square and d divides $2k + (\lambda - \mu)(k + l)$.*

LEMMA 6.8. *$O_\infty(L) = Z(L)$.*

Proof. Assume not. Then there exists $x \in O_\infty(L) = L \cap M$ with $B^x \neq B$. By 6.5, $\beta^x \neq \beta$, so $\beta^x \in (\alpha^*\beta) \cap D_\gamma = \{\beta\}$, a contradiction.

LEMMA 6.9. *$\alpha^*\gamma = \langle\alpha, \gamma\rangle \cap \Omega$ has order $q+1$. If $H/M \cong U_3(q)$ then $m = q^2$.*

Proof. Assume $n \geqq 4$. Then a hyperbolic line $\beta\delta$ in $\mathscr{B}(\Gamma)$ is as claimed. But $\beta^*\delta \subseteqq \beta\delta$ while clearly $\langle\beta, \delta\rangle \cap \Omega \subseteqq \beta^*\delta$. Next assume $n = 2$. Then by 6.3, $D_\alpha \cap D_\gamma = \langle\beta, \delta\rangle \cap \Omega$ for $\beta, \delta \in D_\alpha \cap D_\gamma$, and $D_\beta \cap D_\delta = \langle\alpha, \gamma\rangle \cap \Omega$, so $\alpha^*\gamma$ is as claimed. Finally assume $H/M \cong U_3(q)$. Let $Z = Z(\langle\alpha^\perp\rangle)$. Z acts semiregularly on $\alpha^*\gamma - \{\alpha\}$. So if $|\alpha^*\gamma| = q+1$ then $|Z| = q$. If $|\alpha^*\gamma| \neq q+1$ then $\alpha^*\gamma = D_\beta \cap D_\delta$, for $\beta, \delta \in D_\alpha \cap D_\gamma$. So $|\alpha^*\gamma| = q^3$ and $N_G(\alpha^*\gamma)^{\alpha^*\gamma}$ acts as a subgroup of Aut $(U_3(q))$. But by 3.4, Z is elementary abelian, while an elementary subgroup of Aut $(U_3(q))$ acting semiregularly on q^3 letters has order at most q. Further $|\alpha^*\gamma| - 1 = |N_{M\langle\alpha\rangle}(\alpha^*\gamma)| = |C_{M\langle\alpha\rangle}(L)| = |Z| = q$ by 3.4. So $|\alpha^*\gamma| = q+1$.

Finally $\mu = |\Gamma| = q^3 + 1, \lambda = m - 1$, and $k = \mu m$ by 6.3 and 6.8. Thus by 6.7, $q^3m^2 = l$, while by 6.6, $l = |\langle\alpha^\perp\rangle: N_{\langle\alpha^\perp\rangle}(\gamma)| = |M\langle\alpha\rangle| = qm^3$ by 3.4. Thus $m = q^2$.

LEMMA 6.10. *If $H/M \cong L_2(q)$ then $m = q$ or q^2. If $H/M \cong Sp_n(q)$ or $U_n(q)$, $n \geqq 3$, then $m = q$ or q^2 respectively.*

Proof. Assume $H/M \cong L_2(q)$. Then $\mu = q+1$, $k = \mu m$ and $\lambda = m - 1$. So by 6.7, $l = m^2q$ and $\mu + \lambda = m + q$ divides $2k + (\lambda - \mu)(k + l) \equiv -2(q^2 - 1)q \bmod (m+q)$. By 3.3, an element of order $q - 1$ in L acts semiregularly on $([A, M]/Z)^\#$ of order $m - 1$, so $q - 1$ divides $m - 1$. Thus q divides $m = q^{r+1}$. So $q^r + 1$ divides $2(q^2 - 1)$ and therefore $r \leqq 1$. That is $m = q$ or q^2.

So with 6.9 we can assume $n \geqq 4$. Therefore, singular lines in L have order q or q^2, respectively. Thus as $\alpha^*\beta = \{\alpha\} \cup \beta^M$ these lines are also lines in G.

LEMMA 6.11. *$H/M \cong U_n(q)$ and $m = q^2$.*

Proof. If not $\mu = \lambda + 2$, so $\mathscr{B}(\Omega)$ is a symmetric block design. Further all lines have order $q+1$. Thus a result of Dembowski and Wager [8] implies $\mathscr{B}(\Omega)$ is $(n+1)$-dimensional projective space over $GF(q)$. As G is generated by the set of elations of $\mathscr{B}(\Omega)$ commuting with the symplectic polarity $\alpha \leftrightarrow \alpha^\perp$, $G \cong Sp_{n+2}(q)$.

The case $n = 2$ must be treated differently since in this case the existence of D-subgroups isomorphic to $U_3(q)$ are not assured. The following lemma treats this special case.

LEMMA 6.12. $n \geqq 3$.

Proof. Assume $n = 2$. Let $\beta, \delta \in \Gamma$, and set $X = L_{\beta\delta}$. We first determine the fixed point sets of elements of L.

If $x \in \langle\beta\rangle^{\#}$ then $F(x) = \beta^{\perp}$. If $x \in X - Z(L)$, then $F(x) = \{\beta, \delta\} \cup \alpha^*\gamma$. For if $\sigma \in F(x)$ is not as claimed, then by 3.3, $\sigma \in A_\alpha$. x normalizes $\langle\delta, \alpha\rangle \cong SL_2(q)$ and centralizes α, so x centralizes σ. Thus a similar argument on $\langle\sigma, \beta\rangle$ and $\langle\sigma, \delta\rangle$ shows $\sigma \in D_\beta \cap D_\delta = \alpha^*\gamma$. If $\langle x\rangle = Z(L)$ then $F(x) = \Gamma \cup (\alpha^*\gamma)$. For arguing as above $F(x) = C_\Omega(x)$, and minimality of G implies $\langle C_\Omega(x)\rangle / Z(\langle C_\Omega(x)\rangle) \cong L_2(q) \times L_2(q)$; that is $C_\Omega(x) = \Gamma \cup (\alpha^*\gamma)$. Finally let $x \in L$ act fixed point free on Γ. As above $F(x) = C_\Omega(x)$ and as $D_\alpha \cap C_\Omega(x)$ is empty, $\langle C_\Omega(x)\rangle = Y_{F(x)} \cong SL_2(q)$ or $U_3(q)$. And if $Y \cong U_3(q)$ then Y is doubly transitive so $x \in \langle D_\alpha \cap D_\sigma\rangle$ for $\sigma \in F(x) - \{\alpha\}$. Thus x is in q^2 distinct conjugate of L in H. However, with 3.3, $C_M(x) = \langle\alpha\rangle$, so there are $m^2 q(q-1)/2$ conjugates of $\langle x\rangle$ in H. On the other hand there are m^2 conjugates of L, each containing $q(q-1)/2$ conjugates of $\langle x\rangle$, so $\langle x\rangle$ is in a unique conjugate of L. So $F(x) = \alpha^*\gamma$.

Let $\bar{G} = U_4(q)$, let $\bar{D}$ be the class of subgroups generated by transvections in $\bar{G}$, let $\bar{\alpha}$ consists of the members of $\bar{D}$ whose center is a given singular point of the associated projective space, and let $\bar{\Omega} = \bar{\alpha}^{\bar{G}}$. Let $\bar{\gamma} \in A_{\bar{\alpha}}$ and $\bar{L} = \langle D_{\bar{\alpha}} \cap D_{\bar{\gamma}}\rangle$. The discussion above implies $\bar{L}^{\bar{\Omega}}$ is permutation isomorphic to L^{Ω}.

Lemma 6.3 implies that every σ in $\Omega - (\alpha^*\beta)$ appears in a unique D_{β_1}, $\beta_1 \in \alpha^*\beta$. Set $K = L_\beta$, and let $t \in L$ have cycle (β, δ). Let $\sum_{i=0}^{q+2} \beta_i^K$ be a partition of $\alpha^*\beta$ with $\beta_0 = \alpha$ and $\beta_1 = \beta$. Set $\Lambda_i = (\beta_i^{\perp} - (\alpha^*\beta)) \cup \{\beta_i\}$, and $\Lambda = U\Lambda_i$. Then L maps the edge set of $\mathscr{D}(\Lambda)$ onto the edge set of $\mathscr{D}(\Omega)$, except for edges in $\mathscr{D}(\alpha^*\beta)$.

Let T be permutation isomorphism of L and $\bar{L}$, and let $\bar{\beta} = \beta T$. Let $\bar{\beta}_i^{KT}$ be orbits of KT on $\bar{\alpha}^*\bar{\beta}$ and define $\bar{\Lambda}$ as above with respect to these $\bar{\beta}_i$. There exists an isomorphism S of $\mathscr{D}(\Lambda)$ and $\mathscr{D}(\bar{\Lambda})$ such that S restricted to $\mathscr{D}(\Lambda_i)$ commutes with T restricted to $N_L(\Lambda_i)$ and $N_{\bar{L}}(\sigma S) = (N_L(\sigma))T$ for $\sigma \in \Lambda$. For $\sigma \in \Lambda_i$ there exists $\bar{\sigma} \in \bar{\Lambda}_i$ with $N_{\bar{L}}(\bar{\sigma}) = (N_L(\bar{\sigma}))T$ from the discussion above, so S can be defined in the obvious manner. So we can apply 2.6 to show $\mathscr{D}(\Omega) \cong \mathscr{D}(\bar{\Omega})$ and thus $G \cong \bar{G}$, if we show condition (ii) of 2.6 is satisfied.

Clearly (ii) holds on Λ_0. Suppose $\sigma, \sigma^x \in \Lambda_1, x \in L$. Claim $\sigma^x = \sigma^y$ for $y \in K$. As $L = K \cup KtK$ we can assume $x = t$. Thus $\sigma^x \in D_\beta \cap D_\delta = \alpha^*\gamma$, so $\sigma = \sigma^t$ is fixed by t. But $K = N_L(\Lambda_1)$, so (ii) holds here. Suppose $\sigma, \sigma^x \in \Lambda_i$, $i \geqq 2$. We consider the case $|\sigma^L| = q^2 - 1$; the case $|\sigma^L| = q(q^2-1)$ is analogous. Now $\langle\beta\rangle = N_L(\Lambda_i)$ and $q^2 = |\Lambda_i \cap \bigcup_{\alpha^*\gamma} D_\omega|$ in q orbits of length q under $\langle\beta\rangle$. These are the points in orbits of length $q^2 - 1$ under L. Let θ be the set of edges (β_i^y, ω) with $y \in L$

and $|\omega^L| = q^2 - 1$. Let N be the number of orbits of L on θ. Then $q(q^2-1)N = |(\beta_i, \sigma)^L|N = |\theta| = |\beta_i^L|q^2 = (q^2-1)q^2$, so $N = q$. Thus $(\beta_i, \sigma^x) = (\beta_i, \omega^y)$ for some $\omega \in \Lambda_i$, $y \in \langle\beta\rangle$. That is condition (ii) holds on Λ_i.

This completes the proof of 6.12.

A *unitary* (α, β, γ) in Ω is a triple with $\beta \in A_\alpha$ and

$$\gamma \in \bigcap_{\delta \in \alpha^*\beta} A_\delta .$$

LEMMA 6.13. *If (α, β, γ) is a unitary triple then $\langle\alpha, \beta, \gamma\rangle/Z(\langle\alpha, \beta, \gamma\rangle) \cong U_3(q)$.*

Proof. We can choose a unitary triple $(\beta_1, \beta_2, \beta_3)$ in H. Set $X = \langle\beta_1, \beta_2, \beta_3\rangle$. As $H/M \cong U_n(q)$, $X/Z(X) \cong U_3(q)$. If $n = 3$ we can count the number of unitary triples and the number of such triples centralizing some $\alpha \in \Omega$. These two numbers are equal. So assume $n \geqq 4$, and let $(\sigma_1, \sigma_2, \sigma_3)$ be a unitary triple. Choose $\beta \in D_{\sigma_1} \cap D_{\sigma_2}$. If $\sigma_3 \in D_\sigma$ set $\beta = \alpha$. If not let $\alpha^*\beta$ be a singular line in $D_{\sigma_1} \cap D_{\sigma_2}$. By 6.3, we can assume $\alpha \in D_{\sigma_3}$. Thus as above we are through.

Let (α, γ, δ) be a unitary triple in D_β. Set $J = \langle D_\delta \cap \Gamma\rangle$.

LEMMA 6.14. *$J/Z(J) \cong U_{n-1}(q)$.*

Proof. If $n = 3$, $\langle\alpha, \gamma, \delta\rangle = D_\beta \cap D_\sigma$ for suitable $\sigma \in A_\beta$ and $J = \langle\beta^*\sigma\rangle$. If $n = 4$, J has width one and a counting argument shows $|J \cap \Omega| = q^3 + 1$. Thus by minimality of G, $J/Z(J) \cong U_3(q)$. Finally if $n > 4$, then arguing as in 6.3, J is transitive on $J \cap D$ and $\langle D_\beta \cap J\rangle/O_\infty(\langle D_\beta\rangle) \cong U_{n-3}(q)$, so minimality of G implies the desired result.

LEMMA 6.15. *Let $\theta = \Gamma \cup \delta^L$ and $K = \langle\theta\rangle$. Then $K \cong SU_{n+1}(q)$ and $\Omega = \theta \cup \alpha^K$.*

Proof. Claim $\theta^\theta = \theta$. Clearly L normalizes θ, so it suffices to show δ normalizes θ. Let $\sigma \in \Gamma \cap A_\delta$. Then $\langle\sigma, \delta\rangle \cong SL_2(q)$, so $\sigma^\delta = \delta^\sigma \subseteqq \theta$. Thus $\Gamma^\delta \subseteqq \theta$. Using the fact that 6.15 is true in $U_{n+1}(q)$, one can check that

$$L = J(\bigcup_{\mathscr{L}} \langle\sigma_1{}^*\sigma_2\rangle)$$

where $\mathscr{L}$ is the set of lines in $L - J$. Thus it suffices to show $X \cap \Omega \subseteqq \theta$ when $X = \langle\sigma_1, \sigma_2, \delta\rangle$. But if $(\sigma_1, \sigma_2, \delta)$ is unitary, 6.13 implies $X \cap \Omega = \sigma_1{}^*\sigma_2 \cup \delta^{\langle\sigma_1{}^*\sigma_2\rangle} \subseteqq \theta$ and if $(\sigma_1, \delta, \sigma_2)$ is a triangle then $X/O_p(X) \cong SL_2(q)$ and 3.3 yields the same equality.

So $\theta^\theta = \theta$. $\alpha \notin \theta$, so $K \neq G$. $Y = \langle D_\beta \cap \theta\rangle = \langle D_\beta \cap \Gamma, \delta\rangle$, so

$Y/O_\infty(Y) \cong U_{n-1}(q)$. $[L, \alpha] = 1$ and $\delta \in A_\alpha$, so $\Gamma = D_\alpha \cap \theta$. Arguing as above $\theta \cup \alpha^K$ is self normalizing, so $\Omega = \theta \cup \alpha^K$.

Let $Z = Z(K)$. Z fixes θ pointwise and $K \leqq C_G(Z)$ is transitive on $\Omega - \theta$, so Z does not fix α. $|SU_{n+1}(q)|/|SU_n(q)| = |\alpha^K| = |K: N_K(\alpha)|$ and $LZ/Z \cong SU_n(q)$, so $|Z| = (n + 1, q)$. Considering the covering group of $U_{n+1}(q)$ we get $K \cong SU_{n+1}(q)$.

Put K and D_δ in the roles of H and Λ in 2.6. Then 6.15 and 5.4 together with 2.6 imply $G \cong U_{n+2}(q)$.

This completes the proof of the main theorem.

REFERENCES

1. M. Aschbacher, *Doubly transitive groups in which the stabilizer of two points is abelian*, J. Algebra. **18** (1971), 114-136.
2. ———, *On doubly transitive permutation groups of degree* $n \equiv 2 \bmod 4$, Illinois J. Math., **16** (1972), 276-279.
3. ———, *Finite groups generated by odd transpositions*, (to appear).
4. M. Aschbacher and M. Hall, Jr., *Groups generated by a class of elements of order* 3, (to appear, J. Algebra).
5. H. Bender, *Endliche zweifach transitive Permutationsgruppen, deren Involutionen keine Fixpunkte haben*, Math. Zeitschr., **104** (1968), 175-204.
6. ———, *Transitive Gruppen gerader Ordnung in denen jede Involution genau eineu Punkt feslast*, J. Algebra, **17** (1971), 527-554.
7. R. Brauer and C. Nesbitt, *On the modular characters of groups*, Ann. of Math., **42** (1941), 556-590.
8 P. Dembowski and A. Wagner, *Some characterizations of finite projective space, Arch.* Math., **11** (1960), 465-469.
9. G. Glauberman, *Central elements in core-free groups*, J. Algebra, **4** (1966), 403-420.
10. D. Higman, *Finite permutation groups of rank* 3, Math. Zeitscher., **86** (1964), 145-156.
11. W. Kantor and G. Seitz, *Finite groups having a split BN-pair of rank* 1, (to appear).
12. ———, *Some results on 2-transitive groups*, Inventiones Math., **13** (1971), 125-142.
13. J. Walter, *The characterization of groups with abelian Sylow 2-subgroups*, Ann. Math., **89** (1969), 405-514.

Received February 25, 1972 and in revised form February 26, 1973.

CALIFORNIA INSTITUTE OF TECHNOLOGY