This is to certify that the

dissertation entitled

Core-free Maximal Subgroups of Locally Finite Groups

presented by

Neil Henry Flowers

has been accepted towards fulfillment of the requirements for

Ph.D. degree in Mathematics

Major professor

Date 7/16/96

CORE-FREE MAXIMAL SUBGROUPS OF LOCALLY FINITE GROUPS

By

Neil Henry Flowers

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the Degree of

DOCTOR OF PHILOSOPHY

Department of Mathematics

1996

ABSTRACT

CORE-FREE MAXIMAL SUBGROUPS OF LOCALLY FINITE GROUPS

By

Neil Henry Flowers

In this dissertation we determine the structure of the centers of certain maximal subgroups in both finite groups and locally finite simple groups. In Theorem 1.1 we show that in a finite group G the center $Z(M)$ of a solvable core-free maximal subgroup M is cyclic modulo $O_2(Z(M))O_3(Z(M))$. In Theorem 3.1 we show that, for certain primes p, a nonfinitary locally finite simple group cannot contain a subgroup of type (p,p) in which all nontrivial elements have the same centralizer. As a result we are able to show that the center of a maximal subgroup of a nonfinitary locally finite simple group is locally cyclic modulo one of its Sylow subgroups.

DEDICATION

To my mother Nona and my wonderful daughter Felicia

ACKNOWLEDGEMENTS

I would like to thank my Advisor, Ulrich Meierfrankenfeld, for working closely with me through out the completion of this dissertation. It is from him that I've learned many advanced Group Theory techniques and I feel I've grown tremendously as a result of our interaction. I cannot think of any other way one could have been a better advisor and I am extremely fortunate to have had the oppourtunity to have worked with him.

I would also like to thank Richard Phillips and Susan Schuur for entertaining my various questions concerning my dissertation and other aspects of my personal life.

Finally, I would like to thank Bernd Stellmacher for helping me in the early stages of my dissertation and for being a great Group Theory teacher. It was through taking a class from him that I initially became attracted to the subject.

Contents

Introduction

A common theme throughout Group Theory has been the interplay between a group and its maximal subgroups. Of particular interest has been the phenomena in which properties of the maximal subgroup of a group impose a certain structure on the group itself. In [11], for example, John G. Thompson showed that any finite group which has a nilpotent, maximal subgroup of odd order must be solvable. Its the influence that a maximal subgroup can have on the whole group that makes the study of the structure of maximal subgroups worth while.

A core-free maximal subgroup of a group G is a maximal subgroup in which the intersection of all its conjugates is trivial, that is, $\mathrm{Core}_G(M) = \bigcap_{g \in G} M^g = 1$. In Chapters 1 and 2, we explore the centers of such subgroups and show that in a finite group any core-free maximal subgroup which is solvable has a cyclic center modulo $O_2(Z(M))O_3(Z(M))$.

In [6] Liebeck and Saxl proved that any core-free maximal subgroup of a finite group must have cyclic center. However their proof of this theorem relied on the classification of finite simple groups, a reasonably powerful tool. Although Theorem 1.1 is weaker than this result, the proof of Theorem 1.1 does not rely on the classification of finite simple groups. Rather it depends on The Amalgam Method, a method developed by Daniel Goldschmidt [2] and Bernd Stellmacher [9]. This method is a way of analyzing properties of a group through its action on the coset graphs of some of its subgroups.

After the completion of the classification of finite simple groups a new interest arose in the structure of locally finite simple groups. In [7] Ulrich Meierfrankenfeld showed that a locally finite simple group must be one of three types, a finitary group, a group that is covered by a system of finite subgroups each of which having alternating quotients, or a group that is covered by a system of finite subgroups each of which having quotients isomorphic to projective special linear groups defined over finite fields of prime characteristic. Using this classification, in Chapter 3 we explore the structure of the centers $Z(M)$ of maximal subgroups M of nonfinitary locally finite simple groups G. Indeed, we prove that, for certain primes p, G does not contain a subgroup Z of type (p,p) in which every nontrivial element of Z has the same centralizer in G. Therefore, as a consequence, we show the center $Z(M)$ of M, modulo one of its Sylow-subgroups, is locally cyclic.

Chapter 1

Core-free maximal subgroups of finite groups

In this section we will start a proof of Theorem 1.1 (below) which does not depend on the classification of finite simple groups. The proof of Theorem 1.1 is primarily an application of the Amalgam Method.

Theorem 1.1 *Let G be a finite group and M be a core-free maximal subgroup of G. Suppose further that M is solvable and p a prime with $p \geq 5$. Then $O_p(Z(M))$ is cyclic.*

Let (G, M, p) be a minimal counter example to Theorem 1.1. Then, since $O_p(Z(M))$ is noncyclic and abelian, there exists $Z \leq O_p(Z(M))$ of type (p, p).

Lemma 1.2 *(a) If $N \trianglelefteq G$ and $N \leq M$, then $N = 1$.*

(b) For any $C \leq Z(M)$ and $1 \neq c \in C$, $C_G(c) = C_G(C) = M$.

(c) If $Q \leq G$ is a p'-group and $Z \leq N_G(Q)$, then $[Z, Q] = 1$ and $Q \leq M$.

Proof: For (a), since $N \trianglelefteq G$ and $N \leq M$, we have

$$N \leq \bigcap_{g \in G} M^g = Core_G(M) = 1$$

and therefore $N = 1$.

Now $C \leq Z(M)$ implies $M \leq C_G(c) \leq G$. Hence, by the maximality of M in G, we get $M = C_G(c)$ or $C_G(c) = G$. If $G = C_G(c)$, then $\langle c \rangle \trianglelefteq G$ and $\langle c \rangle \leq M$. Thus, by (a), we get $\langle c \rangle = 1$, a contradiction. Therefore $M = C_G(c)$. But then, since $C \leq Z(M)$, we get $C_G(C) \leq C_G(c) = M \leq C_G(C)$. Thus $M = C_G(c) = C_G(C)$ and we have (b). Finally, for (c), since Z is a noncyclic abelian p-group acting on a p'-group Q, by [3, 6.2.4] we have

$$Q = \langle C_Q(z) | 1 \neq z \in Z \rangle \tag{1}$$

Now by (b), $C_Q(z) \leq C_G(z) = M$ for each $1 \neq z \in Z$. Thus, (1) implies $Q \leq M$. Since $Z \leq Z(M)$, we get $[Z, Q] = 1$.

□

Lemma 1.3 *Suppose T is a finite solvable group and $P \leq T$ is a p-subgroup. Then $O_{p'}(N_T(P)) \leq O_{p'}(T)$.*

Proof First assume $O_{p'}(T) = 1$. Then we want to show $O_{p'}(N_T(P)) = 1$. Let $A = O_{p'}(N_T(P))$ and $B = O_p(T)$. Since A and P are normal subgroups of $N_T(P)$ and $(|A|, |P|) = 1$, we have $[A, P] \leq A \cap P = 1$. Also, since $B \trianglelefteq T$, $A \times P$ acts on B. Further $[A, C_B(P)] \leq A \cap B = 1$, and so by [3, 5.3.4] $[A, B] = 1$. Thus $A \leq C_T(B)$. If $A \neq 1$, then $C_T(B)$ is not a p-group and so $B < C_T(B)B \trianglelefteq T$. Let $\overline{T} = T/B$ and $\overline{C_T(B)}$ be the image of $C_T(B)$ in $\overline{T}$. Then we can pick $\overline{N} = N/B \leq \overline{T}$ minimal such that $\overline{N} \trianglelefteq \overline{T}$ and $\overline{N} \leq \overline{C_T(B)}$. Now T is solvable implies $\overline{T}$ is solvable and so $\overline{N}$ is a elementary abelian q-group. If $q = p$, then N is a p-group. But, since $N \trianglelefteq T$, we get $N \leq O_p(T) = B$ and hence $\overline{N} = 1$, a contradiction. Therefore $q \neq p$. Let $Q \in \mathrm{Syl}_q(N)$. Since $\overline{N}$ is a q-group we have $\overline{Q} = \overline{N}$ and therefore $N = QB$. But $Q \leq BC_T(B)$, and so

$$\frac{QC_T(B)}{C_T(B)} \leq \frac{BC_T(B)}{C_T(B)} \cong \frac{B}{C_T(B) \cap B} \text{ is a } p\text{-group.}$$

Thus $QC_T(B)/C_T(B) = 1$ and so $Q \leq C_T(B)$. But then $N = Q \times B$ and Q char$N \trianglelefteq T$. Therefore Q is a normal p'-subgroup T and hence $Q \leq O_{p'}(T) = 1$. But then we get $N = QB = B$ and $\overline{N} = 1$, a contradiction. Thus $A = O_{p'}(N_T(P)) = 1$.

Now if $O_{p'}(T) \neq 1$, let $\overline{T} = T/O_{p'}(T)$ and $\overline{P}$ be the image of P in $\overline{T}$. Then $O_{p'}(\overline{T}) = 1$ and so by the above argument applied to $\overline{T}$ and $\overline{P}$ we get $O_{p'}(N_{\overline{T}}(\overline{P})) = 1$. Next we claim that $N_{\overline{T}}(\overline{P}) = \overline{N_T(P)}$. Clearly $\overline{N_T(P)} \leq N_{\overline{T}}(\overline{P})$. Let $\bar{t} \in N_{\overline{T}}(\overline{P})$. Then $\overline{P}^{\bar{t}} = \overline{P}$ implies $(PO_{p'}(T))^t = P^t O_{p'}(T) = PO_{p'}(T)$. Therefore P and P^t are p-Sylow subgroups of $PO_{p'}(T)$. Therefore there exists $x \in O_{p'}(T)$ with $P^{tx} = P$. But then $tx \in N_T(P)$ and therefore $\bar{t} \in \overline{N_T(P)}$. Thus $N_{\overline{T}}(\overline{P}) \leq \overline{N_T(P)}$ and the claim holds. Now we have

$$\overline{O_{p'}(N_T(P))} \leq O_{p'}(\overline{N_T(P)}) = O_{p'}(N_{\overline{T}}(\overline{P})) = 1$$

and so $O_{p'}(N_T(P)) \leq O_{p'}(T)$ and the lemma is proved.

$\square$

Lemma 1.4 *(a)* $O_{p'}(G)O_p(G) = 1$, *in particular* $F(G) = Z(G) = 1$.

(b) If $\Omega_1(Z(M)) \leq H < G$, $H \cap M$ *is maximal in* H, *and* $Q = Core_H(H \cap M)$, *then* $\Omega_1(Z(M)) \leq \Omega_1(Z(O_p(Q)))$.

(c) There exists $g \in G$ *with* $\Omega_1(Z(M)) \leq M^g$ *and* $g \notin M$.

(d) $O_{p'}(M) = 1$.

Proof: Clearly, since $Z(G) \leq F(G) \leq O_{p'}(G)O_p(G)$, $O_{p'}(G)O_p(G) = 1$ implies $F(G) = Z(G) = 1$. Now $O_{p'}(G) \trianglelefteq G$ implies Z normalizes the p'-group $O_{p'}(G)$ and so, by Lemma 1.2 (c), we have $[Z, O_{p'}(G)] = 1$. But then, $O_{p'}(G) \leq C_G(Z) = M$, by Lemma 1.2 (b). Therefore, since $O_{p'}(G) \trianglelefteq G$, by Lemma 1.2 (a), we have $O_{p'}(G) = 1$. Next suppose $1 \neq O_p(G)$. Then, since $O_p(G)$ is a normal p-subgroup of G, we have $1 \neq C = C_G(O_p(G)) \trianglelefteq G$. Therefore, by Lemma 1.2 (a) and the maximality of M in G, $C \not\leq M$ and $G = CM$. But then $M \cap O_p(G) \trianglelefteq CM = G$ and so, by Lemma 1.2 (a), $M \cap O_p(G) = 1$. Now Z acts on $O_p(G)$ and for each $1 \neq z \in Z$, $C_{O_p(G)}(z) \leq C_G(z) \cap O_p(G) = M \cap O_p(G) = 1$. Thus, $C_{O_p(G)}(z) = 1$ for each $1 \neq z \in Z$ and Z acts fixed-point freely on $O_p(G)$. But, since Z and $O_p(G)$ are p-groups, this is a contradiction to [3, 2.6.3]. Therefore, $O_{p'}(G)O_p(G) = 1$ and we have (a).

For (b), suppose $Z \cap Q = 1$. Let $\overline{H} = H/Q$ and $\overline{H \cap M}$ be the image of $H \cap M$ in $\overline{H}$. Then $\overline{H \cap M}$ is a core-free maximal subgroup of $\overline{H}$. Moreover, M is solvable implies $\overline{H \cap M}$ is solvable. Thus, by the minimality of G, $O_p(Z(\overline{H \cap M}))$ is cyclic. But $Z \cap Q = 1$ implies $\overline{Z} \cong Z$ and $\overline{Z} \leq O_p(Z(\overline{H \cap M}))$ is of type (p,p), yeilding a contradiction. And so we may assume $Z \cap Q \neq 1$.

Since $Q \leq M$, $[\Omega_1(Z(M)), Q] = 1$ and so $\Omega_1(Z(M)) \leq C_H(Q)$. Now, by Lemma 1.2 (b), we have $C_H(Q) \leq C_G(Z \cap Q) = C_G(Z) = M$ and therefore $C_H(Q) \leq H \cap M$. But then $C_H(Q) \trianglelefteq H$ implies $C_H(Q) \leq \mathrm{Core}_H(H \cap M) = Q$. Thus, $\Omega_1(Z(M)) \leq C_H(Q) \leq Q$. Now, since Q centralizes $\Omega_1(Z(M))$, we have $\Omega_1(Z(M)) \leq \Omega_1(Z(O_p(Q))$.

For (c), if $\langle \Omega_1(Z(M)), \Omega_1(Z(M))^g \rangle = G$ for each $g \in G \setminus M$, then $M \cap M^g \trianglelefteq \langle \Omega_1(Z(M)), \Omega_1(Z(M))^g \rangle = G$ for each $g \in G \setminus M$. Thus, by Lemma 1.2 (a), $M \cap M^g = 1$ for each $g \in G \setminus M$. Now Frobenius' theorem [3, 2.76] implies $G = NM$, where $N = (G \setminus \bigcup_{g \in G} M^g) \cup \{1\} \trianglelefteq G$ and $(|N|, |M|) = 1$. But, since $p \in \pi(|M|)$, N is a p'-

group. Hence, by Lemma 1.4 (a), $N \leq O_{p'}(G)O_p(G) = 1$ and we get $G = MN = M$, a contradiction to the maximality of M.

So there exists $g \in G \setminus M$ with $\langle \Omega_1(Z(M)), \Omega_1(Z(M))^g \rangle \neq G$. We may assume $\langle \Omega_1(Z(M)), \Omega_1(Z(M))^g \rangle \not\leq M$, otherwise, $\Omega_1(Z(M)) \leq M^{g^{-1}}$ and we are done. Thus, we can choose $H < G$ minimal such that $\Omega_1(Z(M)) \leq H$ and $H \not\leq M$. Then $H \cap M$ is a maximal subgroup of H. For if $H \cap M \leq H_0 \leq H$, then $\Omega_1(Z(M)) \leq H_0 \leq H$. Thus, by the minimalty of H, $H_0 \leq H \cap M$ or $H_0 = H$. Now by (b), $\Omega_1(Z(M)) \leq \mathrm{Core}_H(H \cap M) \leq \bigcap_{h \in H} M^h$. Since $H \not\leq M$, pick a $h \in H \setminus M$. Then $\Omega_1(Z(M)) \leq M^h$ and we are done.

Next we want to show $O_{p'}(M) = 1$. By (c), there exists $g \in G \setminus M$ with $Z \leq \Omega_1(Z(M)) \leq M^g$. Then $[Z, Z^g] = 1$ and so $Z^g \leq C_G(Z) = M$, again by Lemma 1.2 (b). Now Z^g acts on the p'-group $O_{p'}(M)$ and so, by Lemma 1.2 (c), $[Z^g, O_{p'}(M)] = 1$ and $O_{p'}(M) \leq M^g$. Hence, $O_{p'}(M) \trianglelefteq M \cap M^g$, and so $O_{p'}(M) \leq O_{p'}(M \cap M^g)$. But $O_{p'}(M \cap M^g) = O_{p'}(N_G(Z) \cap M^g) = O_{p'}(N_{M^g}(Z)) \leq O_{p'}(M^g)$ by Lemma 1.3. Thus, $O_{p'}(M) \leq O_{p'}(M^g)$. Now by the symmetry of this argument, we get $O_{p'}(M) = O_{p'}(M^g)$. And so if $O_{p'}(M) \neq 1$, then

$$M = N_G(O_{p'}(M)) = N_G(O_{p'}(M^g)) = M^g$$

Thus, $M = M^g$ and $g \in N_G(M) = M$, a contradiction to the choice of g.

□

Lemma 1.5 *Let T be a finite group, $P \in Syl_p(T)$, and $H \leq Z(P)$. Then,*

$$O_p(T/C_T(\langle H^T \rangle)) = 1$$

.

Proof Let $V = \langle H^T \rangle$, $\overline{T} = T/C_T(V)$ and $\overline{K} = K/C_T(V) = O_p(\overline{T})$. Then $\overline{K} \trianglelefteq \overline{T}$ implies $K \trianglelefteq T$. Now $P \in \mathrm{Syl}_p(T)$ so $T = N_T(P \cap K)K$ by the Frattini Argument. Since, $\overline{K}$ is a p-group and $K \cap P \in \mathrm{Syl}_p(K)$, we have $\overline{K} = \overline{K \cap P}$ and so $K = (K \cap P)C_T(V)$. Thus, $T = N_T(K \cap P)C_T(V)$. By assumption $H \leq Z(P)$, and so $V = \langle H^T \rangle = \langle H^{N_T(K \cap P)} \rangle \leq C_T(K \cap P)$ Thus, $K \cap P \leq C_T(V)$ and so $K = C_T(V)$. But then, $O_p(\overline{T}) = \overline{K} = 1$.

□

Lemma 1.6 *Suppose A is a elementary abelian p-group which acts on a nilpotent p'-group T. Then*

$$[T, A] = \langle [C_T(B), A] | B \leq_p A \rangle \tag{1}$$

and if in addition A is noncyclic,

$$[T, A] = \langle [C_T(a), A] | 1 \neq a \in A \rangle \tag{2}$$

Proof Since A acts on T, A also acts on $[T, A]$. Since A is an elementary p-group and $[T, A]$ is a p'-group, we have

$$[T, A] = \langle [C_{[T,A]}(B) | B \leq_p A \rangle.$$

Let $C = \langle [C_T(B), A] | B \leq_p A \rangle$. Since A is a p-group and T is a p'-group, by [3, 5.3.6], we have $[T, A] = [T, A, A]$. We claim $\langle C^{[T,A]} \rangle = [T, A]$. First, by the definition of C, we have $C \leq [T, A]$ and so $\langle C^{[T,A]} \rangle \leq [T, A]$. On the other hand, by the commutator laws [3, 2.2.1], (1) implies $[T,A] = [T,A,A] \leq \langle C^{[T,A]}\rangle$. Thus $[T,A] = \langle C^{[T,A]}\rangle$ and the claim holds.

Now suppose $C < [T,A]$ and let $C \leq D \leq [T,A]$, where D is a maximal subgroup of $[T,A]$. Then, since T is nilpotent, $[T,A]$ is nilpotent and so $D \trianglelefteq [T,A]$. But then we get $[T,A] = \langle C^{[T,A]}\rangle \leq D$ and hence $[T,A] = D$. This is a contradiction to the maximality of D. Therefore $C = [T,A]$ and the first statement of the lemma is proved.

If A is noncyclic, then $[T,A] = \langle C_{[T,A]}(a) | 1 \neq a \in A\rangle$ by [3, 6.2.4]. Now the second statement in the lemma follows by the same argument used above applied to $C = \langle C_{[T,A]}(a), A] | 1 \neq a \in A\rangle$.

□

Lemma 1.7 *Let T be a finite group, $H \leq T$ be solvable, and $V \trianglelefteq H$ be an abelian p-group with $O_p(H/C_H(V)) = 1$. Suppose there exists a noncyclic elementary abelian p-group $P \leq T$ such that $C_T(P) = C_T(x)$ for each $1 \neq x \in P$. Then,*

$$H_0 = \langle P^t | P^t \leq H\rangle \leq C_H(V). \tag{1}$$

Proof: Suppose not. Then there exists $t \in T$ with $P^t \leq H$ and $P^t \not\leq C_H(V)$. Let $E = P^t$ and $\overline{H} = H/C_H(V)$. Then, $\overline{E} \neq 1$ and $O_p(\overline{H}) = 1$. Now $E \cap C_H(V) = 1$, otherwise there exists $1 \neq e \in E \cap C_H(V)$ and $V \leq C_T(e) = C_T(E)$ would imply $\overline{E} = 1$. Thus, $\overline{E} \cong E$ is a noncyclic abelian p-group. Since $O_p(\overline{H}) = 1$, $F(\overline{H})$ is a p'-group. Hence, by [3, 6.2.4] applied to $\overline{E}$ and $F(\overline{H})$, we get $F(\overline{H}) = \langle C_{F(\overline{H})}(\overline{e}) | 1 \neq \overline{e} \in \overline{E}\rangle$. But then, by Lemma 1.6, we have

$$[F(\overline{H}), \overline{E}] = \langle [C_{F(\overline{H})}(\overline{e}), \overline{E}] | 1 \neq \overline{e} \in \overline{E}\rangle \tag{2}$$

Let $W_{\overline{e}} = [C_{F(\overline{H})}(\overline{e}), \overline{E}]$ for each $\overline{e} \in \overline{E}$. Since, $C_V(\overline{e}) = C_V(e) \leq C_T(e) = C_T(E)$, we have $[C_V(\overline{e}), \overline{E}] = 1$ and so $[C_V(\overline{e}), \overline{E}, C_{F(\overline{H})}(\overline{e})] = 1$. Also, V $\overline{H}$-invariant implies $[C_V(\overline{e}), C_{F(\overline{H})}(\overline{e})] \leq C_V(\overline{e})$. Thus, $[C_{F(\overline{H})}(\overline{e}), C_V(\overline{e}), \overline{E}] = 1$. So by the Three Subgroup Lemma we get $[W_{\overline{e}}, C_V(\overline{e})] = 1$. Now the p'-group $W_{\overline{e}}$ acts faithfully on the abelian p-group V to give $V = C_V(W_{\overline{e}}) \times [V, W_{\overline{e}}]$. But, $[W_{\overline{e}}, C_V(\overline{e})] = 1$ implies $C_{[V,W_{\overline{e}}]}(\overline{e}) = C_V(\overline{e}) \cap [V, W_{\overline{e}}] \leq C_V(W_{\overline{e}}) \cap [V, W_{\overline{e}}] = 1$. Thus, $C_{[V,W_{\overline{e}}]}(\overline{e}) = 1$. Since both $\langle \overline{e} \rangle$ and $[V, W_{\overline{e}}]$ are p-groups, we conclude $[V, W_{\overline{e}}] = 1$. Thus, as $\overline{H}$ acts faithfully on V, we get $W_{\overline{e}} = 1$. Now, since $\overline{e} \in \overline{E}$ was arbitrary, by (2) we get $[\overline{E}, F(\overline{H})] = 1$. But H is solvable implies $\overline{H}$ is solvable and so, by [3, 6.1.3], $\overline{E} \leq C_{\overline{H}}(F(\overline{H})) \leq F(\overline{H})$. This is a contradiction, since $1 \neq \overline{E}$ is a p-group and $F(\overline{H})$ is a p'-group.

□

Lemma 1.8 *M contains a Sylow p-subgroup of G.*

Proof: Suppose not. Let $S \in \mathrm{Syl}_p(M)$ and $T \in \mathrm{Syl}_p(G)$ with $S \leq T$, $S \neq T$. Then, since S and T are p-groups, there exists $x \in N_T(S) \setminus S$. Now $Z \leq Z(M)$ a p-group implies $Z \leq Z(S)$. Thus, since $x \in N_T(S)$, we have $Z^x \leq Z(S)$ and $[Z^x, O_p(M)] = 1$. Now M is solvable, so by [3, 6.1.3], we have $C_M(F(M)) \leq F(M)$. But $O_{p'}(M) = 1$, by Lemma 1.3 (d), and so we get $Z^x \leq C_M(O_p(M)) \leq O_p(M)$ and, consequently, $Z^x \leq Z(O_p(M))$.

Let $V = \langle (Z^x)^M \rangle$. Then V is a normal abelian p-subgroup of M. Moreover, by Lemma 1.5, $O_p(M/C_M(V)) = 1$. Thus, M, Z, and V satisfy the hypothesis of Lemma 1.5 to give $M_0 = \langle Z^g | Z^g \leq M \rangle \leq C_M(V)$. But then $M_0 \leq M \cap M^x$ and $M_0^x = \langle Z^g | Z^g \leq M^x \rangle \geq M_0$. Therefore $M_0^x = M_0$ and since $1 \neq M_0 \trianglelefteq M$, by Lemma 1.2 (a), we get

$$M = N_G(M_0) = N_G(M_0^x) = M^x$$

This means $x \in N_G(M) = M$ and therefore $x \in M \cap T = S$. This contradicts the choice of x.

$\square$

The following proposition follows quite easily from Thompson's work on quadratic pairs for $p \geq 5$, but we prefer to give an elementary proof.

Proposition 1.9 *Let $p \geq 5$ be a prime, T a finite group, V a finite dimensional $GF(p)T$-module, $P \in Syl_p(T)$, $P \leq H \leq T$, and $Q = \{t \in T | [V,t,t] = 0\}$. Suppose that*

(a) H is the unique maximal subgroup of T containing P,

(b) H is solvable,

(c) $Q \not\subseteq H$.

Then $C_V(H) = C_V(T)$.

Proof Clearly $C_V(T) \leq C_V(H)$, and so we only need to show $C_V(H) \leq C_V(T)$. The proof is by induction on $|T| \cdot \dim_{\mathrm{GF}(p)} V$. If $C_T(V) \neq 1$, let $\overline{T} = T/C_T(V)$, $\overline{Q} = \{\bar{t} \in \overline{T} | [V, \bar{t}, \bar{t}] = 0\}$, and $\overline{S}$, $\overline{H}$ be the images in $\overline{T}$ of S and H respectively. Then $\overline{P} \in \mathrm{Syl}_p(\overline{T})$, $\overline{H}$ is solvable, and V is a $GF(p)\overline{T}$-module. If $H \not\geq C_T(V)$, then $T = HC_T(V)$ by the maximality of H. Hence, $C_V(H) \leq C_T(V)$ and we are done. So we may assume that $C_T(V) \leq H$. Then hypothesis (a) and (c) imply that $\overline{H}$ is the unique maximal subgroup of $\overline{T}$ containing $\overline{S}$ and $\overline{Q} \not\subseteq \overline{H}$. Now by induction we get $C_V(H) = C_V(\overline{H}) \geq C_V(\overline{T}) = C_V(T)$ and we are done. Therefore we may assume that $C_T(V) = 1$ and V is a faithful T-module.

Let $U = \langle C_V(H)^T \rangle$. If $U = 0$ then we get $C_V(H) = 0 \leq C_V(T)$ as desired. Hence, we may assume $U \neq 0$. Suppose $U \neq V$. Then, since $Q \subseteq Q_U = \{t \in T | [U, t, t] = 0\}$, $Q_U \not\leq H$ and so T, P, H, U, and Q_U fullfill the assumptions of the theorem. By induction we conclude that $C_U(H) = C_U(T)$. But then,

$$C_V(H) \leq C_U(H) = C_U(T) \leq C_V(T) = 1$$

and so $C_V(H) = 1$, again we are done. So we may assume that

$$V = \langle C_V(H)^T \rangle. \tag{1}$$

Then by (1) $\mathrm{Core}_T(H) \leq C_T(V) = 1$ and hence

$$\mathrm{Core}_T(H) = 1 \tag{2}$$

Let $X \leq H$ be a p-group maximal with respect to $X = \langle X \cap Q \rangle$ and $N_T(X) \not\leq H$ (we can make this choice since $N_T(1) \not\leq H$). Since X is a p-group there exists $h \in H$ with $X \leq P^h$. Now, since V is a p-group, by [3, 5.3.6] all elements of Q are p-elements. Therefore, since $P^h \in \mathrm{Syl}_p(T)$, each element of Q lies in a conjugate of P^h. Suppose $\langle P^h \cap Q \rangle \trianglelefteq T$. Then, since $\langle P^h \cap Q \rangle \leq H$, $\langle P^h \cap Q \rangle \leq \mathrm{Core}_T(H) = 1$ by (2). But then, since the set Q is T-invariant, $\langle (P^h)^T \cap Q \rangle = 1$. Thus, we get $Q \subseteq \langle (P^h)^T \cap Q \rangle = 1$, a contradiction to assumption (c). Therefore $\langle P^h \cap Q \rangle \ntrianglelefteq T$. Now we have $P \leq N_T(\langle P^h \cap Q \rangle)^{h^{-1}} \neq T$ and so by (a) $N_T(\langle P^h \cap Q \rangle) \leq H$. Hence, $X \neq \langle P^h \cap Q \rangle$.

Suppose $N_{P^h}(X) \cap Q \subseteq X$. Then, since X is a group and $X \cap Q \subseteq N_{P^h}(X) \cap Q$, we have

$$\langle N_{P^h}(X) \cap Q \rangle \leq X = \langle X \cap Q \rangle \leq \langle N_{P^h}(X) \cap Q \rangle$$

and, hence $X = \langle N_{P^h}(X) \cap Q \rangle$. Now, since Q is a T-invariant set, we have $N_{P^h}(N_{P^h}(X)) \leq N_{P^h}(X)$ and so $N_{P^h}(X) = N_{P^h}(N_{P^h}(X))$. But then P^h is a p-group and $N_{P^h}(X) \neq 1$ implies $P^h = N_{P^h}(X)$. Thus, we get $X = \langle N_{P^h}(X) \cap Q \rangle = \langle P^h \cap Q \rangle$, a contradiction. Therefore $N_{P^h}(X) \cap Q \not\subseteq X$.

Let $a \in N_{P^h}(X) \cap Q \setminus X$, $R = X\langle a \rangle$, and choose $K \leq N_T(X)$ minimal such that $K \not\leq H$ and $R \leq K$. Then clearly

$$K \cap H \text{ is the unique maximal subgroup of } K \text{ containing } R \tag{3}$$

Suppose $a \in O_p(K)$. Then, since $K \leq N_T(X)$ and X is a p-group, we have $X \leq O_p(K)$ and so $R = X\langle a \rangle \leq O_p(K)$. Now (3) implies $O_p(K) \leq H$ or $K = O_p(K)$. In the first case put $Y = \langle O_p(K) \cap Q \rangle$ and in the second put $Y = \langle K \cap H \cap Q \rangle$. Then in both cases $X < R \leq Y$ and Y is a p-subgroup of H. Moreover, we claim $K \leq N_T(Y)$ in both cases. In the first case its clear, since $O_p(K) \trianglelefteq K$. In the second, K is a p-group with $K \cap H < K$. Thus $R \leq K \cap H < N_K(K \cap H) \leq K$ and so $N_K(K \cap H) = K$, by (3). Hence, again $K \leq N_T(Y)$. Therefore, in either case, we get a contradiction to the maximal choice of X. Hence, $a \notin O_p(K)$.

Now by Baer's Theorem [3, 3.8.2] there exist conjugates x, y of a in K such that $D = \langle x, y \rangle$ is not a p-group. Since x and y are p-elements, there exists a composition factor W for D on V such that $[W, D] \neq 0$. Let $\overline{D} = D/C_D(W)$. If $[W, x] = 0$, then $\overline{D} = \langle \overline{y} \rangle$ is a p-group and acts faithfully and irreducibly on D. Hence, by [3,], $\overline{D} = 1$ and we get $[W, D] = [W, y] = 0$, a contradiction. Therefore $[W, x] \neq 0 \neq [W, y]$ and $\overline{D} = \langle \overline{x}, \overline{y} \rangle$. Moreover, $\overline{x}$ and $\overline{y}$ are p-elements with $[W, \overline{x}, \overline{x}] = [W, \overline{y}, \overline{y}] = 0$.

Since [3, 3.81] holds for the field GF(p) as well as its closure, by [3, 3.81] there exists $\overline{E} = E/C_D(W) \leq \overline{D}$ with $\overline{x} \in \overline{E}$ and $E/C_D(W) \cong \mathrm{SL}_2(p)$. Now x is conjugate to a in K and so there exists $k \in K$ with $a = x^k$. Hence $a \in E^k$. Moreover $E^k \not\leq H$, otherwise $E^k \leq H$ would imply E^k is solvable and therefore E would be solvable. But then we get $\overline{E} \cong \mathrm{SL}_2(p)$ is solvable, a contradiction as $p \geq 5$. Now we have $R \leq XE^k \leq K$ and $XE^k \not\leq H$, and so $K = XE^k$ by (3).

Suppose that $K = T$. Then $X \trianglelefteq T$ and so $X = 1$ by (2). Thus, $T = K = E^k$. Also as $X = 1$ and $K = T$, from (3) we conclude that

$$H \text{ is the unique maximal subgroup of } T \text{ containing } a \tag{4}$$

Let $\overline{N} = N/C_D(W) = Z(\overline{E})$. Then $1 \neq \overline{N} \trianglelefteq \overline{E}$ and so $1 \neq N \trianglelefteq E$. Thus $1 \neq N^k \trianglelefteq E^k = T$. Now $a \in N^k\langle a\rangle \leq T$ and so $N^k\langle a\rangle \leq H$ or $T = N^k\langle a\rangle$, by (4). If $N^k\langle a\rangle \leq H$ then by (2) we get $N^k \leq \mathrm{Core}_T(H) = 1$, a contradiction. On the other hand, if $T = N^k\langle a\rangle$ then $a \in P^h$ implies $T = N^kP^h$ and therefore $E^k = N^kP^h$. Thus

$$\frac{E^k}{N^k} \cong \frac{N^kP^h}{N^k} = \frac{P^h}{N^k \cap P^h} \text{ is a } p\text{-group.}$$

and consequently E/N and $\overline{E}/\overline{N}$ are p-groups. But then, since $\overline{N} = Z(\overline{E})$, $\overline{E}/Z(\overline{N})$ is a p-group and therefore $\overline{E} \cong \mathrm{SL}_2(p)$ is nilpotent, a contradiction.

Therefore $K \neq T$. Let $P_1 \in \mathrm{Syl}_p(K \cap H)$ with $R \leq P_1$ and $P_2 \in \mathrm{Syl}_p(K)$ with $P_1 \leq P_2$. If $P_2 \not\leq H$, then $K = P_2$ by the minimal choice of K. But then K is a p-group and $a \in O_p(K)$, a contradiction. Thus $P_2 \leq H$ and $P_1 = P_2$. Suppose $K \cap Q \subseteq K \cap H$. Then $x, y \in K \cap Q$ implies $x, y \in K \cap H$ and therefore $E \leq D = \langle x, y\rangle \leq K \cap H$. But then we get $E \leq H$, a contradiction. Hence $K \cap Q \not\subseteq K \cap H$. It follows that K, P_1, $K \cap H$, $K \cap Q$, and V fullfill the assumptions of the theorem. By induction we have

$C_V(K \cap H) \le C_V(K)$. But then $C_V(H) \le C_V(K \cap H) \le C_V(K)$ and $T = \langle H, K \rangle$ implies $C_V(H) \le C_V(T)$ and the lemma is proved.

□

Recall, in Lemma 1.8 we found $S \in \mathrm{Syl}_p(G)$ with $S \le M$. Next we show that there is another subgroup of G containing S.

Lemma 1.10 *There exists $H \le G$, $H \ne G$, with $S \le H$ and $H \not\le M$.*

Proof By Lemma 1.4 (c) we can choose a proper subgroup H of G with $\Omega_1(Z(M)) \le H$, $H \not\le M$ and, in this order,

(1) $|H \cap M|_p$ maximal

(2) $|H|_p$ minimal

(3) $|H|$ minimal

Since $\Omega_1(Z(M))$ is a p-group and $\Omega_1(Z(M)) \le H \cap M$ there exists $T \in \mathrm{Syl}_p(H \cap M)$ with $\Omega_1(Z(M)) \le T$. If $T \in \mathrm{Syl}_p(M)$, then $T = S^m$ for some $m \in M$. And so $S = T^{m^{-1}} \le H^{m^{-1}}$ and we are done. Therefore it is enough to show that $T \in \mathrm{Syl}_p(M)$. Suppose $T \notin \mathrm{Syl}_p(M)$. Then we claim $T \in \mathrm{Syl}_p(H)$. For if $N_H(T) \le M$, then $T \le N_H(T) \le H \cap M$. Hence $T \in \mathrm{Syl}_p(N_H(T))$ as $T \in \mathrm{Syl}_p(H \cap M)$. But then $T \in \mathrm{Syl}_p(H)$. On the other hand, if $N_H(T) \not\le M$, then, $N_G(T) \not\le M$, $\Omega_1(Z(M)) \le N_G(T)$, and $N_G(T) \ne G$. Moreover, since $T \notin \mathrm{Syl}_p(M)$, we have

$$|M \cap N_G(T)|_p = |N_M(T)|_p > |T| = |H \cap M|_p$$

a contradiction to the choice of H. Thus in any case $T \in \mathrm{Syl}_p(H)$. Clearly (1), (2), and (3) imply

$$H \cap M \text{ is the unique maximal subgroup of } H \text{ containing } T$$

and so, by Lemma 1.4 (b), $Z \leq \Omega_1(Z(M)) \leq \Omega_1(Z(O_p(Q))) \leq T$, where $Q = \mathrm{Core}_H(H \cap M)$, and $V = \langle Z^H \rangle$ is a elementary abelian p-subgroup of T.

Suppose $[J(T), V] \neq 1$. Then choose $A \in \mathcal{A}(T)$ such that $[V, A] \neq 1$ and $|V \cap A|$ is maximal. If $V \not\leq N_G(A)$, then by Thompson's Replacement Theorem [3, 8.25], there exists $A^* \in \mathcal{A}(T)$ with $V \cap A < V \cap A^*$ and $A^* \leq N_G(A)$. Then $[V, A^*] = 1$ by the choice of A and therefore VA^* is an abelian subgroup of T containing A^*. Hence, we have $A^* = VA^*$ as $A^* \in \mathcal{A}(T)$. But then $V \leq A^* \leq N_G(A)$, a contradiction. Therefore $V \leq N_G(A)$. Let $Q_0 = \{h \in H | [V, h, h] = 1\}$. Then $[V, A, A] \leq [A, A] = 1$ and $A \leq Q_0$. Now $Q_0 \not\subseteq H \cap M$, otherwise, $Q_0 \subseteq M$ and $[Q_0, Z] = 1$ as $Z \leq Z(M)$. But, since Q_0 is a H-invariant set, we get $[Q_0, V] = 1$ and $[A, V] = 1$, a contradiction to the choice of A. Thus $Q_0 \not\subseteq H \cap M$. Applying Proposition 1.9 to H, T, $H \cap M$, V, and Q_0, we get $C_V(H \cap M) = C_V(H)$. But then

$$Z \leq C_V(H \cap M) = C_V(H)$$

implies H centralizes Z and therefore $H \leq M$ by Lemma 1.2 (b). This is a contradiction to the choice of H. Therefore we have shown $[J(T), V] = 1$.

Now $T \in \mathrm{Syl}_p(H)$ implies $C_T(V) \in \mathrm{Syl}_p(C_H(V))$ and so by the Frattini Argument we have

$$H = N_H(C_T(V))C_H(V) \tag{1}$$

Since $C_T(V)$ is a p-group and $[J(T), V] = 1$, we have $J(T)$ char $\leq C_T(V)$ and consequently $N_H(C_T(V)) \leq N_H(J(T))$. Then $H = N_H(J(T))C_H(V)$, by (1), and so $N_H(J(T)) \not\leq M$ as $H \not\leq M$ and $C_H(V) \leq M$. Thus, $N = N_G(J(T)) \not\leq M$, $\Omega_1(Z(M)) \leq T \leq N$ and, $|M \cap N|_p \geq |N_M(T)|_p > |T| = |H \cap M|_p$. This is a contradiction to our choice of H and this proves the lemma.

□

In the following proposition we summarize the main results of this section.

Proposition 1.11 *Let $S \in Syl_p(M)$. Then $S \in Syl_p(G)$ and there exists $H < G$ such that*

(a) $H \not\leq M$ and $S \in Syl_p(H)$,

(b) $H \cap M$ is the unique maximal subgroup of H containing S.

□

Chapter 2

The Amalgam Method

In this section we continue the proof of Theorem 1.1 by applying the Amalgam Method. This method uncovers information about a given group by studying its action on the coset graph of some of its subgroups.

Let M and H be as in Proposition 1.11 and $\Gamma = \{Mx, Hy | x, y \in G\}$. Then we can define an adjacency relationship on Γ, namely for α, $\beta \in \Gamma$, β is adjacent to α if $\alpha \neq \beta$ and $\alpha \cap \beta \neq \emptyset$. Then G acts on Γ by right multiplication and this action preserves adjacency in Γ. Let $\Delta(\alpha) = \{\beta \in \Gamma | \beta \text{ is adjacent to } \alpha\}$. Since $G = \langle M, H \rangle$, it follows that the graph Γ is connected. Therefore given any two points α, $\beta \in \Gamma$, we can find a path from α to β, by starting with α and jumping from one point of Γ to another adjacent point of Γ until we reach β. We can speak of the length of such a path as the number of jumps taken to make it. By gathering all such paths from α to β, we can choose one with the fewest jumps and let $d(\alpha, \beta) =$ the number of jumps in this path. Define

$$G_\alpha = \{g \in G | \alpha^g = \alpha\}$$

$$Q_\alpha = O_p(G_\alpha)$$

$$G_\alpha^{(1)} = \{g \in G | \beta^g = \beta \text{ for all } \beta \text{ with } d(\alpha, \beta) \leq 1\}$$

$U_\alpha = \Omega_1(Z(G_\alpha))$

$Z_\alpha = \langle U_\beta | \beta \in \Delta(\alpha)\rangle$

It turns out that Z_α, $G_\alpha^{(1)}$, and U_α are all normal subgroups of G_α and G_α is conjugate to M or H for all $\alpha \in \Gamma$. Moreover, since cosets of a subgroup are either the same or disjoint, Γ has an alternating adjacency structure. That is, if $\alpha \in \Delta(\beta)$, then either $G_\alpha \sim M$ and $G_\beta \sim H$ or $G_\alpha \sim H$ and $G_\beta \sim M$. Let $\alpha \in \Gamma$ and $\beta \in \Delta(\alpha)$. By Proposition 1.11 there exists $S \in \mathrm{Syl}_p(G)$ with $S \leq M \cap H$. It follows from the definition of adjacency that there exists $g \in G$ with $S^g \leq G_\alpha \cap G_\beta$. And so all normal p-subgroups of G_α are in G_β and vice-versa.

From here on let $\alpha \in \Gamma$ with $G_\alpha \sim H$. Then, for any $\beta \in \Delta(\alpha)$, by Proposition 1.11, $G_\alpha \cap G_\beta$ is the unique maximal subgroup of G_α containing S^g for some $S^g \in \mathrm{Syl}_p(G)$. Also, since $G_\alpha \sim H$, $G_\beta \sim M$ and so U_β contains a conjugate of Z. In particular, $Z_\alpha \neq 1$. Hence since

$$\bigcap_{\lambda \in \Gamma} G_\lambda \leq \bigcap_{G_\lambda \sim M} G_\lambda = \bigcap_{x \in G} M^x = \mathrm{Core}_G(M) = 1$$

there exists $\gamma \in \Gamma$ with $Z_\alpha \not\leq G_\gamma^{(1)}$. Let $b = \min\{d(\alpha,\gamma) | Z_\alpha \not\leq G_\gamma^{(1)}\}$. Then if μ, $\eta \in \Gamma$ with $G_\mu \sim H$ and $Z_\mu \not\leq G_\eta^{(1)}$, we have $b \leq d(\mu,\eta)$. Now choose $\alpha' \in \Gamma$ with $d(\alpha,\alpha') = b$ and $Z_\alpha \not\leq G_{\alpha'}^{(1)}$.

Lemma 2.1 *Let α and α' be choosen as above. Then*

(a) For any $\delta \in \Gamma$, G_δ acts transitively on $\Delta(\delta)$.

(b) If β, $\delta \in \Gamma$ with $\beta \in \Delta(\delta)$, then $G_\delta^{(1)} = \mathrm{Core}_{G_\delta}(G_\delta \cap G_\beta)$.

(c) Z_α is a elementary p-abelian subgroup of $G_{\alpha'}$.

(d) $C_{G_\alpha}(Z_\alpha) = G_\alpha^{(1)}$.

(e) If $A \leq_p Z_\alpha$, *then* $C_G(A) = C_G(Z_\alpha)$.

(f) If β, $\delta \in \Gamma$ *with* $\beta \in \Delta(\delta)$, *then* $G = \langle G_\delta, G_\beta \rangle$.

Proof For (a) let $\beta, \gamma \in \Delta(\delta)$ and, without loss of generality, let $\delta = Mx$, $\beta = Hy$, and $\gamma = Hz$. Then, by the definition of adjacency, $\delta \cap \beta \neq \emptyset$ and $\delta \cap \gamma \neq \emptyset$. Hence, there exists elements g_1 and g_2 of G with

$$g_1 = m_1 x = h_1 y$$

and

$$g_2 = m_2 x = h_2 z$$

Put $g = (m_1^{-1} m_2)^x$. Then $g \in M^x = G_\delta$ and

$$\begin{aligned} \beta^g = (Hy)g &= (Hh_1 y)g \\ &= (Hm_1) m_1^{-1} m_2 x \\ &= H m_2 x \\ &= H h_2 z \\ &= Hz = \gamma. \end{aligned}$$

Therefore $\beta^g = \gamma$ and we are done.

For (b), for any $\beta \in \Delta(\delta)$ we have

$$\begin{aligned} Core_{G_\delta}(G_\delta \cap G_\beta) = \bigcap_{g \in G_\delta} (G_\delta \cap G_\beta)^g = \bigcap_{g \in G_\delta} (G_\delta \cap G_\beta^g) &= \bigcap_{g \in G_\delta} (G_\delta \cap G_{\beta^g}) \\ &= \bigcap_{\lambda \in \Delta(\delta)} (G_\delta \cap G_\lambda) \\ &= G_\delta^{(1)} \end{aligned}$$

where the fourth equality holds by (a).

For (c), suppose $Z_\alpha \not\leq G_{\alpha'}$. Let $(\alpha, \alpha+1, \alpha+2, \alpha+3, \ldots, \alpha'-1, \alpha')$ be a path from α to α'. Then, $Z_\alpha \not\leq G^{(1)}_{\alpha'-1}$ as $G^{(1)}_{\alpha'-1} \leq G_{\alpha'}$. And so we get, $d(\alpha, \alpha'-1) < d(\alpha, \alpha') = b$, a contradiction to the minimality of b. Therefore $Z_\alpha \leq G_{\alpha'}$. Next we claim that Z_α is elementary p-abelian. Since $Z_\alpha = \langle U_\beta | \beta \in \Delta(\alpha)\rangle$ and the U_β's are elementary p-abelian, its enough to show that Z_α is abelian. Let $\beta \in \Delta(\alpha)$. Then $U_\beta \leq G_\alpha$ and, by Proposition 1.11, $G_\alpha \cap G_\beta$ is a maximal subgroup of G_α. Thus, by Lemma 1.4 (b), $U_\beta \leq \Omega_1(Z(O_p(Q)))$, where $Q = \mathrm{Core}_{G_\alpha}(G_\alpha \cap G_\beta)$. But by (b), $G^{(1)}_\alpha = \mathrm{Core}_{G_\alpha}(G_\alpha \cap G_\beta)$ and so we get $U_\beta \leq Z(G^{(1)}_\alpha)$. But since $\beta \in \Delta(\alpha)$ was chosen arbitrarily, we have $Z_\alpha \leq Z(G^{(1)}_\alpha)$ is abelian.

For (d), from the proof of (c) we have $Z_\alpha \leq Z(G^{(1)}_\alpha)$ and so $G^{(1)}_\alpha \leq C_{G_\alpha}(Z_\alpha)$. On the other hand, for any $\beta \in \Delta(\alpha)$, we have $G_\beta \sim M$. Hence, by Lemma 1.2 (b), we have $C_G(U_\beta) = G_\beta$. Therefore, $U_\beta \leq Z_\alpha$ implies $C_G(Z_\alpha) \leq C_G(U_\beta) = G_\beta$. Thus, since $\beta \in \Delta(\alpha)$ was chosen arbitrarily, $C_{G_\alpha}(Z_\alpha) \leq G^{(1)}_\alpha$ and (d) holds.

For (e), its clear that $C_G(Z_\alpha) \leq C_G(A)$. Since $A \leq_p Z_\alpha$, there exists $\beta \in \Delta(\alpha)$ with $U_\beta \not\leq A$ and $Z_\alpha = AU_\beta$. Moreover, since $G_\beta \sim M$, U_β contains a conjugate of Z. Thus,

$$p = \frac{|Z_\alpha|}{|A|} = \frac{|U_\beta A|}{|A|} = \frac{|U_\beta|}{|U_\beta \cap A|} \geq \frac{p^2}{|U_\beta \cap A|}$$

Hence, $|U_\beta \cap A| \geq p$ and so $U_\beta \cap A \neq 1$. Therefore, by Lemma 1.2 (b), we get $C_G(A) \leq C_G(U_\beta \cap A) = C_G(U_\beta)$ and

$$C_G(A) \leq C_G(U_\beta A) = C_G(Z_\alpha)$$

and we have (e).

Finally, for (f), without loss of generality, let $\delta = Mx$ and $\beta = Hy$ for some x, $y \in G$. Then $\beta \in \Delta(\delta)$ implies $\beta \cap \delta \neq \emptyset$. Thus, there exists $g = mx = hy \in Mx \cap Hy$. Now $G_\delta = M^x$ and $G_\beta = H^y$. Moreover, since M is a maximal subgroup of G, M^x is also a maximal subgroup of G with $M^x \leq \langle M^x, H^y \rangle$. Therefore either $M^x = \langle M^x, H^y \rangle$ or $G = \langle M^x, H^y \rangle$. Suppose $M^x = \langle M^x, H^y \rangle$. Then $H^y \leq M^x$. But $mx = hy$ implies $y^{-1}mx = h^y$ and so there exists $m_0 \in M$ such that $y^{-1}mx = m_0^x$. By tranposing this equation we get $m^{-1}y = m_0^{-1}x \in My \cap Mx$. Thus, $Mx = My$ and so $yx^{-1} \in M$. But then $H^y \leq M^x$ implies $H^{yx^{-1}} \leq M$. Thus, since $yx^{-1} \in M$, we get $H \leq M$, a contradiction to the choice of H. Therefore $G = \langle M^x, H^y \rangle = \langle G_\delta, G_\beta \rangle$, which proves the lemma.

□

It should be noted that Lemma 2.1 parts (c), (d), and (e) hold for any μ, $\eta \in \Gamma$ with $G_\mu \sim H$, $Z_\mu \not\leq G_\eta^{(1)}$, and $d(\mu, \eta) = b$.

At this point the proof splits into the three cases $G_{\alpha'} \sim M$ or H and $b > 1$ or $G_{\alpha'} \sim M$ and $b = 1$. In each case we get a contradiction.

Case 1 $G_{\alpha'} \sim H$ *and* $b > 1$.

Lemma 2.2 *(a) If* $\beta \in \Delta(\alpha)$, *then* $Z_\alpha = \langle U_\beta^{G_\alpha} \rangle$.

(b) $Z_{\alpha'} \leq G_\alpha$.

(c) $O_p(G_\alpha / C_{G_\alpha}(Z_\alpha)) = 1$.

(d) $[Z_\alpha, Z_{\alpha'}] \neq 1$.

(e) $Z_\alpha \leq Q_{\alpha+k}$ *for all* $k \in \{1, 2, \ldots, b-1\}$.

Proof For (a), since $U_\beta \leq Z_\alpha$ and $Z_\alpha \trianglelefteq G_\alpha$, we have $\langle U_\beta^{G_\alpha} \rangle \leq Z_\alpha$. On the other hand, let $\gamma \in \Delta(\alpha)$. Then by (a) there exists $g \in G_\alpha$ such that $\gamma = \beta^g$. But then

$U_\gamma = U_{\beta^g} = U_\beta^g \leq \langle U_\beta^{G_\alpha} \rangle$. Therefore $Z_\alpha = \langle U_\beta^{G_\alpha} \rangle$.

For (b), suppose $Z_{\alpha'} \not\leq G_\alpha$. Then $Z_{\alpha'} \not\leq G_{\alpha+1}^{(1)}$ and as above we have $d(\alpha', \alpha+1) < d(\alpha', \alpha) = b$, a contradiction to the minimality of b.

For (c) let $\beta \in \Delta(\alpha)$. Then there exists $P \in \mathrm{Syl}_p(G_\alpha) \cap \mathrm{Syl}_p(G_\beta)$ and, by (a), $Z_\alpha = \langle U_\beta^{G_\alpha} \rangle$. Hence, since $U_\beta \leq Z(P)$, Lemma 1.2 (b) implies $O_p(G_\alpha / C_{G_\alpha}(Z_\alpha)) = 1$ and we have shown (c).

For (d), if $[Z_\alpha, Z_{\alpha'}] = 1$ then, by Lemma 2.1 (d), $Z_\alpha \leq C_{G_{\alpha'}}(Z_{\alpha'}) = G_{\alpha'}^{(1)}$. This is a contradiction to the choice of (α, α').

Finally for (e) we use induction on k. If $k = 0$, then the result follows as Z_α is a normal p-subgroup of G_α. Now suppose (e) holds for k with $k < b - 1$. Then $k + 1 \leq b - 1$ and so $\alpha + (k+1) \leq \alpha + (b-1)$. Hence, by the minimality of b and induction, we get $Z_\alpha \leq G_{\alpha+(k+1)}^{(1)} \leq G_{\alpha+k}$ and $Z_\alpha \leq Q_{\alpha+k}$. Therefore,

$$Z_\alpha \leq G_{\alpha+(k+1)}^{(1)} \cap Q_{\alpha+k} \leq O_p(G_{\alpha+(k+1)}^{(1)}) \leq Q_{\alpha+(k+1)}$$

and we are done.

$\square$

Now since $[Z_\alpha, Z_{\alpha'}] \neq 1$, there exists $\beta \in \Delta(\alpha')$ with $[Z_\alpha, U_\beta] \neq 1$. Let $P \in \mathrm{Syl}_p(G_{\alpha'}) \cap \mathrm{Syl}_p(G_\beta)$, and $Q = \{g \in G_{\alpha'} | [Z_{\alpha'}, g, g] = 1\}$. Then, by Lemma 2.1 (a) and Proposition 1.11, $Z_{\alpha'}$ is a $GF(p)G_{\alpha'}$-module and $G_{\alpha'} \cap G_\beta$ is the unique maximal subgroup of $G_{\alpha'}$ containing P with $G_{\alpha'} \cap G_\beta$ solvable. Since, by (a) $Z_{\alpha'} \leq G_\alpha$, and $Z_\alpha \trianglelefteq G_\alpha$ we have

$$[Z_{\alpha'}, Z_\alpha, Z_\alpha] \leq [Z_\alpha, Z_\alpha] = 1$$

and so $Z_\alpha \leq Q$. Moreover, $Q \not\leq G_{\alpha'} \cap G_\beta$, otherwise $Z_\alpha \leq Q \leq G_{\alpha'} \cap G_\beta$ and $U_\beta \leq Z(G_\beta)$ would imply $[Z_\alpha, U_\beta] = 1$, a contradiction to the choice of β. Thus, $Z_{\alpha'}$, $G_{\alpha'}$, P, $G_{\alpha'} \cap G_\beta$ and Q satisfy the hypothesis to Lemma 1.9 which yields, $C_{Z_{\alpha'}}(G_{\alpha'}) = C_{Z_{\alpha'}}(G_{\alpha'} \cap G_\beta)$. But then $G_{\alpha'} \leq C_G(U_\beta) = G_\beta$, as $U_\beta \leq Z(G_\beta) \cap Z_{\alpha'}$. Thus, we get $G_{\alpha'} \leq G_\beta$. But, since $\beta \in \Delta(\alpha')$, by Lemma 2.1 (f) we get $G = \langle M, H\rangle = \langle G_{\alpha'}, G_\beta\rangle = G_\beta$, a contradiction to the maximality of M.

$\square$

Case 2 *$G_{\alpha'} \sim M$ and $b > 1$.*

Let $\overline{G_{\alpha'}} = G_{\alpha'}/Q_{\alpha'}$ and $\overline{Q} = Q/Q_{\alpha'} = F(\overline{G_{\alpha'}})$. Then $O_p(\overline{G_{\alpha'}}) = 1$ and $\overline{Q}$ is a p'-group.

Lemma 2.3 *(a) $\overline{Z_\alpha} \neq 1$*

(b) $[Q, Z_\alpha] \not\leq C_{G_{\alpha'}}(Z_{\alpha'-1})Q_{\alpha'}$

(c) There exists $\overline{A} \leq_p \overline{Z_\alpha}$ with $[C_{\overline{Q}}(\overline{A}), \overline{Z_\alpha}] \not\leq \overline{C_{G_{\alpha'}}(Z_{\alpha'-1})}$

(d) Let $\overline{A}$ be as in (c). Then there exists $\overline{x} \in [C_{\overline{Q}}(\overline{A}), \overline{Z_\alpha}]$ with $A \not\leq C_G(Z^x_{\alpha'-1})$

(e) Let $(\alpha' - 1)^x = \alpha' + 1$. Then $A \leq G_{\alpha'-1} \cap G_{\alpha'+1}$

Proof If $\overline{Z_\alpha} = 1$, then $Z_\alpha \leq Q_{\alpha'} \leq G^{(1)}_{\alpha'}$. Hence we get, $Z_\alpha \leq G^{(1)}_{\alpha'}$, a contradiction to the choice of (α, α'). Therefore $\overline{Z_\alpha} \neq 1$ and this shows (a). For (b), again we proceed by contradiction. Suppose $[Q, Z_\alpha] \leq C_{G_{\alpha'}}(Z_{\alpha'-1})Q_{\alpha'}$. Then,

$$[\overline{Q},\overline{Z_\alpha}] \le \overline{C_{G_{\alpha'}}(Z_{\alpha'-1})} = \bigcap_{\gamma\in\Delta(\alpha'-1)} \overline{G_{\alpha'}\cap G_\gamma}$$

And so by Lemma 2.2 (e), we have $[\overline{Q},\overline{Z_\alpha},\overline{Z_\alpha}] \le \overline{Q_{\alpha'-2}\cap Q} = 1$ as $\overline{Q}$ is a p'-group and $\overline{Q_{\alpha'-2}}$ is a p-group.

Therefore $[\overline{Q},\overline{Z_\alpha},\overline{Z_\alpha}] = 1$ and so by the coprime action of the p-group $\overline{Z_\alpha}$ on the p'-group $\overline{Q}$, we have $[\overline{Q},\overline{Z_\alpha}] = [\overline{Q},\overline{Z_\alpha},\overline{Z_\alpha}] = 1$. But then by [3, 6.1.3], $\overline{Z_\alpha} \le C_{\overline{G_{\alpha'}}}(\overline{Q}) \le \overline{Q}$. Since $\overline{Z_\alpha}$ is a p-group and $\overline{Q}$ is a p'-group we get $\overline{Z_\alpha} = 1$, a contradiction to (a).

For (c), by the coprime action of $\overline{Z_\alpha}$ on $\overline{Q}$, we have $\overline{Q} = \langle C_{\overline{Q}}(\overline{A}) | \overline{A} \le_p \overline{Z_\alpha}\rangle$. Now by applying Lemma 1.6 to $\overline{Z_\alpha}$ and $\overline{Q}$ we get

$$[\overline{Q},\overline{Z_\alpha}] = \langle [C_{\overline{Q}}(\overline{A}),\overline{Z_\alpha}] | \overline{A} \le_p \overline{Z_\alpha}\rangle. \tag{1}$$

Now by (b), $[\overline{Q},\overline{Z_\alpha}] \not\le \overline{C_{G_{\alpha'}}(Z_{\alpha'-1})}$ and so by (1) implies there exists $\overline{A} \le_p \overline{Z_\alpha}$ with $[C_{\overline{Q}}(\overline{A}),\overline{Z_\alpha}] \not\le \overline{C_{G_{\alpha'}}(Z_{\alpha'-1})}$.

Suppose (d) does not hold and let $\overline{K} = K/Q_{\alpha'} = [C_{\overline{Q}}(\overline{A}),\overline{Z_\alpha}]$. Then $A \le C_G(Z_0)$ where $Z_0 = \langle Z_{\alpha'-1}^K\rangle$. Now $\overline{A} \le_p \overline{Z_\alpha}$ implies $A \le_p Z_\alpha$. Therefore, by Lemma 2.1 (b), $C_G(Z_\alpha) = C_G(A)$ and consequently $Z_\alpha \le C_G(Z_0)$. Now by the coprime action of the p-group $\overline{Z_\alpha}$ on the p'-group $C_{\overline{Q}}(\overline{A})$ we get

$$[C_{\overline{Q}}(\overline{A}),\overline{Z_\alpha}] = [C_{\overline{Q}}(\overline{A}),\overline{Z_\alpha},\overline{Z_\alpha}]$$

and so,

$$K \le [K,Z_\alpha]Q_{\alpha'} \le C_{G_{\alpha'}}(Z_0)Q_{\alpha'} \le C_{G_{\alpha'}}(Z_{\alpha'-1})Q_{\alpha'}.$$

Thus, by taking images in $\overline{G_{\alpha'}}$, we get $[C_{\overline{Q}}(\overline{A}),\overline{Z_\alpha}] \le \overline{C_{G_{\alpha'}}(Z_{\alpha'-1})}$, a contradiction to (c).

Finally, for (e), Lemma 2.3 (e) implies $A \leq Z_\alpha \leq Q_{\alpha'-1} \leq G_{\alpha'-1}$. Hence, since $Q_{\alpha'} \leq G_{\alpha'-1}$, we get $AQ_{\alpha'} \leq G_{\alpha'-1}$. Now $\overline{x} \in [C_{\overline{Q}}(\overline{A}), \overline{Z_\alpha}] \leq C_{\overline{Q}}(\overline{A})$ implies $x \in N_G(AQ_{\alpha'})$. Therefore

$$AQ_{\alpha'} = (AQ_{\alpha'})^x \leq G^x_{\alpha'-1} = G_{(\alpha'-1)^x} = G_{\alpha'+1}$$

and $A \leq G_{\alpha'-1} \cap G_{\alpha'+1}$.

□

Lemma 2.4 *Let $\delta \in \Gamma$. Define $V_\delta = \langle Z_\lambda | \lambda \in \Delta(\delta)\rangle$. Then*

(a) $V_{\alpha+1} \leq G_{\alpha'}$ and $V_{\alpha'} \leq G_{\alpha+1}$

(b) $V_{\alpha+1} \trianglelefteq G_{\alpha+1}$ and $V_{\alpha'} \trianglelefteq G_{\alpha'}$

(c) $V_{\alpha+1}$ and $V_{\alpha'}$ are elementary abelian p-groups.

(d) $[V_{\alpha'}, V_{\alpha+1}, V_{\alpha+1}] = 1$.

Proof For (a), suppose $V_{\alpha+1} \not\leq G_{\alpha'}$. Then there exists $\gamma \in \Delta(\alpha+1)$ with $Z_\gamma \not\leq G_{\alpha'}$. Then, since $G^{(1)}_{\alpha'-1} \leq G_{\alpha'}$, $Z_\gamma \not\leq G^{(1)}_{\alpha'-1}$. Hence, $G_\gamma \sim H$, $Z_\gamma \not\leq G^{(1)}_{\alpha'-1}$, and $d(\gamma, \alpha'-1) < d(\alpha, \alpha') = b$. This contradicts the minimality of b. A similar argument shows $V_{\alpha'} \leq G_{\alpha+1}$

For (b), let $g \in G_{\alpha+1}$ and $\gamma \in \Delta(\alpha+1)$. Then, since the action of G on the graph Γ preserves adjacency, we have $\gamma^g \in \Delta((\alpha+1)^g) = \Delta(\alpha+1)$ and

$$Z^g_\gamma = Z_{\gamma^g} \leq V_{\alpha+1}$$

Thus, $V_{\alpha+1} \trianglelefteq G_{\alpha+1}$ and a similar argument shows $V_{\alpha'} \trianglelefteq G_{\alpha'}$.

For (c), since $V_{\alpha+1}$ and $V_{\alpha'}$ are generated by elementary abelian p-groups, it is enough to show that $V_{\alpha+1}$ and $V_{\alpha'}$ are abelian. Let $\gamma, \delta \in \Delta(\alpha+1)$. Then $\gamma, \delta \neq \alpha'$, since G_γ and G_δ are both conjugate to H. Moreover, $b > 1$, $G_{\alpha'} \sim M$, and the alternating adjacency structure of Γ imply $b \geq 3$. Hence, since $d(\gamma, \delta) = 2 < 3 \leq b$, by the minimality of b we have $Z_\gamma \leq G_\delta^{(1)}$. But $G_\delta^{(1)} = C_G(Z_\delta)$, by Lemma 2.1 (d) and so $[Z_\gamma, Z_\delta] = 1$ and $V_{\alpha+1}$ is abelian. A similar argument shows $V_{\alpha'}$ is abelian. Finally, (a), (b), and (c) imply

$$[V_{\alpha'}, V_{\alpha+1}, V_{\alpha+1}] \leq [V_\alpha, V_\alpha] = 1$$

and the lemma is proved.

□

Now, since $A \leq Z_\alpha \leq V_{\alpha+1}$ and $Z_{\alpha'+1} \leq V_{\alpha'}$, by Lemma 2.3 (d) and Lemma 2.4 (d), we have $[Z_{\alpha'+1}, A, A] = 1$ and $[Z_{\alpha'+1}, A] \neq 1$. Thus, there $\gamma \in \Delta(\alpha' + 1)$ with $[A, U_\gamma] \neq 1$. Now as before, letting $P \in \mathrm{Syl}_p(G_\gamma) \cap \mathrm{Syl}_p(G_{\alpha'+1})$ and $Q = \{g \in G_{\alpha'+1} | [Z_{\alpha'+1}, g, g] = 1\}$, we see that $G_{\alpha'+1}$, $Z_{\alpha'+1}$, P, Q, and $G_\gamma \cap G_{\alpha'+1}$ satisfy the hypothesis to Proposition 1.9. Just as before we get $G_{\alpha'+1} \leq G_\gamma$, a contradiction.

□

Case 3 $b = 1$

Since $b = 1$ and $Z_\alpha \trianglelefteq G_\alpha$, we have, $Q_{\alpha'} \leq G_\alpha$ and $[Q_{\alpha'}, Z_\alpha, Z_\alpha] \leq [Z_\alpha, Z_\alpha] = 1$. Let $L = \langle Z_\alpha^{G_{\alpha'}} \rangle$. Then L is not a p-group; otherwise, since $L \trianglelefteq G_{\alpha'}$, we get $Z_\alpha \leq L \leq Q_{\alpha'} \leq G_{\alpha'}^{(1)}$, a contradiction to the choice of (α, α'). Since L is not a p-group $O^p(L) \neq 1$. Thus, since $G_{\alpha'}$ is solvable and $O_{p'}(G_{\alpha'}) = 1$, we have $[O^p(L), Q_{\alpha'}] \neq 1$. Therefore, by [3, 5.3.2], there exists a composition factor V for L on $Q_{\alpha'}$ with $[V, O^p(L)] \neq 1$. Now $\Phi(V)$ char $\leq V$ implies $\Phi(V)$ is L-invariant. Since $\Phi(V)$ is a proper subgroup of V, we have $\Phi(V) = 1$, by the irreducibility of L on V. Thus, since V is a p-group, by [3, 3.1.3], V is elementary p-abelian. Let $\overline{L} = L/C_L(V)$. Then V is a faithful and irreducible GF$(p)\overline{L}$-module and so, by [3, 5.1.3], $O_p(\overline{L}) = 1$. Since $[V, L] \neq 1$, there exists $g \in G_{\alpha'}$ with $[V, Z_\alpha^g] \neq 1$. Thus, $\overline{Z_\alpha^g} \neq 1$ and $[V, \overline{Z_\alpha^g}, \overline{Z_\alpha^g}] = 1$. This means $\overline{L}$ is not p-stable, and so, by [3, 3.8.3], $\overline{L}$ involves $\mathrm{SL}_2(p)$. Since $L \leq G_{\alpha'}$ and $G_{\alpha'}$ is solvable, L and $\overline{L}$ are solvable. But $\mathrm{SL}_2(p)$ is not solvable for $p \geq 5$. Thus since $\overline{L}$ involves $\mathrm{SL}_2(p)$ we have a contradicition and therefore we have shown Theorem 1.1.

$\square$

Chapter 3

Maximal subgroups of locally finite simple groups

In this chapter we will show that Theorem 1.1 extends to locally finite simple groups. This result is Theorem 3.1 and its proof relies indirectly on the classification of finite simple groups.

Theorem 3.1 *Let G be a nonfinitary locally finite simple group, p a prime with $p \neq q$ if G is of q-type, and Z a subgroup of G of type (p,p). Then there exist nontrivial elements z, $z' \in Z$ with $C_G(z) \neq C_G(z')$. In particular, if M is a maximal subgroup of G then $O_p(Z(M))$ is locally cyclic.*

Def A group G is called *locally finite* if $|\langle H\rangle| < \infty$ for any finite subset $H \subseteq G$.

Def G is a LFS-group if G is locally finite and simple. A set of pairs $\mathcal{K} = \{(H_i, N_i) | i \in I\}$ is called a *Kegel cover* for G if,

(1) $H_i \leq G$ and $|H_i| < \infty$ for all $i \in I$.

(2) N_i is a maximal normal subgroup of H_i for all $i \in I$.

(3) For each finite subgroup $H \leq G$, there exists $i \in I$ with $H \leq H_i$ and $H \cap N_i = 1$.

The groups H_i/N_i are called the factors of the Kegel cover. It has been shown in [5, 4.3] that every LFS-group has a Kegel cover. Next we define some terminology that will be useful for us. Let G be a LFS-group and $\mathcal{K} = \{(H_i, N_i) | i \in I\}$ be a Kegel cover for G. Also let V be a vector space over a field F and Ω be a nonempty set.

Def Let X be a finite subgroup of G. Then $\mathcal{K}(X) = \{(H_i, N_i) \in \mathcal{K} | X \leq H_i \text{ and } X \cap N_i = 1\}$.

Def G is called *finitary* if there exists a field F and a faithful FG-module V such that $\dim_F[V, g] < \infty$ for all $g \in G$.

Def G is of *alternating type* if it possesses a Kegel cover all of whose factors are isomorphic to alternating groups.

Def If q is a prime, G is of *q-type* if G is non-finitary and every Kegel cover for G has a factor which is isomorphic to a classical group defined over a field of characteristic q.

Def Suppose x is acting on V, then

$$\deg_V(x) = \dim_F[V, x]$$

and

$$\mathrm{pdeg}_V(x) = \min\{\deg_V(\lambda x) | 0 \neq \lambda \in F\}.$$

Let V be a vector space over a field F and Ω be a nonempty set.

Def Suppose x is acting on Ω. Then $\mathrm{Supp}_\Omega(x)$ is the set of elements of Ω that are not fixed by x and

$$\deg_{\Omega}(x) = \mathrm{pdeg}_{\Omega}(x) = |\mathrm{Supp}_{\Omega}(x)|.$$

<u>Def</u> Let $x \in T$ and $T \cong \mathrm{PSL}_F(V)$ or $T \cong \mathrm{Alt}(\Omega)$ and y be the image of x under this isomorphism. Then

$$\deg_T(x) = \deg_V(y) \text{ or } \deg_T(x) = \deg_{\Omega}(y)$$

respectively.

In [7, 3.3] U.Meierfrankenfeld proved:

Theorem 3.2 *Let T be a LFS-group. Then one of the following must hold:*

(a) T is finitary

(b) T is of alternating type

or

(c) There exists a prime q and a Kegel cover $\{(H_i, N_i) | i \in I\}$ for T, such that T is of q-type, $H_i/O_q(H_i)$ is the central product of perfect central extensions of classical groups defined over a field of characteristic q, and H_i/N_i is isomorphic to a projective special linear group for all $i \in I$.

$\square$

Proof of Theorem 3.1 First suppose Theorem 3.1 holds and let M be a maximal subgroup of G. Indeed, if $O_p(Z(M))$ were not locally cyclic for such a prime p, then, since G is locally finite, we can find a finite noncyclic abelian p-subgroup H of

$O_p(Z(M))$. Now inside of H, by the Classification of Finite Abelian Groups, we can find a subgroup K of type (p,p). But then, since G is simple and M is maximal, we get $M = C_G(k) = C_G(k')$ for all nontrivial elements $k\ k' \in K$, a contradiction.

Suppose that Theorem 3.1 does not hold. Then $C_G(z) = C_G(z')$ for all nontrivial elements z, $z' \in Z$. Although G is a locally finite group, Lemma 1.2 (c) still holds for Z and will be used throughout the proof of Theorem 3.1. Since G is a nonfinitary LFS-group the proof of Theorem 3.1 splits naturally into the two cases (b) and (c) referred to in the statement of Theorem 3.2.

3.1 Locally finite simple groups of q-type

In this section we consider the case of Theorem 3.1 in which G is of q-type for some prime $q \neq p$.

Case 1 *There exists a prime $q \neq p$ and a Kegel cover $\mathcal{K}=\{(H_i, N_i)|i \in I\}$ for G, such that G is of q-type, $H_i/O_p(H_i)$ is the central product of perfect central exstensions of classical groups defined over fields in characteristic q, and H_i/N_i is isomorphic to a projective special linear group for all $i \in I$.*

For any $(H_i, N_i) \in \mathcal{K}$, let $H_i/N_i \cong \mathrm{PSL}_{n_i}(q^{t_i}, V_i)$, $\overline{H_i} = H_i/O_q(H_i)$, $\overline{H_i} = \langle\{\overline{L_j}|j \in J\}\rangle$ with $[\overline{L_j}, \overline{L_k}] = 1$ for all $j \neq k$ and $\overline{L_j} = L_j/O_q(H_i)$ are quasi simple for all $j \in J$.

Lemma 3.3 *Let $(H_i, N_i) \in \mathcal{K}$ and $\overline{H_i} = H_i/N_i$. Then*

(a) If $T \trianglelefteq H_i$, then $H_i = TN_i$ or $T \leq N_i$. In particular, $O_q(H_i) \leq N_i$.

(b) There exists $j \in J$ such that $L_j \nleq N_i$.

(c) If $L_j \not\leq N_i$, then $Z(\overline{L_j}) = \overline{N_i \cap L_j}$ and $H_i/N_i \cong \overline{L_j}/Z(\overline{L_j})$

Proof For (a), $T \trianglelefteq H_i$ implies $N_i \leq TN_i \trianglelefteq H_i$. And so by the maximality of N_i, we get $N_i = N_iT$ or $N_iT = H_i$. On one hand, $N_i = N_iT$ implies $T \leq N_i$. And on the other hand, $H_i = N_iT$. In particular, $O_q(H_i) \trianglelefteq H_i$, and if $H_i = O_q(H_i)N_i$, then

$$\mathrm{PSL}_{n_i}(q^{t_i}) \cong H_i/N_i = O_q(H_i)N_i/N_i \cong O_q(H_i)/O_q(H_i) \cap N_i.$$

Hence we get, $\mathrm{PSL}_{n_i}(q^{t_i})$ is a q-group, a contradiction. Therefore $O_q(H_i) \leq N_i$.

Next we show (b) by contradiction. Suppose $L_j \leq N_i$ for all $j \in J$. Then $\overline{L_j} \leq \overline{N_i}$ for all $j \in J$ and

$$\overline{H_i} = \langle \{\overline{L_j} | j \in J\} \rangle \leq \overline{N_i}.$$

Hence, $\overline{H_i} = \overline{N_i}$. Since, by (a), $O_q(H_i) \leq N_i$, we get $H_i = N_i$, a contradiction to the maximality of N_i.

For (c), $Z(\overline{L_j})$ char $\leq \overline{L_j} = K_j \trianglelefteq \overline{H_i}$ implies $Z(\overline{L_j}) \trianglelefteq \overline{H_i}$. Let $Z(\overline{L_j}) = U/O_q(H_i)$. Then, since $Z(\overline{L_j})$ is a abelian normal subgroup of $\overline{H_i}$, we have $U \trianglelefteq H_i$ and $U' \leq O_q(H_i) \leq N_i$. Thus, by (a), we have $U \leq N_i$ or $H_i = N_iU$. Now $H_i = N_iU$ implies

$$\mathrm{PSL}_{n_i}(q^{t_i}) \cong H_i/N_i = N_iU/N_i \cong U/N_i \cap U.$$

But $U/N_i \cap U$ is abelian as $U' \leq N_i \cap U$. Hence, we get $PSL_{n_i}(q^{t_i})$ is abelian, a contradiction. Hence, $U \leq N_i \cap L_j$ and $Z(\overline{L_j}) = \overline{U} \leq \overline{N_i \cap L_j}$. On the other hand, $N_i \trianglelefteq H_i$ implies $N_i \cap L_j \trianglelefteq L_j$ and $\overline{N_i \cap L_j} \trianglelefteq \overline{L_j}$. Thus, since $\overline{L_j}$ is quasi-simple, either $\overline{N_i \cap L_j} \leq Z(\overline{L_j})$ or $\overline{L_j} = (\overline{N_i \cap L_j})Z(\overline{L_j})$. Since $Z(\overline{L_j}) \leq \overline{N_i \cap L_j}$,

$\overline{L_j} = (\overline{N_i \cap L_j})Z(\overline{L_j})$ implies $\overline{L_j} = \overline{N_i \cap L_j}$ and $L_j \leq N_i$, a contradiction to the choice of L_j. Therefore, $\overline{N_i \cap L_j} \leq Z(\overline{L_j})$.

Finally, since $L_j \not\leq N_i$ and $L_j \trianglelefteq H_i$, (a) implies $H_i = N_i L_j$. Thus,

$$H_i/N_i = N_i L_j/N_i \cong L_j/N_i \cap L_j \cong \overline{L_j}/\overline{N_i \cap L_j} = \overline{L_j}/Z(\overline{L_j})$$

and we have (c).

□

Lemma 3.4 *Let q be a prime, $k > 0$ an integer, and V be a n-dimensional vector space over GF(q^k). Also let $0 \neq W \leq V$ be a subspace of V, and $Q_W = C_{GL_n(V)}(W) \cap C_{GL_n(V)}(V/W)$. Then,*

(a) Q_W is a q-subgroup of $SL_n(V)$.

(b) $C_{GL_n(V)}(Q_W) = Q_W Z(GL_n(V))$.

Proof For (a) let $\{w_i\}_{i=1}^m$ be a basis for W. Extend this basis to $B = \{w_i\}_{i=1}^m \cup \{v_i\}_{i=m+1}^n$, a basis for V. Let $a \in Q_W$. Then the matrix $M_B(a)$ for a in the basis B is

$$M_B(a) = \begin{pmatrix} I & 0 \\ A & I \end{pmatrix}$$

where I is the $m \times m$ identity matrix, 0 is the $m \times (n-m)$ zero matrix, and A is some $(n-m) \times m$ matrix. Since the field GF(q^k) has characteristic q, we have

$$\begin{aligned} a^q &= \begin{pmatrix} I & 0 \\ qA & I \end{pmatrix} \\ &= \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} \\ &= I_n \end{aligned}$$

where I_n denotes the $n \times n$ identity matrix. Hence every element of Q_W is a q-element and therefore Q_W is a q-group. Also, since $M_B(a)$ is a lower triangular matrix with 1's along the main diagonal, we have $\det(M_B(a)) = 1$ and $Q_W \leq \mathrm{SL}_n(V)$.

Next we claim that Q_W is abelian. Let $a, b \in Q_W$. Then

$$\begin{aligned} ab &= \begin{pmatrix} I & 0 \\ A & I \end{pmatrix} \begin{pmatrix} I & 0 \\ B & I \end{pmatrix} \\ &= \begin{pmatrix} I & 0 \\ A+B & I \end{pmatrix} \\ &= \begin{pmatrix} I & 0 \\ B+A & I \end{pmatrix} \\ &= ba \end{aligned}$$

Hence, Q_W is abelian and $Q_W \leq C_{\mathrm{GL}_n(V)}(Q_W)$. But then we get $Q_W Z(\mathrm{GL}_n(V)) \leq C_{\mathrm{GL}_n(V)}(Q_W)$. On the other hand, let $g \in C_{\mathrm{GL}_n(V)}(Q_W)$ with

$$M_B(g) = \begin{pmatrix} R & S \\ T & U \end{pmatrix}$$

where R, S, T, and U are $m \times m$, $m \times n-m$, $n-m \times m$, and $n-m \times n-m$ matrices over $\mathrm{GF}(q^k)$ respectively. Let $a \in Q_W$ with

$$M_B(a) = \begin{pmatrix} I & 0 \\ A & I \end{pmatrix}$$

Then $ga = ag$ implies

$$SA = 0 \text{ and } UA = AR \tag{1}$$

Now, since (1) holds for any $n-m \times m$ matrix A over $\mathrm{GF}(q^k)$, let $A = (e_{ij})$ be the $n-m \times m$ matrix with $e_{ij} = 1$ and all other entries zero. Then from (1) we get $S(e_{ij}) = 0$ and consequently the i^{th} column of S is zero. By letting i vary we eventually get all the columns of S are zero and thus $S = 0$. Again, by (1) applied to (e_{ij}) we get $U(e_{ij}) = (e_{ij})R$. Letting i and j vary we get $u_{ii} = r_{ii} = \lambda$ for all i and

$u_{ij} = r_{ij} = 0$ for all $i \neq j$. But this means $R = U = \lambda I$. Hence,

$$\begin{aligned} M_B(g) &= \begin{pmatrix} R & S \\ T & U \end{pmatrix} \\ &= \begin{pmatrix} \lambda I & 0 \\ T & \lambda I \end{pmatrix} \\ &= \begin{pmatrix} I & 0 \\ T\lambda^{-1} & I \end{pmatrix} \begin{pmatrix} \lambda I & 0 \\ 0 & \lambda I \end{pmatrix} \\ &= xy \end{aligned}$$

with $x \in Q_W$ and $y \in Z(\mathrm{GL}_n(V))$. Thus $g \in Q_W Z(\mathrm{GL}_n(V))$ and the lemma is proven.

□

Lemma 3.5 *Let $p \neq q$ be primes, $k > 0$ an integer, and V a n-dimensional vectorspace over $GF(q^k)$. Suppose $P \leq GL_n(V)$ such that $1 \neq P/Z(GL_n(V))$ is a p-group and $|P/Z(GL_n(V))| < n$, then*

(a) There exists a nontrivial, P-invariant, subspace $W \leq V$ with $[Q_W, P] \not\leq Z(GL_n(V))$.

(b) Let $\overline{P}$ denote the image of P in $PGL_n(V)$. Then there exists a nontrivial, q-subgroup $\overline{Q}$ of $PSL_n(V)$ on which $\overline{P}$ acts nontrivially.

Proof Let $0 \neq v \in V$ and $W = \langle v^P \rangle$. Then W is a nonzero, P-invariant, subspace of V. Let $|P/Z(\mathrm{GL}_n(V))| = t < n$ and $\{x_i\}_{i=1}^t$ be a transversal of $Z(\mathrm{GL}_n(V))$ in P. If $x \in P$ then, $x = zx_i$ for some $1 \leq i \leq t$ and some $z \in Z(\mathrm{GL}_n(V))$. Hence, $v^x = v^{zx_i} = (\lambda v)^{x_i} = \lambda(v^{x_i}) \in \langle \{v^{x_i}\}_{i=1}^t \rangle$ for some $\lambda \in \mathrm{GF}(q^k)$. Therefore $W = \langle v^{x_i} | 1 \leq i \leq t \rangle$ and so W is properly contained in V, as W is spanned by less than n vectors. Since W is P-invariant, it follows from the definition of Q_W that Q_W is P-invariant. Now suppose $[Q_W, P] \leq Z(\mathrm{GL}_n(V))$. Let $P_0 \in \mathrm{Syl}_p(P)$ and $\overline{P}$, $\overline{P_0}$ be the images of P, P_0 in $\mathrm{PGL}_n(V)$. Then, since $\overline{P}$ is a p-group, we get $\overline{P} = \overline{P_0}$. Now $[Q_W, P] \leq Z(\mathrm{GL}_n(V))$ implies $[Q_W, P, P] = 1$ and therefore $[Q_W, P_0, P_0] = 1$. But, by Lemma 3.4 (a), Q_W is a q-group, and so by the coprime action of P_0 on Q_W we get $[Q_W, P_0] = 1$. Hence, $P_0 \leq C_{\mathrm{GL}_n(V)}(Q_W)$. But, $C_{\mathrm{GL}_n(V)}(Q_W) = Q_W Z(\mathrm{GL}_n(V))$, by Lemma 3.4 (b). Therefore, since Q_W is a q-group and $Z(\mathrm{GL}_n(V)) \trianglelefteq \mathrm{GL}_n(V)$, we get $P_0 \leq Z(\mathrm{GL}_n(V))$. But then $\overline{P} = \overline{P_0} = 1$ and $P \leq Z((\mathrm{GL}_n(V))$. This is a contradiction, since P is noncentral. Therefore $[Q_W, P] \not\leq Z(\mathrm{GL}_n(V))$ and the lemma is proved.

For (b), let $\overline{Q_W}$ denote the image of Q_W in $\mathrm{PGL}_n(V)$. Then W is P-invariant implies $\overline{Q_W}$ is $\overline{P}$-invariant. Moreover, by Lemma 3.4 (a), $\overline{Q_W}$ is a q-subgroup of $\mathrm{PSL}_n(V)$. Finally, by (a), we have $[Q_W, P] \not\leq Z(\mathrm{GL}_n(V))$. Thus, as $Z(\mathrm{GL}_n(V)) \trianglelefteq \mathrm{GL}_n(V)$, we get $Q_W \not\leq Z(\mathrm{GL}_n(V))$ and $[\overline{Q_W}, \overline{P}] \neq 1$. Therefore $\overline{P}$ acts nontrivially on $\overline{Q_W}$ and $\overline{Q_W} \neq 1$.

□

In [7, 3.1] U.Meierfrankenfeld showed

Theorem 3.6 *Let T be a nonfinitary LFS-group and $\mathcal{T}$ be a Kegel cover for T. Then if k is a positive integer and $1 \neq X \leq T$ with $|X| < \infty$*

$$\mathcal{T}_0 = \{(H, N) \in \mathcal{K}(X) | pdeg_{H/N}(x) \geq k \text{ for all } 1 \neq x \in X\}$$

is also a Kegel cover for T.

□

Let $(H_i, N_i) \in \mathcal{K}(Z)$. Then, since $|Z| = p^2 < \infty$, by Theorem 3.6 we may assume that $\mathrm{pdeg}_{H_i/N_i}(z) \geq p^2 + 1$ for all $1 \neq z \in Z$. Set $H = H_i$, $N = N_i$, $V = V_i$, and

$t = t_i$. Then

$$n = \dim_{GF(q^t)} V \geq \mathrm{pdeg}_{H/N}(z) > p^2$$

for any $1 \neq z \in Z$ and so $p^2 < n$. Moreover, by Lemma 3.3 (c), there exists $j \in J$ such that $L_j \not\leq N$. Let $L = L_j$.

Then by Lemma 3.3 (c), we have

$$\mathrm{PSL}_n(q^t) \cong \frac{H}{N} \cong \frac{\overline{H}}{\overline{N}} = \frac{\overline{LN}}{\overline{N}} \cong \frac{\overline{L}}{\overline{N \cap L}} = \frac{\overline{L}}{Z(\overline{L})}. \tag{1}$$

Hence, since $Z \cap N = 1$, $\overline{L}/\overline{N \cap L}$ contains a copy Z^* of Z. It follows from (1) that $Z^* = \overline{ZN} \cap \overline{L}/\overline{N \cap L}$.

Now, since $\overline{L}/\overline{N \cap L} \cong \mathrm{PSL}_n(q^t)$ and $|Z^*| = p^2 < n$, by Lemma 3.5 (b), there exists a q-group U of $\overline{L}/\overline{N \cap L}$ on which Z^* acts nontrivially on U by conjugation. Let $U = \overline{Q}/\overline{N \cap L}$. Then Z^* acts nontrivially on $\overline{Q}/\overline{N \cap L}$ implies $\overline{ZN} \cap \overline{L}$ acts nontrivially on $\overline{Q}$. Let Q be the preimage of $\overline{Q}$ in L. Then, since both N and L are normal subgroups of H, we have $[N, Q] \leq N \cap L$ and therefore $[\overline{N}, \overline{Q}] \leq \overline{N \cap L} \leq \overline{Q}$. Thus, $\overline{N}$ normalizes $\overline{Q}$ and so $(\overline{ZN} \cap \overline{L})\overline{N} = \overline{ZN}$ acts nontrivially on $\overline{Q}$. But then $\overline{Z}$ acts on $\overline{Q}$.

Since $\overline{Q}/\overline{N \cap L} = \overline{Q}/Z(\overline{L})$ is a q-group, $\overline{Q}/Z(\overline{L})$ is nilpotent. Hence, since $\overline{Q} \leq \overline{L}$, the latter implies $\overline{Q}$ is also nilpotent. Let $\overline{Q_0} \in \mathrm{Syl}_q(\overline{Q})$. Then $\overline{Q_0}$ char $\leq \overline{Q}$ implies $\overline{Z}$ acts on $\overline{Q_0}$. Moreover, since $\overline{Q_0} \in \mathrm{Syl}_q(\overline{Q})$ and $\overline{Q}/\overline{N \cap L}$ is a q-group, we have $\overline{Q} = \overline{Q_0}(\overline{N \cap L})$. Suppose $[\overline{Z}, \overline{Q_0}] = 1$. Then, since $[\overline{N}, \overline{Q}] \leq \overline{N \cap L}$, we have $[\overline{N}, \overline{Q_0}] \leq \overline{N \cap L}$ and therefore $[\overline{ZN} \cap \overline{L}, \overline{Q_0}] \leq \overline{N \cap L}$. Thus we get,

$$[\frac{(\overline{ZN} \cap \overline{L})}{\overline{N \cap L}}, \frac{\overline{Q}}{\overline{N \cap L}}] = [\frac{(\overline{ZN} \cap \overline{L})}{\overline{N \cap L}}, \frac{\overline{Q_0}(\overline{N \cap L})}{\overline{N \cap L}}] = 1$$

a contradiction. Hence $\overline{Z}$ acts nontrivially on $\overline{Q_0}$ and therefore Z acts nontrivially on Q_0, where Q_0 is the preimage of $\overline{Q_0}$ in H. But, since $\overline{H} = H/O_q(H)$, Q_0 is a q-group. Thus Z acts nontrivially on a q-group, a contradiction to Lemma 1.2 (c). This concludes case 1 of Theorem 3.1.

□

3.2 Locally finite simple groups of alternating type

In this section we consider those LFS-groups which admit a Kegel cover all of whose factors are alternating groups, the so-called groups of alternating type.

Case 2 *G is a LFS-group of alternating type.*

Before we begin this case we start by giving a list of some notations used throughout. Suppose H is a group acting on a set Ω with $H/N \cong Alt(\Sigma)$, for some set Σ and some normal subgroup N of H. Let t be a positive integer with $t \leq |\Sigma|/2$.

Def A system of imprimitivity Δ for H on Ω is a set of proper subsets of Ω such that $|D| \geq 2$ for at least one $D \in \Delta$, $D^h \in \Delta$ for all $D \in \Delta$ and $h \in H$, and Ω is the disjoint union of the members of Δ.

Def H acts t-pseudo naturally on Ω with respect to N if H acts transitively on Ω and if there exists a system of imprimitivity Δ for H on Ω such that $C_H(\Delta) = N$ and the action of H on Δ is isomorphic to the action of H on subsets of size t of Σ.

Def H acts essentially on Ω with respect to N if $C_H(\Omega) \leq N$.

Lemma 3.7 *Let H be a finite group and $N \trianglelefteq H$ with H/N perfect. Then there exists a unique subnormal subgroup R which is minimal with respect to $H = RN$.*

Proof The proof is by induction on $|H|$. We first remark that if such an R indeed exists then $R \trianglelefteq H$. For R^h would be a subnormal supplement to N in H for each $h \in H$. Hence, by uniqueness of R, we have $R \leq R^h$ for each $h \in H$, and therefore $R \trianglelefteq H$.

For the proof, suppose R_1 and R_2 are two minimal subnormal supplements to N in H. Let K_j be proper normal subgroups of H with $R_j \trianglelefteq\trianglelefteq K_j$ for $j = 1,2$. Then $H = K_1N = K_2N$ and, since H/N is perfect, $H = H'N$. Hence, since $K_j \trianglelefteq H$ for $j = 1,2$, we get

$$H = H'N = [K_1N, K_2N] = [K_1, K_2]N \tag{1}$$

Let $j \in \{1,2\}$. Then $N \trianglelefteq H$ and (1) implies $N \cap [K_1, K_2] \trianglelefteq [K_1, K_2]$ and $N \cap K_j \trianglelefteq K_j$. We also have

$$\frac{[K_1, K_2]}{[K_1, K_2] \cap N} \cong \frac{[K_1, K_2]N}{N} = \frac{H}{N}$$

and

$$\frac{K_j}{K_j \cap N} \cong \frac{K_jN}{N} = \frac{H}{N}.$$

Thus, both $[K_1, K_2]/[K_1, K_2] \cap N$ and $K_j/N \cap K_j$ are perfect. Since $[K_1, K_2]$ and K_j are proper subgroups of H, by induction on the $|H|$, there exists unique minimal subnormal supplements U and V for $[K_1, K_2] \cap N$ and $K_j \cap N$ in $[K_1, K_2]$ and K_j respectively. Hence we have

$$[K_1, K_2] = U([K_1, K_2] \cap N) \text{ and } K_j = V(K_j \cap N) \tag{2}$$

Also, since $[K_1, K_2] \leq K_j$ and $R_j \leq K_j$, (1) and (2) together imply

$$K_j = K_j \cap H = K_j \cap R_j N = (K_j \cap N) R_j$$

and

$$K_j = K_j \cap H = K_j \cap [K_1, K_2] N = (K_j \cap N)[K_1, K_2] = (K_j \cap N) U.$$

Thus, since $R_j \trianglelefteq\trianglelefteq K_j$ and $U \trianglelefteq\trianglelefteq [K_1, K_2] \trianglelefteq K_j$, by the uniqueness of V we get,

$$V \leq R_j \text{ and } V \leq U \tag{3}$$

But $H = K_j N = (K_j \cap N) V N = V N$ and $V \trianglelefteq\trianglelefteq K_j \trianglelefteq H$. Hence, by the minimality of R_j, we get $R_j = V \leq U$. Now (1) and (2) imply

$$H = [K_1, K_2] N = U([K_1, K_2] \cap N) N = UN. \tag{4}$$

Thus, as before, $N \trianglelefteq H$ implies $N \cap U \trianglelefteq U$ and $U/N \cap U$ is perfect. Thus, since $U < H$, by induction there exists a unique minimal subnormal supplement R for $U \cap N$ in U. Since $R_j \leq U$ and $H = R_j N$, we have $U = (U \cap N) R_j$, and therefore R_j is a supplement for $U \cap N$ in U. Moreover, $R_j \trianglelefteq\trianglelefteq H$ and $R_j \leq U$ implies $R_j \trianglelefteq\trianglelefteq U$. Thus $R \leq R_j$ by the uniqueness of R. Now $R \trianglelefteq\trianglelefteq U \trianglelefteq\trianglelefteq H$ and by (4),

$$H = UN = R(U \cap N) N = RN.$$

Therefore by the minimality of R_j, we get $R_j = R$. Since $j \in \{1, 2\}$ was chosen arbitrarily, we have $R_1 = R = R_2$ and the lemma is proven.

□

Lemma 3.8 *Let H be a finite group acting on a set Ω and N a proper normal subgroup of H such that H/N is perfect and simple. If R is the unique subnormal supplement to N in H, then an orbit $\mathcal{O}$ for H on Ω is essential with respect to N if and only if $\mathcal{O} \not\subseteq Fix(R)$.*

Proof First suppose $\mathcal{O}$ is an essential orbit for H on Ω. Then $C_H(\mathcal{O}) \leq N$. If $\mathcal{O} \subseteq \mathrm{Fix}(R)$, then $R \leq C_H(\mathcal{O}) \leq N$. Hence we get, $R \leq N$ and $H = RN = N$, a contradiction to the choice of N. Therefore $\mathcal{O} \not\subseteq \mathrm{Fix}(R)$. Conversely, suppose $\mathcal{O} \not\subseteq \mathrm{Fix}(R)$ for some orbit of H on Ω. Then, since $\mathcal{O}$ is H-invariant, $C_H(\mathcal{O}) \trianglelefteq H$. Hence, since H/N is simple, we have $C_H(\mathcal{O}) \leq N$ or $H = C_H(\mathcal{O})N$. If $H = C_H(\mathcal{O})N$ then $C_H(\mathcal{O})$ would be a subnormal supplement to N in H. Thus, by the uniqueness of R, we get $R \leq C_H(\mathcal{O})$ and $\mathcal{O} \subseteq \mathrm{Fix}(R)$, a contradiction. Therefore $C_H(\mathcal{O}) \leq N$ and $\mathcal{O}$ is essential.

□

Lemma 3.9 *Let T be a LFS-group with Kegel cover $\mathcal{K}$. If $\mathcal{K}$ is the union of finitely many subsets, $\mathcal{K} = \bigcup_{i=1}^{n} K_i$, then at least one of these subsets K_i is a Kegel cover for T.*

Proof Suppose the lemma is false. Then none of the K_i are Kegel covers for T. Thus, for each $1 \leq i \leq n$ there exists a finite subgroup L_i of T such that for every memeber (H, N) of K_i either $L_i \not\leq H$ or $L_i \leq H$ and $L_i \cap N \neq 1$. Let $L = \langle L_i | 1 \leq i \leq n \rangle$. Then since T is locally finite and L is finitely generated, $|L| < \infty$. Therefore there exists $(H, N) \in \mathcal{K}$, with $L \leq H$ and $L \cap N = 1$. But, since $(H, N) \in \mathcal{K} = \bigcup_{i=1}^{n} K_i$, there exists $1 \leq i \leq n$ with $(H, N) \in K_i$. Hence, we get $L_i \leq L \leq H$ and $L_i \cap N \leq L \cap N = 1$, a contradiction to the choice of L_i.

□

Lemma 3.10 *Let p be a prime, n an integer with $n > 4p$, and Ω a set of order n. If ϕ, $\theta \in Alt(\Omega) = A_n$ such that*

(a) $pdeg_{\Omega}(\phi)$, $pdeg_{\Omega}(\theta) \geq 4p$

and

(b) $\langle \phi, \theta \rangle$ is of type (p, p)

Then $C_{A_n}(\phi) \neq C_{A_n}(\theta)$.

Proof Suppose the lemma is false. Then $C_{A_n}(\phi) = C_{A_n}(\theta)$. Let

$$\phi = \phi_1\phi_2 \ldots \phi_r \text{ and } \theta = \theta_1\theta_2.....\theta_s$$

be the decompositions of ϕ and θ into the product of disjoint p-cycles where

$$\phi_k = (a_{k1}, a_{k2}, \ldots, a_{kp}) \text{ and } \theta_l = (b_{l1}, b_{l2}, \ldots, b_{lp})$$

for all $1 \leq k \leq r$ and $1 \leq l \leq s$. We claim that Supp(ϕ) = Supp(θ). First, suppose Supp(ϕ) $\cap$ Supp(θ) $= \emptyset$. Then if p is odd, let $\pi \in S_n$ be the permutation exchanging the orbits ϕ_1 and ϕ_2 of ϕ and $\sigma = \pi(b_{11}, b_{12})$. Then $\sigma \in A_n$ and $[\sigma, \phi] = 1$. But $[\sigma, \theta] \neq 1$ as $\theta^{\sigma}(b_{12}) = b_{11} \neq b_{13} = \theta(b_{12})$. Hence we get, $\sigma \in C_{A_n}(\phi) \setminus C_{A_n}(\theta)$, a contradiction. If $p = 2$, let $\pi \in S_n$ be the permutation exchanging the orbits ϕ_1 for ϕ_2 and $\sigma = \pi(b_{11}, b_{21})(b_{12}, b_{31})$. Then $\sigma \in A_n$ and $[\sigma, \phi] = 1$. But $[\sigma, \theta] \neq 1$ as

$\theta^\sigma(b_{11}) = b_{22} \neq b_{12} = \theta(b_{11})$. Thus, again we get a contradiction to the assumption that ϕ and θ have same centralizer in A_n. Therefore $\mathrm{Supp}(\phi) \cap \mathrm{Supp}(\theta) \neq \emptyset$.

Without loss of generality, let $a_{11} \in \mathrm{Supp}(\phi_1) \cap \mathrm{Supp}(\theta_1)$. Suppose there exists $1 \leq l \leq s$ with $\mathrm{Supp}(\theta_l) \cap \mathrm{Supp}(\phi) = \emptyset$. We may assume $l = 2$. Let $\sigma \in A_n$ be the permutation exchanging θ_1 for θ_2 and θ_3 for θ_4. Then $[\sigma, \theta] = 1$ but $\phi^\sigma \neq \phi$ as $\mathrm{Supp}(\theta_2) \cap \mathrm{Supp}(\phi) = \emptyset$ and $b_{22} \in \mathrm{Supp}(\phi^\sigma) \cap \mathrm{Supp}(\theta_2) \neq \emptyset$ and so $[\sigma, \phi] \neq 1$. Again we get a contradiction, therefore $\mathrm{Supp}(\theta_l) \cap \mathrm{Supp}(\phi) \neq \emptyset$ for all $1 \leq l \leq s$.

Now suppose $\mathrm{Supp}(\theta) \not\subseteq \mathrm{Supp}(\phi)$. Then there exists $1 \leq l \leq s$ with $\mathrm{Supp}(\theta_l) \not\subseteq \mathrm{Supp}(\phi)$. Assume $l = 2$ and let $b_{2i} \in \mathrm{Supp}(\theta_2) \setminus \mathrm{Supp}(\phi)$. Then from above we know that $\mathrm{Supp}(\theta_2)$ meets $\mathrm{Supp}(\phi)$. Without loss, assume $a_{3j} \in \mathrm{Supp}(\theta_2) \cap \mathrm{Supp}(\phi_3)$. Let $\sigma \in A_n$ be the permutation exchanging the orbits ϕ_1 for ϕ_2 and ϕ_3 for ϕ_4. Then $[\sigma, \phi] = 1$. But $[\sigma, \theta] = 1$ implies $\theta^\sigma = \theta$ and so θ_2^σ and θ_2 are two orbits of θ. Since $b_{2i} \in \mathrm{Supp}(\theta_2) \cap \mathrm{Supp}(\theta_2^\sigma)$ and orbits are either the same or disjoint, we have $\theta_2 = \theta_2^\sigma$. But σ does not centralize θ_2 as $\sigma(b_{2i}) = b_{2i}$ and $\sigma(a_{3j}) = a_{4j} \neq a_{3j}$. Thus we get, $[\sigma, \theta] \neq 1$, a contradiction. Therefore we have shown $\mathrm{Supp}(\theta) \subseteq \mathrm{Supp}(\phi)$. Now by the symmetry of this argument we get $\mathrm{Supp}(\phi) = \mathrm{Supp}(\theta)$.

Next we claim that two elements of the same orbit of ϕ cannot lie in different orbits of θ. First, assume p is odd and, without loss of generality, suppose $a_{11} \in \theta_1$ and $a_{13} \in \theta_2$. Then, since $\mathrm{Supp}(\phi) = \mathrm{Supp}(\theta)$ there exists $1 < k \leq r$ with $\mathrm{Supp}(\theta_1) \cap \mathrm{Supp}(\phi_k) \neq \emptyset$. Let $b_{1i} \in \mathrm{Supp}(\theta_1) \cap \mathrm{Supp}(\phi_k)$. Since p is odd, $\phi_1 \in A_n$ and $[\phi_1, \phi] = 1$. Now $\theta^{\phi_1} = \theta$ implies θ_1 and $\theta_1^{\phi_1}$ are two orbits of θ with $b_{1i} \in \mathrm{Supp}(\theta_1) \cap \mathrm{Supp}(\theta_1^{\phi_1})$. Hence, as before, we get $\theta_1^{\phi_1} = \theta_1$. But this is impossible as $a_{11}, b_{1i} \in \mathrm{Supp}(\theta_1)$ and ϕ_1 fixes b_{1i} but moves a_{11}. Thus ϕ_1 centralizes ϕ but not θ. On the other hand, suppose $p = 2$ and $a_{11} \in \theta_1$, and $a_{12} \in \theta_2$. Consider $\sigma = \phi_k \phi_{k'}$ for some $k' \notin \{1, k\}$. Then $\sigma \in A_n$ and $[\sigma, \phi] = 1$. But $[\sigma, \theta] \neq 1$, as $a_{11}, b_{1i} \in \theta_1$ and σ fixes a_{11} but moves b_{1i}.

Thus, in any case we can find an element of A_n that centralizes ϕ but not θ yeilding a contradiction to our original assumption.

Altogether we have shown $\mathrm{Supp}(\phi) = \mathrm{Supp}(\theta)$, ϕ and θ have the same orbits, and consequently, $r = s$. Without loss of generality we may assume $\mathrm{Supp}(\phi_i) = \mathrm{Supp}(\theta_i)$ for all $1 \le i \le r$. Next we claim that θ is actually a power of ϕ. If $p = 2$ then, since they have the same orbits, we get $\phi = \theta$. Thus, $|\langle \phi, \theta \rangle| = |\langle \phi \rangle| = p$, a contradiction to (b). Therefore from here on we may assume p is odd. Suppose a_{1i} is adjacent to a_{1j} in the orbit θ_1 of θ. Then p odd implies $\phi_1 \in A_n$. Moreover, $[\phi_1, \phi] = 1$ implies $[\phi_1, \theta] = 1$. Now, since ϕ_1 only acts on elements of θ_1, we have $[\phi_1, \theta_1] = [\phi_1, \theta] = 1$. Hence, a_{1i} adjacent to a_{1j} in θ_1 implies $a_{1i}^{\phi_1^m}$ is adjacent to $a_{1j}^{\phi_1^m}$ in θ_1 for all $1 \le m \le p-1$. Therefore $\theta_1 = \phi_1^{j-i}$. Similarly we can show $\theta_i = \phi_i^{l_i}$ for all $1 \le i \le r$. That is,

$$\theta = \phi_1^{l_1} \phi_2^{l_2} \dots \phi_r^{l_r}$$

Now let $\sigma \in A_n$ be the permutation exchanging the orbits ϕ_1 for ϕ_2 and ϕ_3 for ϕ_4. Then $[\sigma, \phi] = 1$ and so, by assumption, $[\sigma, \theta] = 1$. But then we get

$$\phi_1^{l_1} \phi_2^{l_2} \phi_3^{l_3} \phi_4^{l_4} \dots \phi_r^{l_r} = \phi_1^{l_2} \phi_2^{l_1} \phi_3^{l_4} \phi_4^{l_3} \dots \phi_r^{l_r}$$

and therefore $l_1 = l_2$ and $l_3 = l_4$. By the same argument applied several times we eventually get an integer l with $l_i = l$ for all $1 \le i \le r$. But then $\theta = \phi^l$ and $|\langle \phi, \theta \rangle| = |\langle \phi, \phi^l \rangle| = |\langle \phi \rangle| = p$. Hence, we get a contradiction to (b) and this proves the lemma.

$\square$

Now we remark that Lemma 3.3 (a) still holds for Kegel covers that have factors which are alternating groups and will be used throughout this case. Let $\mathcal{K} = \{(H_i, N_i) | i \in I\}$ be a Kegel cover for G with $H_i/N_i \cong Alt(\Omega_i) = A_{n_i}$, where $|\Omega_i| = n_i$. Then, by Lemmas 3.6 and 3.9, we may assume that $\mathcal{K} = \mathcal{K}(Z)$ and $\operatorname{pdeg}_{H_i/N_i}(z) \geq p^2(a+2)$ for all $(H_i, N_i) \in \mathcal{K}(Z)$, where $a = \max(l(u), 5uw(Z)|Z|^2, 9|Z|^4)$ and $u \geq (2\log_{4/3}|Z|) + 2$ from [7, 2.5 and 2.14]. Also, for any positive integer t let

$$\mathcal{K}_t(Z) = \{(H_i, N_i) \in \mathcal{K} | Z \text{ has at least } t \text{ regular orbits on } \Omega_i\}.$$

Proposition 3.11 *For any integer $t > 0$, $\mathcal{K}_t(Z)$ is a Kegel cover for G.*

We prove this by contradiction through a series of lemmas. Suppose there exists a positive integer t for which $\mathcal{K}_t(Z)$ is not a Kegel cover for G. Then, by Lemma 3.9, $\mathcal{K}(Z) \setminus \mathcal{K}_t(Z)$ is a Kegel cover for G. Without loss of generality we may assume $\mathcal{K} = \mathcal{K}(Z) \setminus \mathcal{K}_t(Z)$ and Z has less than t regular orbits on Ω_i for all $i \in I$.

Lemma 3.12 *Z has no regular orbits on Ω_i for all $i \in I$.*

Proof Since $\mathcal{K}$ is a Kegel cover, by embedding H_i into larger and larger H_j's, we can find $(H, N) \in \mathcal{K}$ such that $|H|/|Z| = r \geq t$. Then H has no regular orbits on Ω_k for any $k \in I$ and Ω_k on which H acts. For if $s \in \Omega_k$ with s^H a regular orbit for H, then $s^{h_i Z}$ would be a regular orbit for Z on Ω_k, where $\{h_i\}_{i=1}^r$ is a transversal for Z in H. Moreover, each of the $s^{h_i Z}$'s are distinct since cosets of Z in H are either equal or distinct. Hence, Z would have $r \geq t$ regular orbits on Ω_k, a contradiction to our assumption.

Thus, H has no regular orbits on Ω_k for all $k \in I$. Therefore, by [7, 3.4], there exists a Kegel cover $\mathcal{T} \subseteq \mathcal{K}$ such that whenever (H_l, N_l), $(H_m, N_m) \in \mathcal{T}$ with $H_l \leq H_m$, $H_l \cap N_m = 1$, every essential orbit of H_l on Ω_m is pseudo natural with respect to N_l. As before we may assume $\mathcal{K} = \mathcal{T}$.

Let $d = \max_{i \in I}\{$ number of regular orbits of Z on $\Omega_i\}$ and suppose $d > 0$. Let (H_i, N_i), $(H_j, N_j) \in \mathcal{K}$ such that Z has d regular orbits on Ω_i and $H_i \leq H_j$ and $H_i \cap N_j = 1$. If $\mathcal{O}$ is an essential orbit of H_i on Ω_j then $\mathcal{O}$ is pseudo natural with respect to N_i. Thus, there exists a system of imprimitivity Δ for H_i on $\mathcal{O}$ such that $C_{H_i}(\Delta) = N_i$ and the action of H_i on Δ is isomorphic to the action of H_i on Ω_i. Now Z has d regular orbits on Ω_i implies Z has d regular orbits on Δ.

Let $\{U_k\}_{k=1}^{d}$ be d members of Δ such that U_k^Z are regular orbits of Z on Δ. Let $1 \leq k \leq d$ and pick any $u_k \in U_k$. Then u_k^Z is a regular orbit of Z on Ω_j, otherwise there exists $1 \neq z \in Z$ with $u_k^z = u_k$ and consequently $u_k \in U_k \cap U_k^z$. But then, as Δ is a system of imprimitivity, we get $U_k = U_k^z$, contradicting the assumption that U_k^Z is a regular orbit of Z on Δ.

Thus Z has $\sum_{k=1}^{d} |U_k|$ regular orbits on Ω_j. Since d is the maximum number of regular orbits of Z on any Ω_l for any $l \in I$, we get $|U_k| = 1$ for each $1 \leq k \leq d$. Thus, we get

$$\mathcal{O} = \bigcup_{k=1}^{d} \{u_k\} \cup \bigcup_{\{u_k\} \neq U \in \Delta} U$$

where the above union is disjoint. Moreover, since H_i-orbits on Ω_j form a partition of Ω_j and d is maximal, we get $\mathcal{O}$ is the unique essential orbit of H_i on Ω_j. Since $H_i/N_i \cong \mathrm{Alt}(\Omega_i)$ is perfect, by Lemma 3.7, there exists a unique minimal subnormal supplement to N_i, R_i, in H_i. Then, by Lemma 3.8, $\mathcal{O}$ is the unique orbit of H_i on Ω_j on which R_i acts nontrivially. Therefore $\Omega_j \setminus \mathcal{O} \subseteq \mathrm{Fix}(R_i)$. Also, since $H_i/N_i \cong \mathrm{Alt}(\Omega_i)$, we have $\Omega_i \subseteq \mathrm{Fix}(N_i)$ and therefore $\Delta \subseteq \mathrm{Fix}(N_i)$, as the actions of H_i on Δ and H_i on Ω_i are isomorphic. Since $N_i \trianglelefteq H_i$, H_i leaves $\mathrm{Fix}(N_i)$ invariant. Thus, for any $k \in \{1, 2, ..., d\}$, we have $u_k \in \mathrm{Fix}(N_i)$ and

$$\mathcal{O} = \{u_k^{H_i}\} \subseteq \mathrm{Fix}(N_i).$$

Thus, since R_i acts trivially on all nonessential orbits and N_i acts trivially on the only essential orbit $\mathcal{O}$, we have $\Omega_j \subseteq \mathrm{Fix}(R_i \cap N_i)$ and therefore $R_i \cap N_i \leq N_j \cap H_i = 1$.

Now, since R_i and N_i are both normal subgroups of H_i, we have $[R_i, N_i] \leq R_i \cap N_i = 1$. Also, since $Z \cap N_i = 1$,

$$Z \cong \frac{Z}{N_i \cap Z} \cong \frac{ZN_i}{N_i} \leq \frac{H_i}{N_i} \cong A_{n_i}$$

and therefore a copy of Z sits inside of A_{n_i}. Moreover, we claim the centralizer property of Lemma 1.2 (b) for Z still holds inside A_{n_i}. That is, all elements of ZN_i/N_i have the same centralizer in A_{n_i}. To see this let $z \in Z$, $\overline{H_i} = H_i/N_i$, and $\overline{C_{H_i}(z)}$ be the image of $C_{H_i}(z)$ in $\overline{H_i}$. We claim that $C_{\overline{H_i}}(\overline{z}) = \overline{C_{H_i}(z)}$. Clearly $\overline{C_{H_i}(z)} \leq C_{\overline{H_i}}(\overline{z})$ and so to prove the claim its enough to show $C_{\overline{H_i}}(\overline{z}) \leq \overline{C_{H_i}(z)}$. Let $\overline{h} \in C_{\overline{H_i}}(\overline{z})$. Then, since $H_i = R_iN_i$, we have $h = rn$ for some $r \in R_i$ and $n \in N_i$. Thus, $\overline{h} = \overline{r}$ and $[\overline{r}, \overline{z}] = 1$. But then $[r, z] \in N_i$ and, since $R_i \trianglelefteq H_i$, we get $[r, z] \in R_i \cap N_i = 1$. Therefore $r \in C_{H_i}(z)$ and $\overline{h} = \overline{r} \in \overline{C_{H_i}(z)}$. Thus $C_{\overline{H_i}}(\overline{z}) \leq \overline{C_{H_i}(z)}$ and so we have shown $C_{\overline{H_i}}(\overline{z}) = \overline{C_{H_i}(z)}$. Now if $\overline{z_1}, \overline{z_2} \in \overline{Z}$, by Lemma 1.2 (b), we have

$$C_{\overline{H_i}}(\overline{z_1}) = \overline{C_{H_i}(z_1)} = \overline{C_{H_i}(z_2)} = C_{\overline{H_i}}(\overline{z_2})$$

Hence, all elements of $\overline{Z}$ have the same centralizer in $\overline{H_i}$, $\overline{H_i} \cong A_{n_i}$, and $\overline{Z}$ is of type (p,p). Now, since $\text{pdeg}_{H_i/N_i}(z) \geq 4p$ for all $1 \neq \overline{z} \in \overline{Z}$, we get a contradiction to Lemma 3.10 and this proves Lemma 3.12.

□

Now by Lemma 3.12 we know that Z has no regular orbits on Ω_i for all $i \in I$. Let $1 \neq z_1 \in Z$ and $(H_i, N_i) \in \mathcal{K}$ with $Z \leq H_i$, $Z \cap N_i = 1$, $H_i/N_i \cong \text{Alt}(\Omega_i)$. Since has no regular orbits on Ω_i, every element of Ω_i is fixed by at least one element of Z. Hence, we have

$$\text{Supp}(z_1) = \bigcup_{1 \neq z' \in Z} \text{Supp}(z_1) \cap \text{Fix}(z') \tag{1}$$

Since $|\text{Supp}(z_1)| \geq p^2(a+2)$, (1) implies there exists $z_2 \in Z$ with $|\text{Supp}(z_1) \cap \text{Fix}(z_2)| \geq a+2$. Now $z_2 \notin \langle z_1 \rangle$, otherwise we get $\text{Fix}(z_1) = \text{Fix}(z_2)$ and $\text{Supp}(z_1) \cap \text{Fix}(z_2) = \emptyset$, a contradiction. Therefore $Z = \langle z_1, z_2 \rangle$. Similarly we can find $1 \neq z_3 \in Z$ with $|\text{Supp}(z_2) \cap \text{Fix}(z_3)| \geq a+2$. Let

$$\Delta_1 = \text{Supp}(z_1) \cap \text{Fix}(z_2)$$

$$\Delta_2 = \text{Supp}(z_2) \cap \text{Fix}(z_3)$$

$$\Delta_3 = \Omega_i \setminus (\Delta_1 \cup \Delta_2)$$

Then by the definition of a we have $|\Delta_k| \geq a > 5$ for $k = 1, 2$. Let $A = \{g \in H_i | g \in N_{H_i}(\Delta_3)$ and g is even on $\Delta_1 \cup \Delta_2\}$. Then $A \leq H_i$. Moreover we claim $Z \leq A$. Since

Z is abelian, Z normalizes Δ_3. If p is odd, then all p-cycles are even. Hence z_1, $z_2 \in A$ and therefore $Z \leq A$. If $p = 2$ and $|\Delta_k| \equiv 0(\bmod 4)$ for all $k \in \{1, 2\}$ then again $Z \leq A$. On the other hand, if $p = 2$ and $|\Delta_k| \equiv 2(\bmod 4)$ for some $k \in \{1, 2\}$ we must modify the definition of Δ_k. In this case, we take one z_k-orbit out of Δ_k.

Let $A_k = C_A(\Delta_{3-k})$ and $B = A_1 \cap A_2$ for $k = 1, 2$. Then A_1 and A_2 normalize each other, $z_3 \in A_1$, $z_2 \in A_2$ and

$$A/B \cong \mathrm{Alt}(\Delta_1 \cup \Delta_2) \text{ and } A_k/B \cong \mathrm{Alt}(\Delta_k) \text{ for } k = 1, 2.$$

Thus, by Lemma 3.7, there exists a unique subnormal supplement R for B in A. Finally we let $A_1^* = \langle z_3^{A_1 A_2} \rangle$ and $A_2^* = \langle z_2^{A_1 A_2} \rangle$.

Lemma 3.13 *(a)* $A_2 = A_2^* B$.

(b) $Z \cap B = 1$.

(c) $\mathit{Supp}_{H_i/N_i}(z) \supseteq \Delta_1$ *or* Δ_2 *for all* $1 \neq z \in Z$.

Proof Since $A_2^* \trianglelefteq A_2$ and $A_2/B \cong \mathrm{Alt}(\Delta_2)$ is simple, either $A_2^* \leq B$ or $A_2 = A_2^* B$. If $A_2^* \leq B$ then $z_2 \in B$ as $z_2 \in A_2^*$. But $B = A_1 \cap A_2$ implies $z_2 \in A_1 = C_A(\Delta_2)$, a contradiction as $\Delta_2 \subseteq \mathrm{Supp}(z_2)$. Therefore $A_2 = A_2^* B$ and we have (a).

For (b), let $z \in Z \cap B$. Since $Z = \langle z_1, z_2 \rangle$, we have $z = z_1^m z_2^n$ for some $1 \leq m, n \leq p$. Let $s \in \Delta_1$. Then $z \in B = A_1 \cap A_2$ implies $z(s) = s$ and so $z_1^m z_2^n(s) = s$. Since Z is abelian and $z_2(s) = s$, we have $z_1^m(s) = s$. But $s \in \mathrm{Supp}(z_1)$ implies $m = p$ and therefore $z = z_2^n$. Let $s \in \Delta_2$. Then again $z \in B$ implies $z_2^n(s) = s$ and $n = p$. Thus, $z = z_1^m z_2^m = 1$.

Finally for (c), let $1 \neq z \in Z$ and suppose $\Delta_1 \not\subseteq \mathrm{Supp}(z)$. Then $z = z_1^m z_2^n$ for some $1 \leq m, n \leq p$ and there exists $s \in (\Delta_1 \setminus \mathrm{Supp}(z))$. Hence $z(s) = s$ and, as before, we get $z_1^m(s) = s$ and $m = p$. Therefore $z = z_2^n$ and $z \neq 1$ implies $n \neq p$. Thus $\mathrm{Supp}(z) \supseteq \Delta_2$ and we are done.

□

Let $(H_j, N_j) \in \mathcal{K}$ with $A \leq H_j$, $A \cap N_j = 1$, and $H_j/N_j \cong Alt(\Omega_j)$.

Lemma 3.14 *Let $(H_j, N_j) \in \mathcal{K}$ and $\overline{H_j}$ be as above. Then $[A_1^*, A_2^*] \leq C_A(\mathcal{O})$ for all essential orbits $\mathcal{O}$ of A on Ω_j.*

Proof First, let $\overline{A} = A/C_A(\mathcal{O})$. Then, since $\mathcal{O}$ is essential for A, we have $C_A(\mathcal{O}) \leq B$. Thus $A \cap N_j = B \cap N_j = 1$ implies

$$\frac{\overline{A}}{\overline{B}} = \frac{AN_j/N_j}{BN_j/N_j} \cong \frac{A/A \cap N_j}{B/B \cap N_j} \cong \frac{A}{B} \cong \mathrm{Alt}(\Delta_1 \cup \Delta_2)$$

Therefore $\overline{A} \leq \mathrm{Sym}(\mathcal{O})$, $\overline{B} \trianglelefteq \overline{A}$, $\overline{A}/\overline{B} \cong \mathrm{Alt}(\Delta_1 \cup \Delta_2)$, $|\Delta_1 \cup \Delta_2| \geq 5$, $\overline{Z} \cap \overline{B} = 1$, $\mathrm{pdeg}_{\overline{A}/\overline{B}}(\overline{z}) \geq a$ for all $1 \neq \overline{z} \in \overline{Z}$ and $\overline{Z}$ has no regular orbits on $\mathcal{O}$. Thus, by [7, 2.14], $\mathcal{O}$ is t-pseudo natural for $t \leq |\overline{Z}| - 2$.

Let $P_t(\Delta_1 \cup \Delta_2)$ denote the set of subsets of size t of $\Delta_1 \cup \Delta_2$ and Γ be a set of imprimitvity for $\overline{A}$ on $\mathcal{O}$ such that Γ and $P_t(\Delta_1 \cup \Delta_2)$ are isomorphic as $\overline{A}$-sets.

We claim that $t = 1$. To prove this we proceed by contradiction. Suppose $t \geq 2$. Let $a_k \in \Delta_k$ and $X_k = a_k^Z$ for $k = 1, 2$. Also, let $X \subseteq \Delta_1 \cup \Delta_2$ such that $|X| = t$ and $X \cap X_k = \{a_k\}$ for $k = 1, 2$. We can find such a set X since the order of $\Delta_1 \cup \Delta_2$ is large compared to t. That is, since $t \leq p^2 - 2$ and $|X_k| \leq p^2$, we have $|\Delta_1 \cup \Delta_2| \geq 3p^2 - 4 = p^2 - 2 + 2p^2 - 2 \geq t + 2p^2 - 2$ and so $|\Delta_1 \cup \Delta_2| - (|X_1 \cup X_2|) \geq |\Delta_1 \cup \Delta_2| - 2p^2 \geq t - 2$.

Now Z has no regular orbits on $\mathcal{O}$ implies Z has no regular orbits on Γ. Hence, since Γ and $P_t(\Delta_1 \cup \Delta_2)$ are isomorphic as $\overline{A}$-sets, Z has no regular orbits on $P_t(\Delta_1 \cup$

Δ_2). Therefore there exists $1 \neq z \in Z$ with $X^z = X$. If $a_k^z \neq a_k$ for some $k \in \{1,2\}$, we get a_k, $a_k^z \in X \cap X_k$, a contradiction as $|X \cap X_k| = 1$. Thus, $a_k^z = a_k$ for $k = 1,2$. But, by Lemma 3.27, $\mathrm{Supp}(z) \supseteq \Delta_1$ or Δ_2 and so z cannot fix both a_1 and a_2. Thus, it must be the case that $t = 1$.

Since $t = 1$, we know that Γ and $\Delta_1 \cup \Delta_2$ are isomorphic as $\overline{A}$-sets. Let $i \in \{1,2\}$ and $\Gamma = \Gamma_1 \cup \Gamma_2$ where Γ_i are the images of Δ_i under this isomorphism. Also for $i \in \{1,2\}$, let $Y_i = \bigcup_{X \in \Gamma_i} X$, and $y \in Y_i$ with $y \in X$ for $X \in \Gamma_i$. Since Z has no regular orbits on Ω_j there exists $1 \neq z \in Z$ with $y^z = y$. But then $X^z = X$, otherwise $X^z \neq X$ and we get $y = y^z \in X^z \cap X = \emptyset$, a contradcition as Γ is a system of imprimitivity. But then, since $X \in \Gamma_i$ and Γ_i and Δ_i are isomorphic as $\overline{A}$-sets, we have $X^{z_{i+1}} = X$ but $X^Z \neq X$. Therefore $\langle z_{i+1} \rangle = \langle z \rangle$ and so $y^{z_{i+1}} = y$. Thus, z_{i+1} fixes all elements of Y_i.

Now, since A_1 and A_2 normalize Y_i, $A_{3-i}^* = \langle z_{i+1}^{A_1 A_2} \rangle$ fixes all elements of Y_i and so $[A_1^*, A_2^*]$ fixes all elements of Y_i for $i = 1,2$. Therefore $[A_1^*, A_2^*]$ fixes $\mathcal{O}$ and this proves the lemma.

□

If $A_2^* \cap R = 1$, then $[A_2 \cap R, A_2^*] \leq A_2^* \cap R = 1$ and so $[A_2 \cap R, A_2^*] = 1$. Then, since $A_2 = (A_2 \cap R)B = A_2^* B$, we get $[(A_2 \cap R)B, A_2^* B] \leq B$ and $[A_2, A_2] \leq B$. Therefore A_2/B is abelian, a contradiction as $A_2/B \cong \mathrm{Alt}(\Delta_2)$ is nonabelian. Thus, $A_2^* \cap R \neq 1$.

Now by Lemma 3.14, $[A_1^*, A_2^* \cap R]$ fixes every essential orbit of A on Ω_j. Also R fixes all nonessential orbits of A on Ω_j. Hence $[A_1^*, A_2^* \cap R]$ fixes all orbits of A on Ω_j and therefore $[A_1^*, A_2^* \cap R]$ fixes all of Ω_j. But then $[A_1^*, A_2^* \cap R] \leq H_i \cap N_j = 1$ and so $[A_1^*, A_2^* \cap R] = 1$. Since $z_3 \in A_1^*$ and all elements of Z have the same centralizer in H_i, we have $[z_3, A_2^* \cap R] = 1$ and $[z_2, A_2^* \cap R] = 1$. Hence, $[A_2^*, A_2^* \cap R] = 1$ as A_1 and A_2 normalize $A_2^* \cap R$. Now $[A_2 \cap R, A_2^*] \leq A_2^* \cap R$ implies $[A_2 \cap R, A_2^*, A_2^*] = 1$. But then, as before, we have $[(A_2 \cap R)B, A_2^*B, A_2^*B] \leq B$ and $[A_2, A_2, A_2] \leq B$. Thus, we get $A_2/B \cong \mathrm{Alt}(\Delta_2)$ is nilpotent, a contradiction as $|\Delta_2| \geq 5$. This proves Proposition 3.11.

$\square$

Now we may assume $\mathcal{K} = \mathcal{K}_4(Z)$ and so Z has at least four regular orbits on Ω_i for all $i \in I$. Let $(H_i, N_i) \in \mathcal{K}$, with $Z \leq H_i$, $Z \cap N_i = 1$, and $H_i/N_i \cong A_{n_i} = \mathrm{Alt}(\Omega_i)$. Also let $\Omega_{\mathrm{reg}} = \bigcup_{k=1}^{4} \mathcal{O}_k$ where $\mathcal{O}_k$ is a regular orbit for Z on Ω_i. Finally let $|\Omega_{\mathrm{reg}}| = r$ and put

$$H^* = \{h \in H_i | h \in N_{H_i}(\Omega_{\mathrm{reg}}) \text{ and } h \text{ is even on } \Omega_{\mathrm{reg}}\}$$

and

$$N^* = C_{H_i}(\Omega_{\mathrm{reg}})$$

Then, since Z is a semiregular acting subgroup of $\mathrm{Sym}(\Omega_{\mathrm{reg}})$ of type (p,p), we have $Z \leq H^*$. Moreover, $Z \cap N^* = 1$ and $H^*/N^* \cong \mathrm{Alt}(\Omega_{\mathrm{reg}}) = A_r$. Thus, A_r contains a copy of Z and, since Z acts semiregularly on Ω_{reg}, $r = 4p^2 > 5$ and therefore A_r is simple. Now choose $K \leq H^*$ minimal with respect to $Z \leq K$ and $H^* = KN^*$ and let $L = N^* \cap K$.

Lemma 3.15 *(a) $Z \leq K$ and $Z \cap L = 1$.*

(b) $K/L \cong A_r$.

(c) L is maximal with respect to being normal in K.

(d) If $Z \leq U \leq K$ and $K = UL$, then $K = U$.

Proof By definition of K we have $Z \leq K$. Also, $Z \cap L = Z \cap (N^* \cap K) \leq Z \cap N^* = 1$ and so we have (a). For (b), we have

$$\frac{K}{L} = \frac{K}{N^* \cap K} \cong \frac{KN^*}{N^*} = \frac{H^*}{N^*} \cong A_r$$

For (c), suppose $L \leq K_0 \trianglelefteq K$. Since $K/L \cong A_r$ is simple, we have either $K_0 \leq L$ or $K = K_0$ and so we have (c).

Finally for (d), $K = UL$ implies

$$H^* = KN^* = ULN^* = UN^*.$$

Hence, $H^* = UN^*$ and, since $Z \leq U \leq K$, we get $K = U$ by the minimality of K.

$\square$

Lemma 3.16 *(a) If $U \trianglelefteq K$, then either $U \leq L$ or $K = UZ$.*

(b) $O_p(K) \leq L$.

(c) $K = \langle Z^K \rangle$.

(d) Let $\overline{K} = K/O_p(K)$ and $\overline{L}$ be the image of L in $\overline{K}$. Then $\overline{L}$ is a p'-group and $\overline{L} = \Phi(\overline{K})$.

(e) K' is the unique subnormal supplement for L in K.

(f) $K' = O^p(K')$.

Proof Suppose $U \trianglelefteq K$. Then $L \leq UL \trianglelefteq K$ and so $L = UM$ or $K = UL$, by the maximality of L. If $L = UL$ then $U \leq L$. On the other hand, $K = UL$ implies

$K = UZL$. Moreover, $Z \leq UZ$ and $UZ \not\leq L$. Hence, by Lemma 3.15 (d), we have $K = UZ$ and this proves (a).

Now $O_p(K) \trianglelefteq K$, and so by (a) either $O_p(K) \leq L$ or $K = O_p(K)Z$. But $K = O_p(K)Z$ implies K is a p-group and consequently $A_r \cong K/L$ is a p-group, a contradiction. Thus $O_p(K) \leq L$ and we have (b).

Since $\langle Z^K \rangle \trianglelefteq K$ and $Z \cap L = 1$, by (a) we have $K = Z\langle Z^K \rangle = \langle Z^K \rangle$, which implies (c).

For (d) let $Z \leq T_0 \in \mathrm{Syl}_p(K)$. Then, since $L \trianglelefteq K$, $T = T_0 \cap L \in \mathrm{Syl}_p(L)$ and by the Frattini Argument $K = N_K(T)L$. Now $Z \leq T_0$ and $L \trianglelefteq K$ implies Z normalizes $T = T_0 \cap L$ and so $Z \leq N_K(T)$. Thus, by Lemma 3.15 (d), $K = N_K(T)$ and therefore $T \trianglelefteq K$. But then $T \leq O_p(K)$ and $\overline{T} = 1$. Now $T \in \mathrm{Syl}_p(L)$ implies $1 = \overline{T} \in \mathrm{Syl}_p(\overline{L})$ and therefore $\overline{L}$ is a p'-group. Suppose $\overline{L} \not\leq \Phi(\overline{K})$. Then there exists a maximal subgroup $\overline{U} = U/O_p(K)$ of $\overline{K}$ with $\overline{L} \not\leq \overline{U}$. Since $\overline{U}$ is a maximal subgroup of $\overline{K}$, $\overline{K} = \overline{UL}$. Also, since $\overline{L}$ is a p'-group, $\overline{U}$ contains a Sylow p-subgroup of $\overline{K}$ and so $\overline{Z} \leq \overline{U}^{\overline{k}}$ for some $\overline{k} \in \overline{K}$. Then $\overline{K} = \overline{U}^{\overline{k}}\overline{L}$ and therefore $K = U^k L$ with $Z \leq U^k$. Hence, by Lemma 3.15 (d), we get $K = U^k$. Thus we get $\overline{K} = \overline{U}^{\overline{k}} = \overline{U}$, a contradiction to the maximality of $\overline{U}$. Therefore $\overline{L} \leq \Phi(\overline{K})$. Let $\Phi(\overline{K}) = R/O_p(K)$. Then $\overline{L} \leq \Phi(\overline{K}) \trianglelefteq \overline{K}$ implies $L \leq R \trianglelefteq K$. Thus either $K = R$ or $L = R$ by the maximality of L. If $K = R$ we get, $\overline{K} = \overline{R} = \Phi(\overline{K})$, a contradiction. Therefore $L = R$ and $\overline{L} = \Phi(\overline{K})$ as claimed.

For (e), since $K/L \cong A_r$ is simple, by Lemma 3.7 there exists a unique minimal subnormal supplement K_0 for L in K. Since $K' \trianglelefteq K$ we have $L \leq K'L \trianglelefteq K$ and so either $K = K'L$ or $K' \leq L$ by the maximality of L. Now $K' \leq L$ implies $A_r \cong K/L$ is abelian, a contradiction. Therefore it must be the case that $K = K'L$ and so $K_0 \leq K'$, as K' is a subnormal supplement for L in K. Now $K_0 \not\leq L$ and so by (a) we have $K = K_0 Z$. But then

$$\frac{K}{K_0} = \frac{K_0 Z}{K_0} \cong \frac{Z}{Z \cap K_0} \text{ is abelian.}$$

Hence $K' \leq K_0$ and so $K' = K_0$ is the unique subnormal supplement for L in K.

Finally for (f), its clear that $O^p(K') \leq K'$. Also since $O^p(K')$ char $\leq K' \trianglelefteq K$ we have $O^p(K') \trianglelefteq K$. Thus $O^p(K') \leq L$ or $K = O^p(K')L$ by the maximality of L. Suppose $O^p(K') \leq L$ and let $Q \in \mathrm{Syl}_q(K')$ for some $q \neq p$. Then $Q \leq O^p(K') \leq L$ and therefore $Q \leq L$. Let $\overline{K} = K/L$, and $\overline{K'}$ and $\overline{Q}$ be the images of K' and Q in $\overline{K}$. Then $\overline{Q} = 1$ and so $Q \in \mathrm{Syl}_q(K')$ implies $1 = \overline{Q} \in \mathrm{Syl}_p(\overline{K'})$. But K' is a supplement for L in K by (d) and so $\overline{K'} = \overline{K}$. Hence $1 = \overline{Q} \in \mathrm{Syl}_p(\overline{K})$ and therefore $\overline{K}$ is a q'-group for all $q \neq p$. But this implies $\overline{K} = K/L \cong A_r$ is a p-group, an impossibility. Therefore $K = O^p(K')L$ and so $K' = O^p(K')$ by (e).

□

In Lemmas 3.17 through 3.21, F will be a finite field, T a finite group, and V and E a finite dimensional FT-modules.

Def Let $\sigma \in \mathrm{Aut}(F)$. Then a map s from $V \times V$ to E is called F σ-sesquilinear if

(a) $s(u + v, w) = s(u, w) + s(v, w)$

(b) $s(u, v + w) = s(u, v) + s(u, w)$

(c) $s(\lambda u, v) = \lambda s(u, v)$

(d) $s(u, \lambda v) = \lambda^\sigma s(u, v)$

Def A F σ-sesquilinear map s from $V \times V$ to E is called T-invariant if $s(u, v)^t = s(u^t, v^t)$ for all $u, v \in V$ and $t \in T$. for all u, v, $w \in V$ and $\lambda \in F$.

Lemma 3.17 *Let F be a finite field, T a finite group, V and E be finite dimensional FT-modules, and s be a T-invariant F σ-sesquilinear map from $V \times V$ to E where $\sigma \in Aut(F)$ with $\sigma^2 = 1$. Also let $C = \{t \in T | t$ is a scalar on $V\}$, $|T|/|C| = m$, and $dim_F E = n$. Then for any subspace W of V there exists a subspace X of W with*

$$dim_F X \geq (dim_F W - 4\frac{4^{mn}-1}{3})/4^{mn}$$

and $s\,|_{U \times U} = 0$ where $U = \langle X^T \rangle$.

Proof Let $L = \{t_i\}_{i=1}^m$ be a transversal for C in T, i.e $T = \bigcup_{i=1}^m t_i C$, and $\{\phi_j\}_{j=1}^n$ be a basis for E^*. Define a map s^{ij} from $V \times V$ to F by

$$s^{ij}(u,v) = \phi_j s(u, v^{t_i}) \text{ for all } u, v \in V$$

Then, since s is F σ-sesquilinear and ϕ_j and t_i are are F-linear, s^{ij} is F σ-sesquilinear. Consider s^{11} on W. By [7, 2.1] there exists a subspace X_1 of W with $s^{11}\,|_{X_1 \times X_1} = 0$ and $\dim_F X_1 \geq \frac{1}{4}(\dim_F W - 4)$. Similarly there exists a subspace $X_2 \subseteq X_1$ with $s^{12}\,|_{X_2 \times X_2} = 0$ and

$$\dim_F X_2 \geq \frac{1}{4}(\dim_F X_1 - 4) \geq \frac{1}{4^2}(\dim_F W - 4 - 4^2)$$

By continuing this process we eventually get a subspace $X_n \subseteq X_{n-1}$ with $s^{1n}\,|_{X_n \times X_n} = 0$ and

$$\dim_F X_n \geq \frac{1}{4^n}(\dim_F W - 4\sum_{k=0}^{n-1} 4^k).$$

Next we look at s^{21} on X_n. Again, by [7, 2.1], there exists a subspace $X_{n+1} \subseteq X_n$ with $s^{21} |_{X_{n+1} \times X_{n+1}} = 0$ and $\dim_F X_{n+1} \geq \frac{1}{4^{n+1}}(\dim_F W - 4\sum_{k=0}^{n} 4^k)$. Eventually we get $X_{2n} \subseteq X_{2n-1}$ with $s^{2n} |_{X_{2n} \times X_{2n}} = 0$ and $\dim_F X_{2n} \geq \frac{1}{4^{2n}}(\dim_F W - 4\sum_{k=0}^{2n-1} 4^k)$.

Continuing this process for each $1 \leq i \leq m$ we get a subspace $X_{mn} \subseteq X_{mn-1}$ with $s^{mn} |_{X_{mn} \times X_{mn}} = 0$ and

$$\dim_F X_{mn} \geq \frac{1}{4^{mn}}(\dim_F W - 4\sum_{k=0}^{mn-1} 4^k) = (\dim_F W - 4\frac{4^{mn}-1}{3})/4^{mn}.$$

Now $X_{mn} \subseteq X_{ij}$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$ and so $s^{ij} |_{X_{mn} \times X_{mn}} = 0$ for each i and j. Let $u,v \in X_{mn}$, $i \in \{1,2,\ldots,m\}$ and $j \in \{1,2,\ldots,n\}$. Then $s^{ij}(u,v) = 0$ implies $\phi_j s(u, v^{t_i}) = 0$. Since $i \in \{1,2,\ldots,m\}$ was chosen arbitrarily and $\langle X_{mn}^T \rangle = \langle X_{mn}^L \rangle$, we get $\phi_j s(u,v) = 0$ for all $u \in X_{mn}$ and $v \in \langle X_{mn}^T \rangle$. Now as $\{\phi_j\}_{j=1}^n$ is a basis for E^* and $j \in \{1,2,\ldots,n\}$ was chosen arbitrarily we get $s(u,v) = 0$ for all $u \in X_{mn}$ and $v \in \langle X_{mn}^T \rangle$. But then $s(u,v) = 0$ for $u,v \in \langle X_{mn}^T \rangle$ as s is T-invariant.

□

<u>Def</u> Suppose s is a F σ-sesquilinear map from $V \times V$ to E. A subspace $U \leq V$ is called isotropic if $s |_{U \times U} = 0$.

Lemma 3.18 *Let V, E, F, T, C, m, n, s, and σ be as in Lemma 3.17. Then there exists a increasing function f, defined on the positive integers with the following property: for every subspace $W \leq V$ with $\dim_F W \geq f(mn)$ there exists $0 \neq w \in W$ such that $\langle w^T \rangle$ is isotropic.*

Proof Let $f(x) = 4^x + 4\frac{4^x-1}{3}$ and let $W \leq V$ with $\dim_F W \geq f(mn)$. Then by Lemma 3.17 there exists a subspace $X \leq W$ with $\langle X^T \rangle$ isotropic and

$$\begin{aligned} \dim_F X &\geq \frac{1}{4^{mn}}(\dim_F W - 4\frac{4^{mn}-1}{3}) \\ &\geq \frac{1}{4^{mn}}(4^{mn} + 4\frac{4^{mn}-1}{3} - 4\frac{4^{mn}-1}{3}) \\ &= 1 \end{aligned}$$

Thus, $\dim_F X \geq 1$ and in particular $X \neq 0$. Let $0 \neq w \in X \subseteq W$. Then $\langle X^T \rangle$ is isotropic implies $\langle w^T \rangle$ is isotropic as desired.

□

Lemma 3.19 *Let V, E, F, n, and s be as in Lemma 3.17. If $W \leq V$ is a subspace of V and*

$$W^{\perp} = \{v \in V | s(v,w) = s(w,v) = 0 \textit{ for all } w \in W\}$$

then $dim_F V/W^{\perp} \leq 2n \cdot dim_F W$.

Proof Define the map:

$$\alpha : V \to \mathrm{Hom}_F(W, E)$$

by $\alpha(v)(w) = s(v,w)$ for all $v \in V$ and $w \in W$. Then, since s is linear in its first coordinate, α is a F-linear map. Moreover, Kern $\alpha = \{v \in V | s(v,w) = 0$ for all $w \in W\}$ and

$$\dim_F V/\mathrm{Kern}\ \alpha \leq \dim_F \alpha(V) \leq \dim_F \mathrm{Hom}_F(W,E) = n \cdot \dim_F W.$$

Similarly define a map:

$$\beta : V \to \mathrm{Hom}_F(W, E)$$

by $\beta(v)(w) = s(w, v)$ for all $v \in V$ and $w \in W$. Then, as above, we get Kern $\beta =$ $\{v \in V | s(w, v) = 0$ for all $w \in W\}$ and $\dim_F V/\mathrm{Kern}\ \beta \leq n \cdot \dim_F W$. Thus, $W^\perp =$ Kern $\alpha \cap$ Kern β and,

$$\begin{aligned}
\dim V/W^\perp &= \dim_F(\mathrm{Kern}\ \alpha + \mathrm{Kern}\ \beta) + \dim_F V - \dim_F \mathrm{Kern}\ \alpha - \dim_F \mathrm{Kern}\ \beta \\
&\leq \dim_F V - \dim_F \mathrm{Kern}\ \alpha + \dim_F V - \dim_F \mathrm{Kern}\ \beta \\
&= \dim_F V/\mathrm{Kern}\ \alpha + \dim_F V/\mathrm{Kern}\ \beta \\
&\leq 2n \cdot \dim_F W
\end{aligned}$$

and the lemma is proved.

□

Lemma 3.20 *Let V, E, F, T, C, m, n, s, and σ be as in Lemma 3.17, f be as in Lemma 3.18, and $\mathcal{S} = \{W \leq V | W$ is a T-invariant, isotropic subspace of $V\}$. Then*

(a) If U is a maximal element of $\mathcal{S}$ then $\dim_F U > \frac{1}{2n+1}(\dim_F V - f(mn))$.

(b) If $\dim_F V \geq (2n+1)2mn + f(mn)$ and $x \in T$ with $pdeg_V(x) > f(mn)$ then there exists $U \in \mathcal{S}$ such that x does not act as a scalar on U.

Proof Since 0, the zero subspace, is in $\mathcal{S}$ we have $\mathcal{S} \neq \emptyset$. Let U be a maximal element of $\mathcal{S}$ and $U^\perp = \{v \in V | s(v, u) = s(u, v) = 0$ for all $u \in U\}$. Since U is isotropic, $U \leq U^\perp$ and $U^\perp/U$ is T-invariant. Moreover, by definition of $U^\perp$, s on

$U^\perp/U \times U^\perp/U$ is well defined. Hence, as $U \in \mathcal{S}$ is maximal, $U^\perp/U$ has no nontrivial isotropic T-invariant subspaces. Therefore, by lemma 3.18

$$\dim_F U^\perp/U < f(\widehat{m}n)$$

where

$$\widehat{m} = |T|/|\{t \in T | t \text{ is a scalar on } U^\perp/U\}|.$$

But, since f is an increasing function and $\widehat{m} \leq m$, we have $\dim_F U^\perp/U < f(\widehat{m}n) \leq f(mn)$. Furthermore, by Lemma 3.19, $\mathrm{Codim}_F U^\perp \leq 2n \cdot \dim_F U$. Thus,

$$\dim_F V = \dim_F V/U^\perp + \dim_F U^\perp/U + \dim_F U < 2n \cdot \dim_F U + f(mn) + \dim_F U \quad .$$

Therefore $\dim_F U > \frac{1}{2n+1}(\dim_F V - f(mn))$ and (a) holds.

We show (b) by contradiction. Suppose x is a scalar on all elements of $\mathcal{S}$. Let X and Y be maximal elements of $\mathcal{S}$, $L = \{t_i\}_{i=1}^m$ be a transversal for C in T, $0 \neq y \in Y$, and $W = \langle y^T \rangle$. Since $W = \langle y^T \rangle = \langle \{y^{t_i}\}_{i=1}^m \rangle$, W is spanned by the m vectors $\{y^{t_i}\}_{i=1}^m$ and so $\dim_F W \leq m$. Also as $X \in \mathcal{S}$ maximal, (a) implies

$$\dim_F X > \frac{1}{2n+1}(\dim_F V - f(mn)) \geq \frac{1}{2n+1}((2n+1)2mn + f(mn) - f(mn)) = 2mn. \tag{1}$$

and so $\dim_F X > 2mn$. But then, by Lemma 3.19, we get

$$\dim_F \frac{X}{X \cap W^\perp} = \dim_F \frac{X + W^\perp}{W^\perp} \leq \dim_F \frac{V}{W^\perp} \leq 2n \cdot \dim_F W \leq 2mn. \tag{2}$$

Thus, (1) and (2) imply $X \cap W^{\perp} \neq 0$. Now $X \cap W^{\perp} + W$ is a T-invariant isotropic subspace of V different from X and Y and Therefore $(X \cap W^{\perp}) + W \in \mathcal{S}$ and x acts as the same scalar on $(X \cap W^{\perp}) + W$, X, and Y. Since the choice of X, $Y \in \mathcal{S}$ was arbitrary, x acts as a scalar on all of $\langle \mathcal{S} \rangle$. Let $x(v) = \lambda v$ for all $v \in \langle \mathcal{S} \rangle$ and $V = \langle \mathcal{S} \rangle \oplus D$ for some subspace D of V. Then D has no T-invariant isotropic subspaces and so by Lemma 3.18 $\dim_F D < f(mn)$. Now consider the map $\lambda^{-1}x$ from V onto $[V, \lambda^{-1}x]$. Since $\langle \mathcal{S} \rangle \subseteq \mathrm{Kern}(\lambda^{-1}x)$ we get,

$$\mathrm{pdeg}_V(x) \leq \dim_F[V, \lambda^{-1}x] = \dim_F V/\mathrm{Kern}(\lambda^{-1}x) \leq \dim_F V/\langle \mathcal{S} \rangle = \dim_F D < f(mn)$$

a contradiction as $\mathrm{pdeg}_V(x) > f(mn)$ by assumption. This proves the lemma.

$\square$

Lemma 3.21 *Let V be a n-dimensinal vector space over a field F with $\mathrm{char}F = p$ for some prime p. Then for any p-subgroup P of $GL_F(V)$*

$$\dim_F V \leq |P| \ \dim_F C_V(P)$$

and in particular

$$\dim_F V \leq |P| \ \dim_F V/[V, P]$$

Proof For the proof we use induction on $|P| \cdot \dim_F V$. For $|P| \cdot \dim_F V = 1$ then both $|P|$ and $\dim_F V$ are equal to 1 and the result only states $1 \leq 1$ which is true. Assume the result holds for all vector spaces U over F and p-subgroups T of $GL_F(U)$ with $|T| \cdot \dim_F U < |P| \cdot \dim_F V$.

Then we can assume that V is indecomposable. For suppose $V = U \oplus W$ for some P-invariant subspaces U and W. Let $\overline{P} = P/C_P(U)$ and $\widehat{P} = P/C_P(W)$. Then the p-groups $\overline{P}$ and $\widehat{P}$ act on U and W respectively. Thus, by induction we get

$$\begin{aligned} \dim_F U &\leq \dim_F C_U(\overline{P}) \cdot |\overline{P}| \\ \dim_F W &\leq \dim_F C_W(\widehat{P}) \cdot |\widehat{P}| \end{aligned}$$

Now $V = U \oplus W$ implies $C_V(P) = C_U(\overline{P}) \oplus C_W(\widehat{P})$. Therefore we get,

$$\begin{aligned} \dim_F V = \dim_F U + \dim_F W &\leq \dim_F C_U(\overline{P}) \cdot |\overline{P}| + \dim_F C_W(\widehat{P}) \cdot |\widehat{P}| \\ &\leq \dim_F C_U(\overline{P}) \cdot |P| + \dim_F C_W(\widehat{P}) \cdot |P| \\ &= (\dim_F C_U(\overline{P}) + \dim_F C_W(\widehat{P}))|P| \\ &= \dim_F C_V(P)|P| \end{aligned}$$

as desired.

Let Q be a maximal subgroup of P and assume $Q \neq 1$. Then $Q \trianglelefteq P$ and $|P/Q| < |P|$. Now, since Q is a maximal subgroup of P, we have $C_{C_V(Q)}(P/Q) \leq C_V(P)$. Thus, since P/Q acts on $C_V(Q)$, by induction have

$$\dim_F C_V(Q) \leq |P/Q| \dim_F C_{C_V(Q)}(P/Q).$$

Also, by induction applied to Q on V, we get

$$\dim_F V \leq |Q| \dim_F C_V(Q).$$

But then

$$\dim_F V \leq |Q| \dim_F C_V(Q) \quad \leq \quad |Q|(\frac{|P|}{|Q|} \dim_F C_{C_V(Q)}(P/Q))$$

$$\begin{aligned} &= |P| \dim_F C_{C_V(Q)}(P/Q) \\ &\leq |P| \dim_F C_V(P) \end{aligned}$$

as desired.

Thus we may assume P has no nontrivial maximal subgroups. Then P is cyclic of order p. Let $P = \langle x \rangle$ where $x^p = 1$. Now $x^p = 1$ and $\mathrm{char}F = p$ implies $(x - I)^p = 0$ on V. Hence, since 1 is the only characteristic root of x and V is indecomposable, there is a basis B of V for which the matrix $M_B(x)$ for x has the form

$$M_B(x) = \begin{pmatrix} 1 & 1 & 0 & \ldots & 0 \\ 0 & 1 & 1 & 0\ldots & 0 \\ \vdots & & \ddots & \ddots & \\ 0 & & & & 1 \\ 0 & \ldots & \ldots & \ldots & 1 \end{pmatrix}$$

Now we write $M_B(x) = I + J$ where I is an $n \times n$ identity matrix and

$$J = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & & \ddots & \ddots & \\ 0 & & & 0 & 1 \\ 0 & \ldots & \ldots & \ldots & 0 \end{pmatrix}$$

Now $J^n = 0$ and, in fact, n is the smallest positive integer with this property. Suppose $\dim_F V > p$. Then $n > p$ and so $J^p \neq 0$. Hence, we get

$$(x - I)^p = (I + J - I)^p = J^p \neq 0$$

a contradiction. Thus $\dim_F V \leq p \leq |P| \dim_F C_V(P)$. Now P also acts on the dual space V^* of V by $(\phi)^g(v) = \phi(v^{g^{-1}})$ for any $g \in P$, $v \in V$ and $\phi \in V^*$. Under this action we have $(V/[V,P])^* \cong C_{V^*}(P)$ and so

$$\dim_F V = \dim_F V^* \leq |P| \dim_F C_{V^*}(P) = |P| \dim_F (V/[V,P])^* = |P| \dim_F V/[V,P]$$

and we are done.

□

Now let f be as in Lemma 3.18 and l be as in [7, 2.5]. Then by Lemma 3.6 and Lemma 3.11, the set

$$\mathcal{T} = \{(H_k, N_k) \in \mathcal{K}_4(Z) \cap \mathcal{K}_4(K) | \mathrm{pdeg}_{H_k/N_k}(x) \geq l((2p^2+1)2p^2|K| + f(p^2|K|)) \text{ for all } 1 \neq x \in K\}$$

is a Kegel cover for G. Let $(H_k, N_k) \in \mathcal{T}$, and set $H = H_k$, $N = N_k$, $n_k = n$, and $\Omega_k = \Omega$. Then since $H/N \cong A_n$ is perfect, by Lemma 3.7, there exists a unique subnormal supplement R for N in H.

Proposition 3.22 $C_H(O_p(H)) \leq N$

We prove Proposition 3.22 by contradiction through a series of lemmas. Let $U = C_H(O_p(H))$ and suppose $U \not\leq N$.

Lemma 3.23 *(a)* $[R, F(H)] = 1$.

(b) $R' = R$.

(c) Z normalizes each component of H.

(d) R is a component of H.

Proof $O_p(H) \trianglelefteq H$ implies $U \trianglelefteq H$. Hence, since $U \not\leq N$, Lemma 3.3 implies $H = UN$. Thus U is a subnormal supplement to N in H, and so by uniqueness of R we have $R \leq U$. Since $Z \not\leq N$, a similar argument shows $R \leq \langle Z^H \rangle$. Now $[U, O_p(H)] = 1$ and $R \leq U$ implies $[R, O_p(H)] = 1$. Also, Z normalizes $O_{p'}(H)$ and so by Lemma 1.2 (c) $[Z, O_{p'}(H)] = 1$. Since $O_{p'}(H) \trianglelefteq H$ and $R \leq \langle Z^H \rangle$, we have $[\langle Z^H \rangle, O_{p'}(H)] = 1$ and so $[R, O_{p'}(H)] = 1$. Thus, $[R, F(H)] = 1$ and we have (a).

For (b), R' char $\leq R \trianglelefteq H$ implies $R' \trianglelefteq H$. Thus, by the uniqueness of R and Lemma 3.3, we get $R = R'$ or $R' \leq N$. If $R' \leq N$, then $R' \leq R \cap N$ and we get,

$$A_n \cong \frac{H}{N} = \frac{RN}{N} \cong \frac{R}{R \cap N} \text{ is abelian}$$

a contradiction. Hence, $R = R'$ and R is perfect.

Next we prove (c) by contradiction. If (c) does not hold, then there exists $1 \neq u \in Z$ and a component C_1 of H with $C_1^u \neq C_1$. Let $C_r = C_1^{u^{r-1}}$ for $1 \leq r \leq p$ and $C = \langle C_1, C_2, \ldots, C_p \rangle$. Since C_1 is a component of H and C_r are conjugate to C_1 for all $1 \leq r \leq p$, C_r is also a component of H for each $1 \leq r \leq p$. Furthermore, if $C_r = C_s$ for some $1 \leq r, s \leq p$, then $C_1^{u^{r-1}} = C_1^{u^{s-1}}$ and therefore $C_1^{u^{r-s}} = C_1$. But then $u^{r-s} \in N_H(C_1)$ and, since $|u| = p$, we get $u \in \langle u \rangle = \langle u^{r-s} \rangle \leq N_H(C_1)$, a contradiction. Therefore we have shown $C_r \neq C_s$ for all $r \neq s$. Hence, as C_r and C_s are components of H, we have $[C_r, C_s] = 1$ for all $r \neq s$. Thus $C = C_1 \cdot C_2 \cdot \ldots \cdot C_p$.

Define a map θ from C_1 to $C_C(u)$ by

$$\theta(c) = cc^u c^{u^2} \ldots c^{u^{p-1}} \text{ for each } c \in C_1.$$

Since $[C_r, C_s] = 1$ for all $r \neq s$, we have $c^u c^{u^2} \ldots c^{u^{p-1}} \in C_C(u)$ for all $c \in C_1$. Thus, θ does indeed map C_1 into $C_C(u)$. Moreover, since conjugation by powers of u is a homomorphism and $[C_r, C_s] = 1$ for distinct r and s, θ is a homomorphism.

Suppose $\theta(c) = 1$ for some $c \in C_1$. Then $cc^u c^{u^2} \ldots c^{u^{p-1}} = 1$ and so

$$c = (c^u l^{u^2} \ldots c^{u^{p-1}})^{-1} \in C_1 \cap C_2 \cdot C_3 \cdot \ldots \cdot C_p.$$

Thus $c \in Z(C_1)$ and, since $c \in C_1$ was chosen arbitrarily, we have shown kern $\theta \leq Z(C_1)$.

Let $X = \theta(C_1)$. Then X is a nonabelian, otherwise, by The First Isomorphism Theorem, we get

$$\frac{C_1}{\text{kern } \theta} \cong \theta(C_1) = X.$$

Hence, $C_1/\text{kern } \theta$ is abelian and therefore $C_1 = C_1' \leq \text{Kern } \theta$, as C_1 is a component of H. But then we get $C_1 = \text{Kern } \theta \leq Z(C_1)$ and C_1 is abelian, a contradiction.

Next we claim that Z normalizes the set $\{C_1, C_2, \ldots, C_p\}$. For otherwise, there exists $v \in Z$ and $1 \leq r \leq p$ with $C_r^v \notin \{C_1, C_2, \ldots, C_p\}$. Now C_1 is a component of H implies C_r^v is a component of H. Thus, $C_r^v \notin \{C_1, C_2, \ldots, C_p\}$ implies $[C_r^v, C_s] = 1$ for all $1 \leq s \leq p$. But then $[C_r^v, C] = 1$ and so, by conjugating by powers of u, we get $[C_r^v, C] = 1$ for all $1 \leq r \leq p$. Thus, $[C^v, C] = 1$ and, since $X \leq C$, $[X^v, X] = 1$. But $X \leq C_C(u) = C_C(v)$, by Lemma 1.2 (a). Thus, $X^u = X$ and we get $[X, X] = 1$, a contradiction.

Now since Z normalizes the set $\{C_1, C_2, \ldots, C_p\}$, there exists $1 \neq w \in Z$ with $C_1^w = C_1$. Let $c \in C_1$ and $k = c^u c^{u^2} \ldots c^{u^{p-1}}$. Then $k \in C_2 \cdot C_3 \cdot \ldots \cdot C_p$ and so $k \in C_C(C_1)$. Also, since $\theta(c) = ck$ and $\theta(c) \in C_C(u) = C_C(w)$, we have

$$ck = \theta(c) = \theta(c)^w = c^w k^w$$

Also, since $w \in N_H(C_1)$ and $k \in C_C(C_1)$, we have $c^w \in C_1$ and $k^w \in C_C(C_1)$. But then

$$[c, w] = c^{-1}c^w = kk^{-w} \in C_C(C_1)$$

and so, since $c \in C_1$ was chosen arbitrarily, we have $[C_1, w] \leq C_C(C_1)$. But then we get $[C_1, w, C_1] = 1$ and $[w, C_1, C_1] = 1$. Thus, by the Three Subgroup Lemma, we have $[C_1, C_1, w] = 1$ and so $[C_1, w] = 1$, as C_1 is perfect. Hence, we get

$$C_1 \leq C_H(w) = C_H(u)$$

and so $[C_1, u] = 1$, a contradiction.

Finally let $E(H)$ be the subgroup generated by the components of H and comp$(H) = \{C_1, C_2, \ldots, C_r\}$ be the set of components of H. Let $i \in \{1, 2, \ldots, r\}$. Then by (c), we know that Z normalizes C_i. Thus, since H normalizes the set comp(H), $\langle Z^H \rangle$ also normalizes C_i. But $R \leq \langle Z^H \rangle$, and so R also normalizes C_i. Let $N_i = N_H(C_i)$. Then $R \leq N_i$ and $Z(C_i)$ char $\leq C_i \trianglelefteq N_i$ implies $Z(C_i) \trianglelefteq N_i$. Let $\overline{N_i} = N_i/Z(C_i)$ and $\overline{R}$ and $\overline{C_i}$ be the images of R and C_i in $\overline{N_i}$. Then $\overline{R}$ normalizes $\overline{C_i}$ and $\overline{C_i}$ is simple. But R is perfect implies $\overline{R}$ is perfect. Thus by the Schrier Conjecture, Out$(\overline{C_i})$ is solvable therefore $\overline{R}$ induces inner automorphisms on $\overline{C_i}$. But then $\overline{R} \leq C_{\overline{N_i}}(\overline{C_i})\overline{C_i}$. Hence, by taking preimages, we get $R \leq C_H(\overline{C_i})C_i$.

Now we claim $C_{N_i}(\overline{C_i}) = C_{N_i}(C_i)$. Let $C = C_{N_i}(\overline{C_i})$. Then clearly $C_{N_i}(C_i) \leq C$. On the other hand, $[C, \overline{C_i}] = 1$ implies $[C, C_i] \leq Z(C_i)$ and hence $[C, C_i, C_i] = 1$. But also $[C_i, C, C_i] = 1$ and so by the Three Subgroup Lemma, $[C_i, C_i, C] = [C_i', C] = 1$. Since $C_i \in \text{comp}(H)$, we have $C_i' = C_i$ and so we get $[C_i, C] = 1$. Therefore $C \leq C_{N_i}(C_i)$ and the claim holds.

Now we have $R \leq C_{N_i}(\overline{C_i})C_i = C_{N_i}(C_i)C_i \leq C_H(C_i)C_i$. Since distinct components of H commute and the choice of $i \in \{1, 2, \ldots, r\}$ was arbitrary, we get

$$R \leq \bigcap_{i=1}^{r} C_H(C_i)C_i = (\bigcap_{i=1}^{r} C_H(C_i))(C_1 \cdot C_2 \cdot \ldots \cdot C_r) \leq C_H(E(H))E(H).$$

Thus $R \leq E(H)C_H(E(H))$. Now $E(H) \trianglelefteq H$ implies $C_H(E(H)) \trianglelefteq H$. As before we get $C_H(E(H)) \leq N$ or $R \leq C_H(E(H))$. If $R \leq C_H(E(H))$ then $[R, E(H)] = 1$. Also, by (a), $[R, F(H)] = 1$, and so $[R, F^*(H)] = 1$, where $F^*(H) = E(H)F(H)$ is called the ***generalized fitting subgroup of H***. But then, by [1, 11.31.13], $R \leq C_H(F^*(H)) \leq F^*(H)$ and so $R \leq Z(F^*(H))$. Thus, in this case, we get R is abelian and so $R = R' = 1$, a contradiction. Therefore $C_H(E(H)) \leq N$. But $R \leq C_H(E(H))E(H)$ and $R \not\leq N$ implies $E(H) \not\leq N$. Hence, there exists a component subgroup C_i of H with $C_i \not\leq N$. Now since $C_i \trianglelefteq\trianglelefteq H$ and $C_i \not\leq N$, C_i supplements N in H. That is, $H = C_iN$ and so by the uniqueness of R we have $R \leq C_i$ and therefore $R \trianglelefteq C_i$. Let $\overline{C_i} = C_i/Z(C_i)$ and $\overline{R}$ be the image of R in $\overline{C_i}$. Since C_i is a component of H, $\overline{C_i}$ is simple. Thus, $\overline{R} = 1$ or $\overline{R} = \overline{C_i}$. If $\overline{R} = 1$ we get $R \leq Z(C_i)$ and therefore R is abelian, a contradiction. Hence, $\overline{R} = \overline{C_i}$. But then $C_i = RZ(C_i)$ and C_i/R is abelian. Therefore $C_i = C_i' \leq R$ and so $R = C_i$ and R is a component of H.

□

Lemma 3.24 *(a)* $Z(R) = N \cap R$

(b) $[R, N] = 1$

Proof Now $Z(R)$ char $\leq R \trianglelefteq H$ implies $Z(R) \trianglelefteq H$. Thus, since R is nonabelian, we must have $Z(R) \leq N$. Hence, $Z(R) \leq N \cap R$. Also, $N \trianglelefteq H$ implies $N \cap R \trianglelefteq R$. But, by Lemma 3.23, R is a component of H and therefore $N \cap R \leq Z(R)$ or $R = N \cap R$. The latter implies $R \leq N$ and $H = RN = N$, a contradiction to the maximality of N. Therefore $N \cap R \leq Z(R)$, and so $Z(R) = N \cap R$.

For (b), since R and N are normal subgroups of H we get $[R, N] \leq N \cap R = Z(R)$, by (a). Hence, $[R, N, R] = 1$ and $[N, R, R] = 1$. Thus, and so by the Three Subgroups Lemma we get $[R, R, N] = [R', N] = 1$. But, by Lemma 3.23, $R = R'$ and so we get $[R, N] = 1$.

□

Now since $Z(R) = N \cap R$, we have

$$\frac{R}{Z(R)} = \frac{R}{N \cap R} \cong \frac{RN}{N} = \frac{H}{N} \cong A_n$$

Let $\overline{H} = H/N$ and $\overline{R}$ and $\overline{Z}$ be the images of R and Z in $\overline{H}$. Now, since $Z \cap N = 1$, $\overline{H}$ contains a copy of Z. From here on we will identify $\overline{H}$ and A_n as they are isomorphic.

Now, by [8], $R/Z(R) \cong A_n$ and $R' = R$ implies $|Z(R)| = 1$ or 2. If $Z(R) = 1$ then, by the same argument used in Lemma 3.12, the centralizer property of Z in Lemma 1.2 (b) passes over to $\overline{H}$ to give a contradiction to Lemma 3.10. Therefore we may assume $|Z(R)| = 2$.

Suppose p is odd. Then again the centralizer property of Z in Lemma 1.2 (b) passes over to $\overline{H}$. Since p is odd, $Z(R)$ is a p'-group and $Z(R) \trianglelefteq H$ implies $Z \leq N_H(Z(R))$.

Thus, by Lemma 1.2 (c), $[Z, Z(R)] = 1$ and so $Z(R) \leq C_H(Z)$. Next we claim $C_{\overline{H}}(\overline{z}) = \overline{C_H(z)}$ for all $\overline{z} \in \overline{Z}$. For $\overline{z} \in \overline{Z}$, clearly $\overline{C_H(z)} \leq C_{\overline{H}}(\overline{z})$ and so we only need to show $C_{\overline{H}}(\overline{z}) \leq \overline{C_H(z)}$. Let $\overline{h} \in C_{\overline{H}}(\overline{z})$. Since $H = RN$, there exists $r \in R$ and $n \in N$ with $h = rn$. Then $[\overline{h}, \overline{z}] = [\overline{r}, \overline{z}] = 1$ implies $[r, z] \in Z(R)$. Hence, since $|Z(R)| = 2$, we get $[r, z]^2 = 1$. But, since $[r, z] \in Z(R) \leq C_R(Z)$, $[r, z]$ commutes with both z and r and so, by [3, 2.2.2], $[r, z]^2 = [r, z^2] = 1$. Thus, $r \in C_H(z^2)$ and therefore Lemma 1.2 (b) implies $r \in C_H(z)$. By taking images we finally get $\overline{r} \in \overline{C_H(z)}$ and so we have shown $C_{\overline{H}}(\overline{z}) = \overline{C_H(z)}$.

Now letting $\overline{Z} = \langle \overline{z_1}, \overline{z_2} \rangle$ we have $\overline{H} \cong A_n$, $\overline{Z} \leq \overline{H}$ and, by Lemma 1.2 (b),

$$C_{\overline{H}}(\overline{z_1}) = \overline{C_H(z_1)} = \overline{C_H(z_2)} = C_{\overline{H}}(\overline{z_2}).$$

Moreover, $\overline{Z}$ is of type (p, p) and, by the choice of the (H, N), we have $\mathrm{pdeg}_\Omega(\overline{z}) \geq 4p$. Hence, again we get a contradiction to Lemma 3.10.

Therefore it must be the case that $p = 2 = |Z(R)|$. Since $(H, N) \in \mathcal{K}_4(Z)$, we can find two regular orbits $\mathcal{O}_1$ and $\mathcal{O}_2$ for $\overline{Z}$ on Ω. Since $\overline{Z}$ is regular and transitive on $\mathcal{O}_i$, the action of $\overline{Z}$ on $\mathcal{O}_i$ is isomorphic to the action of $\overline{Z}$ on $\overline{Z}$ by right multiplication. Let $\overline{Z} = \langle \overline{z_1}, \overline{z_2} \rangle$. Then $\overline{z_1}$ has cycles $(1, \overline{z_1})(\overline{z_2}, \overline{z_2 z_1})$ on $\overline{Z}$ while $\overline{z_2}$ has cycles $(1, \overline{z_2})(\overline{z_1}, \overline{z_1 z_2})$ on $\overline{Z}$. Let 1, 2, 3, 4, and 5, 6, 7, 8 be the images of 1, $\overline{z_1}$, $\overline{z_2}$, and $\overline{z_1 z_2}$ under the above isomorphisms respectively. Then $\overline{z_1}$ has cycles $(12)(34)(56)(78)$ on $\mathcal{O}_1 \cup \mathcal{O}_2$ while $\overline{z_2}$ has cycles $(13)(24)(57)(68)$ on $\mathcal{O}_1 \cup \mathcal{O}_2$.

Now let $r \in R$ with $\overline{r} = (135)(246)$. Then $[\overline{r}^2, \overline{z_1}] = 1$ while $[\overline{r}^2, \overline{z_2}] \neq 1$. Thus, $[r^2, z_1] \in Z(R)$ and $[r^2, z_2] \notin Z(R)$. Also $\overline{r}^3 = 1$ and $\overline{r}^2 \neq 1$ implies $r^3 \in Z(R)$ and $r^2 \notin Z(R)$. Let $s = r^2$. Then, since $|Z(R)| = 2$ and $r^3 \in Z(R)$, we have $s^3 = 1$ and $[s, z_1] \in Z(R)$. Suppose $[s, z_1] = 1$. Then, by Lemma 1.2 (b), we get

$[s, z_2] = 1 \in Z(R)$ a contradiction. Thus $[s, z_1] \neq 1$. But then, since $|Z(R)| = 2$, we get $Z(R) = \{1, [s, z_1]\}$. Now $Z(R)$ char $\leq R \trianglelefteq H$ implies $Z(R) \trianglelefteq H$ and therefore $[s, z_1] \in Z(H)$. Thus $[s, z_1]$ commutes with both s and z_1. Now [3, 2.2.2] implies $1 = [s^3, z_1] = [s, z_1^3] = [s, z_1]$. Hence, we get $[s, z_1] = 1$, a contradiction and therefore Proposition 3.22 holds.

□

Now $U = C_H(O_p(H)) \leq N$ implies $R \not\leq U$. Hence, $[R, O_p(H)] \neq 1$ and so we can pick $S \leq O_p(H)$ minimal with respect to $S \trianglelefteq H$ and $[S, R] \neq 1$. Then alot can be said about the structure of S.

Lemma 3.25 *Let S be chosen as above, then*

(a) $S = [S, R]$.

(b) $C_S(R)$ *is the unique subgroup of* S *maximal with respect to being normal in* H. *Moreover, either* S *is abelian or* $Z(S) = C_S(R)$.

(c) If S *is nonabelian, then* $S/Z(S)$ *and* S' *are elementary abelian p-groups.*

Proof Since R and S are normal subgroups of H we have $1 \neq [S, R] \leq S$ and $[S, R] \trianglelefteq H$. So by minimality of S either $S = [S, R]$ or $[S, R, R] = 1$. If $[S, R, R] = 1$ then also $[R, S, R] = 1$. Thus, by the Three Subgroup Lemma we get $[R, R, S] = 1$. But then, since R is perfect, we get $[R, R, S] = [R', S] = [R, S] = 1$, a contradiction. Thus, $S = [S, R]$ and this proves (a).

For (b), since $S \trianglelefteq H$ and $R \trianglelefteq H$, we have $C_S(R) \trianglelefteq H$ and $C_S(R) \neq S$. Now let $S_0 < S$ with $S_0 \trianglelefteq H$. Then by minimality of S we have $[S_0, R] = 1$ and so $S_0 \leq C_S(R)$. Thus, $C_S(R)$ is the unique subgroup of S maximal with respect to being normal in

H. In particular, if S is nonabelian, then $Z(S)$ char $\leq S \trianglelefteq H$ implies $Z(S) \trianglelefteq H$ and therefore $Z(S) \leq C_S(R)$. Also, since $R \trianglelefteq H$, (a) implies $S = [S, R] \leq R$. Hence, $[C_S(R), S] = 1$ and we get $C_S(R) \leq Z(S)$. Therefore $Z(S) = C_S(R)$ and we have (b).

Finally, since both $\Phi(S)$ and S' are characteristic subgroups of S, they are both normal in H. Hence, by (b), $\Phi(S)$ and S' both lie in $Z(S)$. Therefore $S/Z(S)$ is abelian. Now, since S is a p-group, by [3, 5.1.3], $S/\Phi(S)$ is elementary p-abelian. Therefore $S/Z(S)$ is also elementary p-abelian as $\Phi(S) \leq Z(S)$. Let $z = [x, y] \in S'$. Then $S/Z(S)$ elementary p-abelian implies $y^p \in Z(S)$. Moreover, since $z \in S' \leq Z(S)$, z commutes with both x and y. Thus, by [3, 2.2.2], $1 = [x, y^p] = [x, y]^p = z^p$ and so all commutators have order p. Since $S' \leq Z(S)$ is abelian, all elements of S' must have order p and therefore S' is elementary p-abelian.

□

Lemma 3.26 *We may assume $H = KR$.*

Proof If $H \neq KR$, then we can replace (H, N, R) by $(KR, N \cap KR, R)$. For $Z \leq KR$, $Z \cap (N \cap KR) \leq Z \cap N = 1$, and $N \cap KR$ is maximal with respect to being normal in KR as

$$\frac{KR}{N \cap KR} \cong \frac{KRN}{N} = \frac{H}{N} \cong A_n \text{ is simple .}$$

Moreover, we claim that R is the unique minimal subnormal supplement to $N \cap KR$ in KR. Clearly $R \trianglelefteq KR$ and $KR = KR \cap H = KR \cap RN = R(N \cap KR)$. Hence R is a subnormal supplement for $N \cap KR$ in KR. Now suppose $R_0 \leq R$ with $R_0 \trianglelefteq\trianglelefteq KR$ and $KR = R_0(N \cap KR)$. Then

$$H = RN = (KR)N = R_0(N \cap KR)N = R_0N$$

and so $H = R_0N$. Moreover, $R_0 \trianglelefteq\trianglelefteq R \trianglelefteq H$, and so $R_0 \trianglelefteq\trianglelefteq H$. Thus $R = R_0$ by the uniqueness of R and therefore R is a minimal subnormal supplement for $N \cap KR$ in KR. Thus, by Lemma 3.7, R is the unique minimal subnormal supplement for $N \cap KR$ in KR.

$\square$

Proposition 3.27 *There exists an abelian subgroup A of G with $K \leq N_G(A)$ and $C_K(A) \leq L$.*

We now show Proposition 3.27 through a series of lemmas.

Lemma 3.28 *We may assume*

(a) $[H', S'] = 1$

(b) $Z(S) < S$

Proof Since $Z(S)$ is abelian and $Z(S)$ char $\leq S \trianglelefteq H$ implies $Z(S) \trianglelefteq H$, we may assume $C_K(Z(S)) \not\leq L$. Otherwise, we are done by taking $A = Z(S)$. Now $C_K(Z(S)) \trianglelefteq K$ and $C_K(Z(S)) \not\leq L$ and so by Lemma 3.16 $K = C_K(Z(S))Z$. Thus, $K/C_K(Z(S))$ is abelian and so $K' \leq C_K(Z(S))$. Now $K \cap N = 1$ and $K' \leq C_K(Z(S))$ implies $C_K(Z(S)) \not\leq N$. Hence, we have $C_H(Z(S)) \not\leq N$ and $C_H(Z(S)) \trianglelefteq H$. But then $C_H(Z(S))$ supplements N in H and therefore $R \leq C_H(Z(S))$. Since $H = KR$ and R is perfect, we have $H' = K'R$ and therefore $[H', Z(S)] = 1$. By Lemma 3.25

(b) $S' \leq Z(S)$ and so $[H', S'] = 1$. Finally, since $[S, R] \neq 1$ and $[Z(S), R] = 1$ we have $Z(S) < S$ and we are done.

$\square$

Lemma 3.29 *(a)* $H = H'Z$.

(b) $R \leq O^p(H)$.

(c) $O^p(H) \leq H'$.

Proof For (a), recall that $H = KR$ by Lemma 3.26 and $K = K'Z$ by Lemma 3.16. Also $H' \trianglelefteq H$ and $H' \not\leq N$ implies $H = H'N$ and therefore $R \leq H'$. Hence,

$$H = KR = K'ZR \leq H'ZR = H'Z$$

and so $H = H'Z$.

For (b), since $O^p(H) \trianglelefteq H$, by Lemma 3.3, we have either $R \leq O^p(H)$ or $O^p(H) \leq N$. Suppose $O^p(H) \leq N$. Then, since $H/O^p(H)$ is a p-group, we get

$$A_n \cong \frac{H}{N} \cong \frac{H/O^p(H)}{N/O^p(H)} \text{ is a } p\text{-group}$$

a contradiction. Therefore $R \leq O^p(H)$.

Finally, by (a) $H = H'Z$ and therefore $H/H' = H'Z/H' \cong Z/H' \cap Z$ is a p-group. Thus, $O^p(H) \leq H'$ and we are done.

$\square$

Let $V = S/Z(S)$ then, by Lemma 3.25, both V and S' are elementary p-abelian. Since $S \trianglelefteq H$, H acts on V and S' by conjugation making V and S' into GF$(p)H$-modules. Moreover, by Lemma 3.25 (b) and Lemma 3.28 (b), H acts irreducibly on V. Define a map β from $V \times V$ to S' by

$$\beta(\overline{a}, \overline{b}) = [a, b] \text{ for all } \overline{a}, \overline{b} \in V.$$

Lemma 3.30 *(a) β is well defined.*

(b) β is $GF(p)H$-bilinear.

(c) $\beta(\overline{a}, \overline{b}) = \beta(\overline{b}, \overline{a})^{-1}$.

(d) $C_H(V) \leq N$.

Proof For (a), let $(\overline{a}, \overline{b}) = (\overline{c}, \overline{d}) \in V \times V$. Then $\overline{a} = \overline{c}$ and $\overline{b} = \overline{d}$. Thus there exists z_1, $z_2 \in Z(T)$ with $a = z_1 c$ and $b = z_2 d$. Then, writing the operations of V and T' multiplicatively, we have

$$\begin{aligned} [a, b] = [cz_1, z_2 d] &= [z_1, z_2 d]^c [c, z_2 d] \\ &= [z_1, d]^c [z_1, z_2]^{cd} [c, d][c, z_2]^d \\ &= [c, d] \text{ as } z_1, z_2 \in Z(T) \end{aligned}$$

Thus $\beta(\overline{a}, \overline{b}) = \beta(\overline{c}, \overline{d})$ and β is well defined.

For (b) recall $T' \leq Z(T)$ by Lemma 3.25. Thus for any $\overline{a}$, $\overline{b}$, and $\overline{c} \in V$ we have,

$$\begin{aligned} \beta(\overline{a}\overline{b}, \overline{c}) = \beta(\overline{ab}, \overline{c}) &= [ab, c] \\ &= [a, c]^b [b, c] \\ &= [a, c][b, c] \\ &= \beta(\overline{a}, \overline{c}) \beta(\overline{b}, \overline{c}). \end{aligned}$$

A similar argument shows that β is linear in the second component as well. Now let $\lambda \in \mathrm{GF}(p)$. Then, since $[a,b] \in T' \leq Z(T)$, $[a,b]$ commutes with both a and b. Therefore,

$$\begin{aligned}\beta(\bar{a}^{\lambda},\bar{b}) = \beta(\overline{a^{\lambda}},\bar{b}) &= [a^{\lambda},b]\\ &= [a,b]^{\lambda}\\ &= \beta(\bar{a},\bar{b})^{\lambda}\end{aligned}$$

where the third equality is due to [3, 2.2.2]. Again, a similar argument will show $\beta(\bar{a},\bar{b}^{\lambda}) = \beta(\bar{a},\bar{b})^{\lambda}$. Thus β is GF(p)-bilinear and we have (a). Next we show that β commutes with the action of H. Let $h \in H$, then

$$\begin{aligned}[\beta(\bar{a},\bar{b})]^{h} = [a,b]^{h} &= [a^{h},b^{h}]\\ &= \beta(\overline{a^{h}},\overline{b^{h}})\\ &= \beta(\bar{a}^{h},\bar{b}^{h})\\ &= \beta((\bar{a},\bar{b})^{h}).\end{aligned}$$

For (c), we have

$$\beta(\bar{a},\bar{b}) = [a,b] = [b,a]^{-1} = \beta(\bar{b},\bar{a})^{-1}.$$

Finally, since V is H-invariant, $C_H(V) \trianglelefteq H$ and so by Lemma 3.3 (a) either $C_H(V) \leq N$ or $H = NC_H(V)$. If $H = NC_H(V)$ then $R \leq C_H(V)$, as R is the unique subnormal supplement for N in H. Hence, $[R,V] = 1$ and therefore $[R,S] \leq Z(S)$. But recall $S = [R,S]$, by Lemma 3.25 (a). Thus we get $S \leq Z(S)$, a contradiction. Therefore $C_H(V) \leq N$ and we have (d).

□

<u>Def</u> Let F be a finite field of characteristic p, F_0 a subfield of F, T a finite group and V and W finite dimensional FT-modules. Let $G(F, F_0)$ the group of field automorphisms of F which fix F_0. For $\sigma \in G(F, F_0)$ let V^σ be the FT module defined by $V^\sigma = V$ as a F_0T-module but the following new scalar multiplication by elements of F:

$$\lambda \cdot_\sigma v = \lambda^\sigma v$$

for all $\lambda \in F$, $v \in V$. Note that for elements of F_0, this is just the old scalar multiplication.

Lemma 3.31 *Let V, W, F_0, F, and T be as above.*

(a) The map $k \otimes l \to \{k^\sigma l\}_{\sigma \in G(F,F_0)}$ induces a F_0-isomorphism from $F \otimes_{F_0} F$ to $F^{|G(F,F_0)|}$.

(b) Let $\sigma \in G(F, F_0)$. Then the map $k \otimes l \to k^\sigma l$ induces a F-isomorphism from $F \otimes_{F_0} F^\sigma$ to F^σ.

(c) The map $v \otimes w \to \{v \otimes w\}_{\sigma \in G(F,F_0)}$ induces a F_0T-isomorphism from $V \otimes_{F_0} W$ to $\bigoplus_{\sigma \in G(F,F_0)} V \otimes_F W^\sigma$

Proof (a) Since the map $(k, l) \to \{k^\sigma l\}_{\sigma \in G(F,F_0)}$ is F_0-bilinear, there indeed exists a F_0 linear map α from $F \otimes_{F_0} F$ to $F^{G(F,F_0)}$ with $\alpha(k \otimes l) = \{k^\sigma l\}_{\sigma \in G(F,F_0)}$. Moreover, $F \otimes_{F_0} F$ becomes a F vector space by $\lambda \cdot (k \otimes l) = k \otimes \lambda l$ and α is F-linear. Since $\dim_F(F \otimes_{F_0} F) = \dim_{F_0} F = |G(F, F_0)| = \dim_F F^{|G(F,F_0)|}$ it is enough to show that α is surjective. If α is not surjective, then $\alpha(F \otimes_{F_0} F) \neq F^{|G(F,F_0)|}$ and therefore

$F^{|G(F,F_0)|}/\alpha(F \otimes_{F_0} F) \neq 0$. Thus, there exists $0 \neq \theta \in (F^{|G(F,F_0)|}/\alpha(F \otimes_{F_0} F))^*$. Define $\phi \in (F^{|G(F,F_0)|})^*$ by

$$\phi(\{r_\sigma\}_{\sigma \in G(F,F_0)}) = \theta(\{r_\sigma\}_{\sigma \in G(F,F_0)} + \alpha(F \otimes_{F_0} F))$$

for $\{r_\sigma\} \in F^{|G(F,F_0)|}$. Then, for any k, $l \in F$, we have $\phi \circ \alpha(k \otimes l) = \theta(\alpha(k \otimes l) + \alpha(F \otimes_{F_0} F)) = \theta(0) = 0$ and so $\phi \circ \alpha = 0$.

Let e_σ be the element of $F^{|G(F,F_0)|}$ which has a 1 in the σ^{th}-coordinate and a 0 everywhere else. Then $\{e_\sigma\}_{\sigma \in G(F,F_0)}$ is a basis for $F^{|G(F,F_0)|}$. Let $\{\phi_\sigma\}_{\sigma \in G(F,F_0)}$ be the dual basis corresponding to $\{e_\sigma\}_{\sigma \in G(F,F_0)}$. Then $\phi = \sum_{\sigma \in G(F,F_0)} \lambda_\sigma \phi_\sigma$ for some $\lambda_\sigma \in F$ and so

$$\phi(\{r_\sigma\}_{\sigma \in G(F,F_0)}) = \sum_{\sigma \in G(F,F_0)} \lambda_\sigma r_\sigma$$

for all $\{r_\sigma\}_{\sigma \in G(F,F_0)} \in F^{G(F,F_0)}$. But then

$$0 = \phi(\alpha(k \otimes 1)) = \phi(\{k^\sigma\}_{\sigma \in G(F,F_0)}) = \sum_{\sigma \in G(F,F_0)} \lambda_\sigma k^\sigma.$$

Now each $\sigma \in G(F, F_0)$ is of the form $\sigma : l \to l^{p^{i_\sigma}}$ for some integer $i_\sigma \geq 0$ with $p^{i_\sigma} < |F|$. Now $\theta \neq 0$ implies $\phi \neq 0$. Thus $f(x) = \sum_{\sigma \in G(F,F_0)} \lambda_\sigma x^{i_\sigma}$ is a non-zero polynomial over F of degree less than $|F|$ with at least $|F|$-roots, a contradiction, which completes the proof of (a).

For (b), define

$\delta : F \times F^\sigma \to F^\sigma$ by $\delta(k, l) = k^\sigma l$. Then, since $\sigma \in G(F, F_0)$, δ is additive on $F \times F^\sigma$ in both coordinates. Moreover,

$$\delta(\lambda k, l) = (\lambda k)^\sigma l = \lambda^\sigma k^\sigma l = \lambda \cdot_\sigma (k^\sigma l) = \lambda \cdot_\sigma \delta(k, l)$$

and

$$\delta(k, \lambda \cdot_\sigma l) = \delta(k, \lambda^\sigma l) = k^\sigma \lambda^\sigma l = \lambda^\sigma (k^\sigma l) = \lambda \cdot_\sigma \delta(k, l).$$

Hence δ is F-bilinear and so there exists a F-linear map ϕ from $F \otimes_F F^\sigma$ to F^σ with $\phi(k \otimes l) = \delta(k, l)$. Now $\delta \neq 0$, otherwise $\delta(k, l) = 0$ implies $k^\sigma l = 0$ for all k, $l \in F$. Letting $k = 1$ we get $l = 0$ and, as the choice of $l \in F$ was arbitrary, $F = 0$, a contradiction. Therefore $\delta \neq 0$ and consequently $\phi \neq 0$. Thus, since both $F \otimes_F F^\sigma$ and F^σ are 1-dimensonal over F, ϕ is a F-isomorphism and (b) holds.

(c) Since $(v, w) \to \bigoplus_{\sigma \in G(F,F_0)}(v \otimes w)$ is F_0-bilinear there exists a F_0-linear map

$$\beta : V \otimes_{F_0} W \to \bigoplus_{\sigma \in G(F,F_0)} V \otimes_F W^\sigma$$

with

$$\beta(v \otimes w) = \bigoplus_{\sigma \in G(F,F_0)} (v \otimes w).$$

Next we show that β injective. Since V and W are finite dimensional vector spaces over F, both V and W are isomorphic to the direct sum of copies of F. Therefore, since β clearly commutes with action of T and the tensor product of a direct sum is the direct sum of the tensor products, we may assume that $T = 1$ and $V = F = W$.

By (b) there exists a F_0-linear map

$$\gamma : \bigoplus_{\sigma \in G(F,F_0)} F \otimes_F F^\sigma \to F^{G(F,F_0)}$$

with

$$\{k_\sigma \otimes l_\sigma\}_{\sigma \in G(F,F_0)} \to \{k_\sigma^\sigma l_\sigma\}_{\sigma \in G(F,F_0)}$$

Let α be as in (a). Then, for any $k,\ l \in F$, $\gamma\beta(k \otimes l) = \gamma(\bigoplus_{\sigma \in G(F,F_0)}(k \otimes l)) = \{k^\sigma l\} = \alpha(k \otimes l)$ and so $\alpha = \gamma\beta$. Now since α is injective, β is injective as well.

Finally we claim $\dim_{F_0}(F \otimes_{F_0} F) = \dim_{F_0}(\bigoplus_{\sigma \in G(F,F_0)} F \otimes_F F)$. For $\dim_{F_0}(F \otimes_{F_0} F) = (\dim_{F_0} F)^2 = |G(F, F_0)|^2$. On the other hand, $\dim_F(F \otimes_F F^\sigma) = 1$ and $\dim_{F_0} F = |G(F, F_0)|$ implies $\dim_{F_0}(F \otimes_F F^\sigma) = |G(F, F_0)|$. Thus, we get

$$\dim_{F_0}(\bigoplus_{\sigma \in G(F,F_0)} F \otimes_F F^\sigma) = \sum_{\sigma \in G(F,F_0)} \dim_{F_0}(F \otimes_F F^\sigma) = \sum_{\sigma \in G(F,F_0)} |G(F, F_0)| = |G(F, F_0)|^2$$

and so $\dim_{F_0}(F \otimes_{F_0} F) = \dim_{F_0}(\bigoplus_{\sigma \in G(F,F_0)} F \otimes_F F)$ as claimed.

But then β is also surjective and is therefore a F_0T-isomorphism and the lemma is proven.

$\square$

Lemma 3.32 *Let p be a prime, T be a finite group, V a FT-module and F a finite field of characteristic p. Then*

$$V = [V, T] \textit{ if and only if } V = [V, O^p(T)]$$

Proof Clearly, since $[V, O^p(T)] \leq [V, T]$, $V = [V, O^p(T)]$ implies $V = [V, T]$. On the other hand, suppose $V = [V, T]$. Let $\overline{V} = V/[V, O^p(T)]$. Since $O^p(T) \trianglelefteq T$, $[V, O^p(T)]$ is T-invariant and so T acts on $\overline{V}$. Moreover, since $[\overline{V}, O^p(T)] = 0$, $T^* = T/O^p(T)$ acts on $\overline{V}$. But T^* is a p-group and, since $|F|$ is a power of p, $\overline{V}$ is also a p-group. Hence semidirect product $S = T^* * \overline{V}$ is a p-group. Therefore S is nilpotent and there exists a integer $n \geq 0$ such that $[S, n] = 1$. Now $V = [V, T]$ implies $\overline{V} = [\overline{V}, T] = [\overline{V}, T^*]$, and hence $\overline{V} = [\overline{V}, H^*]$. Also, since $\overline{V}$ is abelian, we have $\overline{V} = [\overline{V}, T^*] = [\overline{V}, T^* * \overline{V}] = [\overline{V}, S]$. Thus, we get $\overline{V} = [\overline{V}, S, n-1] \leq [S, n] = 1$ and $\overline{V} = 1$. But this implies $V = [V, O^p(T)]$ and we are done.

$\square$

Lemma 3.33 *Suppose F_0 is a finite field of characteristic p, V is irreducible as F_0T-module on which T acts nontrivially, $F = Hom_{F_0T}(V, V)$ and that $[W, O^p(T)] = 0$ for some F_0T-module W. Let $0 \neq s : V \times V \to W$ be a F_0-bilinear T-invariant map.*

(a) There exists a unique $\sigma \in G(F, F_0)$ with $[V \otimes_F V^\sigma, O^p(T)] \neq V \otimes_F V^\sigma$.

(b) Put $E = V \otimes_F V^\sigma/[V \otimes_F V^\sigma, O^p(T)]$. Then there exist an T-invariant, F-σ sesquilinear map $s^* : V \times V \to E$ and a F_0-linear map $\rho : E \to W$ with $s = \rho s^*$.

(c) $\dim_F E \leq |T/O^p(T)|$.

(d) If $s(u, v) = -s(v, u)$ for all $u, v \in V$, then $\sigma^2 = 1$.

Proof Note first that s defines a F_0-linear T-invariant map $\alpha : V \otimes_{F_0} V \to W$ with $\alpha(u \otimes v) = s(u, v)$ and, since $O^p(T)$ centralizes W, we have $[V \otimes_{F_0} V, O^p(T)] \leq \text{Kern } \alpha$. Note also that, as F_0T-modules,

$$
\begin{aligned}
(\frac{V \otimes_{F_0} V}{[V \otimes_{F_0} V, T]})^* \cong C_{(V \otimes_{F_0} V)^*}(T) &\cong C_{V^* \otimes_{F_0} V^*}(T) \\
&\cong C_{\mathrm{Hom}_{F_0}(V, V^*)}(T) \\
&= \mathrm{Hom}_{F_0 T}(V, V^*).
\end{aligned}
\tag{3.1}
$$

Since $s \neq 0$, α is not zero. Hence, $V \otimes_{F_0} V/[V \otimes_{F_0} V, O^p(T)] \neq 0$ and therefore, by Lemma 3.32, $V \otimes_{F_0} V/[V \otimes_{F_0} V, T] \neq 0$. Thus, (3.1) implies $\mathrm{Hom}_{F_0 T}(V, V^*) \neq 0$. Also, by [1, 4.14.5], V is a irreducible F_0T-module implies V^* is also a irreducible F_0T-module. Thus, by [4, 5.1.1], we conclude that V and V^* are isomorphic as F_0T-modules. But then, as F_0T-modules, $\mathrm{Hom}_{F_0T}(V, V^*) \cong \mathrm{Hom}_{F_0T}(V, V) = F$. Therefore (3.1) implies $V \otimes_{F_0} V/[V \otimes_{F_0} V, T] \cong (V \otimes_{F_0} V/[V \otimes_{F_0} V, T])^* \cong F$.

Notice that, since V is a irreducible F_0T-module, [4, 5.1.1] implies $F = \mathrm{Hom}_{F_0T}(V, V)$ is a division ring. Hence, since $|F| = |\mathrm{Hom}_{F_0T}(V, V)|$ is finite, F is a field by Wedde-burn's Theorem. Now under the action of elements of F, V becomes a FT-module. Moreover, since F_0 acts on V by scalar multiplication and V is a F_0T-module, F contains a copy of F_0 and therefore $G(F, F_0)$ makes sense. For $\sigma \in G(F, F_0)$ let $E_\sigma = V \otimes_F V^\sigma$. Then by Lemma 3.31 (c),

$$
V \otimes_{F_0} V \cong \bigoplus_{\sigma \in G(F, F_0)} E_\sigma \tag{1}
$$

and hence

$$
F \cong \frac{V \otimes_{F_0} V}{[V \otimes_{F_0} V, T]} \cong \bigoplus_{\sigma \in G(F, F_0)} \frac{E_\sigma}{[E_\sigma, T]}. \tag{2}
$$

Since $0 \neq F$, (2) implies there exists $\sigma \in G(F, F_0)$ such that $E_\sigma \neq [E_\sigma, T]$. Moreover, since E_σ is an FT-module, $|E_\sigma/[E_\sigma, T]| \geq |F|$. Therefore σ is the only element of

$G(F, F_0)$ for which $E_\sigma \neq [E_\sigma, T]$. But then $E_\sigma \neq [E_\sigma, T]$ implies $E_\sigma \neq [E_\sigma, O^p(T)]$. Now suppose $\mu \in G(F, F_0)$ with $\mu \neq \sigma$. Then $E_\mu = [E_\mu, T]$ and so, by Lemma 3.32, $E_\mu = [E_\mu, O^p(T)]$ and (a) holds.

For (b), applying (2) with $O^p(T)$ in place of T, (a) implies there exists a F_0T-isomorphism

$$\eta : E = \frac{E_\sigma}{[E_\sigma, O^p(T)]} \cong \frac{V \otimes_{F_0} V}{[V \otimes_{F_0} V, O^p(T)]}.$$

with $\eta((u \otimes v) + [E_\sigma, O^p(T)]) = (u \otimes v) + [V \otimes_{F_0} V, O^p(T)]$.

Define $s^* : V \times V \to E$ by $s^*(u, v) = (u \otimes v) + [E_\sigma, O^p(T)]$ and $\overline{\alpha} : V \otimes_{F_0} V/[V \otimes_{F_0} V, O^p(T)] \to W$ by $\overline{\alpha}(r + [V \otimes_{F_0} V, O^p(T)] = \alpha(r)$. Finally, let $\rho = \overline{\alpha}\eta$. Then, s^* is F σ-sesquilinear and, since α is F_0-linear, $\overline{\alpha}$ is F_0-linear. Thus, since η is a F_0T-isomorphism, $\rho = \overline{\alpha}\eta$ is F_0-linear and

$$\begin{aligned} \rho s^*(u, v) = \rho((u \otimes v) + [E_\sigma, O^p(T)]) &= \overline{\alpha}\eta((u \otimes v) + [E_\sigma, O^p(T)]) \\ &= \overline{\alpha}((u \otimes v) + [V \otimes_{F_0} V, O^p(T)]) \\ &= \alpha(u \otimes v) \\ &= s(u, v) \end{aligned} \tag{3.2}$$

For (c), notice that by (a) and (2), we have

$$\frac{E}{[E, T]} \cong \frac{E_\sigma}{[E_\sigma, T]} \cong \frac{V \otimes_{F_0} V}{[V \otimes_{F_0} V, T]} \cong F. \tag{3}$$

Also, since $O^p(T)$ centralizes E, $\overline{T} = T/O^p(T)$ acts on E. Moreover, (3) implies

$$\frac{E}{[E,\overline{T}]} = \frac{E}{[E,T]} \cong F$$

and therefore $\dim_F E/[E,\overline{T}] = 1$. Now since $\overline{T}$ is a p-group, by Lemma 3.21, we get

$$\dim_F E \leq \dim_F \frac{E}{[E,\overline{T}]} \cdot |\overline{T}| = |\overline{T}|$$

and therefore (c) holds.

For (d), after replacing W by $\alpha(V \otimes_{F_0} V)$, we may assume that α is surjective. Let s^* and ρ be as in (b) and $i : W \to W/[W,T]$ and $j : E \to E/[E,T]$ be the natural maps. By (3) there exists a F_0T-isomorphism $k : E/[E,T] \to F$ which is also F-linear. Now α is T-invariant implies $\overline{\alpha}$ is T-invariant. Thus, since η is a F_0T-isomorphism, $\rho = \overline{\alpha}\eta$ is also T-invariant and so $[E,T] \leq$ Kern $i\rho$. Hence, by the First Isomorphism Theorem, there exists a map $\pi : E/[E,T] \to W/[W,T]$ such that $\pi j = i\rho$. Finally define the maps $\delta : V \times V \to F$ and $\pi^* : F \to W/[W,T]$ by $\delta = kjs^*$ and $\pi^* = \pi k^{-1}$. Then, since s^* is F σ-sesquilinear and k and j are F-linear, δ is F σ-sesquilinear. Also π^* is F_0-linear as π and k are F_0-linear. Moreover,

$$is = i\rho s^* = \pi j s^* = \pi k^{-1} k j s^* = \pi^* \delta. \tag{4}$$

and so $is = \pi^*\delta$.

Let $D =$ kern π^*. Since $s(u,v) = -s(v,u)$ for all $u, v \in V$, we have $s(u,v) + s(v,u) = 0$ and therefore $is(u,v) + is(v,u) = 0$. Now, since $is = \pi^*\delta$, we get $\pi^*(\delta(u,v) + \delta(v,u)) = 0$ and so $\delta(u,v) + \delta(v,u) \in D$ for all u, $v \in V$.

Now $W \neq [W,T]$; otherwise, by Lemma 3.32, we get $W = [W, O^p(T)] = 0$ and therefore $s = 0$, a contradiction. Hence, since α is surjective, $W \neq [W,T]$ implies $\alpha(V \otimes_{F_0} V) \not\leq [W,T]$. Therefore there exists u,$v \in V$ with $\alpha(u \otimes v) \notin [W,T]$ and consequently $is(u,v) \neq 0$. But then (4) implies $\pi^*\delta(u,v) \neq 0$ and therefore $\delta(u,v) \neq 0$.

Put $a = \delta(u,v)$ and $b = \delta(v,u)$ and let λ, $\mu \in F$. Then

$$\delta(\lambda u, \mu v) + \delta(\mu u, \lambda v) = \lambda\mu^\sigma a + \mu\lambda^\sigma b \in D. \tag{5}$$

Applying (5) to $\lambda' = 1$ and $\mu' = \mu\lambda^\sigma$ we obtain

$$\mu^\sigma\lambda^{\sigma^2} a + \mu\lambda^\sigma b \in D. \tag{6}$$

Subtracting (6) from (5) we obtain

$$\mu^\sigma(\lambda - \lambda^{\sigma^2})a \in D. \tag{7}$$

Suppose $\lambda - \lambda^{\sigma^2} \neq 0$. Then, since $\sigma \in \mathrm{Aut}(F)$, $\lambda^{\sigma^{-1}} - \lambda^\sigma \neq 0$. Applying (7) to $\mu'' = \mu(\lambda^{\sigma^{-1}} - \lambda^\sigma)^{-1}$ we get $\mu^\sigma a \in D$. Let $f \in F$. Then, as $\mu \in F$ was chosen arbitrarily and $a \neq 0$, $\mu = (fa^{-1})^{\sigma^{-1}}$ is a well-defined element of F. Moreover, $f = ((fa^{-1})^{\sigma^{-1}})^\sigma a = \mu^\sigma a \in D$ and so $F = D$. But α surjective implies $\overline{\alpha}$ is surjective and therefore $\rho = \overline{\alpha}\eta$ is surjective. Hence, since i is surjective, π and therefore $\pi^* = \pi k^{-1}$ is surjective as well. Thus, $\pi^*(F) = 0$ implies $W/[W,T] = 0$ and $W = [W,T]$, a contradiction. Therefore $\lambda - \lambda^{\sigma^2} = 0$ and, since λ was a arbitrary element of F, we get $\sigma^2 = 1$ and we have shown (d).

□

Let $F = \mathrm{Hom}_{GF(p)H}(V)$. Now V and S' are GF$(p)H$-modules with V irreducible and, by Lemmas 3.28 (a) and 3.29 (d), $[S', O^p(H)] = 1$. Moreover, by Lemma 3.30, $\beta : V \times V \to S'$ is a GF(p)-bilinear H-invariant map with $\beta(\overline{a}, \overline{b}) = \beta(\overline{b}, \overline{a})^{-1}$.

Therefore by Lemma 3.33 (b) there exist an FH-module E, $\sigma \in Aut(F)$ with $\sigma^2 = 1$, a H invariant F σ-sequilinear map $s^* : V \times V \to E$ and $GF(p)$-linear map $\rho : E \to S'$ with $\beta = \rho s^*$. Moreover, by Lemmas 3.26, 3.16 (a), (e), and (f) and 3.29 (c), we get

$$\begin{aligned} O^p(H) = H \cap O^p(H) = KR \cap O^p(H) &= R(K \cap O^p(H)) \\ &= R(K'Z \cap O^p(H)) \\ &= RK'(Z \cap O^p(H)) \\ &= H'(Z \cap O^p(H)). \end{aligned}$$

Thus, $O^p(H) = H'(Z \cap O^p(H))$ and so, by Lemma 3.33 (c), we have

$$\begin{aligned} \dim_F E \leq |H/O^p(H)| = |H/H'(Z \cap O^p(H))| \leq |H|/|H'| &= |H'Z|/|H'| \\ &= |Z|/|Z \cap H'| \leq p^2. \end{aligned}$$

Let $\widehat{H} = H/C_H(V)$ and $\widehat{N}$ and $\widehat{K'}$ be the images of N and K' in $\widehat{H}$. Let $\widehat{x} \in \widehat{K'}$ be an element of order q for some $q \in \pi(|\widehat{K'}|)$. Since V is a FH-module and $N \trianglelefteq H$, $\widehat{H} \leq GL_F(V)$ and $\widehat{N} \trianglelefteq \widehat{H}$. Also, $C_H(V) \leq N$, by Lemma 3.29 (b), and so

$$\frac{\widehat{H}}{\widehat{N}} \cong \frac{H}{N} \cong A_n.$$

Let l be as in [7, 2.5] and f be as in Lemma 3.18. Recall that H was choosen so that

$$\text{pdeg}_{\widehat{H}/\widehat{N}}(\widehat{x}) = \text{pdeg}_{H/N}(x) \geq l[(2p^2+1)2p^2|K| + f(|K|p^2)].$$

Thus by [7, 2.5] applied to $(\widehat{H}, \widehat{N}, \widehat{x}, V)$ we get $\text{pdeg}_{V_F}(\widehat{x}) \geq (2p^2+1)2p^2|K| + f(|K|p^2)$. Since $\dim_F V \geq \text{pdeg}_{V_F}(\widehat{x})$ we also have

$$\begin{aligned} \dim_F V &\geq (2p^2+1)2p^2|K| + f(|K|p^2) \\ &\geq (2\dim_F E + 1)2\dim_F(E)(|K|) + f(|K|\dim_F E). \end{aligned}$$

Therefore by lemma 3.20 (b) applied to $(V, F, \widehat{K}, \widehat{x}, E, s^*)$ there exists a $\widehat{K}$-invariant subspace $\overline{A} = A/Z(S)$ of V such that $s^* |_{\overline{A}\times\overline{A}} = 1$ and $[\overline{A}, \widehat{x}] \neq 1$. Since $\beta = \rho \circ s^*$ we get $\beta |_{\overline{A}\times\overline{A}} = 1$. By the definition of the map β the latter implies $[A, A] = 1$ and A is an abelian subgroup of S.

Also $[\overline{A}, \widehat{x}] \neq 1$ implies $[A, x] \neq 1$ and so $x \notin C_K(A)$. Since $x \in K'$ we have $K' \not\leq C_K(A)$ and $C_K(A) \trianglelefteq K$. Therefore $C_K(A) \leq L$, and we have shown proposition 3.27.

□

Lemma 3.34 *We may assume A is elementary p-abelian.*

Proof If its not the case that A is elementary p-abelian, then we can replace A by $\Omega_1(A)$. Since $p \mid |A|$, we know $\Omega_1(A) \neq 1$. Also $\Omega_1(A)$ char $\leq A$ and so $K \leq N_G(A)$ implies $K \leq N_G(\Omega_1(A))$. Moreover we claim $C_K(\Omega_1(A)) \leq L$. For if $C_K(\Omega_1(A)) \not\leq L$ then $K = C_K(\Omega_1(A))L$ and so $K' \leq C_K(\Omega_1(A))$ by Lemma 3.16 (e). Hence $[K', \Omega_1(A)] = 1$. Now $K' = O^p(K')$ by Lemma 3.16 (f) and so K' is generated by p'-elements. Thus by the coprime action of the p'-elements of K' on the p-group A, [3, 5.2.4] implies $[K', A] = 1$. But then we get $K' \leq C_K(A) \leq L$, a contradiction. Therefore $C_K(\Omega_1(A)) \leq L$ and we can replace A with $\Omega_1(A)$ if need be.

□

Lemma 3.35 *Let A and B be abelian groups with B acting on A and suppose $C_A(b) = C_A(B)$ for all $1 \neq b \in B$. For $Y \subseteq B$ define $C_A(Y, i)$ inductively by $C_A(Y, 0) = 1$ and $C_A(Y, i)/C_A(Y, i-1) = C_{A/C_A(Y,i-1)}(Y)$. Then*

(a) $C_A(Y, i)$ is a subgroup of A maximal with respect to $[C_A(Y, i), Y, i] = 1$.

(b) $C_A(b,i) = C_A(B,i)$ *for all* $1 \neq b \in B$ *and* $i \geq 0$.

(c) If both A *and* B *are elementary abelian* p*-groups, then* $[A,B,p] = 1$.

Proof For (a) its clear that $C_A(Y,i)$ is a subgroup of A. Next we claim that $[C_A(Y,i),Y,i] = 1$. For this we use induction on i. Notice that $C_A(Y,0) = 1$ and $C_A(Y,1) = C_A(Y)$ and so the claim holds for $i = 0, 1$. Now suppose $[C_A(Y,k),Y,k] = 1$ for all $k < i$. Then, by the definition of $C_A(Y,i)$, we have $[C_A(Y,i),Y] \leq C_A(Y,i-1)$ and so, by induction, we get

$$[[C_A(Y,i),Y],Y,i-1] \leq [C_A(Y,i-1),Y,i-1] = 1.$$

But then $[C_A(Y,i),Y,i] = [[C_A(Y,i),Y],Y,i-1] = 1$ and so $[C_A(Y,i),Y,i] = 1$ and the claim holds for each $i \geq 0$. Now we claim that $C_A(Y,i)$ is indeed maximal with respect to the above property. Again we use induction on i. Let $U \leq A$ with $[U,Y,1] = 1$. Then $[U,Y] = 1$ and so $U \leq C_A(Y) = C_A(Y,1)$. Therefore the claim holds for $i = 1$. Assume the claim holds for all $k < i$ and let $U \leq A$ with $[U,Y,i] = 1$. Then $[[U,Y],Y,i-1] = 1$ and so, by induction, $[U,Y] \leq C_A(Y,i-1)$. But then

$$\frac{UC_A(Y,i-1)}{C_A(Y,i-1)} \leq C_{A/C_A(Y,i-1)}(Y) = \frac{C_A(Y,i)}{C_A(Y,i-1)}.$$

Thus, $U \leq C_A(Y,i)$, and we have shown (a).

For (b), we use induction on i. For $i = 0$, both subgroups are equal to 1. If $i = 1$ then, by assumption, we get $C_A(b,1) = C_A(b) = C_A(B) = C_A(B,1)$. Suppose $C_A(b,k) = C_A(B,k)$ for all $k < i+1$ and let $\overline{A} = A/C_A(B,i-1)$. Then, since A is B-invariant and B is abelian, B acts on $\overline{A}$. Moreover, the assumptions on (A,B) still hold for $(\overline{A},B)$. That is,

$$C_{\overline{A}}(b) = C_{A/C_A(b,i-1)}(b) = \frac{C_A(b,i)}{C_A(b,i-1)} = \frac{C_A(B,i)}{C_A(B,i-1)} = C_{\overline{A}}(B)$$

where the first and third equalities hold by induction. Now let $X = C_A(b, i+1)$. Then $[X, b] \leq C_A(b, i)$ and, by induction, $C_A(b, i) = C_A(B, i)$. Thus, $[X, b] \leq C_A(B, i)$ and therefore $[[X, b], B] \leq C_A(B, i-1)$. Also, since B is abelian, we have $[b, B, X] \leq C_A(B, i-1)$. Hence, by The Three Subgroup Lemma, we get $[X, B, b] \leq C_A(B, i-1)$. But then $[\overline{[X, B]}, b] = 1$ in $\overline{A}$ and so, since b and B have the same centralizer on $\overline{A}$, we get $[\overline{[X, B]}, B] = 1$. Thus, $[X, B, B] \leq C_A(B, i-1)$ and therefore $[X, B, B, B, i-1] = [X, B, i+1] = 1$ by (a). Hence, again by (a), we get $X \leq C_A(B, i+1)$. On the other hand, since $[C_A(B, i+1), B, i+1] = 1$ implies $[C_A(B, i+1), b, i+1] = 1$, by (a) we have $C_A(B, i+1) \leq C_A(b, i+1)$. Thus $C_A(b, i+1) = C_A(B, i+1)$ and we are done.

Finally, suppose A and B are elementary abelian p-groups and let $1 \neq b \in B$. Then $b^p = 1$ and, since A is a vector space over GF(p), we have $[A, b, p] = 1$. Thus, by (a) and (b), we get $A = C_A(b, p) = C_A(B, p)$ and so $[A, B, p] = 1$.

□

Now, since A and Z are elementary p-abelian and Z acts on A, by Lemma 3.35 (c), we have $[A, Z, p] = 1$. Let

$$A \trianglerighteq A_1 \trianglerighteq A_2 \trianglerighteq A_3 \trianglerighteq \ldots \trianglerighteq A_k = 1 \tag{1}$$

be a composition series for K on A where A_i are all K-invariant normal subgroups of A_{i-1} for all $1 \leq i \leq k$ and K acts irreducibly on the factors A_i/A_{i+1} for all $1 \leq i \leq k-1$.

Suppose K' acts trivially on all the composition factors A_i/A_{i+1} for K on A. Then the action of the p'-elements of K' stabilize the chain (1) of the p-group A and therefore centralize A by [3, 5.3.2]. Since K' is generated by p'-elements, the latter implies K' centralizes A, a contradicition. Therefore there exists a composition factor B for K on A such that $[K', B] \neq 1$. Let $\widehat{K} = K/C_K(B)$.

Lemma 3.36 *Let B and $\widehat{K}$ be chosen as above. Then*

(a) B is a faithful irreducible $\widehat{K}$-module for which $C_K(B) \leq L$ and $[B, \widehat{Z}, p] = 1$.

(b) $\widehat{L}$ is a p'-group with $\widehat{L} = \Phi(\widehat{K})$.

(c) $\widehat{K}/\Phi(\widehat{K}) \cong A_r$.

Proof For (a), since B is a composition factor for K on A and $[A, Z, p] = 1$, its clear that B is a faithful irredducible $\widehat{K}$-module with $[B, \widehat{Z}, p] = 1$. Moreover, since $C_K(B) \trianglelefteq K$ and $K' \not\leq C_K(B)$, we have $C_K(B) \leq L$. Since $O_p(K) \leq C_K(B)$, (b) follows immediately by the same argument used in the proof of Lemma 3.16 (d).

Finally for (c), since $C_K(B) \leq L$, we have

$$\frac{\widehat{K}}{\Phi(\widehat{K})} = \frac{\widehat{K}}{\widehat{L}} \cong \frac{K}{L} \cong A_r.$$

□

<u>Def</u> Let T be a finite group and $t \in T$. Then $L_t = C_T(t)^\infty$ is the terminal member of the derived series of $C_T(t)$ defined by

$$L_t = C_T(t)^\infty = \bigcap_{i=1}^{\infty} C_T(t)^{(i)}$$

where $C_T(t)^\infty$ denotes the $(i+1)^{\text{th}}$ member of the derived series of $C_T(t)$.

Lemma 3.37 *Let $1 \neq k \in K$. Then*

(a) $L_{\widehat{k}} \trianglelefteq C_{\widehat{K}}(\widehat{k})$.

(b) $L_{\widehat{k}}$ *is generated by p'-elements.*

(c) Let $\widehat{K}^* = \widehat{K}/\Phi(\widehat{K})$ *and* $L^*_{\widehat{z}}$ *be the image of* $L_{\widehat{z}}$ *in* $\widehat{K}^*$. *Then* $L^*_{\widehat{z}} = L_{\widehat{z}^*}$ *for any* $1 \neq z \in Z$.

Proof Clearly, since $L_{\widehat{k}}$ is the intersection of normal subgroups of $C_{\widehat{K}}(\widehat{k})$, we have $L_{\widehat{k}} \trianglelefteq C_{\widehat{K}}(\widehat{k})$. Also, since $L_{\widehat{k}}$ is perfect, $L_{\widehat{k}}/O^p(L_{\widehat{k}})$ is a perfect p-group. Thus, $L_{\widehat{k}}/O^p(L_{\widehat{k}}) = 1$ and therefore $L_{\widehat{k}} = O^p(L_{\widehat{k}})$ and $L_{\widehat{k}}$ is generated by p'-elements. Therefore (a) and (b) hold.

Finally for (c), we claim $C_{\widehat{K}^*}(\widehat{z}^*) = C_{\widehat{K}}(\widehat{z})^*$. Let $\widehat{Y}^* = \widehat{Y}/\Phi(\widehat{K}) = C_{\widehat{K}^*}(\widehat{z}^*)$. Then $[\widehat{Y}^*, \widehat{z}^*] = 1$ implies $[\widehat{Y}, \widehat{z}] \leq \Phi(\widehat{K})$. But then $\langle\widehat{z}\rangle\Phi(\widehat{K}) \trianglelefteq \widehat{Y}$ and $\langle\widehat{z}\rangle \in \mathrm{Syl}_p(\langle\widehat{z}\rangle\Phi(\widehat{K}))$. Thus by The Frattini Argument we get $\widehat{Y} = N_{\widehat{Y}}(\langle\widehat{z}\rangle)\Phi(\widehat{K})$. But, since $\Phi(\widehat{K})$ is a p'-group, we have $[N_{\widehat{Y}}(\langle\widehat{z}\rangle), \langle\widehat{z}\rangle] \leq \langle\widehat{z}\rangle \cap \Phi(\widehat{K}) = 1$. Thus $N_{\widehat{Y}}(\langle\widehat{z}\rangle) = C_{\widehat{Y}}(\langle\widehat{z}\rangle) = C_{\widehat{Y}}(\widehat{z})$ and $\widehat{Y} = C_{\widehat{Y}}(\widehat{z})\Phi(\widehat{K})$. But then

$$C_{\widehat{K}^*}(\widehat{z}^*) = \widehat{Y}^* = \frac{C_{\widehat{Y}}(\widehat{z})\Phi(\widehat{K})}{\Phi(\widehat{K})} = C_{\widehat{Y}}(\widehat{z})^* \leq C_{\widehat{K}}(\widehat{z})^*$$

and so we have shown $C_{\widehat{K}^*}(\widehat{z}^*) \leq C_{\widehat{K}}(\widehat{z})^*$. On the other hand, $[C_{\widehat{K}}(\widehat{z}), \widehat{z}] = 1$ implies $[C_{\widehat{K}}(\widehat{z})^*, \widehat{z}^*] = 1$ and so $C_{\widehat{K}}(\widehat{z})^* \leq C_{\widehat{K}^*}(\widehat{z}^*)$. Hence altogether we have shown $C_{\widehat{K}^*}(\widehat{z}^*) = C_{\widehat{K}}(\widehat{z})^*$ as claimed. Now we get

$$L_{\widehat{z}^*} = C_{\widehat{K}^*}(\widehat{z}^*)^\infty = (C_{\widehat{K}}(\widehat{z})^*)^\infty = (C_{\widehat{K}}(\widehat{z})^\infty)^* = L^*_{\widehat{z}}.$$

$\square$

Let $q \neq p$ be an odd prime. Then by Fermat's Little Theorem we have $p \mid q^{p-1} - 1$. Thus, we can choose t minimal such that $p \mid q^t - 1$.

Lemma 3.38 *Let p, q, and t be chosen as above and E_{q^t} be an elementary q-abelian group of order q^t. Then*

(a) $p \mid |Aut(E_{q^t})|$.

(b) If $x \in Aut(E_{q^t})$ with $x^p = 1$, x acts irreducibly on E_{q^t}.

Proof For (a) E_{q^t} is a vectorspace over GF(q) and therefore $\mathrm{Aut}(E_{q^t}) \cong \mathrm{GL}_t(q)$. Hence, since $p \mid q^t - 1$ and $|\mathrm{Aut}(E_{q^t})| = |\mathrm{GL}_t(q)| = \prod_{i=0}^{t-1}(q^t - q^i)$, we get $p \mid |\mathrm{Aut}(E_{q^t})|$.

For (b), suppose H is a x-invariant subgroup of E_{q^t} of order q^s where $0 < s < t$. Then $x \in \mathrm{Aut}(H)$ and $\mathrm{Aut}(H) \cong \mathrm{GL}_s(q)$. Therefore

$$p = |x| \mid |\mathrm{Aut}(H)| = \prod_{i=0}^{s-1}(q^t - q^i).$$

But since $q \neq p$ we get $p \mid (q^{s_0} - 1)$, for some $s_0 \leq s < t$. This is a contradiction to the minimality of t.

$\square$

Let E_{q^t} and x be as in Lemma 3.38 and $\langle y \rangle$ be a cyclic group of order p. Then we can form the semidirect product $E_{q^t} * \langle x \rangle$. Consider the group

$$W = E_{q^t} * \langle x \rangle \times \langle y \rangle.$$

Then $|W| = p^2q^t$, $O_q(W) = E_{q^t}$, and $\langle x \rangle \times \langle y \rangle \in \mathrm{Syl}_p(W)$. We can embeed W into S_r by letting W act on

$$\Gamma = W \cup (W/O_q(W))^{\frac{1}{p^2}(r-p^2q^t)}$$

by right multiplication. Here $(W/O_q(W))^{\frac{1}{p^2}(r-p^2q^t)}$ denotes $\frac{1}{p^2}(r-p^2q^t)$ distinct copies of $W/O_q(W)$. Moreover, we claim that through this action W becomes a subgroup of A_r. Since $E_{q^t} = O_q(W)$, E_{q^t} acts trivially on $(W/O_q(W))^{\frac{1}{p^2}(r-p^2q^t)}$. Furthermore, since q is odd, any q-cycle is even. Thus, since E_{q^t} is elementary q-abelian and acts semiregularly on W, all elements of E_{q^t} are even on W and are therefore even on Γ. Now x and y act semiregularly on W. Also, since $\mathrm{Stab}_W(wO_q(W)) = O_q(W)^w$ is a q-group for any $w \in W$, both x and y act semiregularly on $(W/O_q(W))^{\frac{1}{p^2}(r-p^2q^t)}$. Thus, $\langle x \rangle \times \langle y \rangle$ is of type (p,p) and acts semiregularly on Γ. If p is odd then all elements of $\langle x \rangle \times \langle y \rangle$ are even on Γ. On the other hand, if $p = 2$, then $4 = p^2 = |\langle x \rangle \times \langle y \rangle|$ divides $|\Gamma|$. Hence, again every element of $\langle x \rangle \times \langle y \rangle$ is even on Γ. Therefore, through this action, W is a subgroup of A_r.

Now by Lemma 3.36 (b), $\widehat{K}^* \cong A_r$, and so henceforth we will identify $\widehat{K}^*$ and A_r. Finally let $\widehat{W}^*$ denote the image of W in A_r.

Lemma 3.39 *Let Ω be a set with $|\Omega| = n$ for some positive integer $n \geq 3$ and A and B be subgroups of $Sym(\Omega) = S_n$ such that*

(a) A and B act semiregularly on Ω.

(b) there exists an isomorphism ϕ from A onto B.

Then there exists $x \in S_n$ such that $\phi(a) = a^x$ for all $a \in A$.

Proof First we claim that A and B have the same number of orbits on Ω. Suppose

$$\Omega = \bigcup_{i=1}^{k} r_i^A \text{ and } \Omega = \bigcup_{j=1}^{l} s_j^B \tag{1}$$

are two partitions of Ω into disjoint unions of orbits of A and B. Then we want to show $k = l$. Since A acts semiregularly on Ω, from (1), we get,

$$\begin{aligned} |\Omega| = |\bigcup_{i=1}^{k} r_i^A| &= \sum_{i=1}^{k} |r_i^A| \\ &= \sum_{i=1}^{k} \frac{|A|}{|\mathrm{Stab}_A(r_i)|} \\ &= \sum_{i=1}^{k} |A| \\ &= k|A|. \end{aligned}$$

Hence $|\Omega| = k|A|$ and similarly we get $|\Omega| = l|B|$. But then, $k|A| = l|B|$ and, since $A \cong B$, we have $|A| = |B|$. Therefore $k = l$ as claimed.

Now we assume that A and B both have k orbits on Ω and define $x \in S_n$ by

$$(r_i^a)^x = s_i^{\phi(a)} \text{ for all } a \in A \text{ and } 1 \leq i \leq k$$

Then x is well defined on Ω since ϕ is well defined and A is semiregular. Moreover, ϕ is surjective implies x maps Ω onto Ω. Finally, B is semiregular and ϕ is injective implies x injective on Ω and therefore x is indeed an element of S_n.

Let $s \in \Omega$ and $a \in A$. Then there exists $1 \leq i \leq k$ and $a_1 \in A$ such that $s = s_i^{\phi(a_1)}$. Hence, we have

$$\begin{aligned} s^{(a^x)^{-1}\phi(a)} = (s_i^{\phi(a_1)})^{(a^x)^{-1}\phi(a)} = (r_i^{a_1})^{a^{-1}x\phi(a)} &= (r_i^{a_1 a^{-1}})^{x\phi(a)} \\ &= (s_i^{\phi(a_1 a^{-1})})^{\phi(a)} \\ &= s_i^{\phi(a_1)} = s. \end{aligned}$$

Thus, since $s \in \Omega$ was chosen arbitrarily, we have $(a^x)^{-1}\phi(a) = 1$ and so $\phi(a) = a^x$ for all $a \in A$.

□

Lemma 3.40 *Let* $1 \neq z \in Z$. *Then*

(a) We may assume $\widehat{Z}^* \in Syl_p(\widehat{W}^*)$ *and* $\widehat{z}^* \in Z(\widehat{W}^*)$.

(b) $\widehat{Z}^* \leq L^*_{\widehat{z}}$.

Proof Let $\widehat{z}^*$, $\widehat{z_0}^* \in \widehat{Z}^*$ such that $\widehat{Z}^* = \langle \widehat{z}^*, \widehat{z_0}^* \rangle$. Then $\langle \widehat{z}^*, \widehat{z_0}^* \rangle \cong \langle \widehat{x}^*, \widehat{y}^* \rangle$. Moreover both of these subgroups of A_r act semiregularly on Ω_{reg}. Therefore, by Lemma 3.39, they are conjugate in S_r. Hence there exists $s \in S_r$ with $\widehat{z}^{*s} = \widehat{y}^*$ and $\widehat{z_0}^{*s} = \widehat{x}^*$. But then $\widehat{z}^{*s} \in Z(\widehat{W}^*)$ and $(\widehat{Z}^*)^s \in \text{Syl}_p(\widehat{W}^*)$ and we have (a).

For (b), since $|\Omega_{\text{reg}}| = 4p^2$, r/p is an integer. Define the subgroup $\widehat{U}^*$ of A_r by

$$\widehat{U}^* = \langle \widehat{t}^* \rangle \times \widehat{A}^*$$

where $\langle \widehat{t}^* \rangle$ is a cyclic group of order p and acts on Ω_{reg} by permuting each of the p subsets of size r/p of Ω_{reg} cyclicly and $\widehat{A}^*$ acts as $A_{\frac{r}{p}}$ on each of these p subsets. Then, since $r = 4p^2$, $r/p = 4p > 5$ and so $\widehat{A}^*$ is perfect and simple. Again, as $4p = r/p$, we can choose $\widehat{t_0}^* \in \widehat{A}^*$ such that $\widehat{t_0}^*$ acts semiregularly on Ω_{reg} and $\widehat{t_0}^{*p} = 1$. Then as above $\langle \widehat{t}^*, \widehat{t_0}^* \rangle \cong \langle \widehat{z}^*, \widehat{z_0}^* \rangle$ and both of these subgroups act semiregularly on Ω_{reg}. Therefore, by Lemma 3.39, there exists $s \in S_r$ such that $\widehat{z_0}^{*s} = \widehat{t_0}^{*}$ and $\widehat{z}^{*s} = \widehat{t}^{*}$. Now $\widehat{t_0}^{*} \in \widehat{A}^{*} \leq C_{\widehat{K}^{*}}(\widehat{t}^{*})$ and, since $\widehat{A}^{*}$ is perfect, we get

$$\widehat{t_0}^{*} \in \widehat{A}^{*} \leq \bigcap_{i=1}^{\infty} C_{\widehat{K}^{*}}(\widehat{t}^{*})^{(i)} = L_{\widehat{t}^{*}}$$

Thus $\widehat{t_0}^{*} \in L_{\widehat{t}^{*}}$ and so, by conjugating by s^{-1}, we get $\widehat{z_0}^{*} \in L_{\widehat{z}^{*}}$. Therefore we have shown $\widehat{z_0}^{*} \in L^{*}_{\widehat{z}}$ for all $\widehat{z_0}^{*} \notin \langle \widehat{z}^{*} \rangle$. Now $\widehat{z_0}^{*}\ \widehat{z}^{*} \notin \langle \widehat{z}^{*} \rangle$ and so $\widehat{z_0}^{*}\ \widehat{z}^{*} \in L^{*}_{\widehat{z}}$. But then we have $p < |\widehat{Z}^{*} \cap L^{*}_{\widehat{z}}| \mid p^2$ and therefore $\widehat{Z}^{*} \cap L^{*}_{\widehat{z}} = \widehat{Z}^{*}$. Thus $\widehat{Z}^{*} \leq L^{*}_{\widehat{z}}$ and this proves the lemma.

$\square$

Lemma 3.41 *Let T be a finite perfect group and B and C subgroups of T. Suppose*

(a) $B \trianglelefteq T$

(b) C is solvable

and

(c) $T = BC$.

Then $T = B$.

Proof Since T is perfect T/B is also perfect. But, C is solvable implies

$$\frac{T}{B} = \frac{BC}{B} \cong \frac{C}{B \cap C} \text{ is solvable .}$$

Thus, T/B is both perfect and solvable. The only way this is possible is if $T/B = 1$ and $T = B$. $\square$

Lemma 3.42 *For any $1 \neq \widehat{z}^* \in \widehat{Z}^*$ let $C = C_{\widehat{K}^*}(\widehat{z}^*)$, C_p be a cyclic group of order p, and $C_p^{\frac{r}{p}} = C_p \times C_p \times \ldots \times C_p$ be the direct product of $\frac{r}{p}$ distinct copies of C_p. Then*

(a) If p is odd, $C \cong C_p$ wr $A_{\frac{r}{p}}$.

(b) If $p = 2$, $C \sim (C_p^{\frac{r}{p}} \cap A_r)S_{\frac{r}{p}}$.

(c) $Solv(L_{\widehat{z}}^*)$ is a p-group, $L_{\widehat{z}}^* = Solv(L_{\widehat{z}}^*)A_{\frac{r}{p}}$, and $L_{\widehat{z}}^*/Solv(L_{\widehat{z}}^*) \cong A_{\frac{r}{p}}$.

(d) $L_{\widehat{z}}^* = \langle \widehat{Z}^{*L_{\widehat{z}}^*} \rangle$.

(e) $L_{\widehat{z}} = \langle \widehat{Z}^{L_{\widehat{z}}} \rangle$.

Proof For (a), let $S_r = \mathrm{Sym}(\Omega_{\mathrm{reg}})$ and, since $\widehat{K}^* \cong A_r$, identify $\widehat{K}^*$ and A_r. Now $\widehat{Z}^*$ acts semiregularly on Ω_{reg} and $\widehat{z}^*$ has order p, thus $\widehat{z}^*$ is the product of $\frac{r}{p}$ distinct p-cycles. Therefore, by [10, 3.2.13], we have $C_{S_r}(\widehat{z}^*) \cong C_p$ wr $S_{\frac{r}{p}}$. But then $C_{S_r}(\widehat{z}^*) = AU$ where $A \cong C_p^{\frac{r}{p}}$, $A \trianglelefteq C_{S_r}(\widehat{z}^*)$, $U \cong S_{\frac{r}{p}}$, $A \cap U = 1$, and $C_{S_r}(\widehat{z}^*)/A \cong U$. Now since p is odd, every p-cycle is an even permutation. Therefore, since every element of A is the product of p-cycles, we have $A \leq A_r$. Moreover, if $u \in U$ is an even permutation in S_r, then since p is odd, u must be an even permutation on each subset of size $\frac{r}{p}$ of Ω_{reg} and therefore $U \cap A_r = A_{\frac{r}{p}}$. Thus we get,

$$C = C_{A_r}(\widehat{z}^*) = A_r \cap C_{S_r}(\widehat{z}^*) = A_r \cap AU = A(A_r \cap U) = AA_{\frac{r}{p}}.$$

Now $A \trianglelefteq C_{S_r}(\widehat{z}^*)$ and $A \cap U = 1$ implies $A \trianglelefteq C_{A_r}(\widehat{z}^*)$ and $A \cap A_{\frac{r}{p}} = 1$. Therefore $C = C_p$ wr $A_{\frac{r}{p}}$.

For (b), $p = 2$ implies every permutation of U is the product of two disjoint permutations of the same type. Thus, every element of U is even and therefore $U \leq A_r$. But then

$$C = A_r \cap C_{S_r}(\widehat{z}^*) = A_r \cap AU = (A_r \cap A)U.$$

For (c), first suppose p is odd. Then by (a) we have $C = A * A_{\frac{r}{p}}$. Now $L^*_{\frac{r}{z}} = C^\infty$ is the unique maximal perfect subgroup of C. Therefore, since $A_{\frac{r}{p}}$ is perfect, we have $A_{\frac{r}{p}} \leq L^*_{\frac{r}{z}}$. But then we get

$$L^*_{\frac{r}{z}} = L^*_{\frac{r}{z}} \cap C = L^*_{\frac{r}{z}} \cap AA_{\frac{r}{p}} = (L^*_{\frac{r}{z}} \cap A)A_{\frac{r}{p}}. \tag{1}$$

Let $S = \mathrm{Solv}(L^*_{\frac{r}{z}})$. We claim $S = A \cap L^*_{\frac{r}{z}}$. First $A \trianglelefteq C_{S_r}(\widehat{z}^*)$ implies $A \cap L^*_{\frac{r}{z}} \trianglelefteq L^*_{\frac{r}{z}}$. Therefore, since A is a p-group, A is solvable and $A \cap L^*_{\frac{r}{z}} \leq S$. On the other hand, $S \cap A_{\frac{r}{p}} \trianglelefteq A_{\frac{r}{p}}$ and so $S \cap A_{\frac{r}{p}} = 1$ or $A_{\frac{r}{p}}$, as $A_{\frac{r}{p}}$ is simple. But $S \cap A_{\frac{r}{p}} = A_{\frac{r}{p}}$ implies $A_{\frac{r}{p}} \leq S$. Hence, in this case we get, $A_{\frac{r}{p}}$ is solvable, a contradiction. Therefore $S \cap A_{\frac{r}{p}} = 1$ and so

$$S = S \cap L^*_{\frac{r}{z}} = S \cap A_{\frac{r}{p}}(A \cap L^*_{\frac{r}{z}}) = (S \cap A_{\frac{r}{p}})(L^*_{\frac{r}{z}} \cap A) = L^*_{\frac{r}{z}} \cap A \tag{2}$$

and the claim holds. Moreover, since A is a p-group, S is a p-group. Now, by combining (1) and (2), we get $L^*_{\frac{r}{z}} = SA_{\frac{r}{p}}$ and, since $S \trianglelefteq L^*_{\frac{r}{z}}$ and $S \cap A_{\frac{r}{p}} = 1$, we have $L^*_{\frac{r}{z}}/S \cong A_{\frac{r}{p}}$.

Now if $p = 2$, then (a) implies $C = (A_r \cap A)U$. Thus, since $L^*_{\frac{r}{z}}$ is perfect, A is abelian, and $S'_{\frac{r}{p}} = A_{\frac{r}{p}}$, we get

$$L^*_{\frac{r}{z}} \leq ((A_r \cap A)U)' = [A_r \cap A, U]A_{\frac{r}{p}}. \tag{3}$$

Then, again since $A_{\frac{r}{p}} \leq L^*_{\frac{z}{z}}$, from (3) we have

$$L^*_{\bar{z}} = L^*_{\bar{z}} \cap [A_r \cap A, U] A_{\frac{r}{p}} = (L^*_{\bar{z}} \cap [A_r \cap A, U]) A_{\frac{r}{p}}. \tag{4}$$

Let $S_0 = L^*_{\bar{z}} \cap [A_r \cap A, U]$ and $S = \mathrm{Solv}(L^*_{\bar{z}})$. We claim $S_0 = S$. Since $A \trianglelefteq C_{S_r}(\widehat{z}^*)$, $S_0 \leq A$ and therefore S_0 is a p-group. Also, $[A_r \cap A, U] \trianglelefteq \langle A_r \cap A, U \rangle = C_{S_r}(\widehat{z}^*)$ implies $S_0 = L^*_{\bar{z}} \cap [A_r \cap A, U] \trianglelefteq L^*_{\bar{z}}$ and therefore $S_0 \leq S$. But then, as before, $S \cap A_{\frac{r}{p}} = 1$ and so from (4) we get

$$S = S \cap L^*_{\bar{z}} = S \cap S_0 A_{\frac{r}{p}} = (S \cap A_{\frac{r}{p}}) S_0 = S_0.$$

Therefore $S = S_0$, $L^*_{\bar{z}} = S A_{\frac{r}{p}}$, S is a p-group and $L^*_{\bar{z}}/S \cong A_{\frac{r}{p}}$.

For (d), let $L_0 = \langle \widehat{Z}^{*L^*_{\bar{z}}} \rangle$, $S = \mathrm{Solv}(L^*_{\bar{z}})$, $\overline{L^*_{\bar{z}}} = L^*_{\bar{z}}/S$ and $\overline{L_0}$ be the image of L_0 in $\overline{L^*_{\bar{z}}}$. Then we want to show $L^*_{\bar{z}} = L_0$. Well $L_0 \trianglelefteq L^*_{\bar{z}}$ implies $\overline{L_0} \trianglelefteq \overline{L^*_{\bar{z}}}$. But, by (c), $\overline{L^*_{\bar{z}}} \cong A_{\frac{r}{p}}$ is simple and so we get $\overline{L_0} = 1$ or $\overline{L_0} = \overline{L^*_{\bar{z}}}$.

If $\overline{L_0} = 1$ then $L_0 \leq S$. Now, from the proof of Lemma 3.40, there exists $s \in S_r$ with $\widehat{A}^{*s^{-1}} \leq L^*_{\bar{z}}$. Thus, since $L_0 \trianglelefteq L_{*\bar{z}}$, $L_0 \cap \widehat{A}^{*s^{-1}} \trianglelefteq \widehat{A}^{*s^{-1}}$. But $\widehat{A}^{*s^{-1}}$ is simple and so $L_0 \cap \widehat{A}^{*s^{-1}} = 1$ or $\widehat{A}^{*s^{-1}}$. Now

$$1 \neq \widehat{z_0}^* = \widehat{t_0}^{*s^{-1}} \in L_0 \cap \widehat{A}^{*s^{-1}}$$

and therefore $L_0 \cap \widehat{A}^{*s^{-1}} \neq 1$. On the other hand, if $\widehat{A}^{*s^{-1}} = L_0 \cap \widehat{A}^{*s^{-1}}$ then $\widehat{A}^{*s^{-1}} \leq L_0$. But, from above we have, $L_0 \leq S$ is solvable and therefore we get $\widehat{A}^{*s^{-1}}$ is solvable, a contradiction.

Therefore it must be the case that $\overline{L_0} = \overline{L^*_{\bar{z}}}$. But then $L^*_{\bar{z}} = L_0 S$. Now $L^*_{\bar{z}}$ is perfect, $L_0 \trianglelefteq L^*_{\bar{z}}$, and S is solvable. Thus, by Lemma 3.41, we get $L^*_{\bar{z}} = L_0$ and

(d) holds.

Finally, by Lemma 3.37, $L_{\hat{z}}^{*} = \langle \widehat{Z}^{*L_{\hat{z}}^{*}} \rangle$ implies $L_{\hat{z}} \leq \langle \widehat{Z}^{L_{\hat{z}}} \rangle \Phi(\widehat{K})$. Let $L_0 = \langle \widehat{Z}^{L_{\hat{z}}} \rangle$. Then $L_{\hat{z}} \leq L_0 \Phi(\widehat{K})$ and $L_0 \leq L_{\hat{z}}$ implies

$$L_{\hat{z}} = L_{\hat{z}} \cap L_0 \Phi(\widehat{K}) = L_0 (L_{\hat{z}} \cap \Phi(\widehat{K})). \tag{5}$$

Thus, since $L_{\hat{z}}$ is perfect, $L_0 \trianglelefteq L_{\hat{z}}$, and $L_0 \cap \Phi(\widehat{K})$ is solvable, again by Lemma 3.41, (5) implies $L_{\hat{z}} = L_0$ and therefore (e) holds.

□

Lemma 3.43 *Let Ω be a finite set, p a prime, and B a semiregularly acting subgroup of $Alt(\Omega)$ of type (p,p). If $|\Omega| \geq max\{p^2+1, 5p\}$ then*

$$Alt(\Omega) = \langle L_a, L_b \rangle$$

for all a, $b \in B$ with $B = \langle a, b \rangle$.

Proof First, let a, $b \in B$ with $B = \langle a, b \rangle$ and consider the set $\Omega' = R \times X$ where $R = \mathrm{GF}(p)$ and X is a set of order $|\Omega|/p$. For any $(r,x) \in \Omega'$, define a', $b' \in \mathrm{Sym}(\Omega')$ by $a' : (r,x) \to (r+1, x)$ and $b' : (r,x) \to (r, x^{\rho})$ where $\rho \in \mathrm{Alt}(X)$ is the product of $|X|/p$ p-cycles. Then $a'^{p} = b'^{p} = 1$, $[a', b'] = 1$ and therefore $B' = \langle a', b' \rangle$ is of type (p,p). Moreover, since a' and b' are semiregular on Ω', it follows that B' is also semiregular on Ω'. Now since $|\Omega| = |\Omega'|$, we have $\mathrm{Alt}(\Omega) \cong \mathrm{Alt}(\Omega')$. Let this isomorphism be ϕ. Suppose we are able to show that $\mathrm{Alt}(\Omega')$ is generated in the desired way, that is, $\mathrm{Alt}(\Omega') = \langle L_{a'}, L_{b'} \rangle$. Then, since both $\langle a, b \rangle$ and $\langle \phi(a), \phi(b) \rangle$ are isomorphic semiregular acting subgroups of Sym(Ω), by Lemma 3.39 there exists $s \in$ Sym(Ω) such that $\phi(a)^s = a$ and $\phi(b)^s = b$. Thus, $\mathrm{Alt}(\Omega) = \langle L_{\phi(a)}, L_{\phi(b)} \rangle$ implies $\mathrm{Alt}(\Omega)^s = \langle L^s_{\phi(a)}, L^s_{\phi(b)} \rangle = \langle L_{\phi(a)^s}, L_{\phi(b)^s} \rangle = \langle L_a, L_b \rangle$. Now by the normality of Alt(Ω) in Sym(Ω), we get $\mathrm{Alt}(\Omega) = \langle L_a, L_b \rangle$. Therefore we may assume $\Omega = \Omega'$, $a' = a$, $b' = b$, and $B' = B$.

Let $\pi \in \mathrm{Alt}(X)$. Define $\pi^* \in \mathrm{Sym}(\Omega)$ by $\pi^* : (r, x) \to (r, x^\pi)$ for each $(r, x) \in \Omega$. Then $\pi \in \mathrm{Alt}(X)$ implies $\pi^* \in \mathrm{Alt}(\Omega)$. Let $A = \{\pi^* | \pi \in \mathrm{Alt}(X)\}$. Then clearly $A \cong \mathrm{Alt}(X)$ and $A \leq C_{\mathrm{Alt}(\Omega)}(a)$. Moreover, since $|\Omega| \geq 5p$, we have $|X| \geq 5$. Hence A is perfect and $A \leq L_a$.

For $x \in X$, define $a_x \in \mathrm{Sym}(\Omega)$ by

$$a_x(r, x') = \begin{cases} (r+1, x) & \text{if } x' = x \\ (r, x) & \text{if } x' \neq x \end{cases}$$

Then a_x is the cycle of a containing $(0, x)$ and therefore $a_x \in C_{\mathrm{Sym}(\Omega)}(a)$. Moreover, $a_x^{\pi^*} = a_{x^\pi}$. Let x and x' be two distinct elements of X. Then there exists $\pi \in \mathrm{Alt}(\Omega)$ with $\pi(x) = x'$. But then, since $\pi^* \in A \leq L_a$ and $L_a \trianglelefteq C_{\mathrm{Sym}(\Omega)}(a)$, $a_x \in C_{\mathrm{Sym}(\Omega)}(a)$ implies $[a_x, \pi^*] \in L_a$. But

$$[a_x, \pi^*] = a_x^{-1} a_x^{\pi^*} = a_x^{-1} a_{x'}$$

and so we have shown that for any two cycles c and c' of a we have $c^{-1}c' \in L_a$. Moreover, since a and b are conjugate in Sym(Ω), the corresponding statement holds for b and L_b.

For $i \in R$ define, $X_i = \{i\} \times X$, and $A_i = \{\sigma \in \mathrm{Alt}(\Omega) | \sigma \in C_{\mathrm{Alt}(\Omega)}(\Omega \setminus X_i)$ and σ is even on $X_i\}$. Then, since A_i fixes the first components of elements of Ω, we have $A_i \cong \mathrm{Alt}(X_i) \cong \mathrm{Alt}(X) \cong A$. Now $|\Omega| > p^2$ implies $|X| > p$.

Thus, since b acts semiregularly on Ω, ρ has at least two different cycles, say d_1 and d_2. Define c_1 and $c_2 \in \mathrm{Sym}(\Omega)$ by

$$c_k(r,x) = \begin{cases} (r, x^{d_k}) & \text{if } r = i \\ (r,x) & \text{if } r \neq i \end{cases}$$

for $k = 1,2$. Then c_k is just the cycle of b containing (i, x_k) where $x_k \in \mathrm{Supp}(d_k)$ for $k = 1,2$. Therefore $e = c_1^{-1}c_2 \in L_b$.

Next we claim $A_i = [e, A]$. First, since $\Omega \setminus X_i \subseteq \mathrm{Fix}(e)$ we have $e \in C_{\mathrm{Alt}(\Omega)}(\Omega \setminus X_i) = A_i$. Also, since A normalizes $\Omega \setminus X_i$, we get $\Omega \setminus X_i \subseteq \mathrm{Fix}([e, A])$ and therefore $[e, A] \leq A_i$. On the other hand, $A \cong \mathrm{Alt}(X) \cong \mathrm{Alt}(X_i) \cong A_i$ and e acts nontrivially on X_i. Thus, identifying A and e as subgroups of $\mathrm{Alt}(X_i)$, we get $1 \neq [e, A] \trianglelefteq A$. But, since A is simple, we get $A = [e, A]$. Hence $[e, A] \cong \mathrm{Alt}(X_i)$ and therefore $|[e, A]| = |A_i|$. But then $A_i = [e, A]$, and the claim holds.

Let $L = \langle L_a, L_b \rangle$. Then, since $e \in L_b$ and $A \leq L_a$, we have $A_i = [e, A] \leq L$. But then L contains three cycles, as $A_i \cong \mathrm{Alt}(X_i)$.

Finally, we claim L acts primitively on Ω. Since $A_i \cong \mathrm{Alt}(X_i)$, we know A_i acts primitively on X_i. Suppose that Δ is a block for L on Ω with $2 \leq |\Delta| < |\Omega|$. Then, since A_i normalizes X_i, $\Delta \cap X_i$ is a block for A_i on X_i. But then A_i is primitive on X_i implies either $|\Delta \cap X_i| \leq 1$ or $X_i \leq \Delta$.

Suppose that $|\Delta \cap X_i| = 1$. Then, since $|\Delta| \geq 2$, we have $\Delta \setminus X_i \neq \emptyset$. Now A_i fixes $\Delta \setminus X_i$ and Δ is a block implies A_i normalizes Δ. But then A_i also normalizes $\Delta \cap X_i$, a contradiction, since $A_i \cong \mathrm{Alt}(X_i)$.

Hence we proved that for all $i \in R$ either $\Delta \cap X_i = \emptyset$ or $X_i \subseteq \Delta$. Since Ω is the disjoint union of the X_i's we conclude that $\Delta = \bigcup_{j \in J} X_j$ for some proper subset J of R. Pick $j \in J$ so that $j + 1 \notin J$ (This is possible since $\Delta \neq \Omega$ implies

$J \neq R$). Let x, x', and x'' be distinct elements of X and put $u = a_x^{-1}a_{x'}$. Then u fixes (j, x''). Moreover, since $u \in L_a \leq L$ and Δ is a block, $(j, x'') \in \Delta$ implies that u normalizes Δ. But this is a contradiction as $(j, x') \in \Delta$, $(j+1, x') \notin \Delta$ and $(j, x')^u = (j+1, x')$. Therefore L acts primitively on Ω.

Now since L is primitive on Ω and L contains three cycles, by [12, 2.13.3], $L = \mathrm{Alt}(\Omega)$ and the lemma is proved.

□

Lemma 3.44 *Let $\widehat{K}^* = \widehat{K}/\Phi(\widehat{K})$ and z_1, $z_2 \in Z$ with $\widehat{Z}^* = \langle \widehat{z_1}^*, \widehat{z_2}^* \rangle$. Then $\widehat{K} = \langle L_{\widehat{z_1}}, L_{\widehat{z_2}} \rangle$.*

Proof Since $\widehat{K}^* \cong A_r$, $\widehat{Z}^*$ is a semiregularly acting subgroup of $\widehat{K}^*$ of type (p,p), and $r = 4p^2 \geq \max\{p^2+1, 5p\}$, by Lemma 3.43, we have $\widehat{K}^* = \langle L_{\widehat{z_1}^*}, L_{\widehat{z_2}^*} \rangle$. But then $\widehat{K} = \langle L_{\widehat{z_1}}, L_{\widehat{z_2}} \rangle \Phi(\widehat{K})$. But then, by [3, 5.1.1], we get $\widehat{K} = \langle L_{\widehat{z_1}}, L_{\widehat{z_2}} \rangle$.

□

Lemma 3.45 *There exists a $1 \neq \widehat{z} \in \widehat{Z}$ and a composition factor C for $L_{\widehat{z}}$ on $[B, \widehat{z}]$ with $[L_{\widehat{z}}, C] \neq 1$.*

Proof First notice that both $L_{\widehat{z}}$ and $\widehat{Z}$ centralize $\widehat{z}$ and so both $L_{\widehat{z}}$ and $\widehat{Z}$ act on $[B, \widehat{z}]$. Now suppose the lemma is false. Then, for all $1 \neq \widehat{z} \in \widehat{Z}$, $L_{\widehat{z}}$ centralizes all the composition factors of $L_{\widehat{z}}$ on $[B, \widehat{z}]$. But $L_{\widehat{z}}$ is generated by p'-elements, by Lemma 3.37 (b). Hence, by the coprime action of these p'-elements on the p-group $[B, \widehat{z}]$, [3, 5.3.2] implies $[B, \widehat{z}, L_{\widehat{z}}] = 1$ for all $1 \neq \widehat{z} \in \widehat{Z}$. Let $\widehat{z_1}$, $\widehat{z_2}$, and $\widehat{z_3} \in \widehat{Z}$ with $\widehat{Z} = \langle \widehat{z_1}, \widehat{z_2} \rangle = \langle \widehat{z_1}, \widehat{z_3} \rangle = \langle \widehat{z_2}, \widehat{z_3} \rangle$. Then,

$$\begin{aligned}[C_B(\widehat{z_1}),\widehat{z_2}] = [C_B(\widehat{z_1}),\langle\widehat{z_1},\widehat{z_2}\rangle] &= [C_B(\widehat{z_1}),\widehat{Z}] \\ &= [C_B(\widehat{z_1}),\langle\widehat{z_1},\widehat{z_3}\rangle] \\ &= [C_B(\widehat{z_1}),\widehat{z_3}]\end{aligned}$$

and therefore

$$[C_B(\widehat{z_1}),\widehat{z_2}] = [C_B(\widehat{z_1}),\widehat{z_3}] = [C_B(\widehat{z_1}),\widehat{Z}]. \tag{1}$$

Now, by Lemma 3.44, $\widehat{K} = \langle L_{\widehat{z_2}}, L_{\widehat{z_3}}\rangle$. Hence, since $[B,\widehat{z},L_{\widehat{z}}] = 1$ for all $1 \neq \widehat{z} \in \widehat{Z}$, we have

$$\begin{aligned}[C_B(\widehat{z_1}),\widehat{z_2}] = [C_B(\widehat{z_1}),\widehat{z_3}] &\leq C_B(L_{\widehat{z_2}}) \cap C_B(L_{\widehat{z_3}}) \\ &\leq C_B(\langle L_{\widehat{z_2}}, L_{\widehat{z_3}}\rangle) \\ &= C_B(\widehat{K}).\end{aligned}$$

Now, since $C_B(\widehat{K}) \leq B$ is $\widehat{K}$-invariant and B is a irreducible $\widehat{K}$-module, either $C_B(\widehat{K}) = 1$ or B. Now $C_B(\widehat{K}) = B$ implies $[K,B] = [\widehat{K},B] = 1$ and therefore $K = C_K(B) \leq L$, a contradiction. Thus $C_B(\widehat{K}) = 1$ and so from above we get $[C_B(\widehat{z_1}),\widehat{z_2}] = [C_B(\widehat{z_1}),\widehat{z_3}] = [C_B(\widehat{z_1}),\widehat{Z}] = 1$. But this implies

$$C_B(\widehat{z_1}) = C_B(\widehat{z_2}) = C_B(\widehat{Z}). \tag{2}$$

Again, since $\widehat{K} = \langle L_{\widehat{z_1}}, L_{\widehat{z_2}}\rangle$, (2) implies $C_B(\widehat{Z})$ is a $\widehat{K}$-invariant subgroup of B. Hence, by the irreducibility of B, we get $C_B(\widehat{K}) = 1$ or B. But, since $\widehat{Z}$ is a p-group and B is a vector space over GF(p), by [3, 2.6.3], $C_B(\widehat{Z}) \neq 1$. Thus $C_B(\widehat{Z}) = B$ and so $[B,Z] = [B,\widehat{Z}] = 1$. Hence we get, $Z \leq C_K(B) \leq L$, a contradiciton.

□

Let $1 \neq \hat{z} \in \widehat{Z}$ and C be a composition factor for $L_{\hat{z}}$ on $[B, \hat{z}]$ such that $[C, L_{\hat{z}}] \neq 1$.

Lemma 3.46 *p is odd.*

Proof Suppose $p = 2$. Then, by Lemma 3.35, $[A, Z, Z] = 1$ and so also $[B, \hat{z}, \widehat{Z}] = 1$. Hence $[C, \widehat{Z}] = 1$, as C is a composition factor of $[B, \hat{z}]$. But then, by Lemma 3.42 (b), we get

$$[C, L_{\hat{z}}] = [C, \langle \widehat{Z}^{L_{\hat{z}}} \rangle] = 1$$

a contradiction to Lemma 3.45. Therefore p must be odd.

□

By Lemma 3.40 we may assume $\widehat{W^*}$ has the form

$$\widehat{W^*} = \langle \widehat{z_0}^* \rangle \times \widehat{E_{q^t}}^* * \langle \widehat{z^*} \rangle$$

where $\widehat{E_{q^t}}^*$ is an elementary abelian q-group of order q^t, q is an odd prime, $\widehat{Z^*} = \langle \widehat{z^*}, \widehat{z_0}^* \rangle$, and $\widehat{z_0}^*$ acts nontrivially and irreducibly on $\widehat{E_{q^t}}^*$.

Lemma 3.47 *Let $\widehat{W^*}$, $\widehat{E_{q^t}}^*$, $\widehat{z^*}$, $\widehat{z_0}^*$, and C, be as above. Then*

(a) $\widehat{E_{q^t}}^* = [\widehat{E_{q^t}}^*, \widehat{Z^*}]$.

(b) $\widehat{W^*} \leq L^*_{\hat{z}}$.

(c) $\widehat{Z} \leq L_{\hat{z}}$.

(d) $[C, \hat{z}] = 1$.

Proof Since $\widehat{E_{q^t}}^*$ is $\widehat{Z}^*$-invariant we have $[\widehat{E_{q^t}}^*, \widehat{Z}^*] \leq \widehat{E_{q^t}}^*$ and $[\widehat{E_{q^t}}^*, \widehat{Z}^*]$ is $\widehat{z_0}^*$-invariant. But, since $\widehat{z_0}^*$ acts nontrivially and irreducibly on $\widehat{E_{q^t}}^*$, we have $\widehat{E_{q^t}}^* = [\widehat{E_{q^t}}^*, \widehat{Z}^*]$.

For (b), since $\widehat{E_{q^t}}^* = [\widehat{E_{q^t}}^*, \widehat{Z}^*] \leq \langle \widehat{Z}^{*\widehat{W}^*} \rangle$ and $\widehat{Z}^* \leq \langle \widehat{Z}^{*\widehat{W}^*} \rangle$, we have $\widehat{W}^* = \langle \widehat{Z}^{*\widehat{W}^*} \rangle$. But, by Lemma 3.40 (b), $\widehat{Z}^* \leq L_{\hat{z}}^* \trianglelefteq C_{\widehat{K}^*}(\hat{z}^*)$ and $\widehat{W}^* \leq C_{\widehat{K}^*}(\hat{z}^*)$. Thus $\widehat{W}^* = \langle \widehat{Z}^{*\widehat{W}^*} \rangle \leq L_{\hat{z}}^*$ and we have (b).

For (c), $\widehat{Z}^* \leq L_{\hat{z}}^*$ implies $\widehat{Z} \leq L_{\hat{z}} \Phi(\widehat{K})$. Hence

$$
\begin{aligned}
\widehat{Z} &\leq L_{\hat{z}} \Phi(\widehat{K}) \cap C_{\widehat{K}}(\hat{z}) \\
&= L_{\hat{z}} (\Phi(\widehat{K}) \cap C_{\widehat{K}}(\hat{z})) \\
&= L_{\hat{z}} C_{\Phi(\widehat{K})}(\hat{z})
\end{aligned}
$$

Thus $\widehat{Z} \leq L_{\hat{z}} C_{\Phi(\widehat{K})}(\hat{z})$. But then

$$
\frac{\widehat{Z} L_{\hat{z}}}{L_{\hat{z}}} \leq \frac{L_{\hat{z}} C_{\Phi(\widehat{K})}(\hat{z})}{L_{\hat{z}}} \cong \frac{C_{\Phi(\widehat{K})}(\hat{z})}{C_{\Phi(\widehat{K})}(\hat{z}) \cap L_{\hat{z}}} \text{ is a } p' - \text{group}
$$

Therefore, since $\widehat{Z}$ is a p-group, we have $\widehat{Z} L_{\hat{z}} / L_{\hat{z}} = 1$ and so $\widehat{Z} \leq L_{\hat{z}}$.

Since $L_{\hat{z}}$ centralizes $\hat{z}$, we have $C_C(\hat{z})$ is a $L_{\hat{z}}$-invariant subgroup of C. Thus, since $L_{\hat{z}}$ acts irreducibly on C, we have either $C_C(\hat{z}) = 1$ or C. But since both C and $\langle \hat{z} \rangle$ are p-groups $C_C(\hat{z}) \neq 1$ by [3, 2.6.3]. Therefore $C_C(\hat{z}) = C$ and we have (d).

$\square$

Now $\widehat{z_0}^*$ acts nontrivially on $\widehat{E_{q^t}}^*$ and $1 \neq \widehat{E_{q^t}}^* \trianglelefteq \widehat{W}^*$ implies $\widehat{E_{q^t}}^*$ is $\widehat{Z}^*$-invariant and $[\widehat{E_{q^t}}^*, \widehat{Z}^*] \neq 1$. Thus $1 \neq \widehat{E_{q^t}} \trianglelefteq \widehat{W}$ and $[\widehat{E_{q^t}}, \widehat{Z}] \neq 1$ where $\widehat{W}$ and $\widehat{E_{q^t}}$ denote the preimages of $\widehat{W}^*$, $\widehat{E_{q^t}}^*$ in $\widehat{K}$ and $\widehat{Z}$ is the image of Z in $\widehat{K}$.

Lemma 3.48 *Let $\widehat{W}$, $\widehat{Z}$ and $\widehat{E_{q^t}}$ be as above. Then*

(a) $\widehat{E_{q^t}}$ is a p'-group.

(b) $\widehat{E_{q^t}} \cap L_{\hat{z}} \neq 1$.

(c) $[\widehat{E_{q^t}} \cap L_{\hat{z}}, \widehat{Z}] \neq 1$.

(d) There exists a $\widehat{Z}$-invariant q-Sylow subgroup $\widehat{E_0}$ of $\widehat{E_{q^t}} \cap L_{\hat{z}}$ with $[\widehat{E_0}, \widehat{Z}] \neq 1$.

Proof For (a), since $\widehat{E_{q^t}}^*$ is a q-group, $q \neq p$, and $\Phi(\widehat{K})$ is a p'-group, we have $\widehat{E_{q^t}}$ is a p'-group.

For (b), $\widehat{E_{q^t}}^* \leq \widehat{W}^* \leq L_{\hat{z}}^*$ implies $\widehat{E_{q^t}} \leq L_{\hat{z}}\Phi(\widehat{K})$ and therefore

$$\widehat{E_{q^t}} = \widehat{E_{q^t}} \cap L_{\hat{z}}\Phi(\widehat{K}) = (\widehat{E_{q^t}} \cap L_{\hat{z}})\Phi(\widehat{K}).$$

Hence, since $1 \neq \widehat{E_{q^t}}^*$, we have $\widehat{E_{q^t}} \neq \Phi(\widehat{K})$ and therefore $\widehat{E_{q^t}} \cap L_{\hat{z}} \neq 1$.

For (c), $\widehat{E_{q^t}} = (\widehat{E_{q^t}} \cap L_{\hat{z}})\Phi(\widehat{K})$ implies $\widehat{E_{q^t}}^* = (\widehat{E_{q^t}} \cap L_{\hat{z}})^*$. Therefore, since $[\widehat{E_{q^t}}^*, \widehat{Z}^*] \neq 1$, we have $[(\widehat{E_{q^t}} \cap L_{\hat{z}})^*, \widehat{Z}^*] \neq 1$ and so $[(\widehat{E_{q^t}} \cap L_{\hat{z}}), \widehat{Z}] \neq 1$.

Finally, since $\widehat{Z} \leq L_{\hat{z}}$ and $\widehat{E_{q^t}}$ is $\widehat{Z}$-invariant, we know that $1 \neq \widehat{E_{q^t}} \cap L_{\hat{z}}$ is a $\widehat{Z}$-invariant p'-group. Therefore by the [3, 6.2.2], there exists $\widehat{E_0} \in \mathrm{Syl}_q(\widehat{E_{q^t}} \cap L_{\hat{z}})$ with $\widehat{E_0}$ $\widehat{Z}$-invariant. Since $(\widehat{E_{q^t}} \cap L_{\hat{z}})^* = \widehat{E_{q^t}}^*$ is a q-group, we have $\widehat{E_0}^* = \widehat{E_{q^t}}^*$. Thus, $[\widehat{E_{q^t}}^*, \widehat{Z}^*] \neq 1$ implies $[\widehat{E_0}^*, \widehat{Z}^*] \neq 1$ and therefore $[\widehat{E_0}, \widehat{Z}] \neq 1$.

□

Now let $\widehat{E} = [\widehat{E_0}, \widehat{Z}]$. Then, by Lemma 3.48 (d), $1 \neq \widehat{E}$ is a $\widehat{Z}$-invariant q-group. Also let $\widehat{Y} = \widehat{E}\widehat{Z}$ and $X = \overline{\widehat{Y}} = \widehat{Y}/C_{\widehat{Y}}(C)$.

Lemma 3.49 *Let $\widehat{Y}$, X, and $\widehat{E}$ be choosen as above. Then* *(a)* $\widehat{E} = [\widehat{E}, \widehat{Z}]$.

(b) $L^*_{\hat{z}} = \langle \widehat{E}^{*L^*_{\hat{z}}} \rangle$ *and* $L_{\hat{z}} = \langle \widehat{E}^{L_{\hat{z}}} \rangle$.

(c) $O_p(X) = 1$.

Proof For (a), by the coprime action of the p-group $\widehat{Z}$ on the q-group $\widehat{E_0}$, [3, 5.3.6] implies

$$\widehat{E} = [\widehat{E_0}, \widehat{Z}] = [\widehat{E_0}, \widehat{Z}, \widehat{Z}] = [\widehat{E}, \widehat{Z}].$$

For (b) let $L_0 = \langle \widehat{E}^{*L^*_{\hat{z}}} \rangle$, $S = \mathrm{Solv}(L^*_{\hat{z}})$, $\overline{L^*_{\hat{z}}} = L^*_{\hat{z}}/S$, and $\overline{L_0}$ be the image of L_0 in $\overline{L^*_{\hat{z}}}$. Then, as in Lemma 3.42, the simplicity of $\overline{L^*_{\hat{z}}}$ implies $\overline{L_0} = 1$ or $\overline{L_0} = \overline{L^*_{\hat{z}}}$. Now $\overline{L_0} = 1$ implies $L_0 \leq S$ and therefore $\widehat{E}^* \leq S$. But, since S is a p-group and $\widehat{E}^*$ is a q-group, we get $\widehat{E}^* = 1 = [\widehat{E_0}^*, \widehat{Z}^*] = [\widehat{E_{q^t}}^*, \widehat{Z}^*]$, a contradiciton.

On the other hand, if $\overline{L_0} = \overline{L^*_{\hat{z}}}$, then $L^*_{\hat{z}} = L_0 S$. Thus, and therefore by Lemma 3.41, we get $L^*_{\hat{z}} = L_0$. The same argument used in Lemma 3.42 (e) now shows $L_{\hat{z}} = \langle \widehat{E}^{L_{\hat{z}}} \rangle$.

Finally, suppose (c) is false. Then $O_p(X) \neq 1$ and therefore $|X|_p \neq 1$. Now $\widehat{Z} \in \mathrm{Syl}_p(\widehat{Y})$ implies $\overline{\overline{\widehat{Z}}} \in \mathrm{Syl}_p(\overline{\overline{\widehat{Y}}}) = \mathrm{Syl}_p(X)$. Therefore $|\overline{\overline{\widehat{Z}}}| = p$ or p^2. Suppose $|\overline{\overline{\widehat{Z}}}| = p^2$. Then, since $|\widehat{Z}| = p^2$, we have

$$p^2 = |\overline{\overline{\widehat{Z}}}| = \frac{|\widehat{Z} C_{\widehat{Y}}(C)|}{|C_{\widehat{Y}}(C)|} = \frac{|\widehat{Z}|}{\widehat{Z} \cap C_{\widehat{Y}}(C)} = \frac{p^2}{|\widehat{Z} \cap C_{\widehat{Y}}(C)|}.$$

Thus we get $\widehat{Z} \cap C_{\widehat{Y}}(C) = 1$, a contradiction to Lemma 3.47 (d). Therefore $|\overline{\overline{\widehat{Z}}}| = p$ and so $\overline{\overline{\widehat{Z}}} = O_p(X) \trianglelefteq X$. Now $\widehat{Z}$ and $\widehat{E}$ normalize each other. Hence, since $\overline{\overline{\widehat{Z}}}$ is a p-group and $\overline{\overline{\widehat{E}}}$ is a q-group, we have $[\overline{\overline{\widehat{E}}}, \overline{\overline{\widehat{Z}}}] \leq \overline{\overline{\widehat{E}}} \cap \overline{\overline{\widehat{Z}}} = 1$. Thus

$[\widehat{E}, \widehat{Z}] \leq C_{\widehat{Y}}(C)$. But $\widehat{E} = [\widehat{E}, \widehat{Z}]$ by (a) and so $\widehat{E} \leq C_{\widehat{Y}}(C)$. Hence, we get $[\widehat{E}, C] = 1$ and therefore $[L_{\hat{z}}, C] = [\langle \widehat{E}^{L_{\hat{z}}} \rangle, C] = 1$, a contradiction. $\square$

Now, since X is a pq-group, X is solvable and therefore p-solvable. Moreover, C is a vector space over GF(p) and so X acts as a group of linear transformations on C. Consider $\overline{\widehat{z_0}} \in X$. By Lemma 3.35 (c) we have $[A, Z, p] = 1$ and so, since B is a section of A, $[B, \widehat{Z}, p] = 1$. Hence, $[B, \hat{z}, \widehat{z_0}, p-1] = 1$ and therefore $[C, \overline{\widehat{z_0}}, p-1] = 1$, as C is a section of $[B, \hat{z}]$. But then $(\overline{\widehat{z_0}} - 1)^{p-1} = 0$ on C. Now suppose p is a fermat prime. Then, since the sylow-2-subgroups of X are abelian (in fact, since p and q are odd, there trivial), by [3, 11.1.2], we get $\min_C(\overline{\widehat{z_0}}) = (x-1)^p$, a contradiction as $\overline{\hat{z}}$ satisfies a polynomial of degree less than p. On the other hand, suppose p is not a fermat prime. Then, since $p \neq 2$, again, by [3, 11.1.2], we get $\min_C(\overline{\widehat{z_0}}) = (x-1)^p$, a contradiction. This concludes the case in which G is of alternating type and therefore we have shown Theorem 3.1.

$\square$

Bibliography

Bibliography

[1] Micheal Aschbacher, *Finite group theory*, Cambridge University Press, 1986.

[2] Daniel Goldschmidt, *Automorphisms of Trivalent Graphs*, Ann. of Math.,111(1980) 377-404.

[3] D.Gorenstein, *Finite Groups*, Chelsa Publishing Company, New York 1982.

[4] Larry C. Grove, *Algebra*, Academic Press, Inc, 1983.

[5] O.Kegel and B.A.F Wehrfritz, *Locally Finite Groups*, North-Holland, 1973.

[6] Martin W. Liebeck and Jan Saxl, *On point stabilizers in primitive permutation groups*, Communications in Algebra, 19(10), (1991) 2777-2786.

[7] Ulrich Meierfrankenfeld, *Non-Finitary Locally Finite Simple Groups.*

[8] I.Schur, *Uber die Dantellungen der symmetrischen Gruppen und alternieren der gruppen durch gebrochenen linearen substitutionen*, Crelle J., 139 (1911) 155-250.

[9] Bernd Stellmacher, D.Goldschmidt, A.Delgado, *Groups and Graphs: New results and Methods*, Birkhausser, Basel 1985.

[10] Michio Suzuki, *Finite Groups*, Springer-Verlag, 1982.

[11] John. G Thompson, *Finite with normal p-complements*, Proceedings of Symposia in Pure Mathematics, vol1 (Finite Groups), 1-4 (1959).

[12] Helmut Wielandt, *Finite Permutation Groups*, Academic Press Inc. New York and London, 1964.