Large Abelian Subgroups of Finite p-Groups

George Glauberman

August 19, 1997

1 Introduction

Let p be a prime and S be a finite p-group. Define $d(S)$ to be the maximum of $|A|$ as A ranges over the abelian subgroups of S, and $\mathcal{A}(\mathcal{S})$ to be the set of all abelian subgroups A for which $|A| = d(S)$. Let $J(S)$ be the subgroup of S generated by $\mathcal{A}(\mathcal{S})$.

In 1964, John Thompson introduced [T2] a subgroup similar to $J(S)$ and used it to obtain an improved version of his first normal p-complement theorem [T1]. Since then, several variants of $J(S)$ have been used to obtain related results. Most of their proofs have required a further result of Thompson, the Replacement Theorem ([Gor, p.273], [HB, III, p.21]):

Suppose $A \in \mathcal{A}(\mathcal{S}), \mathcal{B}$ is an abelian subgroup of S normalized by A, and B does not normalize A. Then there exists $A^* \in \mathcal{A}(\mathcal{S})$ such that

$$A^* \leq AB, \quad A \cap B < A^* \cap B, \quad \text{and} \quad A^* \text{ normalizes } A.$$

It would be interesting to extend this result by allowing B to have nilpotence class 2 instead of necessarily being abelian. This cannot be done if $p = 2$ (Example 4.2), but perhaps it is possible for p odd. (It was done by the author ([Gor, p.274]; [HB, III, p.21]) for the special case in which p is odd and $[B, B] \leq A$.) However, there is an application of Thompson's Replacement Theorem that can be extended when p is odd and B has class 2, and this extension is our first main result. In order to state it, we require a definition.

Let $\mathcal{S}$ be a central series

$$1 = Z_0 \leq Z_1 \leq \cdots \leq Z_n = S$$

of a $p-$group S. For any abelian subgroups A, A^* of S, define $A <_{\mathcal{S}} A^*$ if

$$\begin{array}{rcll} |A| & = & |A^*| & \\ |A \cap Z_i| & \leq & |A^* \cap Z_i|, & \text{for } i = 1, 2, \ldots, n, \\ \text{and } A \cap Z_i & < & A^* \cap Z_i, & \text{for some } 1 \leq i \leq n \end{array}$$

Extending the notation of [Gor, pp.19,274] slightly, we define $[X, Y, Z]$ to be $[[X, Y], Z]$, for subsets or elements X, Y, Z of S, and define inductively

$$[T, u; 1] = [T, u]$$

and

$$[T, u; n+1] = [\ [T, u; n], u],\ \text{for } T \leq S,\ u \in S,\ \text{and } n \geq 1.$$

Theorem 1 Suppose p is an odd prime, S is a finite p-group, $A \in \mathcal{A}(\mathcal{S})$, and B is a subgroup of S that does not normalize A. Assume that

(i) B has nilpotence class at most 2 and is normalized by A,

or

(ii) $p \geq 5$, and $A \lhd < A^B >$, and $[A, u; 3] = 1$, for every $u \in B$.

Then there exists $A^* \in \mathcal{A}(\mathcal{S})$ such that

(a) $A^* \leq < A^B >$ and A^* normalizes A,

(b) for every central series $\mathcal{S}$ of S, $A <_{\mathcal{S}} A^*$, and

(c) if A normalizes B, then $|A^* \cap B| \geq |A \cap B|$.

Corollary Suppose p is an odd prime, S is a finite p-group, and $\mathcal{S}$ is a central series of S. Let A be a maximal element of $\mathcal{A}(\mathcal{S})$ under $<_{\mathcal{S}}$.

Then A is normalized by every subgroup B of S for which

(i) B has nilpotence class at most 2 and is normalized by A,

or

(ii) $p \geq 5$, $A \lhd < A^B >$, and $[A, u; 3] = 1$, for every $u \in B$.

Theorem 1 is proved by reducing to the case in which A itself is contained in a normal subgroup $\hat{A}$ of class at most 3 (class at most 2, if p =3) in a subgroup of $< A^B >$. Then, by a result of M. Lazard, one may regard $\hat{A}$ as a Lie ring. As in the proof of the Replacement Theorem, one explicitly constructs the subgroup A^*. The ideas in the proofs of Lemma X.3.1 and Corollary X.3.2, pp. 19-20, of [HB, III] (applications of Thompson's Replacement Theorem) are used to prove that $A <_{\mathcal{S}} A^*$.

We say that an abelian subgroup A of S is *irreplaceable with respect to class* 2 *subgroups of* S if A satisfies the conclusion of the corollary of Theorem 1. We write $\mathcal{A}_{\in}(\mathcal{S})$ for the set of all such subgroups in $\mathcal{A}(\mathcal{S})$. Thus, $\mathcal{A}_{\in}(\mathcal{S})$ is not empty.

Although there are examples in which no member of $\mathcal{A}(\mathcal{S})$ is normal in S (Example 4.1), our next main result and Corollary 1 show that, if $p \geq 5$, every subgroup in $\mathcal{A}_{\in}(\mathcal{S})$ is close to being a normal subgroup in some sense:

Theorem 2 Suppose p is a prime and $p \geq 5$, S is a finite p-group and $A, A_0 \in \mathcal{A}_{\in}(\mathcal{S})$. Then

(a) A and A_0 normalize each other,

and

(b) A is normalized by every subgroup B of S such that $[A, u; 3] = 1$ for every $u \in B$.

Corollary 1 Suppose $p \geq 5$ and $A \in \mathcal{A}_{\in}(\mathcal{S})$. Then

(a) A^x and A^y normalize each other, for every $x, y \in S$.

(b) $\prod_{x \in S} A^x \lhd S$ and $A \lhd \prod_{x \in S} A^x$.

and

(c) $[S, A, A, A] = 1$.

These results allow us to define a characteristic subgroup of S, contained in $J(S)$, in the next corollary. A similar characteristic subgroup is used in Theorems 3 and 4.

Corollary 2 Suppose $p \geq 5$. Let $H = < A \mid A \in \mathcal{A}_{\in}(\mathcal{S}) >$. Then

(a) H is a characteristic subgroup of S.

(b) $H = \prod_{A \in \mathcal{A}_{\in}(\mathcal{S})} A$.

(c) $A \lhd H$ for every $A \in \mathcal{A}_{\in}(\mathcal{S})$.

We do not know whether analogous results are valid for $p = 2$ or $p = 3$, possibly for A maximal under $<_{\mathcal{S}}$ for some central series $\mathcal{S}$, although we are dubious about $p = 2$. We have not attempted to generalize Theorem 1 to the case in which B has nilpotence class 3 or more, or $[A, B; k] = 1$ for some $k \geq 4$. Some results of this sort for *elementary* abelian subgroups of maximal order in S are obtained by different methods in [AG].

Now let us consider the situation in which S is contained in a finite group G, not necessarily a p-group. Assume that

(1.1) S is a Sylow p-subgroup of G

and

(1.2) for $T = O_p(G),\ C_G(T) \leq T$.

In 1968, using Thompson's Replacement Theorem and other methods, we proved [G1, I] that

$$\text{if } J(S) \not\!\lhd G, \text{ then there exists } u \in S - T \quad \text{such that}$$

$[X, u; 6] \leq Y$, for every chief factor X/Y of G such that $X \leq T$.

Thompson asked whether, for some suitable characteristic subgroup in place of $J(S)$, one could obtain the stronger condition

$$[X, u; 2] \ \leq \ Y.$$

In 1970, we improved our 1968 result ([G2, p.35]; [S, p.231]; [HB, III, p.63]) to

$$[X, u; 4] \leq Y \text{ if } K_{\infty}(S) \not\!\lhd G \text{ or } K^{\infty}(S) \not\!\lhd G,$$

for certain characteristic subgroups $K_{\infty}(S), K^{\infty}(S)$ of S. Now, by using Theorems 1 and 2, we have found a characteristic subgroup, $ZJ^N(S)$, for which we can obtain $[X, u; 3] \leq Y$, which is closer to Thompson's condition:

Theorem 3 Let p be a prime. Assume (1.1) and (1.2), and suppose that $ZJ^N(S) \not\trianglelefteq G$. Then

(a) G is not p-stable

and

(b) there exists $u \in S - T$ such that $[X, u; 3] \leq Y$, for every chief factor X/Y of G such that $X \leq T$.

We note that if $S > 1$, then $K_\infty(S), K^\infty(S), ZJ^N(S) \geq Z(S) > 1$. The definition of $ZJ^N(S)$ is given in Definitions 6.1, 6.2 and 6.11.

Theorem 3 yields the following consequence:

Theorem 4 Suppose $p \geq 5$, S is a Sylow p-subgroup of a group G, and $Z = ZJ^N(S)$. Then

$$G/O^p(G) \;\cong\; N_G(Z)/O^p(N_G(Z)).$$

This is proved from Theorem 3 by the same argument that yields the analogous results for $K_\infty(S)$ and $K^\infty(S)$ ([S, pp. 242-3]; [HB, III, p.65]).

Our 1970 result was applied by D. Holt [Hol] and M. Miyamoto [M] to prove results on cohomology. Because of the improvement from

$$[X, u; 4] \leq Y \quad \text{in 1970}$$

to

$$[X, u; 3] \leq Y \quad \text{in Theorem 3,}$$

their proofs remain valid almost word-for-word with the substitution of some smaller numbers. First, Holt's results now assert:

> Suppose $p \geq 7$ and S is a Sylow p-subgroup of a group G. Then the p-primary parts of the Schur multipliers of G and $N_G(ZJ^N(S))$ are isomorphic. Moreover, for any G-module M on which G acts trivially, $H^2(G, M)$ and $H^2(N_G(ZJ^N(S)), M)$ have isomorphic p-primary parts.

(In pp.196 and 198 in [Hol], replace "$[X, g^{(4)}] \leq Y$" with "$[X, g^{(3)}] \leq Y$" and "$[U, g^{(7)}] \leq V$" with "$[U, g^{(5)}] \leq V$.")

Second, Miyamoto's Theorem B immediately gives:

Suppose S is a Sylow p-subgroup of a group G, m is an integer, $m \geq 2$, and $p \geq 3 + 8 \cdot 6^{m-2}$. Then the restriction map induces an isomorphism of cohomology

$$H^m(G, M) \;\cong\; H^m(N_G(ZJ^N(S)), M)$$

for every trivial p-primary G-module M.

The main part of the above-mentioned reduction of Theorem 1 to a special case is given in Section 2. In Section 3, Lazard's result and a result on Lie rings are used to finish the proof of Theorem 1. A short proof of Theorem 2, and some counterexamples, appear in Section 4. Theorem 3 is proved in Sections 5 and 6.

All of these results stem originally from a failed counterexample to Theorem 1. There is a natural choice for the subgroup A^* in Theorem 1 (Remark 3.3) but the author constructed some examples in which this choice is not abelian. However, our attempt to show that *no* subgroup A^* satisfied the theorem met with unexpected obstacles that eventually resolved themselves into Theorem 3.2 and Theorem 1.

Our notation is standard and generally taken from [Gor], except that we write $A \leq B$ to mean that A is a subgroup of B and $A < B$ to mean that $A \leq B$ and $A \neq B$. In particular, we usually denote the commutator subgroup $[H, H]$ of a group H by H'.

All groups in this paper are finite, except possibly those appearing as additive groups of algebras. In addition,

throughout this paper p denotes a fixed but arbitrary prime, and S denotes a fixed but arbitrary finite p-group.

Often p will be assumed to be odd.

During the preparation of this paper, the author enjoyed the support of a National Security Agency grant and the hospitality of the Institute for

Advanced Study and the Drive Train Research Institute. He thanks each of these institutions. He also thanks the referee for a very careful reading of the original version and many corrections.

2 Reduction for Theorem 1

We now start toward the proof of Theorem 1. We will sometimes use the following lemma without explicitly mentioning it.

Lemma 2.1 [H, pp.254,257-8,292] Let G be a group generated by a subset X, and let

$$G = G_1 \geq G_2 \geq \cdots$$

be the lower central series of G.

(a) (E. Witt) For $x, y, z \in G$,

$$[x, y^{-1}, z]^y \; [y, x^{-1}, x]^z \; [z, x^{-1}, y]^x = 1$$

(b) (P. Hall: Three Subgroups Lemma) For $H, K, L \leq G$ and $N \lhd G$,

$$\text{if } [H, K, L] \leq N \quad \text{and} \quad [K, L, H] \leq N, \text{ then } [L, H, K] \leq N.$$

(c) For $k = 1, 2, 3, \ldots$,

$$\begin{aligned} G_k &= \; < [x_1, x_2, \ldots, x_k]^y \mid x_1, \ldots, x_k \in X \text{ and } y \in G > \\ &= \; < [x_1, x_2, \ldots, x_k], G_{k+1} \mid x_1, \ldots, x_k \in X > \end{aligned}$$

(d) Suppose $k, a_1, \ldots, a_k, n_1, \ldots, n_k, n$ are all integers and $k \geq 2$, and $n_1, \ldots, n_k \geq 1$, and $n = n_1 + \ldots + n_k$. Let $x_i \in G_{n_i}$ for $i = 1, 2, \ldots k$. Then

$$[x_1^{a_1}, \ldots, x_k^{a_k}] \equiv [x_1, \ldots, x_k]^{a_1 \ldots a_k} \quad (\text{modulo } G_{n+1}).$$

Lemma 2.2 Suppose $A \leq S$ and $b \in S$, and let

$$T =< A, b > \quad \text{and} \quad \hat{A} =< A^T > .$$

For each positive integer k, let $R_k =< A^{b^i} \mid 0 \leq i \leq k >$. Then

(a) $\hat{A} = < A^{b^k} \mid k$ an integer $>$,

(b) for each positive integer k,

$$R_k = < a, [a, b; i] \mid a \in A, 1 \leq i \leq k >,$$

(c) if $k \geq 2$, and $[A, b; k] = 1$, then $\hat{A} = R_{k-1}$ and, if in addition A is abelian and $A \lhd \hat{A}$, then $\hat{A}$ has nilpotence class at most k,

(d) if $[A, b; 3] = 1$, then $[A, < b >; 3] = 1$,

and

(e) if $[A, b; 2] = 1$, then $[A, < b >; 2] = 1$.

<u>Proof:</u> (a) Let $A^* = < A^{b^k} \mid k \in \mathbb{Z} >$. Then $A \leq A^* \leq < A^T > = \hat{A}$ and $N_T(A^*) \geq < b, A > = T$. So

$$\hat{A} = < A^T > \leq < A^{*T} > = A^* \leq \hat{A}, \quad \text{and} \quad A^* = A.$$

(b) For every $x \in T$, $x^b = x[x, b]$. This proves (b) for $k = 1$. Since $R_{k+1} = < R_k, R_k^b >$ for every $k \geq 1$, the general case follows by induction.

(c) Here, by (b), we have $R_{k-1} = R_i$ for every $i \geq k - 1$. So

$$R_{k-1}^b \leq R_k = R_{k-1}; \ b \in N_T(R_{k-1}); \quad \text{and} \quad N_T(R_{k-1}) \geq < A, b > = T.$$

Arguing as in the proof of (a), we obtain that $\hat{A} = R_{k-1}$.

Suppose A is abelian and $A \lhd \hat{A}$. Then $A, A^b, \cdots, A^{b^{k-1}}$ are abelian normal subgroups of $\hat{A}$ that generate $\hat{A}$. By Lemma 2.1, to complete the proof it will suffice to show that, for any $x_1, \ldots, x_{k+1}$ in the set-theoretic union of these subgroups,

$$[x_1, x_2, \ldots, x_{k+1}] = 1.$$

However, this is obvious because at least two of the elements x_i must lie in the same abelian normal subgroup A^{b^j} of $\hat{A}$.

(d) Assume $[A, b; 3] = 1$. Let $D_1 = [A, < b >], D_2 = [A, b], E = [A, b; 2]$, and $R = < D_2, b >$. Then $E = [D_2, b]$, which is normalized by D_2 (as in the proof of [Gor], Theorem 2.2.1(iii), p.18), and E is centralized by b. Hence R normalizes E. As $E \le R$, we have $E \lhd R$.

We claim that $D_1 \le R$. Since b has finite order,

$$D_1 \;=\; <[a, b^i] \mid a \in A, i \ge 1> .$$

So we will show by induction on i that $[a, b^i] \in R$ for all a and i. The proof is trivial for $i = 1$. Assume it is proved for some $i \ge 1$. Then

$$[a, b^i] \in R \;=\; <D_2, b> \quad \text{and} \quad [a, b^{i+1}] = [a, b][a, b^i]^b \in R,$$

as desired. Thus

$$D_1 \;\le\; R \;=\; <D_2, b> .$$

Now, $E \lhd R$ and, modulo E, the coset of b centralizes D_2E/E and R/E. Therefore,

$$[A, <b>; 2] \;=\; [D_1, <b>] \;\le\; [R, <b>] \;\le E \;=\; [A, b; 2] \;\le\; C_R(b),$$

and

$$[A, <b>; 3] \;\le\; [C_R(b), <b>] = 1,$$

as desired.

(e) The proof is similar to the proof of (d), but easier.

Q.E.D.

We now begin to reduce the proof of Theorem 1 to the case in which A is contained in a normal subgroup $<A, B>$ of nilpotence class 2.

Theorem 2.3 Suppose p is odd, $A \in \mathcal{A}(\mathcal{S})$, and B is a subgroup of S of nilpotence class at most 2 normalized by A. Assume that B does not normalize A.

Then there exists $b \in B - N(A)$ such that, for

$$T = <b, A> \quad \text{and} \quad \hat{A} = <A^T> = <A^x | x \in T>,$$

$\hat{A}$ has nilpotence class 2.

Proof

We may assume that B is minimal subject to the hypothesis of the theorem. Take $b \in B - N(A)$. Since S is nilpotent, $B' = [B, B] < B$ and $[B, A] < B$.

As A normalizes B' and $[B, A]$,

$$B'[B, A] \text{ normalizes } A \tag{2.1}$$

Let

$$T = < b, A > \text{ and } \hat{A} = < A^T > .$$

Then $B \cap T$ is normal in T and hence is normalized by A. By the minimal choice of B,

$$B = B \cap T \leq T \quad \text{and} \quad T = < b, A > \ = \ BA.$$

Therefore, by (2.1),

$$T' = [T, T] = B'[B, A] \leq N_B(A). \tag{2.2}$$

Let the lower central series of T be

$$T = T_1 \geq T_2 \geq T_3 \geq \cdots .$$

<u>Step 1</u>: We have $T_5 \leq Z(T)$ and $T_6 = 1$.

<u>**Proof:**</u>

From (2.1),

$$\begin{aligned}
T_3 &= [T', T] \leq [N_B(A), BA] \leq B'(A \cap B), \\
T_4 &= [T_3, T] \leq [B'(A \cap B), BA] \leq B', \\
T_5 &\leq [B', BA] = [B', A] \leq B' \cap A \leq Z(B) \cap A \leq Z(T) \text{ (by (2.1))}, \\
T_6 &\leq [Z(T), T] = 1.
\end{aligned}$$

Recall that, in a group of odd order, each element u has a unique square root $u^{\frac{1}{2}}$, and $u^{\frac{1}{2}} = u^i$ for some integer i. For any $u, v \in T$, we write u^{-v} for $(u^{-1})^v$.

<u>Step 2</u>: For all $a, a' \in A$,

(a) $[b, a, b, a'] \in Z(T)$,

and

(b) $[b, a, a', b] = [b, a', a, b] \in Z(T)$.

Proof:

Take any $a, a' \in A$. Then, by (2.1),

$$[b, a, b, a'] \in [B', A] \leq B' \cap A \leq Z(T),$$

which proves (a). Moreover,

$$[b, a] = b^{-1}b^a,\ \ [b, a, a'] = (b^{-1}b^a)^{-1}(b^{-1}b^a)^{a'} = b^{-a}bb^{-a'}b^{aa'}.$$

Similarly,

$$[b, a', a] = b^{-a'}bb^{-a}b^{aa'}.$$

Since B/B' is abelian and $aa' = a'a$,

$$[b, a, a'] \equiv bb^{-a}b^{-a'}b^{aa'} \equiv [b, a', a] \quad (\text{modulo } B')$$

As $B' \leq Z(B)$,

$$[b, a, a', b] = [b, a', a, b]. \tag{2.3}$$

By several applications of Lemma 2.1 we obtain (modulo T_5)

$$\begin{aligned} 1 \ &\equiv \ [\ [b, a], a', b]\ [a', b, [b, a]\ ]\ [b, [b, a], a'] \\ &\equiv \ [b, a, a', a]\ [\ [b, a'],\ [b, a]\ ]^{-1}[b, a, b, a']^{-1}, \end{aligned}$$

and

$$[b, a, a', b] \equiv [b, a, b, a']\ [[b, a'], [b, a]\ ] \quad (\text{modulo } T_5). \tag{2.4}$$

Interchanging a with a' yields

$$[b, a', a, b] \equiv [b, a', b, a]\ [\ [b, a], [b, a']\ ] \quad (\text{modulo } T_5). \tag{2.5}$$

However,

$$[\ [b, a], [b, a']\ ] \ = \ [\ [b, a'], [b, a]\ ]^{-1} \quad (\text{modulo } T_5).$$

Therefore, (2.3), (2.4), (2.5) yield

$$[b, a, a', b]^2 \ \equiv \ [b, a, b, a'][b, a', b, a] \quad (\text{modulo } T_5).$$

By (a) and Step 1, $[b, a, a', b]^2 \in Z(T)$. Since T has odd order, this and (2.3) yield (b).

Step 3: We have $T_4 \leq Z(T)$ and $T_5 = 1$.

Proof:

Let X be the set-theoretic union of $\{b\}$ with A. By Lemma 2.1, since $T =< b, A >=< X >$,

(2.6) $$T_4 =< [x_1, x_2, x_3, x_4], T_5 \mid x_i \in X \text{ for } i = 1, 2, 3, 4 >$$

By Step 1,

(2.7) $$T_5 \ \leq \ Z(T)$$

Suppose y is a commutator $[x_1, x_2, x_3, x_4]$ of the form in (2.6). We must show that $y \in Z(T)$. We may assume that $y \neq 1$. Then $[x_1, x_2] \neq 1$. Hence, one of x_1, x_2 is b, and the other is in A. From Lemma 2.1,

$$\begin{aligned} [x_2, x_1, x_3, x_4] &\equiv [[x_1, x_2]^{-1}, x_3, x_4] \equiv [x_1, x_2, x_3, x_4]^{-1} \\ &\equiv y^{-1} \quad (\text{modulo } T_5). \end{aligned}$$

So, by (2.7), we may assume that

$$x_1 = b \quad \text{and} \quad x_2 \in A.$$

Now, $[x_1, x_2] \in [B, A] \leq N_B(A)$, by (2.1). Hence,

$$y \in [N_B(A), A, A] \leq [A, A] = 1, \text{ if } x_3, x_4 \in A;$$

$$y \in [N_B(A), B, B] \leq [B', B] \ = 1, \text{ if } x_3 = x_4 = b.$$

Therefore, one of x_3, x_4 is b, and the other is in A. By Step 2, $y \in Z(T)$, as desired.

By (2.6) and (2.7), $T_4 \leq Z(T)$. Thus, $T_5 \leq [Z(T), T] = 1$.

Recall that $\hat{A} =< A^T >=< A^x | x \in T >$.

Step 4: We have

(a) $T_4 \leq Z(T) \leq Z(\hat{A})$;

(b) $\hat{A} =< A^{b^k} | k \ \in \ \mathbb{Z} \ >$;

(c) if $a \in A$ and $a^b \equiv a$ (modulo $Z(\hat{A})$), then $a \in Z(\hat{A})$;

(d) $\hat{A} =< a, [a, b], [a, b, b] | a \in A >$;

(e) $\hat{A}' \leq Z(\hat{A})$.

Proof:

(a) By Step 3, $T_4 \leq Z(T) \leq C_S(A) = A \leq \hat{A}$, so $Z(T) \leq Z(\hat{A})$.

(b) Apply Lemma 2.2(a).

(c) Here, let $C = C_{\hat{A}}(a)$. Then $A \leq C \leq \hat{A}$, and for every integer k,

$$C \geq C_{\hat{A}}(aZ(\hat{A})) = C_{\hat{A}}((aZ(\hat{A}))^{b^k}) = (C_{\hat{A}}(aZ(\hat{A})))^{b^k} \geq A^{b^k}.$$

By (b), $C \geq \hat{A}$.

(d) Apply Lemma 2.2(c)

(e) Here, it suffices to show that the third term of the lower central series of $\hat{A}$ reduces to the identity group. We take the set of generators of $\hat{A}$ given in (d). So we merely need to show that

$$[x_1, x_2, x_3] = 1$$

if each x_i has the form $a, [a, b]$, or $[a, b, b]$ for some $a \in A$.

By Step 3, $T_5 = 1$. Therefore, we may assume that each x_i has the form a or $[a, b]$, and that only one has the form $[a, b]$. Since $[A, A] = 1$, there exist $a_1, a_2, a_3 \in A$ such that

$$[x_1, x_2, x_3] \;=\; [[a_1, b], a_2, a_3] \in [[B, A], A, A] \leq [N_T(A), A, A] = 1$$

or

$$[x_1, x_2, x_3] \;=\; [a_1, [a_2, b], a_3] \in [A, [B, A], a] = [[B, A], A, A] = 1.$$

This completes the proof of (e), of Step 4, and of the theorem.

Q.E.D

3 Proof of Theorem 1

The goal of this seection is to prove Theorem 1. However, most of our proof consists of results on Lie rings. Recall that a *derivation* of a Lie ring δ is an additive endomorphism of L such that

$$\delta[u,v] \;=\; [\delta u, v] \;+\; [u, \delta v], \quad \text{for all} \quad u, v \in L.$$

We say that an additive group A is *divisible by 2* if, for each $u \in A$, there exists a unique element v of A such that $2v = u$. In this case, for an automorphism α of A such that

$$0 = A(\alpha - 1)^3 \;=\; \{u\alpha^3 - 3u\alpha^2 + 3u\alpha - u \mid u \in A\},$$

we define

$$\log \alpha = (\alpha - 1) - \frac{1}{2}(\alpha - 1)^2.$$

Similarly, for an endomorphism γ such that $\gamma^3 = 0$, we define

$$\exp(\gamma) \;=\; 1 + \gamma + \frac{1}{2}\gamma^2.$$

Note that A is divisible by 2 if A is finite of odd order, or if A is a vector space over a field of characteristic other than 2.

The following appears to be a special case of a result that is well known, but hard to find. Related results are proved in [AG, Propositions 2.1, 2.4 and 2.5].

Lemma 3.1. Suppose L is a Lie ring divisible by 2, $\alpha \in \mathrm{Aut}\ L$, and $L(\alpha - 1)^3 = 0$. Let $\delta = \log(\alpha)$. Assume that

(3.1) $$L = 3L \quad \text{or} \quad [\ L(\alpha - 1),\ L(\alpha - 1)^2\ ] \;=\; 0.$$

Then δ is a derivation of L, and $\alpha = \exp \delta$.

Proof:
We have

$$\delta = (\alpha - 1) - \frac{1}{2}(\alpha - 1)^2 = -\frac{3}{2} + 2\alpha - \frac{\alpha^2}{2},$$

and it is easy to show that $\delta^3 = 0,\ \alpha = \exp \delta$, and $\alpha^2 = \exp 2\delta$.

Take any $u, v \in L$. Then

$$\begin{aligned}
\delta[u,v] &= -\frac{3}{2}[u,v] + 2[u,v]^{\alpha} - \frac{1}{2}[u,v]^{\alpha^2} \\
&= -\frac{3}{2}[u,v] + 2[u^{\alpha},v^{\alpha}] - \frac{1}{2}[u^{\alpha^2},v^{\alpha^2}] \\
&= -\frac{3}{2}[u,v] + 2[u+u\delta+\frac{1}{2}u\delta^2, v+v\delta+\frac{1}{2}v\delta^2] \\
&\qquad - \frac{1}{2}[u+2u\delta+2u\delta^2, v+2v\delta+2v\delta^2].
\end{aligned}$$

By performing the obvious calculations, one obtains,

$$\delta[u,v] = [u,v\delta] + [u\delta,v] - [u\delta,v\delta^2] - [u\delta^2,v\delta] - \frac{3}{2}[u\delta^2,v\delta^2]. \tag{3.2}$$

Since $\alpha^2 = \exp 2\delta$, we may substitute 2δ for δ in (3.2). Then, dividing by 2 yields

$$\delta[u,v] = [u,v\delta] + [u\delta,v] - 4[u\delta,v\delta^2] - 4[u\delta^2,v\delta] - 12[u\delta^2,v\delta^2]. \tag{3.3}$$

Subtracting (3.3) from (3.2) yields

$$0 = 3(\ [u\delta,v\delta^2] + [u\delta^2,v\delta]\ ) + \frac{21}{2}[u\delta^2,v\delta^2]. \tag{3.4}$$

Assume first that $L \neq 3L$. By hypothesis,

$$[\ L(\alpha-1), L(\alpha-1)^2\ ] \ = \ 0.$$

It follows that

$$[\ L(\alpha-1)^2, L(\alpha-1)^2\ ] \ = \ 0.$$

Since $\alpha = \exp\delta$, easy calculations give

$$[L\delta^2, L\delta^2] \ = \ 0 \qquad \text{and} \qquad 0 \ = \ [L\delta, L\delta^2] \ = \ [L\delta^2, L\delta].$$

By (3.2), δ is a derivation.

Now assume $L = 3L$. Take any $u, v \in L$. Then $u = 3u'$ for some $u' \in L$. Substituting u' for u in (3.4) yields (since $3[u'\delta, v\delta^2] = [u\delta, v\delta^2]$ etc.)

$$(3.5) \qquad 0 \;=\; [u\delta, v\delta^2] + [u\delta^2, v\delta] + \frac{7}{2}[u\delta^2, v\delta^2].$$

Substituting $u\delta$ for u in (3.5) yields $0 = [u\delta^2, v\delta^2]$. Then (3.5) yields

$$0 = [u\delta, v\delta^2] + [u\delta^2, v\delta].$$

Now (3.2) reduces to the assertion that δ is a derivation.

Q.E.D.

We write $Z(L)$ for the center of a Lie ring L.

Theorem 3.2. Let A be an abelian subring of a Lie ring L, and δ be a derivation of L. Assume that

(L1) A and L are divisible by 2,

(L2) $\delta^3 = 0$,

(L3) $A = 3A$ or $[\delta^2 L, \delta L] = 0$,

(L4) $L = A + \delta A + \delta^2 A$.

and

(L5) $A \geq Z(L)$.

Let

(L6) $A_1 = \{a - 2\delta b \mid a, b \in A \text{ and } \delta a - \delta^2 b \in Z(L)\}$ and $A^* = A_1 + \delta^2 A$.

Then

(a) A^* is a δ-invariant abelian subring of L that contains $Z(L)$;

(b) for each $a \in A$,

$$a \in Z(L) \quad \text{if and only if} \quad \delta a \in Z(L);$$

and

(c) if $a \notin Z(L)$, then either

(c1) $\delta^2 a \in A^* - A$,

or

(c2) $\delta^2 a \in Z(L) \leq A$ and $\delta a \in A^* - A$.

In addition, the following conditions are satisfied:

(d) Suppose $A < L$, and

$$0 \ = \ Z_0 \leq Z_1 \leq Z_2 \leq \ldots \leq Z_n = L$$

is a series of additive subgroups of L such that $\delta(Z_i) \ \leq \ Z_{i-1}$, for $i = 1, 2, \ldots, n$.

Then $A \cap Z_i = Z(L) \cap Z_i < A^* \cap Z_i$ for some $i, \ 1 \leq i \leq n$.

(e) Suppose L is finite of odd order. Then $|A^*| = |A|$ and $|A^* \cap M| \geq |A \cap M|$ for every δ-invariant additive subgroup M of L.

Remark 3.3. It would seem more natural to use $a - \delta b$ to define A_1 in (L6), but this sometimes yields a non-abelian group. Perhaps (L6) may seem more natural in view of [AG, Proposition 2.2].

The proof of (e) can be easily adapted to prove the following variation:

Suppose in Theorem 3.2 that L is a finite-dimensional Lie algebra over a field of characteristic other than 2, A is an F-subalgebra of L, and δ is a linear transformation over F. Then A^* is an F-subalgebra of L,

$$\dim_F \, (A^*) \ = \ \dim_F \, (A).$$

and

$$\dim_F \, (A^* \cap M) \geq \ \dim_F \, (A \cap M)$$

for every δ-invariant F-subspace M of L.

Proof of Theorem 3.2:

Consider any $a, b \in A$. Since A is abelian, $[a, b] = 0$. Therefore,

(3.6) $$0 = \delta[a, b] = [\delta a, b] + [a, \delta b], \quad \text{for} \quad a, b \in A;$$

(3.7) $$0 = \delta^2[a, b] = [\delta^2 a, b] + 2[\delta a, \delta b] + [a, \delta^2 b], \quad \text{for} \quad a, b \in A.$$

Since $\delta^3 = 0$, similar calculations for any $u, v \in L$ yield

$$\begin{aligned} 0 &= \delta^3[u,v] = [\delta^3 u, v] + 3[\delta^2 u, \delta v] + 3[\delta u, \delta^2 v] + [u, \delta^3 v] \\ &= 3\{[\delta^2 u, v] + [\delta u, \delta^2 v]\}. \end{aligned}$$

Substituting δu for u gives $0 = 3[\delta^2 u, \delta^2 v]$. By (L3) and the method for the last part of the proof of Lemma 3.1,

$$[\delta^2 u, \delta v] + [\delta u, \delta^2 v] = [\delta^2 u, \delta^2 v] = 0, \quad \text{for all} \quad u, v \in L. \tag{3.8}$$

(a) Now we check the properties of A^*. It is easy to see that A_1 and A^* are additive subgroups of L, and that $\delta(Z(L)) \leq Z(L)$. For $a \in Z(L)$ and for $b = 0$, we have (by (L5))

$$a, b \in A \quad \text{and} \quad \delta a - \delta^2 b = \delta a \in Z(L).$$

Hence, $a = a - 2\delta b \in A_1 \leq A^*$, and $Z(L) \leq A^*$.

Take any $a, b \in A$ such that $\delta a - \delta^2 b \in Z(L)$, as in the definition of A_1 in (L6). Then

$$\delta(a - 2\delta b) \equiv \delta a - 2\delta^2 b \equiv \delta^2 b - 2\delta^2 b \equiv -\delta^2 b \quad (\text{modulo } Z(L)),$$

and $-\delta^2 b \in \delta^2 A$. Thus, $\delta A_1 \leq \delta^2 A + Z(L) \leq A^*$, and

$$\delta A^* = \delta A_1 + \delta(\delta^2 A) \leq A^* + 0 = A^*.$$

So A^* is invariant under δ.

To complete the proof of (a), we must show that A^* is an abelian subring of L. By (3.8), $[\delta^2 A, \delta^2 A] = 0$. Next, suppose $a, b, c \in A$ and $\delta a - \delta^2 b \in Z(L)$. Then

$$\begin{aligned} [a - 2\delta b, \delta^2 c] &= [a, \delta^2 c] - 2[\delta b, \delta^2 c] \quad (\text{by } (3.7)) \\ &= -2[\delta a, \delta c] - [\delta^2 a, c] - 2[\delta b, \delta^2 c] \\ &= -2[\delta^2 b, \delta c] - [\delta^3 b, \delta c] - 2[\delta b, \delta^2 c] \\ &= -2([\delta^2 b, \delta c] + [\delta b, \delta^2 c]) = 0 \quad (\text{by } (3.8)). \end{aligned}$$

Thus $[A_1, \delta^2 A] = 0$.

Finally, assume $a, b, a', b' \in A$ and $\delta a - \delta^2 b, \delta a' - \delta^2 b' \in Z(L)$. Then

$$\begin{aligned}
[a - 2\delta b, a' - 2\delta b'] &= -2[a, \delta b'] - 2[\delta b, a'] + 4[\delta b, \delta b'] \quad \text{by (3.6)} \\
&= 2[\delta a, b'] + 2[b, \delta a'] + 4[\delta b, \delta b'] \\
&= 2[\delta^2 b, b'] + 2[b, \delta^2 b'] + 4[\delta b, \delta b'] \ = \ 0 \quad \text{(by (3.7))}.
\end{aligned}$$

Thus $[A_1, A_1] = 0$. Together with the previous paragraph, this shows that A^* is an abelian subring of L, and completes the proof of (a).

(b) Let $a \in A$. If $a \in Z(L)$, then $\delta a \in Z(L)$.

Conversely, assume $\delta a \in Z(L)$. Then $\delta^2 a \in Z(L)$. Take any $b \in A$. Then $[a, b] = 0$ and, by (3.6) and (3.7),

$$[a, \delta b] = -[\delta a, b] = 0 \quad \text{and} \quad [a, \delta^2 b] = -[\delta^2 a, b] - 2[\delta a, \delta b] = 0.$$

Since $L = A + \delta A + \delta^2 A$ by (L4), $a \in Z(L)$.

(c) By (L1) and a short argument,

$$\text{(3.9)} \qquad \text{whenever } x \in L \quad \text{and} \quad 2x \in Z(L), \quad \text{then} \quad x \in Z(L).$$

Suppose $a \in A - Z(L)$. Then $\delta(\delta^2 a) = \delta^3 a = 0 \in Z(L)$. So, by (b),

$$\text{either} \quad \delta^2 a \in Z(L) \quad \text{or} \quad \delta^2 a \notin A.$$

If $\delta^2 a \notin A$, then $\delta^2 a \in \delta^2 A \leq A^*$ and $\delta^2 a \in A^* - A$, which gives (c1).

Now assume $\delta^2 a \in Z(L)$. By (b), either $\delta a \in Z(L)$ or $\delta a \notin A$. But (b) also gives that $\delta a \notin Z(L)$ because $a \in A - Z(L)$. Hence,

$$\text{(3.10)} \qquad \delta a \notin A$$

By (L1), there exists a unique element $b \in A$ such that $2b = a$. Then $2\delta^2 b = \delta^2(2b) = \delta^2 a \in Z(L)$. By (3.9), $\delta^2 b \in Z(L)$.

Let $a' = 0$. Then

$$a', b \in A \quad \text{and} \quad \delta a' - \delta^2 b = -\delta^2 b \in Z(L).$$

So $-\delta a = -2\delta b = a' - 2\delta b \in A_1 \leq A^*$. By (3.10), $\delta a \in A^* - A$, which gives (c2).

(d) Here, $A < L$. By (L4) and (L5), $L = A + \delta A + \delta^2 A$, and $A \geq Z(L)$. Therefore,

$$L > A \geq Z(L) \quad \text{and} \quad A > Z(L).$$

Take i as large as possible such that $A \cap Z_i = Z(L) \cap Z_i$; i exists, since $Z_0 = 0$. Since $Z_n = L$, $i < n$. Then

$$A \cap Z_{i+1} > Z(L) \cap Z_{i+1}.$$

Take $a \in (A \cap Z_{i+1}) - Z(L)$. Then $\delta a, \delta^2 a \in Z_i$. By (c), either $\delta a \in A^* - A$ or $\delta^2 a \in A^* - A$. Either way, Z_i contains an element of $A^* - A$, and

$$A^* \cap Z_i \;>\; Z(L) \cap Z_i \;= A \cap Z_i.$$

(e) Here, L is finite and M is a δ-invariant additive subgroup of L. Let

$$B = A \cap M, \; Z = Z(L) \cap M, \; B_0 = \{a \in B \mid \delta a \in \delta^2 B + Z\},$$

$$B_1 \;=\; \{a - 2\delta b \mid a, b \in B \text{ and } \delta a - \delta^2 b \in Z\}, \quad \text{and} \quad B^* = B_1 + \delta^2 B.$$

In addition, let $\bar{M} = M/Z$. For each element x and additive subgroup K of M, let

$$\bar{x} \;=\; x + Z \quad \text{and} \quad \bar{K} \;=\; (K + Z)/Z.$$

Since $\delta(Z) \leq Z$, δ induces an endormorphism on $\bar{M}$, which we also denote by δ, for convenience. Clearly,

$$\text{(3.11)} \qquad \begin{cases} Z \leq B_0;\; Z \leq B_1 \leq B^* \leq A^* \cap M; \\ \text{and, if } M = L, \text{ then } B^* = A^*. \end{cases}$$

We may now divide the calculation of $|B^*|$ into several steps:

Step 1 $\bar{B}_1 \cap \delta^2 \bar{B} = \delta \bar{B}_0$, and $|\bar{B}_1 \cap \delta^2 \bar{B}| = |\bar{B}_0|$.

Proof

Take $x \in \bar{B}_1 \cap \delta^2 \bar{B}$. Then $x \in \delta^2 \bar{B}$ and, for some $a, b \in B$, $\delta \bar{a} = \delta^2 \bar{b}$ and $x = \bar{a} - 2\delta \bar{b}$.

Then

$$\delta x \in \delta^3 \bar{B} = 0 \quad \text{and} \quad 0 = \delta x = \delta \bar{a} - 2\delta^2 \bar{b} = -\delta \bar{a},$$

i.e. $\delta a \in Z = Z(L) \cap M$. By (b), $a \in Z(L) \cap B = Z(L) \cap M = Z$, and $\bar{a} = 0$. Therefore,

$$\delta(-2\bar{b}) = \bar{a} - 2\delta\bar{b} = x \in \delta^2 \bar{B}, \text{ whence } -2b \in B_0 \text{ and } x \in \delta \bar{B}_0.$$

Thus, $\bar{B}_1 \cap \delta^2 \bar{B} \leq \delta \bar{B}_0$.

Conversely, let $c \in B_0$. Since $|L|$ is odd, $c = 2d$ for some multiple d of c. Then $\delta \bar{d} \in \delta^2 \bar{B}$ (and $\delta^2 \bar{d} = 0$) because $\delta \bar{c} \in \delta^2 \bar{B}$. Moreover, $\delta \bar{c} \in \bar{B}_1$ because

$$0, -d \in B, \ \delta\bar{0} = 0 = \delta^2(-\bar{d}), \quad \text{and} \quad \delta\bar{c} = \bar{0} - 2\delta(-\bar{d}).$$

Therefore, $\bar{B}_1 \cap \delta^2 \bar{B} = \delta \bar{B}_0$.

By (b), δ maps $\bar{B}_0$ injectively onto $\delta \bar{B}_0$. So $|\bar{B}_1 \cap \delta^2 \bar{B}| = |\bar{B}_0|$.

Step 2 Define a surjection $\Psi : \bar{B} \to \delta^2 \bar{B}$ by $\Psi(x) = \delta^2 x$, for $x \in \bar{B}$. Then

$$|\bar{B}_1| = |\bar{B}_0||\ker \Psi|.$$

Proof

An element of $\bar{B}_1$ has the form $\bar{a} - 2\delta\bar{b}$, where $\bar{a}, \bar{b} \in \bar{B}$ and $\delta\bar{a} = \delta^2\bar{b}$. Given $\bar{a} \in \bar{B}$, such an element $\bar{b}$ exists precisely when $\bar{a} \in \bar{B}_0$, by the definition of B_0. Thus, $|\bar{B}_1|$ is the number of distinct elements $\bar{a} - 2\delta\bar{b}$ for which

$$\bar{a} \in \bar{B}_0, \ \bar{b} \in \bar{B}, \quad \text{and} \quad \delta\bar{a} = \delta^2\bar{b}. \tag{3.12}$$

When can we have $\bar{a'} - 2\delta\bar{b'} = \bar{a} - 2\delta\bar{b}$? Then

$$\begin{aligned} \bar{a} - \bar{a'} &= 2\delta(\bar{b} - \bar{b'}) \\ 2\delta^2(\bar{b} - \bar{b'}) &= \delta(\bar{a} - \bar{a'}) = \delta^2(\bar{b} - \bar{b'}), \text{ and} \\ 0 &= \delta^2(\bar{b} - \bar{b'}) = \delta(\bar{a} - \bar{a}'). \end{aligned}$$

By (b), $\bar{a} - \bar{a'} = 0$, i.e. $\bar{a'} = \bar{a}$. But then $0 = \bar{a} - \bar{a'} = \delta(2(\bar{b} - \bar{b'}))$, $2(\bar{b} - \bar{b'}) = 0$ (by (b)), $\bar{b} - \bar{b'} = 0$ by (3.9), and $\bar{b'} = \bar{b}$. Thus, $|\bar{B}_1|$ is the number of distinct pairs $(\bar{a}, \bar{b})$ as in (3.12).

Take any $\bar{a} \in B_0$. As mentioned just before (3.12), there exists some element $\bar{b_0}$ satisfying (3.12) for $\bar{b} = \bar{b_0}$. For any other element $\bar{b}$ of $\bar{B}$, the following are equivalent:

$\bar{b}$ satisfies (3.12); $\quad \delta^2\bar{b} = \delta\bar{a} = \delta^2\bar{b_0}$; $\quad \delta^2(\bar{b} - \bar{b_0}) = 0$; $\quad \bar{b} \in \bar{b_0} + \ker\, \Psi$.

Thus, there are altogether $|\ker\, \Psi|$ choices of $\bar{b}$ for any given element $\bar{a}$ of B_0, and

$$|\bar{B}_1| = |\bar{B}_0|\ |\ker\, \Psi|.$$

Step 3 Conclusion.

Proof

By Steps 1 and 2,

$$\begin{aligned} |\bar{B^*}| &= |\bar{B}_1 + \delta^2\bar{B}| = |\bar{B}_1||\delta^2\bar{B}|\ /\ |\bar{B}_1 \cap \delta^2\bar{B}| \\ &= |\bar{B}_0|\ |\ker\, \Psi|\ |\mathrm{Image}\ \Psi|\ /\ |\bar{B}_0|\ =\ |\bar{B}|. \end{aligned}$$

Now, $B = A \cap M \geq Z(L) \cap M = Z$. By (3.11), $Z \leq B^* \leq A^* \cap M$, and, if $M = L$, then $B^* = A^*$ (and $B = A \cap M = A$). So

$$|B^*/Z|\ =\ |\bar{B^*}|\ =\ |\bar{B}|\ =\ |(A \cap M)/Z|$$

and

$$|A^* \cap M|\ \geq |B^*|\ \geq\ |A \cap M|$$

and the case of $M = L$ yields $|A^*| = |A|$. This completes the proof of (e) and of the theorem.

Q.E.D.

Now we may apply Theorem 3.2 to obtain part of Theorem 1. We first need a special case of an important theorem ([L] Theorem II.4.6, pp. 179-80; see pages 142-3 and results II.4.2 - II.4.3 and II.4.5) of M. Lazard that allows us to convert groups into Lie rings (and vice versa).

Theorem 3.4 **(M. Lazard)** Suppose S has nilpotence class at most $p-1$. Then we may define operations $+$ and $[,]$ on S by canonical formulas using the group operation on S, under which S becomes a nilpotent Lie ring of the same class as S. A subset of S is a subgroup (respectively, normal subgroup) of S as a group if and only if it is a subring (respectively, ideal) of S as a Lie ring. Every automorphism of S as a group is an automorphism of S as a Lie ring, and vice versa.

Moreover, for $x, y \in S$ and any integer n,

$$x^n \text{ in the group is equal to } nx \text{ in the Lie ring.}$$

and

$$xy = yx \text{ in the group if and only if } [x, y] = 0 \text{ in the Lie ring.}$$

For every abelian subgroup or quotient group in S, + coincides with the group operation.

If S has class 2 and p is odd, Lazard's construction reduces to a construction of R. Baer ([HB, II, Lemma VIII.9.6, pages 347-9])

$$x + y \ = x^{\frac{1}{2}} y x^{\frac{1}{2}} \quad \text{and} \quad [x, y] \ = \ x^{-1} y^{-1} x y.$$

Now we finally obtain Theorem 1.

Theorem 1 Suppose p is odd, $A \in \mathcal{A}(\mathcal{S})$, and B is a subgroup of S that does not normalize A. Assume that

(3.13) B has nilpotence class at most 2 and is normalized by A, ,

or

(3.14) $p \geq 5$, $A \lhd < A^B >$, and $[A, u; 3] = 1$ for every $u \in B$.

Then there exists $A^* \in \mathcal{A}(\mathcal{S})$ such that

(a) $A^* \leq < A^B >$ and A^* normalizes A,

(b) for every central series $\mathcal{S}$ of S, $A <_{\mathcal{S}} A^*$, and

(c) if A normalizes B, then $|A^* \cap B| \ \geq \ |A \cap B|$.

Proof:

We first choose an element b of $B - N(A)$ as follows:

if (3.14) holds, b can be any element of $B - N(A)$; otherwise, take b as in Theorem 2.3.

Then let $T =< b, A >$ and $\hat{A} =< A^T >$. Then

$$(3.15) \qquad \begin{cases} T =< A, B \cap T >, \hat{A} =< A^{B\cap T} >\leq< A^B >, \text{ and} \\ Z(\hat{A}) \leq C_S(A) = A. \end{cases}$$

If (3.14) fails, then, by Theorem 2.3, $\hat{A}$ has class 2 and $\hat{A}' \leq Z(\hat{A}) \leq A$. So by (3.14),

$$(3.16) \qquad A \lhd \hat{A} \text{ in all cases, and } \hat{A} \text{ has class 2 if (3.14) fails.}$$

Now we divide the proof into several steps.

Step 1: The nilpotence class of $\hat{A}$ is at most $p-1$, $\hat{A} =< A, A^b, A^{b^2} >$ and

$$[A, u; 3] = 1 \quad \text{for every } u \in B.$$

Proof

If (3.14) fails, then B has class at most 2, and

$$[A, B; 3] \leq [B, B, B] \leq [B', B] = 1.$$

Therefore, in all cases, $[A, u; 3] = 1$, for every $u \in B$. Now, by Lemma 2.2(c), $\hat{A} =< A, A^b, A^{b^2} >$. So, by (3.16), we are done if (3.14) fails. Assume (3.14) holds. Then $p \geq 5$ and by Lemma 2.2(c), $\hat{A}$ has class at most 3.

Q.E.D.

Step 2 Regard $\hat{A}$ as a Lie ring as in Theorem 3.4. Let α be the mapping on $\hat{A}$ given by

$$\alpha(x) \;=\; x^b \;=\; b^{-1}xb \text{ (in the group } T\text{), for } x \in \hat{A}.$$

Then:

(a) A and $\hat{A}$ are divisible by 2 as Lie rings, and

(b) α is an automorphism of $\hat{A}$ as a group and as a Lie ring.

Consider $\hat{A}$ as a Lie ring. Then

(c) $\hat{A}(\alpha - 1)^3 = 0$,

(d) $\hat{A} = 3\hat{A}$ or $[\hat{A}(\alpha - 1), \hat{A}(\alpha - 1)^2] = 0$, and

(e) $\log \alpha$ is well defined and is a derivation of $\hat{A}$, and $\alpha = \exp(\log \alpha)$.

<u>Proof</u>:
Inside the group T, let $D = [A, < b >]$ and $E = [A, < b >; 2]$. By (3.15),

(3.17) $$D \leq \hat{A} \text{ and } D \lhd < A, b >= T.$$

(a) Since $|\hat{A}|$ is a power of an odd prime p, A and $\hat{A}$ are divisible by 2.

(b) Clearly, α is an automorphism of $\hat{A}$ as a group, hence as a Lie ring, by Theorem 3.4. Since $D \lhd T$, we have $\alpha(D) = D$.

(c) For each $a \in A$,

$$\alpha a \ \equiv \ a^b \ \equiv \ a[a, b] \ \equiv \ a \qquad (\text{modulo } D);$$

similarly, $a^{b^2} \equiv a \quad (\text{modulo } D)$. By Step 1,

$$\hat{A} \ = \ < A, A^b, A^{b^2} > .$$

Therefore,

$$\hat{A} \ = \ < A, D > \ = \ AD \quad \text{and} \quad \alpha \text{ acts trivially on } \hat{A}/D.$$

For each $x \in \hat{A}$,

$$\alpha x \equiv x \quad \text{and} \quad x(\alpha - 1) \ \equiv \ x\alpha - x \ \equiv \ x - x \ \equiv 0 \quad (\text{modulo } D).$$

Thus, $\hat{A}(\alpha - 1) \leq D$. A similar argument shows that

$$\hat{A}(\alpha - 1)^2 \leq D(\alpha - 1) \leq E$$

and

$$\hat{A}(\alpha - 1)^3 \leq [a, < b >; 3] \leq [A, b; 3] = 1 \quad \text{by Lemma 2.2 and Step 1.}$$

Hence, in the Lie ring notation, $\hat{A}(\alpha - 1)^3 = 0$.

(d) If $p \geq 5$, then $\hat{A} = 3\hat{A}$ because $\hat{A}$ is a group under $+$ and $|\hat{A}|$ is a power of p.

Assume $p = 3$. Then (3.14) fails. Hence (3.13) holds, and B has nilpotence class at most 2 and is normalized by A. Then, in the group T,

$$\begin{aligned} D &= [A, B \cap T] \leq B \\ E &= [A, B \cap T, B \cap T] \leq [B, B] = B' \leq Z(B), \\ \text{and } [D, E] &= 1. \end{aligned}$$

So $E \leq Z(D)$. From the proof of (c),

$$\hat{A}(\alpha - 1)^2 \leq E \leq Z(D), \text{ and } \hat{A}(\alpha - 1)^2 \leq Z(\hat{A}(\alpha - 1)).$$

So, for $x \in \hat{A}(\alpha - 1)$ and $y \in \hat{A}(\alpha - 1)^2$, $xy = yx$ in the group $\hat{A}$; by Theorem 3.4, $[x, y] = 0$ in the Lie ring $\hat{A}$. This proves (d).

(e) As described in the beginning of this section, define

$$\log(\alpha) = (\alpha - 1) - \frac{1}{2}(\alpha - 1)^2.$$

By Lemma 3.1, $\log(\alpha)$ is a derivation of $\hat{A}$, and $\alpha = \exp(\log \alpha)$.

Q.E.D

Step 3: Conclusion

Proof:

We continue with the notation of Step 2. Let

$$\delta = \log \alpha = (\alpha - 1) - \frac{1}{2}(\alpha - 1)^2. \tag{3.18}$$

We first verify the hypothesis of Theorem 3.2 for $L = \hat{A}$.

By Step 2(e),

$$\alpha = \exp(\delta) = 1 + \delta + \frac{1}{2}\delta^2.$$

This equation and (3.18) yield

$$\hat{A}\delta = \hat{A}(\alpha - 1), \quad \hat{A}\delta^2 = \hat{A}(\alpha - 1)^2, \quad \hat{A}\delta^3 = \hat{A}(\alpha - 1)^3. \tag{3.19}$$

Now Step 2 gives (L1), (L2), and (L3).

By (3.16) and Theorem 3.4, $\hat{A}$ contains A as a normal subgroup and as a Lie ideal. Since α is an automorphism of$\hat{A}$ (both as a group and as a Lie ring), $\hat{A}$ contains $A\alpha(= A^b)$ and $A\alpha^2(= A^{b^2})$ similarly. Let

$$L_0 \ = \ A + A\alpha + A\alpha^2.$$

Then L_0 is a Lie ideal, and hence a normal subgroup of $\hat{A}$, and

$$L_0 = A + A(\alpha - 1) + A(\alpha - 1)^2 = A + A\delta + A\delta^2 \text{ by (3.19).}$$

By Step 2(c), $(\alpha - 1)^3 = 0$, and

$$L_0\alpha \leq L_0 + L_0(\alpha - 1) = A + A(\alpha - 1) + A(\alpha - 1)^2 = L_0.$$

Thus, $L_0 = L_0\alpha$. In group-theoretic terms, L_0 is a normal subgroup of $\hat{A}$ and $L_0 = L_0^b$. Since

$$T =< A, b > \quad \text{and} \quad N_T(L_0) \geq < \hat{A}, b > \geq T,$$

we have $\hat{A} =< A^T > \leq < L_0^T >= L_0 \leq \hat{A}$. Hence $L_0 = \hat{A}$, which gives (L4).

By Theorem 3.4, the center $Z(\hat{A})$ is the same whether $\hat{A}$ is regarded as a group or as a Lie ring. Hence,

$$Z(\hat{A}) \ \leq \ C_S(a) \ = \ A,$$

which gives (L5).

We have now verified the hypothess of Theorem 3.2 for $L = \hat{A}$, and we will apply the conclusion of the theorem. For A^* as in (L6), Theorem 3.4 and part (a) of Theorem 3.2 assert that A^* is an abelian subgroup of $\hat{A}$. By Theorem 3.2(e), $|A^*| = |A|$, so $A^* \in \mathcal{A}(\mathcal{S})$. By (3.15) and (3.16),

$$A^* \ \leq \ \hat{A} \ \leq \ < A^B > \ \cap N_T(A).$$

This proves (a) of Theorem 1.

Now take any central series $\mathcal{S}$ of S, say

$$1 = S_0 \leq S_1 \leq S_2 \leq \ldots \leq S_n = S.$$

Let $Z_i = \hat{A} \cap S_i$, for $i = 0, 1, 2, \ldots, n$. Then

$$[Z_i, b] \leq \hat{A} \cap [S_i, B] \leq \hat{A} \cap S_{i-1} = Z_{i-1}, \quad 1 \leq i \leq n.$$

Going over to Lie ring notation for $\hat{A}$, we have, by Theorem 3.4 and the proof of Step 2,

$$Z_i \text{ is a Lie ideal of } \hat{A} \quad \text{and} \quad Z_i\delta = Z_i(\alpha - 1) \leq Z_{i-1}, \quad 1 \leq i \leq n.$$

By Theorem 3.2(d),(e),

$$|A^* \cap Z_i| \geq |A \cap Z_i| \text{ for all } i, \text{ and } A^* \cap Z_i > A \cap Z_i \text{ for some } i.$$

Therefore, $A <_{\mathcal{S}} A^*$, according to the definition in Section 1.

Suppose A normalizes B. Then $B \lhd AB$, and there exists a central series of AB in which B is one of the terms. The previous paragraph yields

$$|A^* \cap B| \;\geq\; |A \cap B|.$$

Now we have proved (b) and (c) of Theorem 1, which complete the proof of the theorem.

Q.E.D

4 Proof of Theorem 2

Consider the following conditions on a subgroup A of S.

Whenever B is a subgroup of S and

(4.1) $$A \lhd < A^B > \quad \text{and} \quad [A, u; 3] = 1 \text{ for every } u \in B,$$

then B normalizes A.

Whenever B is a subgroup of S and

(4.2) $$[A, u; 3] = 1 \text{ for every } u \in B,$$

then B normalizes A.

Theorem 4.1 Suppose A is an abelian subgroup of S that satisfies (4.1).

(a) If B is an abelian subgroup of S that satisfies (4.1), then A and B normalize each other.

Moreover,

(b) A satisfies (4.2).

Proof:
(a) We use induction on $|S|$. We may assume that

$$A, B < S.$$

Let M be a maximal subgroup of S that contains A, and let $Q =< A^B >$. Since S is nilpotent,

$$M \triangleleft S \quad \text{and} \quad A =< A^B >\leq< M^S >= M.$$

For each $x \in B$, it is easy to see that A^x satisfies (4.1); since $A, A^x \leq M$, induction yields that A and A^x normalize each other. Therefore,

$$A \triangleleft < A^B >= Q$$

and

$$[B, A; 3] = [\ [B, A], A, A] \leq [\ [Q, A], A] \leq [A, A] = 1.$$

By symmetry, $[A, B; 3] = 1$. Hence, by (4.1), B normalizes A. By symmetry, A normalizes B.

(b) Take B as in part (b). By part (a), for each $x \in B$, A and A^x normalize each other. Thus,

$$A \triangleleft < A^B > .$$

By (4.1), B normalizes A.

Q.E.D

Proof of Theorem 2:
Now suppose A, A_0 satisfy the hypothesis of Theorem 2. Then $p \geq 5$ and A, A_0 satisfy (4.1). By Theorem 4.1, we obtain (a) and (b) of Theorem 2.

Q.E.D

Example 4.1 (J. Alperin, [H, p.349]) Here, p may be any prime. Let T be the group generated by elements

$$x_1, y_1, x_2, y_2, \ldots, x_p, y_p,$$

(with subscripts taken modulo p) subject only to the relations

$$x_i^p = y_i^p = [x_i, y_i] = 1, \quad \text{for} \quad i = 1, 2, \ldots, p$$

and

$$[x, y, z] = 1 \quad \text{for all} \quad x, y, z \in T.$$

(Thus, T has nilpotence class two, and, if p is odd, may be obtained from a Lie ring by using Theorem 3.4) .

Let α be the automorphism of T of order p given by

$$x_i^\alpha = x_{i+1}, \ y_i^\alpha = y_{i+1}, \quad \text{for all } i.$$

Assume S is the semi-direct product of T by $< \alpha >$. Then it is not difficult to see that

$$|T'| = p^k \quad \text{for } k = \begin{pmatrix} 2p \\ 2 \end{pmatrix} - p = 2p^2 - 2p,$$

$$|T| = p^{2p^2}, \ |S| = p^{2p^2+1}, \ d(S) = p^{2p^2-2p+2},$$

and $\mathcal{A(S)}$ consists of the p different groups $< x_i, y_i, T' >$. Therefore, no element of $\mathcal{A(S)}$ is normal in S.

Example 4.2 Here, we assume $p = 2$ and S and T are as in Example 4.1.

Since T/T' is elementary abelian and $p = 2$,

$$\begin{aligned} S' &= [T, < \alpha >]T' =< uu^\alpha, T' \mid u \in T > \\ &= < x_1x_2, y_1y_2, T' > \end{aligned}$$

Similarly,

(4.3) $$[T', \alpha] = \{uu^\alpha \mid u \in T'\} \leq C_{T'}(\alpha).$$

Let $B =< \alpha > S'$. Clearly, $B \lhd S$ and B normalizes neither of the two elements of $\mathcal{A(S)}$. Therefore, S is a counterexample for $p = 2$ to Theorem 1 and its corollary and to Theorem 2(b), if B has nilpotence class 2. To show the latter, we will show that $1 < B' \leq C_{T'}(\alpha)$. Let $R = C_{T'}(\alpha)$.

Now, for some $v \in T'$,

$$x_1 x_2 v = x_2 x_1 = x_1^\alpha x_2^\alpha = (x_1 x_2)^\alpha,$$

and

$$x_1 x_2 = (x_1 x_2 v)^\alpha = (x_1 x_2)^\alpha v^\alpha = x_1 x_2 v v^\alpha, \quad v^\alpha = v^{-1} = v.$$

So $v \in C_{T'}(\alpha) = R$, and α centralizes $x_1 x_2$ (modulo R). Similarly, α centralizes $y_1 y_2$ (modulo R). Therefore, by (4.3),

$$\alpha \text{ centralizes } S'/R. \tag{4.4}$$

By our choice of relations for defining T, we have $1 \neq [x_1, x_2] = v \in B'$.

Since $T' \leq Z(T)$ and α centralizes $x_1 x_2$ and $y_1 y_2$ (modulo T'), α centralizes $[x_1 x_2, y_1 y_2]$, which must be in $C_{T'}(\alpha)(= R)$. Therefore, $(S')' \leq R$. As $B =< \alpha > S'$, (4.4) yields

$$B' \leq R = C_{T'}(\alpha) \leq Z(B).$$

Hence, B has nilpotence class 2, as desired.

5 Preliminary Results for Characteristic Subgroups

In this section, we assume the following condition:

Hypothesis 5.1

(a) S is a Sylow p-subgroup of a group G.

(b) B, X and R are subgroups of S.

(c) B and X normalize R, and $X \lhd G$.

Lemma 5.2 Assume that $R \lhd G$ and $R \leq X$ and that X centralizes every abelian normal subgroup of G that is contained in R.

$$\text{Then } [R,X] \;\le\; Z(X).$$

Proof:

Use induction on $|R|$. We may assume that $R > 1$. Let $Q = [R,X]$. Since S is nilpotent and $R, X \lhd G$, we have

$$Q \;<\; R \quad \text{and} \quad Q \;\lhd\; G.$$

By induction,

$$[Q,X] \;\le\; Z(X)$$

so $[X,Q,X] = [Q,X,X] \le [Z(X),X] = 1$. By the Three Subgroups Lemma

$$1 = [X,X,Q] \;\ge\; [R,X,Q] \;=\; [Q,Q].$$

Thus Q is abelian. By hypothesis, X centralizes Q. So

$$[R,X] \;=\; Q \;\le Z(X).$$

Q.E.D

Lemma 5.3 Assume that $R \lhd G$ and that X centralizes every abelian normal subgroup of G contained in $R \cap X$. Then

$$[R,X,X] \;\le\; Z(X).$$

Proof:

By Lemma 5.2, $[R \cap X, X] \le Z(X)$. Since $X, R \lhd G$,

$$[R,X,X] \;\le\; [R \cap X, X] \;\le\; Z(X).$$

So $[R,X;3] = 1$.

Q.E.D

Theorem 2 and the following results are the main tools for improving on our 1970 result (mentioned in the introduction) to obtain Theorem 3.

Proposition 5.4 Let Y be a normal subgroup of G contained in X. Assume that

(a) X/Y is abelian and $C_X(R) \leq Y$,

(b) R is abelian and $[R, X, X] \leq Z(X)$,

(c) $[R, B, B] = 1$

and

(d) $p \geq 5$.

Then

$$[X, B; 3] \ \leq \ Y.$$

<u>Proof</u>

Let $X' = [X, X]$. By (b), $[X, R, X] = [R, X, X] \leq Z(X)$. Hence, by the Three Subgroups Lemma,

(5.1) $$[R, X'] = [X, X, R] \leq Z(X).$$

Similarly,

$$[R, X, X'] = [\ [R, X], X'] \ \leq \ [\ [R, X], X, X] \ \leq \ [Z(X), X] = 1.$$

Then

$$[\ [X', X], R] \ \leq \ [X, R, X'] \ [R, X', X] \ \leq \ [R, X, X'] \ [Z(X), X] \ = \ 1.$$

Thus,

(5.2) $$[X', X] \ \leq \ C_X(R).$$

Let $\bar{X} = X/C_X(R)$. Conjugation by X on R induces a faithful action of $\bar{X}$ by automorphisms on R. Let H be the semi-direct product of R by $\bar{X}$. We claim that

(5.3) H has nilpotence class at most 3.

To prove (5.3), it suffices (by Lemma 2.1) to show that

(5.4) $$[x_1, x_2, x_3, x_4] \ = \ 1$$

for all x_1, x_2, x_3, x_4 in the set-theoretic union $\bar{X}$ and R. If $x_1, x_2, x_3 \in \bar{X}$ then $[x_1, x_2, x_3] = 1$ by (5.2). So we may assume that $x_i \in R$ for some $i = 1, 2$ or 3. As R is abelian and $R \lhd H$, we obtain (5.4) except possibly if $x_j \in \bar{X}$ for all $j \neq i$. But now (5.4) follows from (b) if $i = 1$ or 2, and from (5.1) if $i = 3$. Hence (5.3) follows.

Now we invoke our assumption that $p \geq 5$. By (5.3) we may use Lazard's construction (Theorem 3.4), to obtain operations $+$ and $\{\ ,\ \}$ under which H becomes a Lie ring. (We write $\{\ ,\ \}$ for the Lie bracket operation to avoid confusion with the group commutator $[x, y] = x^{-1}y^{-1}xy$). Moreover, since $R \lhd H$, we obtain a bilinear mapping on $\bar{X}$ and R (under $+$) into R (under $+$) given by

$$(\bar{x}, y) \ \mapsto \ \{\bar{x}, y\}.$$

In the usual way, this mapping induces an additive group homomorphism

$$\phi : \bar{X} \rightarrow \ \text{Hom}\ (R, R).$$

We can make several observations at this point:

(5.5) Since R is abelian, the $+$ operation on R coincides with the given group operation on R.

(5.6) Since $\bar{X}$ acts faithfully on R, ϕ is an injection.

(5.7) Conjugation by B on R and on X induces automorphisms on the Lie rings $R, \bar{X}$, and H, and ϕ is a $B-$module injection.

By hypothesis, $[R, B, B] = 1$. For $y \in R$ and $b \in B$, (5.5) and (5.7) give

$$y^b - y \ = \ (b^{-1}yb)y^{-1} \ = \ y^{-1}b^{-1}yb.$$

Therefore, in the usual notation for modules, we obtain that the module commutator $[y, b]$ coincides with the group commutator $[y, b]$. Hence, in module notation,

$$[\ [R, B], B] \ = \ 0.$$

Now, a calculation ([S, pp.236-7] or [G2, Lemma A2.3, p.57]) shows

(5.8) $$[\ [\ [\ \text{Hom}\ (R, R), B], B], B] \ = \ 0.$$

Consequently by (5.6),

$$[\ [\ [\bar{X}, B], B], B] \ = \ 0.$$

We have assumed that X/Y is abelian and $C_X(R) \leq Y$. Therefore, the arguments in the previous paragraph show that, in the usual notation for groups,

$$[X, B; 3] \ \leq \ Y.$$

Q.E.D.

At this point, it is useful to quote the following result (with a minor change that requires no significant change in the proof).

Proposition 5.5 ([G2, Theorem A2.4, pp.57-9]) Suppose

$$R \leq P \leq S, \qquad R, P \lhd G, \qquad C_P(R) \leq R,$$

and X/Y is a chief factor of G such that $X \leq P$.

Then either X/Y is $G-$isomorphic to a chief factor X_1/Y_1 of G for which $X_1 \leq Z(R)$, or there exist chief factors U/U_1 and V/V_1 of G such that

(i) $U \leq R$,

(ii) $V \leq [U, P] \leq [R, P]$, and

(iii) X/Y is $G-$isomorphic to a composition factor of $\mathrm{Hom}(U/U_1, V/V_1)$ under G.

Corollary 5.6 Suppose $P = O_p(G), g \in G,\ R \lhd G,\ C_P(R) \leq R$, and $[R, g, g] = 1$, and X/Y is a chief factor of G. Then

$$[X, g; 3] \ \leq \ Y.$$

Proof:
Since R and X are normal $p-$subgroups of G, they are contained in P. So we may apply Proposition 5.5. Since

$$[Z(R), g; 3] \ \leq \ [R, g; 2] \ = \ 1,$$

we may assume that X/Y is $G-$isomorphic to a composition factor of $\mathrm{Hom}(U/U_1, V/V_1)$ under G, for U/U_1, and V/V_1 as in the proposition. Then

$$[V, g; 2] \ \leq \ [U, g; 2] \ \leq \ [R, g; 2] \ = \ 1.$$

Now the proof of (5.8) (in the proof of Proposition 5.4) shows that

$$[\text{ Hom } (U/V_1, V/V_1), g; 3] \;=\; 0.$$

Therefore, $[X, g; 3] \;=\; 1$.

Q.E.D.

6 Characteristic Subgroups

Throughout this section we assume that $p \geq 5$.

Take $\mathcal{A}_{\in}(\mathcal{S})$ as in Section 1, so that $\mathcal{A}_{\in}(\mathcal{S})$ is a non-empty subset of $\mathcal{A}(\mathcal{S})$.

Definition 6.1 Let $\mathcal{A}$ be a non-empty subset of $\mathcal{A}(\mathcal{S})$. Define

$$J(\mathcal{A}) \;=\; <\; \mathcal{A} \;> \quad \text{and} \quad \mathcal{N}^*_{\mathcal{S}}(\mathcal{A}) \;=\; \cap_{\mathcal{A}\in\mathcal{A}}\, \mathcal{N}_{\mathcal{S}}(\mathcal{A}).$$

Then $\mathcal{A}$ is an N-set if

$$A \quad \text{normalizes} \quad B \quad \text{for every} \quad A, B \in \mathcal{A}.$$

Remark Thus, $\mathcal{A}$ is an N-set if and only if $J(A) \leq N^*_{\mathcal{S}}(\mathcal{A})$, that is $A \lhd J(\mathcal{A})$ for every $A \in \mathcal{A}$.

Definition 6.2 Let $\mathcal{A}$ be a non-empty subset of $\mathcal{A}(\mathcal{S})$. Let $J = J(\mathcal{A})$. Then $\mathcal{A}$ is an N^*-set (in S) if it satisfies the following conditions:

(N1) $\mathcal{A}$ is an N-set and $J \lhd S$;

(N2) whenever $x \in S$ and $[J, x, x] = 1$, then $x \in N^*_{\mathcal{S}}(\mathcal{A})$;

(N3) whenever $\mathcal{B}$ is an N-set in S, then $J(\mathcal{B}) \leq \mathcal{N}^*_{\mathcal{S}}(\mathcal{A})$, if the following conditions are satisfied:

- (N3a) J normalizes $J(\mathcal{B})$, and
- (N3b) $N^*_{\mathcal{S}}(\mathcal{B})$ contains every abelian subgroup of J normalized by $J(\mathcal{B})$.

Remark 6.3 Under this definition, the question of whether $\mathcal{A}$ is an N^*-set in S depends on the whole group S and not merely on $J(S)$. It would be desirable to have it depend on $J(S)$ alone, but we do not see how to obtain our results in this case (in particular, how to prove (N2) in Proposition 6.9).

Let us recall the definition of a p-stable group.

Definition ([Gor, pp.268-9]) Suppose that p is odd, G is a group, and that $O_p(G) > 1$. Then G is p-stable if it has the following property:

Whenever A and R are p-subgroups of G such that

$$O_{p'}(G)R \lhd G, \quad A \leq N_G(R), \quad \text{and} \quad [R, A, A] = 1$$

then

$$AC_G(R)/C_G(R) \ \leq \ O_p(N_G(R)/C_G(R)).$$

Definition 6.4 A special pair for S is an ordered pair (G, T) satisfying the following conditions.

(P1) S is a Sylow p-subgroup of G;

(P2) $T = O_p(G)$ and $C_G(T) \leq T$;

(P3) G is p-stable or satisfies

(P3a) whenever $u \in S$ and $[X, u; 3] \leq Y$ for every chief factor X/Y of G such that $X \leq T$, then $u \in T$.

A special pair satisfying (P3a) will be called a 3-special pair.

Lemma 6.5 Suppose (G, T) is a special pair, $x \in G$, and $U \leq T$. Assume that

$$U \lhd G, \quad C_T(U) \leq U, \quad \text{and} \quad [U, x, x] = 1.$$

Then $x \in T$.

Proof:

If (G, T) is a 3-special pair, apply Corollary 5.6 with T, U, and x in place of P, R and g. By (P3a), $x \in T$.

Henceforth, assume that G is p-stable. Let $C = C_G(U)$. By Lemma 2.2, $[U, < x >, < x >] = 1$. Since G is p-stable,

$$< x > \ C/C \ \leq O_p(G/C).$$

To complete the proof , it suffices to show that $C \leq T$, for then

$$O_p(G/C) \ = \ T/C.$$

Take any p'-element y in C. Then y induces a p'-automorphism α on T by conjugation, and

$$[T, < y >] \ \leq T \cap C \ = \ C_T(U) \ \leq \ U, \qquad [U, < y >] = 1.$$

Thus, α stabilizes the normal series $T \geq U \geq 1$ of T. Therefore, α has a p-power order [Gor, pp.178-9]. Since α is a p'-automorphism,

$$\alpha = 1 \qquad \text{and} \qquad y \in C_G(T) \ \leq \ T.$$

As y is a p'-element, $y = 1$. This shows that 1 is the only p'-element of C.

Now C is a p-group. As $C \lhd G$, we have $C \leq O_p(G) = T$, as desired.

Q.E.D.

Proposition 6.6

(a) There exists an N^*-set. In particular, $\mathcal{A}_\in(\mathcal{S})$ is an N^*-set.

(b) If $\mathcal{A}_\infty$ and $\mathcal{A}_\in$ are N^*-sets, then so is $\mathcal{A}_\infty \cup \mathcal{A}_\in$.

Proof:

(a) Let $\mathcal{A} = \mathcal{A}_\in(\mathcal{S})$. Let $J = J(\mathcal{A}) =< \mathcal{A} >$. Then $J \lhd S$, so $J \lhd J(S)$. By Theorem 2, $\mathcal{A}$ is an N-set. Thus $\mathcal{A}$ satisfies (N1).

Take x as in (N2). By Lemma 2.2, $[J, < x >, < x >] = 1$. Hence, for each $A \in \mathcal{A}$,

$$[A, < x >; 3] \ = \ 1,$$

and x normalizes A, by the definition of $\mathcal{A}_{\in}(\mathcal{S})$. Thus, $x \in N_S^*(\mathcal{A})$, as desired.

Similarly, for $\mathcal{B}$ as in (N3), $J(\mathcal{B}) \leq \mathcal{N}_{\mathcal{S}}^*(\mathcal{A})$.

(b) Let $\mathcal{A}_\infty$ and $\mathcal{A}_\in$ be N^*-sets. Let

$$J_i = J(\mathcal{A}_\rangle) \quad \text{for} \quad \rangle = \infty, \in; \qquad \mathcal{A} = \mathcal{A}_\infty \cup \mathcal{A}_\in; \qquad \text{and} \qquad \mathcal{J} = \mathcal{J}(\mathcal{A}).$$

By (N1), $J_1, J_2 \lhd S$. Hence,

$$J = J_1 J_2 \lhd S \tag{6.1}$$

Suppose D is an abelian subgroup of J_1, normalized by J_2. Then

$$[J_2, D, D] \;\leq\; [D, D] \;=\; 1.$$

By (N2), $D \leq N_S^*(\mathcal{A}_\in)$. Therefore, if we now replace $\mathcal{A}$ and $\mathcal{B}$ by $\mathcal{A}_\infty$ and $\mathcal{A}_\in$, (N3b) is satisfied; and (N3a) is also satisfied because J_1 normalizes J_2. Since $\mathcal{A}_\infty$ is an N^*-set, (N3) gives

$$J_2 \;=\; J(\mathcal{A}_\in) \;\leq\; \mathcal{N}_{\mathcal{S}}^*(\mathcal{A}_\infty).$$

As $\mathcal{A}_\infty$ is an N-set, $J_1 \leq N_S^*(\mathcal{A}_\infty)$. Hence, by (6.1),

$$J \;=\; J_1 \; J_2 \;\leq\; N_S^*(\mathcal{A}_\infty).$$

By symmetry, $J \leq N_S^*(\mathcal{A}_\in)$. Therefore, $\mathcal{A}$ is an N-set. By (6.1), $\mathcal{A}$ satisfies (N1).

Take x as in (N2). Then $[J_1, x, x] \leq [J, x, x] = 1$. Since $\mathcal{A}_\infty$ is an N^*-set, $x \in N_S^*(\mathcal{A}_\infty)$. By symmetry, $x \in N_S^*(\mathcal{A}_\in)$. Hence, $x \in N_S^*(\mathcal{A})$, and $\mathcal{A}$ satisfies (N2).

A similar argument shows that $\mathcal{A}$ satisfies (N3). Therefore, $\mathcal{A}$ is an N^*-set.

Q.E.D.

Proposition 6.6 obviously yields:

Corollary 6.7 There exists a unique maximal N^*-set $\mathcal{A}_{\mathcal{N}}(\mathcal{S})$ in S.

Our strategy is to show that, for a special pair (G, T), $\mathcal{A}_{\mathcal{N}}(\mathcal{S}) \subset \mathcal{A}_{\mathcal{N}}(\mathcal{T})$, and, if (G, T) is a 3-special pair, then $\mathcal{A}_{\mathcal{N}}(\mathcal{S}) = \mathcal{A}_{\mathcal{N}}(\mathcal{T})$.

Proposition 6.8 Let (G, T) be a special pair for S. Then:

(a) $d(T) = d(S)$, and

(b) every N^*-set in S is an N^*-set in T.

Proof:

Take any $A_0 \in \mathcal{A}_{\in}(\mathcal{S})$ and let U be a critical subgroup of T [Gor, p.186]. Then U has nilpotence class at most 2, $C_T(U) \leq U$, and $U \lhd G$. By the definition of $\mathcal{A}_{\in}(\mathcal{S})$ and Lemma 6.5,

$$[U, A_0, A_0] \leq [A_0, A_0] = 1 \quad \text{and} \quad A_0 \leq T.$$

Therefore, $d(T) = d(S)$ and $\mathcal{A}_{\in}(\mathcal{S}) \leq \mathcal{A}(\mathcal{T})$.

Clearly, $\mathcal{A}_{\in}(\mathcal{S}) \leq \mathcal{A}_{\in}(\mathcal{T})$. Take any N^*-set $\mathcal{A}$ in S, and let

$$J = J(\mathcal{A}), \qquad \mathcal{B} = \mathcal{A}_{\in}(\mathcal{T}), \qquad \mathcal{U} = \mathcal{J}(\mathcal{B}).$$

By Theorem 2, $\mathcal{B}$ is an N-set. For every abelian subgroup D of J normalized by U,

$$1 = [U, D, D] = [J(\mathcal{A}_{\in}(\mathcal{T})), \mathcal{D}, \mathcal{D}],$$

and $D \leq T$ by Lemma 6.5; then $D \leq N^*_{\mathcal{S}}(\mathcal{B})$ by the definition of $\mathcal{A}_{\in}(\mathcal{T})$. Thus, $\mathcal{A}$ and $\mathcal{B}$ satisfy condition (N3b) of the definition of a N^*-set. Since $J(\mathcal{B}) \lhd \mathcal{G}$, they satisfy (N3a) as well. Therefore, by (N3),

$$U = J(\mathcal{B}) \leq \mathcal{N}^*_{\mathcal{S}}(\mathcal{A}).$$

For every $A \in \mathcal{A}$, U normalizes A; hence,

$$[U, A, A] = 1,$$

and $A \leq T$ by Lemma 6.5. This shows that $\mathcal{A} \subseteq \mathcal{A}(\mathcal{T})$. Since $\mathcal{A}$ satisfies conditions (N1), (N2), and (N3) with respect to S, it is easy to see that $\mathcal{A}$ satisfies them with respect to T. Thus, $\mathcal{A}$ is an N^*-set in T.

Q.E.D.

__Proposition 6.9__ Suppose (G,T) is a 3-special pair, $\mathcal{A}$ is an N^*-set in T that contains an element of $\mathcal{A}_{\in}(\mathcal{S})$, and $J(\mathcal{A}) \lhd \mathcal{G}$.

Then $\mathcal{A}$ is an N^*-set in S.

__Proof__:

Take $A_0 \in \mathcal{A}_{\in}(\mathcal{S}) \cap \mathcal{A}$, and let $J = J(\mathcal{A})$. Then

$$d(T) = d(S), \qquad \mathcal{A} \subseteq \mathcal{A}(\mathcal{T}) \subseteq \mathcal{A}(\mathcal{S})$$

and

$$C_S(J) \leq C_S(A_0) \leq A_0 \leq J.$$

Since $\mathcal{A}$ is an N^*-set in T, $\mathcal{A}$ is an N-set By hypothesis, $J \lhd G$. Hence, $\mathcal{A}$ satisfies condition (N1) of the definition of an N^*-set in S (rather than T).

The proof that $\mathcal{A}$ satisfies (N2) in S follows easily from Lemma 6.5, since $C_S(J) \leq J$ and $\mathcal{A}$ satisfies (N2) in T. Therefore, we need only prove that $\mathcal{A}$ satisfies (N3) in S.

Take $\mathcal{B}$ as in (N3). Since $\mathcal{A}$ is an N-set in T, it suffices to show that $J(\mathcal{B}) \leq \mathcal{T}$. Now,

$$[J, B; 3] \ \leq \ [J(\mathcal{B}), \mathcal{B}, \mathcal{B}] = \infty, \quad \text{for} \mathcal{B} \in \mathcal{B}. \tag{6.2}$$

and

$$[D, B, B] = 1 \tag{6.3}$$

for every $B \in \mathcal{B}$ and every abelian subgroup D of J normalized by $J(\mathcal{B})$.

We must show that $J(\mathcal{B}) \leq \mathcal{T}$. As (G,T) is a 3-special pair,

$$\text{it suffices to show that } [X, B; 3] \ \leq \ Y \tag{6.4}$$

for every chief factor X/Y of G such that $X \leq T$, and every $B \in \mathcal{B}$.

Now consider an arbitrary chief factor X/Y of G for which $X \leq T$. We may assume that X is minimal in the sense that

(6.5) If X_1/Y_1 is a chief factor of G isomorphic to X/Y as a G-module, and if $X_1 \leq X$, then $X_1 = X$.

We must show that $[X, B; 3] \leq Y$ for every $B \in \mathcal{B}$.

Step 1. Whenever $N \lhd G$ and $N < X$, then $N \leq Y$.

Proof: Suppose not. Then $Y < NY \leq X$ and $NY \lhd G$. By the definition of a chief factor, $NY = X$. Then, as G-modules,

$$N/(N \cap Y) \;\cong\; NY/Y \;=\; X/Y,$$

contrary to (6.5).

Step 2. We may assume that

$$X \cap J \leq Y \tag{6.6}$$

and that

(6.7) X centralizes every normal abelian subgroup of G contained in J.

Proof:

Take any $B \in \mathcal{B}$. If $X \leq J$, then $[X, B; 3] = 1 \leq Y$, by (6.2). If X is not contained in J, then $X \cap J \leq Y$ by Step 1. Thus, we may assume (6.6).

Suppose R is a normal abelian subgroup of G contained in J, and X does not centralize R. We may assume that R is minimal subject to these conditions. Since

$$[R, X] \lhd G \qquad \text{and} \qquad [R, X] < R,$$

X centralizes $[R, X]$. So

$$[R, X, X] \;=\; 1 \;\leq\; Z(X).$$

As $C_X(R) \lhd G$ and $C_X(R) < X$, Step 1 yields that $C_X(R) \leq Y$.

By (6.3), $[R, B, B] = 1$, and by the hypothesis of this entire section, $p \geq 5$. Therefore, Hypothesis 5.1 is satisfied and Proposition 5.4 yields

$$[X, B; 3] \leq Y.$$

This completes the proof of Step 2.

Henceforth, we will assume conditions (6.6) and (6.7) in Step 2.

Step 3. Let $B \in \mathcal{B}$. Then

(a) $[J, X, X] \leq Z(X)$ and $[J, X; 3] = [J, B; 3] = 1$,

(b) $A_0 \leq J$, and A_0 is normalized by X and B, and

(c) $[A_0, B, B] = 1$.

Proof:

Observe that Hypothesis 5.1 is satisfied for $R = J$.

Therefore, by (6.7) and Lemma 5.3,

$$[J, X, X] \leq Z(X) \quad \text{and (hence)} \quad [J, X; 3] = 1.$$

By (6.2), we obtain (a).

Since $A_0 \in \mathcal{A}, \mathcal{A}_{\prime} \leq \mathcal{J}(\mathcal{A}) = \mathcal{J}$. By (a),

$$[A_0, X; 3] = [A_0, B; 3] = 1.$$

Now the definition of $\mathcal{A}_{\in}(\mathcal{S})$ gives (b). Thus, $J(\mathcal{B})$ normalizes A_0, and (6.3) gives (c).

Step 4. Let $B \in \mathcal{B}$. Then

$$[X, B; 3] \leq Y.$$

Proof:

Since $A_0 \in \mathcal{A}(\mathcal{S}), \mathcal{C}_{\mathcal{X}}(\mathcal{A}_{\prime}) = \mathcal{X} \cap \mathcal{A}_{\prime} \leq \mathcal{X} \cap \mathcal{J} \leq \mathcal{Y}$, by (6.6). Now observe that Hypothesis 5.1 is satisfied for $R = A_0$. Finally, Step 3 and Proposition 5.4 yield that $[X, B; 3] \leq Y$, as desired.

By Step 4 and (6.4), we have verified that $\mathcal{A}$ satisfies (N3) in S, and not merely in T. Therefore, $\mathcal{A}$ is an N^*-set in S, not merely in T.

Q.E.D

Now we obtain our main result about 3-special pairs from Corollary 6.7 and Propositions 6.8 and 6.9.

Theorem 6.10 Let (G,T) be a 3-special pair for S, and let $\mathcal{A}_{\mathcal{N}}$ be the unique maximal N^*-set in S.

Then $\mathcal{A}_{\mathcal{N}}$ is the unique maximal N^*-set in T, and $J(\mathcal{A}_{\mathcal{N}}) \lhd \mathcal{G}$.

Definition 6.11 Let $\mathcal{A}_{\mathcal{N}}(\mathcal{S})$ denote the unique maximal N^*-set in S, and let $J_N(S) = J(\mathcal{A}_{\mathcal{N}}(\mathcal{S})) =< \mathcal{A}_{\mathcal{N}}(\mathcal{S}) >$.

Let $\mathcal{A}^{\mathcal{N}}(\mathcal{S})$ be the set of all $A \in \mathcal{A}(\mathcal{S})$ such that $J_N(S)$ normalizes A, and let

$$J^N(S) \ = \ < \mathcal{A}^{\mathcal{N}}(\mathcal{S}) > \quad \text{and} \quad \mathcal{Z}\mathcal{J}^{\mathcal{N}}(\mathcal{S}) = \mathcal{Z}(\mathcal{J}^{\mathcal{N}}(\mathcal{S})).$$

It is easy to see that

$$\mathcal{A}_{\mathcal{N}}(\mathcal{S}) \ \leq \mathcal{A}^{\mathcal{N}}(\mathcal{S}), \quad \mathcal{J}_{\mathcal{N}}(\mathcal{S}) \leq \mathcal{J}^{\mathcal{N}}(\mathcal{S})$$

and

$$Z(S) \leq ZJ(S) \leq ZJ^N(S) \leq Z(J_N(S)).$$

Suppose (G,T) is a 3-special pair for S. Theorem 6.10 asserts that $\mathcal{A}_{\mathcal{N}}(\mathcal{S}) = \mathcal{A}_{\mathcal{N}}(\mathcal{T})$. Part (b) of our next result asserts that $\mathcal{A}^{\mathcal{N}}(\mathcal{S}) = \mathcal{A}^{\mathcal{N}}(\mathcal{T})$ as well. We do not know whether these results extend to all special pairs for S. Part (a) of our next result gives the weaker result that $ZJ^N(S) \lhd G$ for all special pairs (G,T).

Theorem 6.12 Let (G,T) be a special pair for S. Then

(a) $ZJ^N(S) \lhd G$, and

(b) if (G,T) is a 3-special pair, then

$$\mathcal{A}^{\mathcal{N}}(\mathcal{S}) = \mathcal{A}^{\mathcal{N}}(\mathcal{T}) \quad \text{and} \quad \mathcal{J}^{\mathcal{N}}(\mathcal{S}) = \mathcal{J}^{\mathcal{N}}(\mathcal{T}) \lhd \mathcal{G}.$$

<u>Proof</u>:

Let $J = J_N(S)$.

First, assume (G, T) is a 3-special pair. By Theorem 6.10, $J = J_N(T)$. Take any $A \in \mathcal{A}^{\mathcal{N}}(\mathcal{S})$. Then

$$[J, A, A] \ \leq \ [A, A] = 1,$$

and $A \leq T$ by Lemma 6.5. It is easy to see now that

$$\mathcal{A}^{\mathcal{N}}(\mathcal{S}) \ = \ \mathcal{A}^{\mathcal{N}}(\mathcal{T}), \qquad \mathcal{J}^{\mathcal{N}}(\mathcal{S}) = \mathcal{J}^{\mathcal{N}}(\mathcal{T}) \lhd \mathcal{G},$$

and

$$ZJ^N(S) \ = \ ZJ^N(T) \ \lhd \ G.$$

This proves (b), and proves (a) for 3-special pairs.

From the definition of a special pair, we may now assume that G is p-stable. Let

$$Z \ = \ Z(J_N(T)) \qquad \text{and} \qquad C \ = \ C_G(Z)$$

and define $D \leq G$ by

$$D \ \geq \ C \qquad \text{and} \qquad D/C \ = \ O_p(G/C).$$

By Proposition 6.8, $J = J_N(S) \leq J_N(T)$. Since $\mathcal{A}_{\mathcal{N}}(\mathcal{T})$ is a N-set,

(6.8) $$\mathcal{A}_{\mathcal{N}}(\mathcal{T}) \ \leq \ \mathcal{A}^{\mathcal{N}}(\mathcal{S}) \quad \text{and}$$

$$ZJ^N(S) \ \leq \ C_S(J_N(T)) \ = \ Z \leq Z(J) \leq J,$$

and

(6.9) $$ZJ^N(S) \ = \ C_Z(J^N(S)).$$

Take any $A \in \mathcal{A}^{\mathcal{N}}(\mathcal{S})$. Then J normalizes A. By (6.9),

$$[Z, A, A] \ \leq \ [J, A, A] \ = \ 1.$$

By the definition of p-stability, $A \leq D$. Thus,

(6.10) $$J^N(S) \ \leq \ D \cap S.$$

Let $\mathcal{A} = \mathcal{A}_{\mathcal{N}}(\mathcal{D} \cap \mathcal{S})$. Since $\mathcal{A}_{\mathcal{N}}(\mathcal{S})$ is an N^*-set contained inside T, hence inside $D \cap S$,

$$\mathcal{A}_{\mathcal{N}}(\mathcal{S}) \ \subseteq \ \mathcal{A}.$$

We claim that $\mathcal{A}_{\mathcal{N}}(\mathcal{S}) = \mathcal{A}$. It will suffice to show that $\mathcal{A}$ is an N^*-set with respect to S. Condition (N1) is obvious. For x as in (N2), $[Z, x, x] \leq [J(\mathcal{A}), \S, \S] = \infty$; so $x \in D \cap S$, and (N2) for $D \cap S$ yields (N2) for S. For $\mathcal{B}$ as in (N3) and $B \in \mathcal{B}$,

$$[Z, B, B] = 1, \quad \text{and hence} \quad B \leq D \cap S, \quad \text{for every} \quad B \in \mathcal{B}.$$

So we get (N3) for S, and $\mathcal{A}$ is an N^*-set in S. Therefore

$$\mathcal{A}_{\mathcal{N}}(\mathcal{S}) \ = \ \mathcal{A} \ = \ \mathcal{A}_{\mathcal{N}}(\mathcal{D} \cap \mathcal{S}).$$

It is easy to see from (6.10) that

$$J^N(S) \ = \ J^N(D \cap S) \ \lhd \ N_G(D \cap S). \tag{6.11}$$

As D/C is a normal p-subgroup of G/C,

$D \cap S$ is a Sylow p-subgroup of D, and $D = (D \cap S)C = C(D \cap S)$.

By the Frattini argument, $G = DN_G(D \cap S) = C(D \cap S)N_G(D \cap S) = CN_G(D \cap S)$. Recall equation (6.9),

$$ZJ^N(S) \ = \ C_Z(J^N(S)).$$

As $C = C_G(Z)$, the subgroup $ZJ^N(S)$ is centralized by C. By (6.11), it is normalized by $N_G(D \cap S)$ Therefore, it is normalized by G. This proves (a).

Q.E.D

References

[AG] J. Alperin and G. Glauberman, "Limits of abelian subgroups in finite p-groups," in preparation.

[G1] G. Glauberman, "Prime-power factor groups of finite groups, I, II," *Math. Zeit.* **107** (1968), pp. 159-72; **117** (1970), pp. 45-56.

[G2] G. Glauberman, "Global and local properties of finite groups," Chap. I of *Finite Simple Groups*, M.B. Powell and G. Higman, ed., Academic Press, (1971) New York.

[Gor] D. Gorenstein, *Finite Groups*, Second Edition, Chelsea, (1980), New York.

[Hol] D. Holt, "More on the Local Control of Schur Multipliers," *Quart. J. Math. Oxford*, **(2), 31**, (1980), pp. 191-208.

[H] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, (1967), Berlin.

[HB] B. Huppert and N. Blackburn, *Finite Groups II, III*, Springer-Verlag, (1982), Berlin.

[L] M. Lazard, "Sur les groupes nilpotents et les anneaux de Lie," *Ann. Sci. Ecole Norm. Sup.*, **(3), 71**, (1954), 101-90.

[M] M. Miyamoto, "An affirmative answer to Glauberman's conjecture," *Pacific J. Math.*, **102**, (1982), pp. 89-105.

[S] M. Suzuki, *Group Theory II*, Springer-Verlag, (1986), Berlin.

[T1] J.G. Thompson, "Normal p-complements for finite groups," *Math. Zeit*, **72**, (1968), pp. 332-54.

[T2] J.G. Thompson, "Normal p-complements for finite groups," *J. Alg.*, **1**, (1964), pp. 43-46.