Limits of Abelian Subgroups of Finite p-groups

J.L. Alperin *
University of Chicago
alperin@math.uchicago.edu

G. Glauberman †
University of Chicago
gg@math.uchicago.edu

1 Introduction

Abelian subgroups play a key role in the theory and applications of finite p-groups. Our purpose is to establish some very general results motivated by special results that have been of use. In particular, it is known [KJ] that if a finite p-group, for odd p, has an elementary abelian subgroup of order p^n, $n \leq 5$, then it has a normal elementary abelian subgroup of the same order. Our first main result is a general one of this type.

Theorem A

If A is an elementary abelian subgroup of order p^n in a p-group P, then there is a normal elementary abelian subgroup B of the same order contained in the normal closure of A in P, provided that p is odd and greater than $4n-7$.

We are very grateful to the referee for an improvement to our argument which gives this linear bound and many other useful comments. The additional information about the location of B is essential for the inductive argument we shall employ. The strategy is to first reduce this theorem to another, namely the following.

Theorem B

If A is an abelian subgroup of order p^n in a p-group of exponent p and class at most $p+1$, then there is a normal abelian subgroup B of the same order contained in the normal closure of A in P.

*Supported in part by NSF
†Supported in part by NSA

The second theorem is now reducible to a question of Lie algebras via Lazard's functor connecting p-groups and Lie rings; our hypothesis allows use of this functor even though the bound on the class is not $p-1$, which is the usual situation. It is now a consequence of the following result. Fix a field F of prime characteristic p.

Theorem C

If A is an abelian subalgebra of the Lie algebra L over F and L is nilpotent of class at most p, then there is an abelian ideal B of L, in the ideal closure of A in L, of the same dimension as A.

Our proof of this result is direct but the motivation is entirely from algebraic groups. The analogous result for Lie algebras over the complex numbers is due to Kostant [Kos, p.155]. Let L^* be the extension of L to the algebraic closure F^* of F. The idea is that in characteristic p one can use the algebraic group corresponding to L^* and apply the fixed-point theorem of Borel to the Grassmannian of all subspaces of the Lie algebra L^* which are of the same dimension as A. In particular, one could use the form of Borel's theorem which gives rational fixed points. The authors would like to thank W. Fulton for his helpful comments.

We need to introduce some standard notation. For elements or subsets X and Y of a group P we let $(Y, X; k)$, for k non-negative, be defined inductively, as usual, by setting

$$(Y, X; 0) \;=\; Y; \;\text{ then } (Y, X; 1) \;=\; (Y, X)$$

is the subgroup generated by all commutators of the form (y, x) as x runs over X and y runs over Y; and $(Y, X; i+1) = ((Y, X; i), X)$. We now turn to our final main result, which shows that if we are willing to relax the conclusion on normality in Theorem A then we can achieve striking improvements in the bounds on the prime p.

Theorem D

If p is at least 5 and A is an elementary abelian subgroup of order p^n of the p-group P, then there is an elementary abelian subgroup B, also of order p^n, satisfying the following conditions:

(a) B is normal in its normal closure in P;

(b) $(P, B; 3) = 1$;

(c) B is normalized by any element x of P satisfying

$$\left(B, x; \frac{p+1}{2}\right) = 1.$$

However, let us occupy the rest of this introductory section with a proof of the reduction of Theorem A to Theorem B.

Proof. The technique is to prove Theorem A by induction and argue until the situation of Theorem B arises. In fact, we shall do a double induction, first on n and then on the order of P. The case $n = 1$ is trivial so we can proceed with the induction. Again if P has order p^n there is nothing to prove. Let Q be a maximal subgroup of P containing A. Thus, there is a normal elementary abelian subgroup A_1 of Q, contained in the normal closure of A in Q, also of order p^n.

The normal closure of A_1 in P is contained in the normal closure of A in P so we can assume, by replacing A_1 by A, that A is normal in a maximal subgroup of P. In particular, A is normal in its normal closure A^P in P. Thus, the series of intersections of A with the upper central series of A^P will be a series without any equalities until the central series reaches A^P. Thus, A^P will be of class at most n, so it will be of exponent p, being generated by elements of order p and having class certainly less than p.

By induction on n there is an elementary abelian subgroup B of A^P of order p^{n-1} normal in P. If B does not coincide with its centralizer in A^P, then it is of order p^{n-1} contained in the center of a subgroup H of A^P, where H is normal in P and has order p^n. Since A^P is of exponent p, we are done. Hence, we can assume that B is a maximal normal abelian subgroup of A^P.

Let $C = C_P(B)$ and $N = A^P$ so $C \cap N = B$. Since B has order p^{n-1} we have that $B \leq Z_{n-1}(P)$. This implies [Hup, III.2.11] that B centralizes P_{n-1}, the $(n-1)$st term of the lower central series of P. Consider a commutator $[x_1, \ldots, x_{n-1}]$ of elements of P with $x_1 \in N$. It lies in $P_{n-1} \cap N$ which is in $C \cap N = B$ so that we have $N/B \leq Z_{n-2}(P/B)$. But $B \leq Z_{n-1}(P)$ so $N \leq Z_{2n-3}(P)$ and so P_{2n-3} centralizes N. Thus, $P/C_P(N)$ has class at most $2n-4$.

We now form another p-group, the semi-direct product of N by $P/C_P(N)$ and call it P^*. Since $N \leq Z_{2n-3}(P^*)$ and $P/C_P(N)$ has class at most $2n-4$, we have that P^* has class at most $4n-7$. We claim that P^* is generated by elements of order p. This is enough to complete the proof. Indeed, then

P^* will be of exponent p, by our assumption on the size of p [S I, Lemma 4.3.13(ii) and Thrm. 4.3.14(ii), pp.46-7] and Theorem B applies to P^* and immediately yields the result.

Since N is generated by elements of order p, it suffices to prove that the same holds for $P/C_p(N)$. Suppose that $x \in P/C_P(N)$ and $y \in N$. It suffices to prove that x^p and y commute. But $(x^p)^y = (x[x,y])^p$ and the commutator collection process [Hup, III.9] shows this is x^p since N is of exponent p and contained in $Z_{2n-3}(P^*)$ while p is large. $\square$

The rest of the paper is organized in the following way. In Section 2 we study a unipotent automorphism of a non-associative algebra and conditions under which the existence of a subalgebra A with $A^2 = 0$ implies the existence of a similar subalgebra of the same dimension which is invariant under the automorphism. In Section 3 we extend this result to a group of automorphisms and derive Theorem C. In the next section we use Lazard's work to derive Theorems A and B and then in the last section we can apply some of the second author's earlier work [GG 1] to obtain Theorem D.

2 Unipotent automorphisms of algebras

In this section we let L be an algebra (not necessarily associative) over our field F of prime characteristic p, α a unipotent automorphism of L (so $\alpha - 1$ is nilpotent) and shall be studying the abelian subalgebras A (those A for which $A^2 = 0$) of L. We also fix a sequence of α-invariant subspaces $0 = L_0 \leq L_1 \leq \ldots, \leq L_s = L$ such that α induces the identity on each of the successive quotients. Fix a dimension d and define a partial order $\prec$ on the set of abelian subalgebras of L of dimension d in the following way. We set $B \prec B'$ provided $\dim(B \cap L_i) \leq \dim(B' \cap L_i)$ for all $i > 0$, and $\dim(B \cap L_j) < \dim(B' \cap L_j)$ for some j.

The main result is the following.

Theorem 2.8. *If B is maximal under the partial order $\prec$, then B is $\alpha-$invariant provided the following conditions hold:*

1. $(\alpha - 1)^p = 0$;
2. $((\alpha - 1)^i u)((\alpha - 1)^j v) = 0$ *for all u and v in B and for all $i, j \geq 1$ with $i + j \geq p$.*

It is worth mentioning that the result holds in characteristic zero without the two conditions but we do not need this for any application. One could strengthen the definition of the relation $\prec$ by requiring that $B \cap L_j < B' \cap L_j$ instead of $\dim(B \cap L_j) < \dim(B' \cap L_j)$ (see Proposition 2.2(e)). But then $\prec$ would no longer be a partial order.

To obtain this result, we first obtain a "limit" B^* of images of B (Proposition 2.2). This is basically a result from algebraic geometry that requires only that L be a vector space, and does not require Condition 2. Then we use Condition 2 to show, in effect, that taking limits induces an isomorphism of B onto B^* (Proposition 2.4(b) and Theorem 2.6). Finally, we show that, if $B \neq B^*$, then $B \prec B^*$, a contradiction.

Note that every unipotent linear transformation τ of V is invertible because, if $(\tau - 1)^n = 0$,

$$1 - (\tau - 1) + (\tau - 1)^2 + \ldots + (-1)^{n-1}(\tau - 1)^{n-1} = (1 + (\tau - 1))^{-1} = \tau^{-1}.$$

Moreover, if $n \leq p - 1$, we can define

$$\mathrm{Log}\,\tau \ = \ \sum_{i=1}^{p-1} (-1)^{i+1} \frac{(\tau - 1)^i}{i}.$$

Clearly, Log τ is nilpotent because $(\mathrm{Log}\,\tau)^p = 0$.

Similarly, suppose ν is a nilpotent linear transformation of V over F and $\nu^p = 0$. We define

$$\mathrm{Exp}\ \nu \ = \ \sum_{i=0}^{p-1} \frac{\nu^i}{i!}.$$

Then $((\mathrm{Exp}\ \nu) - 1)^p = 0$, and Exp ν is unipotent.

The following result appears to be well known, but we have not found a complete published proof. Most of it is proved by finite methods in [Greg]. We give a shorter proof that requires infinite methods.

Proposition 2.1. *Suppose V is a vector space over F, τ is a unipotent linear transformation of V over F, and ν is a nilpotent linear transformation of V over F. Assume*

$$(\tau - 1)^p = \nu^p = 0. \tag{2.1}$$

Then

(a) *Exp* (*Log* τ) *and Log* (*Exp* ν) *are well defined and*

$$Exp\ (Log\ \tau) = \tau, \qquad Log\ (Exp\ \nu) = \nu,$$

and

(b) *for every natural number* r*, Exp* $r\nu$ *is well defined and*

$$Exp\ r\nu \ = \ (Exp\ \nu)^r.$$

Proof. (a) Let $\mathbb{Q}$ be the field of rational numbers and A_1 be the $\mathbb{Q}$-algebra $Q[[X]]$ of all power series in an indeterminate X. In A_1, define

$$e^X = \sum_{i\geq 0} \frac{X^i}{i!}, \qquad e(X) = e^X - 1, \quad \text{and} \quad l(x) = \sum_{i\geq 1} (-1)^{i-1} \frac{X^i}{i!}.$$

Define $e^Y, e(Y)$ and $l(Y)$ similarly for every Y in A_1 such that Y has zero constant term. It is easy to see that these give well defined elements of A_1 and that e^X and $l(X)$ are the familiar Maclaurin series for the functions e^t and $\log(t-1)$. It is shown in [B, p.A.IV.40] that $l(e(X)) = e(l(X)) = X$.

We take the natural homomorphism Ψ of A_1 onto the algebra

$$A_2 = \mathbb{Q}[X]/(X^p).$$

i.e. the quotient of the polynomial algebra $\mathbb{Q}[X]$ by the principal ideal generated by X^p. For $\overline{X} = \Psi(X)$ and for functions e and l on A_2 defined like $e(X)$ and $l(X)$ above,

$$l(e(\overline{X})) = e(l(\overline{X})) = \overline{X}.$$

Let $\mathbb{Z}[1/(p-1)!]$ be the subring of $\mathbb{Q}$ obtained by adjoining the number $1/(p-1)!$ to the ring of integers $\mathbb{Z}$, and let A_3 be the subring of A_2 generated by

$$\mathbb{Z}[1/(p-1)!] \qquad \text{and} \qquad \overline{X}.$$

Then the functions e and l on A_2 map A_3 into A_3.

Now we take the natural homomorphism Ψ' of A_3 into the algebra over F spanned by ν, with $\overline{X}$ mapping to ν. We define the functions e and l similarly on the image of $\overline{X}A_3$ under Ψ'. Then, using our previous definitions, we have

$$\nu = l(e(\nu)) = l(\exp \nu - 1) = \log(\exp \nu).$$

A similar homomorphism of A_3 with $\overline{X}$ mapping to $\tau - 1$ yields

$$\tau - 1 = e(l(\tau - 1)) = e(\log \tau) = -1 + \exp(\log \tau),$$

and thus $\tau = \exp(\log \tau)$.

(b) The proof is similar to that of (a). For commuting indeterminate X, Y and the algebra of formal power series $\mathbb{Q}[X, Y]$, it is proved in [B, pp.A.IV.39-40] that

$$e^{X+Y} = e^X e^Y.$$

By the method of (a), this yields a proof of (b) by induction on r. □

Now take an indeterminate t over F, and let $F(t)$ be the field obtained by adjoining t to F. For a vector space V over F, let $V(t)$ be the vector space $F(t) \otimes_F V$ over $F(t)$.

Proposition 2.2. *Suppose λ is a linear transformation of a vector space V over F, and $\lambda^p = 0$. For each $u \in V$, let*

$$\tau_t(u) \;= \text{‘} \sum_{i=1}^{p-1} \frac{\lambda^i(u)}{i!} t^i \qquad (\textit{in } V(t)). \tag{2.2}$$

Suppose U is a subspace of V. Let $s = \dim U$, and take a basis $u_1, \ldots, u_s$ of U. On the exterior product space $\Lambda^s(V(t))$, let

$$c(t) = \tau_t(u_1) \wedge \tau_t(u_2) \wedge \ldots \wedge \tau_t(u_s) = \sum_{k=0}^{s(p-1)} c_k t^k, \tag{2.3}$$

where $c_k \in \Lambda^s(V)$ for each k. Then

$$c_0 = u_1 \wedge u_2 \wedge \ldots \wedge u_s.$$

Take the largest integer e for which $c_e \neq 0$. Then the following conditions are satisfied:

(a) Up to scalar multiples, $c(t)$ is independent of the choice of the basis $u_1, \ldots, u_s$.

(b) For some linearly independent vectors $u_1^*, u_2^*, \ldots, u_s^*$ in V,

$$u_1^* \wedge u_2^* \wedge \ldots \wedge u_s^* = c_e.$$

(c) *The subspace* $U^* = \langle u_1^*, u_2^*, \dots, u_s^* \rangle$ *of* V *has dimension* s *and is invariant under* λ.

(d) *For each* λ*-invariant subspace* X *of* V,

$$\dim U^* \cap X \geq \dim U \cap X.$$

(e) *Suppose* $0 = V_0 \leq V_1 \leq \dots V_m = V$ *is an increasing series of subspaces of* V *such that*

$$\lambda V_i \leq V_{i-1}, \quad \textit{for } i = 1, 2, \dots, m. \tag{2.4}$$

If U *is not invariant under* λ, *then*

$$U^* \cap V_i > U \cap V_i \qquad \textit{for some } i.$$

Remark. *By (c) and (d),* U^* *is contained in the smallest* λ*-invariant subspace of* V *containing* U, *i.e., in*

$$U + \lambda(U) + \lambda^2(U) + \dots + \lambda^{p-1}(U).$$

Proof. (a) Since

$$\tau_t(u + v) = \tau_t(u) + \tau_t(v), \qquad \text{and} \qquad \tau_t(au) = a\tau_t(u)$$

for every $u, v \in V$ and $a \in F$, this follows from the standard properties of the exterior product.

(b) Let $h_1(t), \dots, h_s(t)$ be polynomials in t with coefficients from V chosen such that

$$h_1(t) \wedge h_2(t) \wedge \dots \wedge h_s(t) = c(t) \tag{2.5}$$

and $\sum \deg h_i$ is minimal subject to (2.5).

For each i, let d_i be the degree of h_i.and u_i^* be the coefficient of t^{d_i} in $h_i(t)$. Set $d = \sum d_i$. Clearly, from (2.5),

$$u_1^* \wedge u_2^* \wedge \dots \wedge u_s^* \quad \text{is the coefficient of } \; t^d \text{ in } c(t) \tag{2.6}$$

and is equal to c_e if $u_1^* \wedge u_2^* \wedge \dots \wedge u_s^* \neq 0$ (in which case $d = e$).

Suppose $u_1^*, \dots, u_s^*$ are linearly dependent. Let

$$a_1 u_1^* + \dots + a_s u_s^* = 0,$$

where $a_i \in F$ for each i and $a_i \neq 0$ for some i. Among all subscripts i for which $a_i \neq 0$, choose one, i_0 for which d_i has the highest degree. We may assume that $i_0 = 1$ and that $a_1 = 1$. Let

$$h_1^*(t) = h_1(t) + \sum_{2 \le i \le s} a_i t^{d_1 - d_i} h_i(t).$$

Then $h_1^* \wedge h_2(t) \wedge h_3(t) \wedge \ldots \wedge h_s(t) = c(t)$, but

$$\deg h_1^* + \sum_{2 \le i \le s} \deg h_i \; < \; \deg h_1 + \sum_{2 \le i \le s} \deg h_i,$$

contrary to the choice of $h_1(t), \ldots, h_s(t)$. This contradiction shows that $u_1^*, \ldots, u_s^*$ are linearly independent. Now (b) follows from (2.6).

(c) From (b), U^* has dimension s. Since $\lambda^p = 0$, we may let

$$\tau = \tau_1 = \text{Exp } \lambda \; = \; \sum_{i=1}^{p-1} \frac{\lambda^i}{i!}.$$

Then τ operates on V and, in an obvious way, on $V(t)$. From (2.2), we may describe $\tau_t(u)$ as $(\text{Exp } \lambda t)(u)$ for each $u \in V$. The usual calculations for multiplying exponentials show that, for $u \in V$,

$$\tau(\tau_t(u)) = \sum_{i=1}^{p-1} \frac{\lambda^i}{i!} \left(\sum_{j=0}^{p-1} \frac{\lambda^j(u)}{j!} t^j \right) = \sum_{k=0}^{p-1} \frac{\lambda^k(u)}{k!} (t+1)^k = \tau_{t+1}(u)$$

Therefore, from (2.3) and (2.6),

$$\begin{aligned} \sum_{k=0}^{e} \tau(c_k) t^k &= \tau(c(t)) = \tau(\tau_t(u_1) \wedge \tau_t(u_2) \wedge \ldots \wedge \tau_t(u_s)) \\ &= \tau_{t+1}(u_1) \wedge \tau_{t+1}(u_2) \wedge \ldots \wedge \tau_{t+1}(u_s) \\ &= c(t+1) = \sum_{k=0}^{e} c_k (t+1)^k, \end{aligned}$$

and (by comparison of coefficients of t^e)

$$\tau(u_1^* \wedge u_2^* \wedge \ldots \wedge u_s^*) = \tau(c_e) = c_e = u_1^* \wedge u_2^* \wedge \ldots \wedge u_s^*.$$

Hence, $\tau(U^*) = U^*$.

Since

$$\lambda = \text{Log}\ (\text{Exp}\ \lambda) = \text{Log}\ \tau = \sum_{i=1}^{p-1} (-1)^{i+1} \frac{(\tau - 1)^i}{i},$$

we have $\lambda(U^*) \leq U^*$.

(d) Let $r = \dim(U \cap X)$. We may assume that $u_1, \dots, u_r \in X$.

Let us apply the process in the proof of (b) to X and $U \cap X$ in place of V and U. We obtain polynomials $f_1(t), \dots, f_r(t)$ in t with coefficients from X such that

$$f_1(t) \wedge f_2(t) \wedge \dots \wedge f_r(t) = \tau_t(u_1) \wedge \tau_t(u_2) \wedge \dots \tau_t(u_r) \tag{2.7}$$

and the leading coeffcients $u_1^*, \dots, u_r^*$ of $f_1(t), \dots, f_r(t)$ are linearly independent.

From (2.3) and (2.7), and the associativity of the exterior algebra of $V(t)$,

$$f_1(t) \wedge \dots f_r(t) \wedge \tau_t(u_{r+1}) \wedge \dots \tau_t(u_s) = c(t).$$

Now we choose polynomials $h_1(t), \dots, h_s(t)$ in t with coefficients from V such that $\sum \deg h_i$ is minimal subject to

(2.8)

$$h_1(t) \wedge \dots \wedge h_s(t) = c(t), \text{ and the leading coefficients of } h_1(t), \dots, h_s(t)$$

$$\text{span a subspace of } V \text{ that contains } u_1^*, \dots, u_r^*.$$

Then $h_1, \dots, h_s$ exist, since

$$f_1(t), f_2(t), \dots, f_r(t), \tau_t(u_{r+1}), \dots, \tau_t(u_s)$$

satisfy (2.8). The proof of (b) can be adopted to this case; note that, in that proof, the leading coefficient of h_1 is a linear combination of the leading coefficients of $h_2, \dots, h_s$, so that replacing h_1 by h_1^* either preserves or enlarges the subspace of V spanned by the leading coefficients.

Thus,

$$\langle u_1^*, \dots, u_r^* \rangle \leq U^* \cap X,$$

and $\dim U^* \cap X \geq r = \dim U \cap X$.

(e) Assume U is not invariant under λ. Take i to be maximal subject to

$$U^* \cap V_i = U \cap V_i. \tag{2.9}$$

Then $0 \le i < m$ and

$$U^* \cap V_{i+1} \neq U \cap V_{i+1}, \tag{2.10}$$

Suppose $U \cap V_{i+1} \le U^* \cap V_{i+1}$. By (2.10), $U^* \cap V_{i+1} > U \cap V_{i+1}$, as required.

Next, suppose $U \cap V_{i+1}$ is not contained in $U^* \cap V_{i+1}$. Take $u \in U \cap V_{i+1}$ such that $u \notin U^* \cap V_{i+1}$. Then $u \notin U^*$ and $\lambda^p(u) = 0$. Take r minimal so that $\lambda^r(u) = 0$. Let

$$X = \langle u, \lambda(u), \lambda^2(u), \dots, \lambda^{r-1}(u) \rangle.$$

Then X is invariant under λ. By (d),

$$\dim U^* \cap X \ge \dim U \cap X.$$

Since $u \in U \cap X$ and $u \notin U^*$, there exists $v \in U^* \cap X$ such that $v \notin U$.

By (2.4),

$$\lambda V_j \le V_{j-1} \qquad \text{for } j = 1, 2, \dots, m. \tag{2.11}$$

Therefore, each subspace V_j is invariant under λ,and $\lambda(u) \in \lambda(V_{i+1}) \le V_i$. Hence,

$$\lambda(u), \lambda^2(u), \dots, \lambda^{r-1}(u) \in V_i.$$

Since $v \in U^*$ and $v \notin U$, (2.9) shows that $v \notin V_i$. So

$$v = a_0 u + a_1 \lambda(u) + \cdots + a_{r-1} \lambda^{r-1}(u),$$

with $a_0, a_1, \dots, a_{r-1} \in F$ and $a_0 \neq 0$. Replacing v by $a_0^{-1} v$, we may assume that $a_0 = 1$.

As U^* is invariant under λ, we get

$$\lambda^{r-1}(u) = \lambda^{r-1}(v) \in U^*.$$

Similarly,

$$\lambda^{r-2}(u) = \lambda^{r-2}(v) - a_1 \lambda^{r-1}(u) \in U^*.$$

By an obvious induction,

$$\lambda^{r-3}(u), \lambda^{r-4}(u), \dots, \lambda(u), u \in U^*,$$

contrary to $u \notin U^*$. This contradiction completes the proof of (e) and of Proposition 2.2. □

We now consider the following situation:

Hypothesis 2.3. *(a) L is a non-associative algebra over a field F of prime characteristic p;*

(b) α is an automorphism of L;

(c) $(\alpha - 1)^p = 0$;

(d) $\lambda = Log\ \alpha$;

(e) U is a subspace of L;

(f) moreover,

$$((\alpha-1)^i u)((\alpha-1)^j v) = 0,$$

for all $u, v \in U$ and all natural numbers i, j such that $i + j \geq p$.

Note that, by (c), λ is well defined and $\lambda^p = 0$. For applications, usually L will be a Lie algebra.

Proposition 2.4. *Assume Hypothesis 2.3. Let t be an indeterminate over F, and let $F(t)$ be the field obtained by adjoining t to F. Let*

$$L(t) = F(t) \otimes_F L,$$

and regard $L(t)$ as an algebra over $F(t)$ in the usual way. Define τ_t on $L(t)$ as in Proposition 2.2, i.e.,

$$\tau_t = \sum_{i=0}^{p-1} \frac{\lambda^i(u)}{i!} t^i, \qquad \text{for each } u \in L.$$

Then

(a) for each natural number k,

$$\lambda^k(uv) = \sum_{i=0}^{k} \binom{k}{i} \lambda^i(u)\lambda^{k-i}(v), \qquad \text{for all } u, v \in U,$$

and

(b)

$$\tau_t(uv) \;=\; \tau_t(u)\tau_t(v) \qquad \textit{for all } u, v \in U.$$

Proof. By Proposition 2.1, $\alpha^r = \operatorname{Exp} r\lambda$ for every natural number r, including $r = 1$. Note that we may think of τ_t as $\operatorname{Exp} t\lambda$.

For $u, v \in U$ and each natural number r,

$$\sum_{k=0}^{p-1} \frac{r^k \lambda^k(uv)}{k!} = (\operatorname{Exp} r\lambda)(uv) = \alpha^r(uv) = \alpha^r(u) \cdot \alpha^r(v) \tag{2.12}$$

$$= \left(\sum_{i=0}^{p-1} \frac{r^i \lambda^i(u)}{i!} \right) \left(\sum_{j=0}^{p-1} \frac{r^j \lambda^j(v)}{j!} \right) = \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \frac{r^{i+j} \lambda^i(u) \lambda^j(v)}{i! j!}.$$

(a) Take $u, v \in U$. By Hypothesis 2.3, $\lambda^p = 0$ and

$$(\alpha - 1)^i u \cdot (\alpha - 1)^j v = 0$$

whenever $i, j \geq 1$ and $i + j \geq p$. Since

$$\lambda = \operatorname{Log} \alpha = \sum_{1 \leq i \leq p-1} (-1)^{i+1} \frac{(\alpha - 1)^i}{i},$$

it follows that

$$\lambda^i(u) \cdot \lambda^j(v) = 0 \quad \text{whenever } i, j \geq 1 \text{ and } i + j \geq p. \tag{2.13}$$

Now we may rewrite (2.12) as

$$\sum_{k=0}^{p-1} \frac{r^k \lambda^k(uv)}{k!} = \sum_{k=0}^{p-1} r^k \sum_{i=0}^{k} \frac{\lambda^i(u) \lambda^{k-i}(v)}{i!(k-i)!}.$$

and then as

$$\sum_{k=0}^{p-1} r^k \left\{ \frac{\lambda^k(uv)}{k!} - \sum_{i=0}^{k} \frac{\lambda^i(u) \lambda^{k-i}(v)}{i!(k-i)!} \right\} = 0. \tag{2.14}$$

We may think of r as a natural number or as an element of F; note that $0^0 = p^0 = 1$.

Let $M = (m_{sr})$ be the Vandermonde matrix of degree p given by

$$m_{sr} = r^s, \quad \text{for } s, r = 0, 1, \ldots, p-1 \text{ (where } 0^0 = 1).$$

Let y be the row vector $(y_0, \ldots, y_{p-1})$ given by

$$y_k = \frac{\lambda^k(uv)}{k!} - \sum_{i=0}^{k} \frac{\lambda^i(u)\lambda^{k-i}(v)}{i!(k-i)!}.$$

Since (2.14) holds for all r, the product yM is the zero row vector of length p. As the matrix M is nonsingular, y is the zero row vector. Therefore, for $k = 0, 1, \ldots, p-1$,

$$0 = k!y_k = \lambda^k(uv) - \sum_{i=0}^{k} \binom{k}{i} \lambda^i(u)\lambda^{k-i}(v).$$

This proves (a) for $k \leq p-1$. Since $\lambda^p = 0$, (2.13) yields (a) for $k \geq p$.

(b) Let $u, v \in U$ Here, in effect, we reverse the proof of (a). We have

$$\begin{aligned} \tau_t(u)\tau_t(v) &= \left(\sum_{i=0}^{p-1} \frac{t^i\lambda^i(u)}{i!}\right)\left(\sum_{j=0}^{p-1} \frac{t^j\lambda^j(v)}{j!}\right) \\ &= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \frac{t^{i+j}\lambda^i(u)\lambda^j(v)}{i!j!}. \end{aligned}$$

By (2.13), we can write

$$\tau_t(u)\tau_t(v) = \sum_{k=0}^{p-1} t^k \sum_{i=0}^{k} \frac{\lambda^i(u)\lambda^{k-i}(v)}{i!(k-i)!} = \sum_{k=0}^{p-1} \frac{t^k}{k!} \sum_{i=0}^{k} \binom{k}{i} \lambda^i(u)\lambda^{k-i}(v).$$

By (a),

$$\tau_t(u)\tau_t(v) = \sum_{k=0}^{p-1} \frac{t^k}{k!}\lambda^k(uv) = \tau_t(uv).$$

This proves (b). □

For later use, we now state what is roughly a converse to Proposition 2.4. Recall that a *derivation* of L over F is an endomorphism δ of L over F such that

$$\delta(xy) = \delta(x)y + x\delta(y), \qquad \text{for all } x, y \in L.$$

Proposition 2.5. *Assume Hypothesis 2.3. Suppose δ is a derivation of L.*

(a) For every natural number k,

$$\delta^k(xy) = \sum_{i=0}^{k} \binom{k}{i} \delta^i(x)\delta^{k-i}(y), \qquad \text{for all } x, y \in L.$$

(b) Assume $\delta^p = 0$ and

$$\delta^i(u)\delta^j(v) = 0,$$

for all $u, v \in U$ and all $i, j \geq 1$ such that $i + j \geq p$.

Then Exp δ exists and

$$(Exp\ \delta)(uv) = (Exp\ \delta)(u) \cdot (Exp\ \delta)(v),$$

for all $u, v \in U$.

Proof. (a) This follows from induction on k and the use of the identity

$$\binom{k+1}{i} = \binom{k}{i} + \binom{k}{i-1}, \qquad 1 \leq i \leq k.$$

(b) As discussed before Proposition 2.1, Exp δ is well defined, unipotent and hence invertible, and

$$((\mathrm{Exp}\ \delta) - 1)^p = 0 \quad \text{and} \quad \delta = \mathrm{Log}\ (\mathrm{Exp}\ \delta).$$

Let $\beta = \mathrm{Exp}\ \delta$. By (a), δ satisfies the conditions on λ in Proposition 2.4(a). The proof of Proposition 2.4(b) shows that

$$\beta(uv) = \beta(u)\beta(v), \qquad \text{for all } u, v \in U.$$

(However, β need not be an automorphism of L if $U \neq L$.) $\square$

Theorem 2.6. *Assume Hypothesis 2.3. Suppose $U^2 = 0$, i.e.*

$$uv = 0, \qquad \text{for all } u, v \in U.$$

Define a subspace U^* of L by letting $V = L$ in Proposition 2.2.
Then $U^{*2} = 0$ and U^* is invariant under α.

Remark. *Of course, U^* also satisfies conclusions (a) - (e) of Proposition 2.2.*

Proof. Let us recall our notation from Proposition 2.2. We let $s = \dim(U)$ and choose a basis $u_1, u_2, \ldots, u_s$ of U. Take $t, F(t), L(t)$ and τ_t as in Proposition 2.4. In the exterior product space $\Lambda^s(L(t))$, let

$$c(t) = \tau_t(u_1) \wedge \tau_t(u_2) \wedge \ldots \wedge \tau_t(u_s) = \sum_{k=0}^{s(p-1)} c_k t^k,$$

where $c_k \in \Lambda^s(L)$ for each k. Let e be the largest subscript for which $c_e \neq 0$.

Let

$$\tau_t(U) \;=\; \{\tau_t(u) \bigm| u \in U\}.$$

Since τ_t is a vector space endomorphism of $L(t)$ over $F(t)$,

$$\tau_t(U) \;=\; \langle \tau_t(u_1), \ldots, \tau_t(u_s)\rangle.$$

As $U^2 = 0$, Proposition 2.4(b) yields

$$(\tau_t(U))^2 = 0. \tag{2.15}$$

In the proof of Proposition 2.2, we found polynomials $h_1(t), \ldots, h_s(t)$ in $L(t)$, and a basis $u_1^*, \ldots, u_s^*$ of U^* such that

$$h_1(t) \wedge \ldots \wedge h_s(t) = c(t) = \tau_t(u_1) \wedge \ldots \wedge \tau_t(u_s)$$

and, for $i = 1, \ldots, s$ with $d_i = \deg h_i$,

$$u_i^* \text{ is the leading coefficient (the coefficient of } t^{d_i}\text{) of } h_i(t).$$

Then $h_1(t), \ldots, h_s(t)$ form a basis of $\tau_t(U)$ over $F(t)$ and, for each i, j,

$$u_i^* u_j^* = \text{ coefficient of } t^{d_i + d_j} \text{ in } h_i(t) h_j(t) = 0.$$

This shows that $U^{*2} = 0$.

Since U^* is invariant under λ and $\alpha = \operatorname{Exp} \lambda$, U^* is invariant under α. $\square$

We give counterexamples to some generalizations of Theorem 2.6 in Example 3.6.

Remark 2.7. *An examination of the proof of Theorem 2.6 shows that, by strengthening Hypothesis 2.3(f), we may replace the condition*

$$U^2 = 0$$

by $U^2 \cdot U = 0$*, or* $U^2 \cdot U = U \cdot U^2 = 0$*, or various identities, and obtain the analogous condition for* U^**.*

Now we come to the proof of the main result of this section (which is stated at the beginning of the section).

Proof. Recall that $(\alpha - 1)^p = 0$. Therefore, we may define

$$\lambda = \mathrm{Log}\ \alpha.$$

Observe that Hypothesis 2.3 is satisfied for $U = B$. Now define a subspace U^* of L by letting $V = L$ in Proposition 2.2. By Theorem 2.6,

$$U^{*2} = 0 \text{ and } U^* \text{ is invariant under } \alpha.$$

By parts (c), (d) and (e) of Proposition 2.2, $U \prec U^*$ if U is not invariant under α. However, we chose B to be maximal under $\prec$. Therefore, B is invariant under α, as desired. □

3 Unipotent groups of automorphisms of algebras

Throughout this section, F is a field of prime characteristic p. (As mentioned above, our results can be extended to characteristic zero.)

In this section, we extend our main result on a single unipotent automorphism (Theorem 2.8) to a result about a group of automorphisms (Theorem 3.1). We also apply the results of Section 2 to Lie algebras in Theorem 3.1 and Corollary 3.4 (which gives Theorem C). The rest of this section consists of counterexamples (Examples 3.5 and 3.6) to generalizations of Theorems 3.1 and 3.3. The reader interested only in groups may skip this section. Our next result is an immediate consequence of Theorem 2.8.

Theorem 3.1. *Suppose* G *is a group of automorphisms of a finite-dimensional algebra* L *over* F*, and*

$$0 = L_0 \le L_1 \le \ldots \le L_s = L$$

is a sequence of subspaces of L such that

$$(3.1) \qquad (\alpha - 1)L_i \leq L_{i-1}, \quad \text{for } i = 1, 2, \ldots, s \text{ and every } \alpha \in G$$

Let B_0 be a subspace of L for which $B_0^2 = 0$. Define a partial ordering $\prec$ on the set of all subspaces B of L for which

$$B^2 = 0 \quad \text{and} \quad \dim B = \dim B_0$$

by setting $B \prec B'$ if

(i) $\dim B \cap L_i \leq \dim B' \cap L_i$ *for $i = 1, 2, \ldots, s$,*

and

(ii) $\dim(B \cap L_i) < \dim(B' \cap L_i)$*, for some $i\,(1 \leq i \leq s)$.*

Take B^* maximal under $\prec$. Let n be a natural number. Assume that G is generated by a set S of elements α such that

$$(3.2) \qquad (\alpha - 1)^p = 0$$

and

$$(3.3) \qquad ((\alpha - 1)^i u)((\alpha - 1)^j v) = 0$$

for all $u, v \in B^*$ and all $i, j \geq 1$ such that $i + j \geq p$.

Then B^* is invariant under G.

Remark 3.2. *As in Remark 2.7, one may generalize this result by replacing the condition $B^2 = 0$ by $B^2 \cdot B = 0$ or various other identities (and strengthening condition (3.3)).*

Recall that an *abelian* subalgebra of a Lie algebra L is a subalgebra B such that $[B, B] = 0$.

Notation

For elements x, y in a Lie algebra, define the iterated commutator $[y, x; i]$ for each natural number i inductively by

$$[y, x; 1] \;=\; [y, x]$$

and

$$[y, x; i+1] = [[y, x; i], x], \quad \text{for each } i = 1, 2, 3, \ldots.$$

For subalgebras X, Y, define $[Y, X; i]$ to be the subspace spanned by all elements $[y, x; i]$ for $x \in X, y \in Y$.

Theorem 3.3. *Suppose L is a finite-dimensional nilpotent Lie algebra over F and B_0 is an abelian subalgebra over L. Let*

$$0 = L_0 \le L_1 \le \ldots \le L_s = L \tag{3.4}$$

be a central series for L, and let

$$\hat{B}_0 = B_0 \oplus \sum_{i \ge 1} [B_0, L; i].$$

Define a partial ordering $\prec$ as in Theorem 2.8 (or 3.1)on the set of all abelian subalgebras B of L for which

$$B \le \hat{B}_0 \quad \textit{and} \quad \dim B = \dim B_0,$$

and take B^* maximal under $\prec$.

Assume that L is generated by a set E of elements x such that

$$[y, x; p] = 0 = [[u, x; i], [v, x; j]] \tag{3.5}$$

for all $y \in L$ and $u, v \in B^*$, and all natural numbers i, j such that $i + j \ge p$.

Then B^* is an ideal of L.

Proof. Take E as given. Because of the Jacobi identity, it suffices to show that $[B^*, x] \subset B^*$ for every $x \in E$. So take an arbitrary element x of E.

Let K be the subspace of L spanned by B^* and all iterated commutators

$$[u, x; i], \quad u \in B^*, \quad i \ge 1.$$

It is easy to see, by using this spanning set, that

(3.6) If $p > 0$, then (3.5) is valid with B^* replaced with K.

Note that $K \le \hat{B}_0$.

Now let M be the vector space external direct sum $K \oplus [KK]$, i.e.

$$M = \{(y, z) \mid y \in K, \, z \in [KK]\}.$$

Then M is a vector space over F in the usual way. Define multiplication on M by

$$[(y, z), (y', z')] \; = \; (0, [y, y']) \, .$$

It is easy to see that M becomes a Lie algebra over F under this definition. Moreover,

(3.7) for every abelian subalgebra B of L, the subspace

$$B \oplus [KK] \;=\; \{(y,z) \bigm| y \in B,\; z \in [KK]\}$$

is an abelian subalgebra of M.

Recall that the adjoint of x is the linear mapping on L given by

$$(\mathrm{ad}\, x)(y) \;=\; [y,x],$$

and that ad x is a derivation of L. Define $\delta : M \to M$ by

$$\delta(y,z) \;=\; ((\mathrm{ad} x)(y)\,,\,(\mathrm{ad} x)(z)) \;=\; ([y,x],[z,x]).$$

It is easy to see that δ is a derivation of M. Since (3.4) is a central series of L,

$$(\mathrm{ad} x)(L_i) \;=\; [L_i,x] \le L_{i-1}, \quad i = 1,2,\ldots,s. \tag{3.8}$$

From (3.6), it is easy to see that

$$\delta^p = 0 \text{ and } [w\delta^i, w'\delta^j] = 0, \tag{3.9}$$

for all w, w' in M and all natural numbers i, j such that $i + j \ge p$.

Let α and λ be the identity and zero mappings of M and let $U = M$. Then Hypothesis 2.3 is satisfied with M in place of L. By (3.9) and Proposition 2.5(b), Exp δ is defined and is an automorphism of M.

Now we change notation to let α be Exp δ and λ be δ, and let U be $B^* \oplus [KK]$. Let

$$V_0 = 0 \text{ and } V_i = L_{i-1} \oplus [KK], \quad i = 1,2,\ldots,s+1.$$

Note that $\lambda(V_i) = \delta(V_i) \le V_{i-1}$ for each i. Take U^* as in Proposition 2.2 (with $V = M$). From Proposition 2.2(d),(e) and our maximal choice of B^*, we have

$$U^* = U = B^* \oplus [KK].$$

Therefore, by Theorem 2.6, U^* is invariant under α, and hence under δ. It follows that

$$B^* \ge (\mathrm{ad} x)(B^*) = [B^*, x]$$

as desired. □

Corollary 3.4. *Suppose L is a finite-dimensional nilpotent Lie algebra over F and B is an abelian subalgebra of L. Assume one of the following conditions:*

(i) L is generated by elements x such that

$$[y,x;p] = 0 = [[u,x;i],[v,x;p-i]],$$

for all $y,u,v \in L$ and $i = 1,2,\dots,p-1$,

(ii) L is generated by elements x such that

$$[y,x;n] = 0 \quad \textit{for} \quad n = \left[\frac{p+1}{2}\right] \ \textit{and all } y \in L;$$

or

(iii) L has nilpotence class at most p.

Then there exists an abelian ideal B^* of L for which

$$B^* \le B + \sum_{i\ge 1}[B,L;i] \quad \textit{and} \quad \dim B^* = \dim B.$$

Proof. Note that L satisfies (i), since (ii) and (iii) are clearly stronger than (i). However, (3.5) follows from (i). Take B^* as in Theorem 3.3 (with B in place of B_0). □

Proof of Theorem C

Clearly Theorem C follows from Corollary 3.4.

Example 3.5. We give an example to show that Theorem 3.3, Corollary 3.4 and Theorem C are false, if one deletes the hypotheses on L.

Let $F = \mathbb{F}_p$. Let r be an integer, given by

$$r = 3 \text{ if } p = 2;\ r = 6 \text{ if } p = 3;\ r = \frac{p+3}{2} \text{ if } p \ge 5.$$

Let M be the Lie algebra over F given by the generators

$$u_0, u_1, \dots, u_r$$

subject to the relations

$$[[x,y],z]=0 \quad \text{for all } x,y,z\in M. \tag{3.10}$$

Then $[M,M]$ has a basis given by

$$[u_i,u_j], \quad 0\le i<j\le r. \tag{3.11}$$

Define $u_i=0$ for $i=r+1,r+2,\ldots$. We may define a linear transformation D on M by

$$Du_i=u_{i+1} \text{ and } D[u_i,u_j]=[u_{i+1},u_j]+[u_i,u_{j+1}]\ (0\le i<j\le r)$$

Thus $Du_r=0$ and $D[u_i,u_r]=[u_{i+1},u_r]$ for $i=0,1,\ldots,r-1$. Clearly, D is a derivation of M.

By Proposition 2.5,

$$D^k[u_0,u_2]=\sum_{i=0}^{k}\binom{k}{i}[D^iu_0,D^{k-i}u_2]=\sum_{i=0}^{k}\binom{k}{i}[u_i,u_{k+2-i}], \tag{3.12}$$

for each positive integer k. If $k\ge 2r-2$, then each summand has

$$i\ge r+1 \quad\text{or}\quad k+2-i\ge r+1 \quad\text{or}\quad i=k+2-i=r,$$

whence $[u_i,u_{k+1-i}]=0$; thus $D^k[u_0,u_2]=0$. Let M_1 be the subspace of M spanned by $[u_0,u_2]$ and $D^k[u_0,u_2]$ for $k=1,2,\ldots 2r-3$. Since M_1 is contained in the center of M, M_1 is an ideal of M.

Let L_0 be the quotient M/M_1. Then D induces a derivation D_0 on L_0. For each $i=0,1,2,\ldots$, let x_i be the element u_i+M_i in L_0.

We claim that $[x_{r-1},x_r]\ne 0$. To see this, we need only show that $[u_{r-1},u_r]$ is not in the subspace M_1. We use the basis (3.11) of $[M,M]$. By (3.12), the only integer for which $[u_{r-1},u_r]$ can possibly appear with nonzero coefficient in $D^k[u_0,u_2]$ is $2r-3$ (since $i+(k+2-i)=k+2$ for all i). Since $u_j=0$ whenever $j\ge r+1$, we need only consider summands for which

$$i\le r \quad\text{and}\quad k+2-i\le r, \quad \text{i.e., } r-1=k+2-r\le i\le r.$$

So

$$D^{2r-3}[u_0,u_2]=\binom{2r-3}{r-1}[u_{r-1},u_r]+\binom{2r-3}{r}[u_r,u_{r-1}]=s[u_{r-1},u_r],$$

$$\text{for } s = \begin{pmatrix} 2r-3 \\ r-1 \end{pmatrix} - \begin{pmatrix} 2r-3 \\ r \end{pmatrix}.$$

If $p = 2$, we have

$$r = 3 \text{ and } s = \begin{pmatrix} 3 \\ 2 \end{pmatrix} - \begin{pmatrix} 3 \\ 3 \end{pmatrix} = 3 - 1 = 2 = 0 \quad \text{in } \mathbb{F}_2.$$

If $p = 3$, then

$$r = 6 \text{ and } s = \begin{pmatrix} 9 \\ 5 \end{pmatrix} - \begin{pmatrix} 9 \\ 6 \end{pmatrix} = 3^2 \cdot 14 = 3 \cdot 28 = 0 \quad \text{in } \mathbb{F}_3.$$

If $p = 5$ then

$$r = \frac{p+3}{2}, \quad 1 \leq r-1 < r \leq p-1, \quad 2r-3 = p,$$

and hence

$$s = \begin{pmatrix} p \\ r-1 \end{pmatrix} - \begin{pmatrix} p \\ r \end{pmatrix} = 0.$$

(More generally, $D^p = 0$ whenever $p \geq 5$.) Thus, in all cases,

$$[x_{r-1}, x_r] \neq 0.$$

Now let L be the semi-direct product $L_0 \oplus FD_0$, and let $L_1 = [L_0, L_0]$, $d = \dim L_1$, and $B = Fx_0 \oplus Fx_2 \oplus L_1$. Then

$$B \text{ is an abelian subalgebra of } L \text{ and } \dim B = 2 + d.$$

Suppose L has an abelian ideal B^* of dimension $2+d$. Since L_1 is clearly an ideal of L, we obtain an abelian ideal

$$(B^* + L_1)/L_1 \leq L/L_1.$$

Because $D_0 u_i = u_{i+1}$ for $i = 0, 1, \ldots, r-1$, it is easy to see that the only nonzero D_0-invariant subspaces of L_0/L_1 are

$$(\langle x_i, x_{i+1}, \cdots, x_r \rangle \oplus L_1)/L_1, \quad i = 1, 2, \ldots, r.$$

Therefore, $((B^* \cap L_0) \oplus L_1)/L_1$ is one of these, or is 0. Since L_1 is contained in the center of L_0 and $[x_{r-1}, x_r] \neq 0$,

$$B^* \cap L_0 \leq (B^* \cap L_0) \oplus L_1 = L_1 \text{ or } \langle x_r \rangle \oplus L_1.$$

Now $\dim\langle x_r\rangle \oplus L_1 = 1 + d = \dim B^* - 1$, and L/L_0 is 1-dimensional. Therefore,

$$B^* \cap L_0 = \langle x_r\rangle \oplus L_1 \quad \text{and} \quad B^* \nleq L_0.$$

So there exists $y \in B^* - (B^* \cap L_0)$. But then L_1 lies in the center of $\langle L_0, y\rangle = L$. This is impossible, since

$$[x_{r-2}, x_r] \in L_1 \text{ and } D_0[x_{r-2}, x_r] = [x_{r-1}, x_r] + [x_{r-2}, x_{r+1}] = [x_{r-1}, x_r] \neq 0.$$

This contradiction shows that L has no abelian ideal of dimension $d+2$, although it has an abelian subalgebra of dimension $d+2$. Therefore, Theorem 3.3, Corollary 3.4 and Theorem C do not hold in general without some restriction like (3.5).

We give counterexamples to generalization of some of our other results, based on an example by the first author [Hup, Aufg. 31, p.349].

Example 3.6. Suppose p is a prime and $F = \mathbb{F}_p$. Let L be the Lie algebra over F with generators

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

and relations

$$[x_i, y_i] = 0 \ (i = 1, \dots, p), \quad [[x, y], z] = 0 \text{ for all } x, y, z \in L.$$

Let $L' = [L, L]$. One sees that

$$L' \text{ has basis } [x_i, x_j], [y_i, y_j], [x_i, y_{i'}] \ (1 \leq i, i', j' \leq p),$$

$$\text{subject to } i < j \text{ and } i \neq i');$$

$$\dim\ L' = 4 \begin{pmatrix} p \\ 2 \end{pmatrix} = 2p^2 - 2p,\ \dim L = 2p^2;$$

$$L \text{ has a unique automorphism } \alpha \text{ such that}$$

$$x_i^\alpha = x_{i+1},\ y_i^\alpha = y_{i+1} \text{ (for } i \bmod p\text{), and } \alpha^p = 1;$$

and the only abelian subalgebras of L of dimension $2p^2 - 2p + 2$ are $\langle x_i, y_i, L'\rangle$, $(i = 1, 2, \dots, p)$, and none is invariant under the group $\langle\alpha\rangle$.

Let $G = \langle\alpha\rangle$. In this example, $(\alpha - 1)^p = \alpha^p - 1 = 0$, but L and G violate the conclusion (and hence (3.3)) in Theorem 3.1. The proof of Theorem 3.1 and its predecessors show that this is also a counterexample to some generalization of Proposition 2.4 and Theorems C and 2.6.

4 Applications to p-Groups

In this section, we transform Theorem 2.8, a result about algebras, into Theorem 4.5, a result about p-groups. Then we prove a special case of Theorem B that allows us to prove Theorem A.

Our main tool for applying the results of the previous section to p-groups is the Baker-Campbell-Hausdorff Formula [J, pp.170-4]. As usually stated, one starts with a Lie algebra L over a field F of characteristic 0, and turns L into a group by defining, for $x, y \in L$,

$$xy = x + y + \frac{1}{2}[x, y] + \cdots \tag{4.1}$$

Some restrictions are necessary to make the series converge, e.g. L may be nilpotent. However, M. Lazard showed in [L, Theorem 4.3] that

1. (4.1) can be used to define a group if F has some prime characteristic p and L is nilpotent of class at most $p - 1$; and
2. in many situations, one may start with a group G and invert (4.1) to convert G into a Lie algebra.

Our approach here is to apply (2) and then use Theorem 2.8 to assert that a particular abelian subgroup of G is normal in G, or invariant under some group of automorphisms of G. Such applications for groups defined over infinite fields appear to be well known, and then one may apply other methods; e.g., Kostant used the Borel Fixed Point Theorem for his result mentioned in the introduction. For this reason, we restrict our attention to finite p-groups.

Henceforth in this section, assume that P is an arbitrary finite p-group for an arbitrary prime p, and all groups are finite.

Consider the following conditions on a triple (Q, R, A).

Hypothesis 4.1.

(4.1a) R is a p-group. $Q \lhd R$, and A is an elementary abelian subgroup of Q.

(4.1b) There exists a central series of Q,

$$1 = Q(0) \leq Q(1) \leq \ldots, \leq Q(s) = Q,$$

which can be extended to a central series of R, such that:

whenever B is an elementary abelian subgroup of Q and
$|B| = |A|$ *and* $|B \cap Q(i)| \geq |A \cap Q(i)|$ *for all* $i, (0 \leq i \leq s)$
then there is no value of $i, (0 \leq i \leq s)$ *for which* $B \cap Q(i) > A \cap Q(i)$.

Proposition 4.2. *Suppose a triple (Q, R, A_0) satisfies condition (4.1a) in Hypothesis 4.1.*

(a) for every central series Q that can be extended to a central series of R, there exists an elementary abelian subgroup A of Q such that $|A| = |A_0|$ and (Q, R, A) satisfies Hypothesis 4.1, and

(b) for some choice of the central series Q and of A in (a), $A \leq \langle A_0^R \rangle$.

Proof. (a) Consider the set of all elementary abelian subgroups of Q of order $|A_0|$. Put a partial ordering on this set similar to the partial ordering in Theorem 2.8 (with order in place of dimension). Then take a maximal element A such that $A_0 \prec A$ or $A_0 = A$.

(b) Extend the series $1 \leq \langle A_0^R \rangle \leq Q \leq R$ to a central series of R, and take the portion from 1 to Q as the central series in Hypothesis 4.1(b). Then take A as in (a). We obtain

$$|A \cap \langle A_0^R \rangle| \geq |A_0 \cap \langle A_0^R \rangle| = |A_0| = |A|.$$

Therefore, $A \leq \langle A_0^R \rangle$. □

Now we state the special case of Lazard's results that we need:

Theorem 4.3. *[L, Théorème II.4.6, pp 179-80]*

Suppose P has exponent 1 or p and nilpotence class at most $p-1$. Then, by means of an inversion of the formula (4.1), P may be regarded as a Lie algebra over F_p. For these structures, the notions of subgroup (respectively, normal subgroup) and of subalgebra (respectively, ideal) coincide.

Moreover, for $x, y, \in P$ and any integer n, x^n in the group is equal to nx in the algebra, and $xy = yx$ in the group if and only if $[x, y] = 0$ in the algebra.

Note The second paragraph of Theorem 4.3 is not stated explicitly in the result quoted, but is easy to derive from (4.1), eg. as discussed in [L, pp. 142-3]. Note that each automorphism of P as a group becomes an automorphism of P as a Lie algebra and, in particular, becomes a linear transformation of P.

Notation We recall some notation from Section 1. For $x, y \in P$, let

$$(x, y) \;=\; x^{-1}y^{-1}xy.$$

(This disagrees with [L][p.105], but we will not make further references to [L].) Then, we define $(y, x; i)$ for each positive integer i inductively by

$$(y, x; 1) = (y, x) \text{ and } (y, x; i+1) = ((y, x; i), x) \text{ for each } i = 1, 2, 3, \ldots$$

(This is analogous to our definition of iterated commutators $[v, u; i]$ for u, v in a Lie algebra, before Theorem 3.3.)

For $x \in P$ and a subgroup Q of P, let (Q, x) be the subgroup of P generated by all the elements (y, x) for $y \in Q$.

Lemma 4.4. *Suppose $Q \leq P$ and $g \in P$. Assume that Q has exponent 1 or p and nilpotence class at most $p-1$, and g normalizes Q. Let α be the automorphism on Q given by conjugation by g in the group P, i.e.*

$$\alpha(x) \;=\; g^{-1}xg.$$

Consider α as a linear transformation of Q, for Q represented as a Lie algebra. Then

(a) (Q, g) is normalized by Q, and

(b) $(\alpha - 1)Q$ is contained in (Q, g).

Proof.

(a) For $x, y \in Q$,

$$(xy, g) = y^{-1}x^{-1}x^g y^g = y^{-1}x^{-1}x^g y y^{-1} y^g = (x, g)^y (y, g),$$

so

$$(x, g)^y = (xy, g)(y, g)^{-1} \in (Q, g).$$

(b) Take $x \in Q$. Let $y = x^{-1}x^g$. Then $y \in (Q, g)$ and

$$\alpha(x) = g^{-1}xg = x^g = xx^{-1}x^g = xy.$$

By (a) and Theorem 4.3, (Q, g) is an ideal of the Lie algebra Q.

Hence, by (4.1), modulo this ideal we have

$$\alpha(x) \equiv xy \equiv x + y + \frac{1}{2}[x, y] + \ldots \equiv x,$$

and

$$(\alpha - 1)x \equiv \alpha(x) - x \equiv 0.$$

So $(\alpha - 1)x \in (Q, g)$.

$\square$

Theorem 4.5. *Assume Hypothesis 4.1. Suppose that Q has nilpotence class at most $p-1$ and that R is generated by a set S of elements g such that*

$$g^p \text{ centralizes } A, \text{ or } (A, g; p) = 1, \tag{4.2}$$

and

$$((u, g; i), (v, g; j)) = 1 \tag{4.3}$$

for every $u, v \in A$ and all positive integers i, j such that $i + j \geq p$.

Then $A \triangleleft R$.

Proof. Let $Q_0 = \{x \in Q \big| x^p = 1\}$. Since Q has nilpotence class at most $p-1$, Q is a *regular* p-group, whence Q_0 is a subgroup of Q ([Hall] or [S II, pp.46-7]). By Theorem 4.3, we can convert Q_0 into a Lie algebra over $\mathbb{F}_p$.

Take any $g \in S$, and let

$$Q_1 = \langle A^{g^i} \big| \ i \geq 0 \rangle \text{ and } R_1 = \langle A, g \rangle.$$

Then Q_1 is a subalgebra of Q_0. As in Lemma 4.4, let α be the automorphism of Q_1 given by conjugation by g. If g^p centralizes A, then

$$\alpha^p = 1 \text{ and } 0 = (\alpha^p - 1)A = (\alpha - 1)^p A.$$

Otherwise, by (4.2), Lemma 4.4 and an induction argument,

$$(\alpha - 1)^p A \leq (A, g; p) = 1.$$

Thus in both cases, $(\alpha - 1)^p A = 0$.

Let

$$Q_2 = A + (\alpha - 1)A + (\alpha - 1)^2 A + \cdots + (\alpha - 1)^{p-1} A.$$

Then Q_2 is invariant under $\alpha - 1$, hence under α and under conjugation by g. Since $A \leq Q_2 \leq Q_1$, we have $Q_2 = Q_1$. Therefore, $(\alpha - 1)^p = 0$. Now, from (4.3), we have

$$\big[(\alpha - 1)^i u, (\alpha - 1)^j v\big] = 0, \tag{4.4}$$

for all $u, v \in A$ and all positive integers i, j such that $i + j \geq p$. Recall the subgroups $Q(0), Q(1), \dots, Q(s)$ from Hypothesis 4.1. Now we use (4.4) to apply Theorem 2.8 with Q_1 and A in place of L and B_0, and with

$$L_i = Q(i) \cap Q_1, \quad \text{for } i = 0, 1, \dots, s.$$

By Hypothesis 4.1, A is maximal with respect to the partial ordering in the theorem. Therefore, A is invariant under α, that is, under conjugation by g. Since g is an arbitrary element of S,

$$A \lhd R,$$

as desired. □

Now we may obtain a special case of Theorem B.

Corollary 4.6. *Suppose A_0 is an abelian subgroup of order p^n in P, and P has exponent p and nilpotence class at most $p - 1$. Then there is a normal abelian subgroup A of P of order $|A_0|$ contained in $\langle A_0^P \rangle$.*

Proof. Let $Q = R = P$. Take A as in Proposition 4.2(b). Let $S = P$. Then Theorem 4.5 applies, and yields that $A \lhd P$. □

Proof of Theorem A

In Section 1, we reduced the theorem to the case where P has exponent p and order p^p, and hence has class at most $p - 1$. Now apply Corollary 4.6.

Example 4.7. ([Hup, p.349]; [GG 1, Example 4.1]; or [A, pp.11-2]).

Theorem A is false for n sufficiently large. The first author has given a family of examples, one for each prime p, in which

$$|P| = p^{2p^2+1}, \quad |A| = p^{2p^2-2p+2},$$

and A has exactly p distinct conjugates (including A) in P. Here, A is elementary abelian, and $|B| < |A|$ for every abelian subgroup P that is not conjugate to A.

5 Proof of Theorems

We have proved Theorem C in Section 3 and Theorem A in Section 4. Here, we prove the other results in our introduction.

Throughout this section, p denotes a prime and P denotes an arbitrary finite p-group. We retain the notation for commutators

$$(x, y) \qquad (y, x; i), \qquad (Q, x)$$

mentioned after Theorem 4.3. From Section 1, for subgroups Q and R,

$$(Q, R) \; = \; \langle (Q, x) \big| \; x \in R \rangle.$$

For every $n \geq 3$ and for $x_1, \ldots, x_n \in P$, we define the iterated commutator $(x_1, \ldots, x_n)$ as usual:

$$(x_1, x_2, \ldots, x_{i+1}) = ((x_1, x_2, \ldots, x_i), x_{i+1}) \text{ for } i = 2, 3, \ldots, n+1.$$

Lemma 5.1. *Let*

$$P = P(1) \geq P(2) \geq \cdots \geq P(s) = 1 = P(s+1) = \cdots$$

be the lower central series of P, i.e.,

$$P(i+1) = (P(i), P) \quad \textit{for } i = 1, 2, 3, \ldots$$

Then:

(a) For every $n \geq 2$ and every subset X of P that generates P,

$$P(n) = \langle (x_1, \ldots, x_n), P(n+1) \big| x_1, \ldots, x_n \in X \rangle.$$

(b) If $P = A_1 A_2 \ldots A_k$ for some abelian normal subgroups $A_1, A_2, \ldots, A_k$ of P, then P has nilpotence class at most k.

Proof.

(a) [Hup, p.258].

(b) This is a special case of a result of Fitting (from [Hup, p.276] and induction).

□

We will apply Lemma 5.1(b) to a product of p normal abelian subgroups, but we wish to obtain nilpotence class at most $p-1$. Therefore, we will need the following result.

Lemma 5.2. *Suppose $p \geq 3$. A is an abelian subgroup of P, and $g \in P$. Assume that*

$$P = \langle A, g \rangle; \qquad A \triangleleft \langle A^P \rangle;$$

$$g^p \textit{ normalizes } A \textit{ or } (A, g; p) = 1;$$

and

$$((A, g; i), (A, g; j)) = 1 \textit{ whenever } i, j \geq 1 \textit{ and } i + j \geq p,$$

Then $\langle A^P \rangle$ has nilpotence class at most $p-1$.

Proof. Let $Q = \langle A^P \rangle$ and $Q' = (Q, Q)$. Then

(5.1)
$$(A, \langle g \rangle) \triangleleft \langle A, \langle g \rangle \rangle = P, \quad Q = A(A, \langle g \rangle) \text{ and } Q' \leq (A, \langle g \rangle).$$

Let $R = \langle (A, g; i) \big| \ i \geq 1 \rangle$. The identities

$$x^y = x(x, y) \quad \text{and} \quad (x, y^{i+1}) = (x, y)(x, y^i)^y$$

show that $R^g \leq R$ and, by induction, $(A, g^i) \leq R$. Therefore, $R^g = R$ and $(A, \langle g \rangle) \leq R$. By (5.1) and the hypothesis,

$$Q' \text{ centralizes } (A, g; p-1). \tag{5.2}$$

A similar argument shows that, for each $i \geq 0$,

$$\langle A, A^g, \ldots, A^{g^i} \rangle = \langle A, (A, g), \ldots, (A, g; i) \rangle.$$

Taking $i = p-2$ and $i = p-1$, we obtain

$$Q = \langle A, A^g, \ldots, A^{g^{p-1}} \rangle = \langle A, A^g, \ldots, A^{g^{p-2}}, (A, g; p-1) \rangle \tag{5.3}$$

To obtain the conclusion, we must show that $Q(p) = 1$.

By hypothesis, $Q = AA^gA^{g^2} \ldots A^{g^{p-1}}$. Let X be the set-theoretic union of $A, A^g, A^{g^2}, \ldots, A^{g^{p-1}}$. We will apply Lemma 5.1(b). Take

$$x_1, \ldots, x_p \in X, \quad y = (x_1, x_2, \ldots, x_{p-1}) \quad \text{and } z = (x_1, \ldots, x_p) = (y, x_p).$$

We will assume that $z \neq 1$ and obtain a contradiction.

Now $x_p \in A^{g^r}$ for some integer r. Replacing x_i by $x_i^{g^{p-1-r}}$ for each i, we may assume that $x_p \in A^{g^{p-1}}$. Then

$$\text{for } i = 1, 2, \ldots, p-1, \ x_i \text{ lies in } A \text{ or } A^g \text{ or} \cdots \text{or } A^{g^{p-2}},$$

since otherwise, x_i and y lie in $A^{g^{p-1}}$ and $z = (y, x_p) = 1$. Similarly, for $1 \leq i < j \leq p-1$, x_i and x_j cannot lie in the same subgroup A^{g^k}, $0 \leq k \leq p-2$. Therefore, $y \in A \cap A^g \cap \cdots \cap A^{g^{p-2}}$. Since $p \geq 3$, $y \in Q'$. Therefore, y centralizes $A, A^g, \ldots, A^{g^{p-2}}$ and $(A, g; p-1)$, by (5.2) So $y \in Z(Q)$ by (5.3) and $z = 1$, a contradiction.

□

It is convenient to introduce the following condition on a pair (Q, A) for a p-group Q and a subgroup A.

Hypothesis 5.3. *The triple (Q, Q, A) satisfies Hypothesis 4.1*

Now we come to our main results. We first prove an analogue of [GG 2, Theorem 2(a)].

Theorem 5.4. *Suppose A and B are elementary abelian subgroups of P, and the pairs (P, A) and (P, B) satisfy Hypothesis 5.3 (possibly for different central series of P). Assume either that $p = 3$ and P has nilpotence class at most 4 or that $p \geq 5$.*

Then A and B normalize each other.

Proof. We use induction on $|P|$. We may assume that

$$A, B < P.$$

Let M be a maximal subgroup of P that contains A, and let

$$Q = \langle A^P \rangle.$$

Then $Q \triangleleft P$. Since P is nilpotent, $M \triangleleft P$ and $Q \leq \langle M^P \rangle = M$. Observe that, for each $g \in P$, Hypothesis 5.3 is satisfied by the pair (P, A^g) and then by the pair (M, A^g). Therefore, by induction,

(5.4) $\qquad A^g$ and A^h normalize each other for every $g, h \in P$

Hence $A \triangleleft Q$, and

$$(P,A) \leq (P,Q) \leq Q, \quad (P,A;2) \leq (Q,A) \leq A, \quad (P,A;3) = 1.$$

By the symmetry of A and B,

$$(P,B;3) = 1. \tag{5.5}$$

Now take any $u \in B$. Let

$$R = \langle A, u \rangle \quad \text{and} \quad Q_0 = \langle A^R \rangle.$$

We claim that the hypothesis of Theorem 4.5 is satisfied with Q_0 in place of Q and with S equal to the set-theoretic union of A with $\{u\}$.

First of all, it is easy to see that the triple (Q_0, R, A) satisfies Hypothesis 4.1. If $p = 3$, then P has nilpotence class at most 4, whence

$$((v,g;i),(w,g;j)) = 1 \text{ for all } g \in S,\ v,w \in A, \tag{5.6}$$

$$\text{and all } i,j \text{ such that } i,j \geq 1 \text{ and } i+j \geq p.$$

If $p > 3$, we obtain (5.6) from (5.5). Therefore, (5.6) holds for all p, and Lemma 5.2 yields that Q_0 has nilpotence class at most $p-1$, We have now verified the hypothesis of Theorem 4.5; the conclusion says that $A \triangleleft R$. Since u is arbitrary in B,

$$B \text{ normalizes } A.$$

By symmetry, A normalizes B. □

Theorem 5.5. *Suppose A is an elementary abelian subgroup of P and the pair (P,A) satisfies Hypothesis 5.3. Assume that $p \geq 5$ or that $p = 3$ and P has nilpotence class at most 4. Then*

(a) $A \triangleleft \langle A^P \rangle$, *and*

(b) $(P,A;3) = 1$.

Proof. (Just repeat part of the proof of Theorem 5.4.)

□

Now we may remove the restriction on the nilpotence class of Q in Theorem 4.5 if $p \geq 5$.

Theorem 5.6. *Suppose A is an elementary abelian subgroup of P, the pair (P, A) satisfies Hypothesis 5.3, and $p \geq 5$ or P has exponent p.*

Then A is normalized by every element g of P such that

$$g^p \text{ centralizes } A, \qquad \text{or} \qquad (A, g; p) = 1, \tag{5.7}$$

and

$$((u, g; i), (v, g; j)) = 1, \tag{5.8}$$

for every $u, v \in A$ and all positive integers i, j such that $i + j \geq p$.

Proof. If $p = 2$, then P is abelian. So we may assume that $p \geq 3$.

Now take $g \in P$ as in the hypothesis and let

$$R = \langle A, g\rangle \quad \text{and} \quad Q = \langle A^R\rangle.$$

Let S be the set-theoretic union of A with $\{g\}$. If $p = 3$, then P has nilpotence class at most 3, by [Hall, (18.2.10), p.322]. Therefore, by Theorem 5.4, $A \triangleleft Q$ for all p. Then, by Lemma 5.2, Q has nilpotence class at most $p - 1$. Now $A \triangleleft R$ by Theorem 4.5. In particular, g normalizes A. □

Proposition 5.7. *Suppose A_0 is an elementary abelian subgroup of P. Then there exists an elementary abelian subgroup A of $\langle A_0^P\rangle$ such that $|A| = |A_0|$ and the pair (P, A) satisfies Hypothesis 5.3.*

Proof. Take A as in Corollary 4.6, i.e. as in Proposition 4.2(b) with $Q = R = S = P$.

□

Proof of Theorem D:

Here, $p \geq 5$. Apply Proposition 5.7 to obtain B, and then Theorems 5.5 and 5.6.

Theorem 5.8. *Suppose*

(a) P has nilpotence class at most p.

or

(b) P has exponent p and nilpotence class at most $p + 1$,

or

(c) $p \leq 3$ and P has exponent p.

Let A be an elementary abelian subgroup of P.

Then there exists an elementary abelian subgroup B of $\langle A^P \rangle$ such that $|B| = |A|$ and $B \lhd P$.

Remark. *Consider case (c). From the proof of Theorem 5.6, P has class at most p. Therefore, this is a special case of (b). In addition, P is metabelian, so that the conclusion follows from a result of Gillam [JG].*

Proof. As mentioned above, (c) is a special case of (b). Now just follow the proof of Corollary 4.6, using Theorem 5.6 in place of Theorem 4.5, with slight changes. $\square$

Corollary 5.9. *Let n be a positive integer. Suppose $p > n$, $|P| = p^n$, and A is an elementary abelian subgroup of P.*

Then there exists an elementary abelian subgroup of $\langle A^P \rangle$ such that $|B| = |A|$ and $B \lhd P$.

Proof of Theorem B:

This is a special case of Theorem 5.8.

The second author shows in [GG 2] that Theorem 5.8(c) does not extend to groups of exponent p for $p > 3$.

Theorem D does not apply when $p < 5$. The following example shows that it cannot be extended to the case in which $p = 2$. The case in which $p = 3$ is open.

Example 5.10. Suppose $p = 2$ and P is a dihedral group of order 32. Take $x, y \in P$ such that

$$x^2 = y^{16} = 1, \quad x^{-1}yx = y^{-1}, \quad \text{and} \quad \langle x, y \rangle = P.$$

Let $A = \langle x, y^8 \rangle$. Then $|A| = 4$.

Now A is not normal in P. Moreover,

$$A^y = \langle y^{-1}xy, y^8 \rangle = \langle xy^2, y^8 \rangle \text{ and } A^{xy^2} = \langle y^{-2}xy^2, y^8 \rangle = \langle xy^4, y^8 \rangle \neq A.$$

Thus A is not normalized by A^y. Similarly, for $B = \langle xy, y^8 \rangle$, B is not normalized by B^y. However, every elementary abelian group of order 4 in P is conjugate to A or B. Thus, *P has no elementary abelian subgroup E of order 4 that is normalized by P, or even by all of its conjugates in P.*

Example 5.11. For P of exponent 3, P must have nilpotence class at most 3, by [Hall, (18.2.10), p.322]. Let $P' = (P, P)$. Then P' is abelian and

$$1 \leq Z(P) \cap P' \leq P' \leq P \tag{5.9}$$

is a central series of P. For any elementary abelian subgroup A of maximal order in P,

$$Z(P) \cap P' \leq Z(P) \leq A.$$

Therefore, if we choose A such that $|A \cap P'|$ is as large as possible, then (Q, A) satisfies Hypothesis 5.3, with (5.9) being the central series in condition (4.1)(b).

One might guess that $A \geq P'$, since P' is abelian. But it is easy to construct a counterexample. Let F be the freeest group of exponent 3 on four generators x_1, x_2, x_3, x_4. This is the group denoted by $B(3, 4)$ in [Hall, p.320]. Let R be the smallest normal subgroup of F containing (x_1, x_2). Let

$$\overline{F} = F/R, \quad \overline{x_i} = x_i R, \text{ for each } i.$$

The analysis of F in [Hall, pp.320-324] (particularly (18.2.9)) shows that

$$|F| = 3^{14}, R = \langle (x_1, x_2), ((x_1, x_2), x_i) \big| \; i = 3, 4 \rangle, \; |R| = 3^3;$$

$$(\overline{F}, \overline{F}) = ((\overline{F}, \overline{F}) \cap C_{\overline{F}}(\langle \overline{x_1}, \overline{x_2} \rangle)) \times \langle (\overline{x_3}, \overline{x_4}) \rangle :$$

and

$$\langle \overline{x_1}, \overline{x_2} \rangle \times C_{(\overline{F}, \overline{F})}(\langle \overline{x_1}, \overline{x_2} \rangle)$$

has maximal order, which is 3^8, while

$$C_{\overline{F}}((\overline{F}, \overline{F})) = (\overline{F}, \overline{F}),$$

which has order 3^7.

References

[A] J. Alperin, *"Large abelian subgroups of p-groups,"* Trans. A.M.S. **117** (1965), 10-20.

[B] N. Bourbaki, Algebra, Chaps. 4-7, Springer (1989), Berlin.

[JG] J.D. Gillam, *A note on finite metabelian p-groups*, Proc. A.M.S. **25** (1970), 189-190.

[GG 1] G. Glauberman, *"Large abelian subgroups of finite p-groups,"* J. Algebra, to appear.

[GG 2] G. Glauberman, *"Large abelian subgroups of groups of prime exponent,"* in preparation.

[Greg] T. B. Gregory, *"Winter Map Invariants,"* preprint.

[Hall] M. Hall, The Theory of Groups, Macmillan (1959), New York.

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

[J] N. Jacobson, Lie Algebras, Wiley (1962), New York.

[KJ] M. Konvisser and D. Jonah, *"Counting abelian subgroups of p-groups, a projective approach."* J. Algebra **34** (1975), 309-30.

[Kos] B. Kostant, *"Eigenvalues of a Laplacian and Commutative Lie subalgebras,"* Topology **3, Suppl. 2** (1965), 147-59.

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

[S I] M. Suzuki, Group Theory I, Springer-Verlag, (1982), Berlin.

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