PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 126, Number 9, September 1998, Pages 2525–2533
S 0002-9939(98)04496-7

THE MAXIMAL NORMAL p–SUBGROUP OF THE AUTOMORPHISM GROUP OF AN ABELIAN p–GROUP

JUTTA HAUSEN AND PHILLIP SCHULTZ

(Communicated by Ronald M. Solomon)

Abstract. Let p be a prime number and let G be an abelian p–group. Let Δ be the maximal normal p–subgroup of $\operatorname{Aut} G$ and ζ the maximal p–subgroup of its centre. Let $\mathbf{t}$ be the torsion radical of $\mathcal{E}(G)$. Then $\Delta = (1+\mathbf{t})\zeta$. The result is new for $p = 2$ and 3, and the proof is new and valid for all primes p.

§1. Introduction

Throughout, p is an arbitrary but fixed prime and G is an abelian p–group. We let $\mathcal{E} = \mathcal{E}(G)$ denote the endomorphism ring of G, $\operatorname{Aut} G$ its automorphism group, and $\Delta = O_p(\operatorname{Aut} G)$ the maximal normal p–subgroup of $\operatorname{Aut} G$. The importance of Δ in determining the structure of $\operatorname{Aut} G$, characterising the action of $\operatorname{Aut} G$ on G and recovering invariants of G from $\operatorname{Aut} G$ has long been recognized; see for example [3, Section 114], [6] and [1].

For $p \geq 5$, Δ considered as a group of units of $\mathcal{E}$ has been determined in a series of papers starting with Shoda [17] for finite groups, Freedman [2] for countable reduced groups, Hill [9] for totally projective groups and Hausen [5] for arbitrary p–groups: if $\mathbf{t}$ denotes the torsion radical of $\mathcal{E}$ (i.e. $\mathbf{t}$ is the ideal consisting of all elements of finite order in the Jacobson radical of $\mathcal{E}$), then $\Delta = 1 + \mathbf{t}$.

Crucial for the proof is the following result, first stated in [5]. It was inspired by Freedman [2], stated by Leptin for $k = 1$ [11] and, in fact, is easily proven by induction on k following Leptin's arguments [11, p.101]. The Pierce radical of $\mathcal{E}$ is defined to be

$$\mathbf{P} = \{\varepsilon \in \mathcal{E} : p^n G[p]\varepsilon \leq p^{n+1} G \text{ for all integers } n \geq 0\}.$$

Clearly, $\mathbf{P}$ is a two–sided ideal in $\mathcal{E}$ containing the Jacobson radical of $\mathcal{E}$ [13, p. 289]. Let $1 + \mathbf{P}$ denote the coset containing 1 in the quotient ring $\mathcal{E}/\mathbf{P}$.

The Freedman–Leptin Lemma. *Let $p \geq 5$, let G be a reduced abelian p–group, and let $\alpha = 1 + \eta \in \operatorname{Aut} G \cap (1 + \mathbf{P})$. Then, for any natural number k, $\alpha^{p^k} = 1$ if and only if $p^k \eta = 0$.*

For $p \geq 5$, the description of Δ proceeds as follows: the ideal $\mathbf{t}$ is contained in the Jacobson radical of $\mathcal{E}$; since $\mathbf{t}$ consists of all elements in $\mathbf{P}$ of finite order, it follows that $1 + \mathbf{t}$ is a normal p–subgroup of $\operatorname{Aut} G$ and thus is contained in Δ [3, Theorem 114.4]. Conversely, Δ induces the identity mapping in all Ulm factors

---

Received by the editors January 28, 1997.
1991 *Mathematics Subject Classification.* Primary 20K10, 20F28, 20K30.

$p^nG[p]/p^{n+1}G[p]$ where n is a non-negative integer [2], so that $\Delta \leq 1 + \mathbf{P}$, and the Freedman–Leptin Lemma proves $\Delta = 1 + \mathbf{t}$.

Two new phenomena make this approach impossible for the two smallest primes. First, the maximal p–subgroup of the center $\zeta \operatorname{Aut} G$ of $\operatorname{Aut} G$ is contained in Δ. While $[\zeta \operatorname{Aut} G]_p = 1$ if p is odd, $[\zeta \operatorname{Aut} G]_2 = \langle -1 \rangle$ if $p = 2$. But if G is an unbounded 2–group, multiplication by -2 is an endomorphism in P of infinite order, so -1 is not in $1 + \mathbf{t}$.

Second, while for primes $p \geq 5$ the *set* of all automorphisms in $1 + \mathbf{P}$ of finite order forms a *group*, in fact a p–group which must be normal in $\operatorname{Aut} G$ and hence equals $1 + \mathbf{t}$, we shall show by examples that this need not be the case when $p = 2$ or $p = 3$. For these primes, there exist p–groups G having an automorphism α of order p for which $\alpha - 1 \in \mathbf{P}$ has infinite additive order. This answers in the negative a problem posed by Leptin [11, p. 102]. Moreover, for $p = 2$, our example will be such that $\alpha \notin (1 + \mathbf{t}) \langle -1 \rangle$.

Nevertheless, we are able to prove the following theorem, which is valid for all primes:

Theorem. *Let p be a prime, let G be an abelian p–group, and let Δ be the maximal normal p–subgroup of the automorphism group of G. Then $\Delta = (1+\mathbf{t})\zeta$, where ζ denotes the maximal p–subgroup of the centre of* $\operatorname{Aut} G$. *Thus, $\Delta = 1 + \mathbf{t}$ if $p \geq 3$ or G is bounded, and $\Delta = (1 + \mathbf{t}) \times \langle -1 \rangle$ if G is an unbounded 2–group.*

It is interesting to note that if G has an unbounded basic subgroup, then as an abstract ring, $\mathbf{t}$ determines G up to isomorphism; furthermore, every automorphism of $\mathbf{t}$ is induced by an automorphism of G [8]. One may well conjecture that the same is true of Δ. If true, this would be a far–reaching extension of the results of Leptin [10] and Liebert [12].

The strategy of the proof may be outlined as follows: it is easy to show that $1 + \mathbf{t} \leq \Delta$ (2.6). Of course, $\langle -1 \rangle \leq \Delta$ when $p = 2$. For the reverse inclusion, we first show that $\Delta \subseteq 1 + P$ and assume the existence of some $\alpha \in \Delta$ such that $\alpha - 1$ (and, for $p = 2$, $-\alpha - 1$, too) has infinite order. We then use an elaborate construction to produce mixed commutators of the form $[\gamma, \alpha]$ (and $[\beta, -\alpha]$ if $p = 2$) which have infinite order. Since they would have to belong to Δ, this is a contradiction.

Any unexplained notation can be found in the standard references [3] for abelian groups and [15] for general group theory. In particular, $[x, y] = x^{-1}y^{-1}xy$.

§2. Preliminaries

We begin with the promised examples which show that for $p = 2$ and $p = 3$ no substitute for the Freedman–Leptin Lemma can be hoped for. The examples also illustrate a simple case of the strategy outlined above.

Examples 2.1. For each prime $p \in \{2, 3\}$, there exist an abelian p–group G and an automorphism $\alpha = 1 + \eta \in 1 + \mathbf{P}$ such that $\alpha^p = 1$ but η has infinite additive order. When $p = 2$, $\eta + 2$ also has infinite order. In addition, there exists $\beta \in \operatorname{Aut} G$ such that $[\beta, \alpha]$ has infinite multiplicative order.

Proof. If $p = 2$, let $G = \bigoplus_{i \in \mathbb{N}} (\langle a_i \rangle \oplus \langle b_i \rangle)$, where a_i has order 2^{i+1} and b_i has order 2^i. For each i, define $a_i\eta = b_i$ and $b_i\eta = -2b_i$. Then $\eta \in \mathbf{P}$, $2^k\eta \neq 0$ and $2^k(\eta + 2) \neq 0$ for all positive integers k. Furthermore, $\eta^2 + 2\eta = 0$.

If $p = 3$, let $G = \bigoplus_{i\in\mathbf{N}}(\langle a_i\rangle \oplus \langle b_i\rangle \oplus \langle c_i\rangle)$, where a_i, b_i and c_i have orders 3^{3i}, 3^{3i-1} and 3^{3i-2}, respectively. For each i, define $a_i\eta = b_i$, $b_i\eta = c_i$, and $c_i\eta = -3c_i - 3b_i$. Then $\eta \in \mathbf{P}$, $3^k\eta \neq 0$ for all k, and $\eta^3 + 3\eta^2 + 3\eta = 0$.

In either case, let $\alpha = 1 + \eta$. Then $\alpha^p = 1$, so $\alpha \in \mathrm{Aut}G \cap (1 + \mathbf{P})$, and $\alpha \notin (1 + \mathbf{t})\zeta$.

We construct the automorphism β only for the case $p = 2$, the case $p = 3$ being similar. For each $i \geq 1$, define

$$a_i\varepsilon = 0 \text{ and } b_i\varepsilon = \begin{cases} a_{i-1} & \text{if } i \text{ is even,} \\ 0 & \text{if } i \text{ is odd.} \end{cases}$$

Then $\varepsilon^2 = 0$, so $\beta = 1 + \varepsilon \in \mathrm{Aut}\,G$ with inverse $1 - \varepsilon$. Since $\alpha^{-1} = \alpha$ and $\varepsilon\eta\varepsilon = 0$, a routine calculation shows that $[\beta, \alpha] = 1 + \psi$, where $\psi = \eta\varepsilon + \varepsilon\eta + \eta\varepsilon\eta$. But $\psi^2 = 0$, while ψ has infinite additive order. Hence $[\beta, \alpha]^k = 1 + k\psi$ for all $k \in \mathbb{N}$, so $[\beta, \alpha]$ has infinite multiplicative order. □

We shall need some results of elementary number theory. The first one is well known.

Lemma 2.2. *Let r, n and k be positive integers such that n is not divisible by p and $p^r n \leq p^k$. Then*

(1) *The maximal p–power dividing $\binom{p^k}{p^r n}$ is p^{k-r}.*

(2) *If*

$$M = M(p, k, r, n) = \sum_{j=1}^{p^k} \binom{p^k}{j} (p^r\, n)^j \ ,$$

then p^{k+r} divides M, and if p^{k+r+1} divides M, then $p = 2$ and $r = 1$.

Proof. The first assertion is easily proved in the spirit of [15, p. 39]. In order to verify the second, let j be an integer such that $1 \leq j \leq p^k$, and let $x_j = \binom{p^k}{j} p^{rj} n^j$. By (1), x_j is divisible by p^{k+rj} if $(j, p) = 1$. Suppose $j = p^t m$, with t and m positive integers and m relatively prime to p. By (1), p^{k-t+rj} divides x_j, and $k - t + rp^t m = k + r + r(p^t m - 1) - t \geq k + r$ since $r(p^t m - 1) \geq 2^t - 1 \geq t$. Thus, each x_j is divisible by p^{k+r}. Suppose that p^{k+r+1} divides M. Since p^{k+r+1} does not divide x_1, there must exist $j \geq 2$ such that p^{k+r+1} does not divide x_j, and j cannot be relatively prime to p. Thus, $j = p^t m$ with t and m as above, and $k - t + rj = k + r$. It follows that

$$t = r(j-1) = r(p^t m - 1) \geq r(2^t - 1) \geq 2^t - 1 \,.$$

Since $t \geq 1$, this implies $t = 1 = r$ and $p = 2$. □

The maximal normal p–subgroups of the automorphism groups of elementary and of divisible groups are known:

Lemma 2.3 ([2], [5]). *Let A be an elementary abelian and D a divisible p–group. Then $O_p(\mathrm{Aut}A) = 1$, and $O_p(\mathrm{Aut}D) = 1$ unless $p = 2$, in which case $O_2(\mathrm{Aut}D) = \langle -1 \rangle$.*

Proof. The first assertion is Lemma 4.8 of [2]. Let D be divisible. By Theorem 6.5 of [5], every normal torsion subgroup of $\mathrm{Aut}D$ is contained in the centre, which consists of the multiplications by p–adic units [3, 115.1]. It is well known that the

p–component of the group of p–adic units is trivial except when $p = 2$, in which case it is cyclic of order two generated by -1 [16, II.3.8]. □

Corollary 2.4. *Let $G = H \oplus D$, where H is reduced and D is divisible. Let $\delta \in \Delta$. Then $\delta - 1 \in \mathbf{P}$, and $D(\delta - 1) = 0$ unless $p = 2$, in which case $\delta|_D \in \langle -1 \rangle$.*

Proof. Let n be a nonnegative integer. Every automorphism of $p^nG[p]/p^{n+1}G[p]$ is induced by an automorphism of G [3, 114.1]; clearly, every automorphism of D is induced by an automorphism of G. Thus, the result follows from Lemma 2.3. □

From now on we shall assume that $G = H \oplus D$, where H is reduced and D is divisible.

The following subset of $\mathbf{P}$ will play an important rôle. It contains $\mathbf{t}$, and equals $\mathbf{t}$ if G is reduced. Let

$$\Phi = \{\, \varepsilon \in \mathbf{P} \,|\, p^m G\varepsilon \le D \text{ for some } m \in \mathbb{N} \text{ and } D\varepsilon = 0 \,\}.$$

Lemma 2.5. *Let $\varepsilon \in \Phi$ and let m be a natural number such that $p^mG\varepsilon \le D$. Then $\varepsilon^{2m+3} = 0$, and $(1+\varepsilon)^{p^n} = 1 + p^n\varepsilon$ for all integers $n \ge 3m+2$.*

Proof. The hypotheses imply $G\varepsilon \le G[p^m] + D$. Let $\overline{G} = G/D$ and let $\overline{\varepsilon}$ be the endomorphism of $\overline{G}$ induced by ε. Then $p^m\overline{\varepsilon} = 0$, so that

$$\overline{G}\overline{\varepsilon} \le \overline{G}[p^m] \le \overline{G}[p^{m+1}] = (G[p^{m+1}] + D)/D.$$

The restriction of $\overline{\varepsilon}$ to $\overline{G}[p^{m+1}]$ is in $\mathbf{P}(\overline{G}[p^{m+1}])$, which equals the Jacobson radical of $\mathcal{E}(\overline{G}[p^{m+1}])$ since $\overline{G}[p^{m+1}]$ is bounded [7]. By [14], $\mathbf{J}\mathcal{E}(\overline{G}[p^{m+1}])$ is nilpotent of class at most $2m+1$. Thus, $(\overline{\varepsilon}\,|_{\overline{G}[p^{m+1}]})^{2m+1} = 0$, which implies $G[p^{m+1}]\varepsilon^{2m+1} \le D$. Hence,

$$G\varepsilon^{2m+3} \le (G[p^m] + D)\varepsilon^{2m+2} \le D\varepsilon = 0.$$

Let n be an integer such that $n \ge 3m+2$. Then

$$(1+\varepsilon)^{p^n} = 1 + p^n\varepsilon + \sum_{j=2}^{p^n} \binom{p^n}{j} \varepsilon^j = 1 + p^n\varepsilon + \sum_{j=2}^{2m+2} \binom{p^n}{j} \varepsilon^j.$$

Fix $2 \le j \le 2m+2$. By hypothesis, $p^m\varepsilon^2 = 0$. Let $j = p^r \cdot q$ for some integers r and q with p and q relatively prime. By Lemma 2.2, $\binom{p^n}{j}\varepsilon^j = p^{n-r}\ell\varepsilon^j$ for some integer ℓ not divisible by p. Suppose $n - r < m$. Then $r > n - m \ge 3m+2-m = 2m+2$, which implies

$$j = p^r q \ge 2^r > r > 2m+2.$$

Thus, $\binom{p^n}{j}\varepsilon^j = 0$. □

While our Examples 2.1 demonstrate that the *only if* part of the Freedman-Leptin Lemma is lost in the general case, we do have the following weak version of the *if* part.

Proposition 2.6. *Let $\varepsilon \in \Phi$. The following conditions are equivalent:*

(1) $(1+\varepsilon)^{p^k} = 1$ *for some positive integer k.*
(2) $\varepsilon \in \mathbf{t}$.

(3) $1+\varepsilon \in \Delta$.

In particular, $1+\mathbf{t} \leq \Delta$.

Proof. Let $\varepsilon \in \Phi$ and let $m \in \mathbb{N}$ be such that $p^m G\varepsilon \leq D$. By 2.5, $(1+\varepsilon)^{p^n} = 1+p^n\varepsilon$ for all integers $n \geq 3m+2$. Assume (1), and choose $n \geq \max(k, 3m+2)$. Then $1 = 1+p^n\varepsilon$, which implies (2). Conversely, assume (2). Then $p^\ell\varepsilon = 0$ for some natural number ℓ . Choose $n \geq \max(\ell, 3m+2)$. Then $(1+\varepsilon)^{p^n} = 1$. Thus, (1) and (2) are equivalent. Since $\mathbf{t}$ is an ideal of $\mathcal{E}$ contained in the Jacobson radical of $\mathcal{E}$, it follows that $1+\mathbf{t}$ is a normal p–subgroup of $\operatorname{Aut} G$. Hence, $1+\mathbf{t} \leq \Delta$, and (2) implies (3). Trivially, (3) implies (1). ☐

Corollary 2.7. *For every prime p and every p–group G ,* $(1+\mathbf{t})\zeta \leq \Delta$.

§3. The reduced case

The following result will be crucial for the proof of our theorem. It shows that the construction of Examples 2.1 can be extended to deal with arbitrary p–groups.

Proposition 3.1. *Let G be a reduced abelian p–group and let $\alpha = 1+\eta \in \Delta$. Then $\eta \in \mathbf{t}$, or $p=2$ and $2+\eta \in \mathbf{t}$.*

The proof will be by contradiction using an elaborate construction. Throughout, we shall assume the following

Situation and Notations: The p–group G is reduced, $\alpha = 1+\eta$ is an element of Δ , and $k \in \mathbb{N}$ is a fixed integer such that $\alpha^{p^k} = 1$. Then

$$\sum_{j=1}^{p^k} \binom{p^k}{j} \eta^j = 0 \ . \tag{3.2}$$

We let $\sigma = \alpha^{-1} - 1$. By Corollary 2.4

$$\eta\,, \sigma \in \mathbf{P} \tag{3.3}$$

and

$$\eta + \sigma + \eta\sigma = 0\,, \quad \eta\sigma = \sigma\eta\,. \tag{3.4}$$

Also, we let $\alpha' = -\alpha$ and put $\eta' = \alpha' - 1$, and $\sigma' = (\alpha')^{-1} - 1$. Then

$$\eta' = -(2+\eta)\ , \quad \sigma' = -(2+\sigma)\,. \tag{3.5}$$

The primed elements will come into play only when $p=2$. Since the entire construction would have to be repeated, we consider them in any case.

We also fix a basic subgroup B of G and a canonical set S of (nonzero) independent generators. Thus $B = \bigoplus_{s\in S}\langle s\rangle = \bigoplus_{i\in\mathbb{N}} B_i$, where B_i is generated by the elements in S of order p^i . For each $n \in \mathbb{N}$, put $B^{(n)} = \bigoplus_{i=1}^n B_i$ and $G_n = p^nG + \bigoplus_{i\geq n+1} B_i$. Then, for each n , $G = B^{(n)} \oplus G_n$ [13, p. 280]. Choose a family $\{\pi_s\}_{s\in S}$ of canonical projections such that $t\pi_s = \delta_{st}s$, $t \in S$, and $G_n\pi_s = 0$ if $s \in B^{(n)}$. Define $G_0 = G$.

It will be convenient to write $e(x) = n$ if $x \in G$ and $o(x) = p^n$.

Lemma 3.6. *Assume the situation and notations above and, furthermore, assume that both η and η' have infinite order. Then there exist natural numbers u_i', u_i, v_i and elements a_i', a_i, b_i in G belonging to the canonical set of generators of B such that, for each $i \in \mathbb{N}$, the following hold:*

(1) $e(a_i') = u_i'$, $\quad e(a_i) = u_i$, $\quad e(b_i) = v_i$,

(2) *$e(a'_i\eta') \le u'_i < 3u'_i < e(a_i\eta) \le u_i < 3u_i < v_i$,*
(3) *$v_{i-1} < e(a'_i\eta')$ (put $v_0 = 0$),*
(4) *if $\pi_i : G \to \langle b_i\rangle$ denotes the canonical projection to $\langle b_i\rangle$ and r_i, m_i, r'_i, m'_i are integers such that $b_i\sigma\pi_i = p^{r_i}m_ib_i$, $b_i\sigma'\pi_i = p^{r'_i}m'_ib_i$, and m_i, m'_i are not divisible by p , then $r_i \notin [u_i - 2u_{i-1} - k , u_i - 2u_{i-1} - 1]$ and $r'_i \notin [u'_i - 2u'_{i-1} - k , u'_i - 2u'_{i-1} - 1]$ (put $u_0 = u'_0 = 0$).*

Proof. We claim that, for each natural number n , there exist u'_i, u_i, v_i and canonical generators a'_i, a_i, b_i of B , $i = 1, \ldots, n$, satisfying (1) through (4). The proof is by induction on n . Since the proof for $n = 1$ is almost identical to the inductive step from n to $n+1$, it is left to the reader. Assume the claim holds for n . Since $p^{v_n}G\eta' \neq 0$, there exists i such that $p^{v_n}B_i\eta' \neq 0$, and there is a canonical generator x of B_i with $v_n < e(x\eta')$. Now $p^{3i+k}G\eta' \neq 0$; thus there exist j and a canonical generator y of B_j such that $3i + k < e(y\eta')$. Proceeding this way, there exist ℓ and m and canonical generators z and w of B_ℓ and B_m , respectively, such that

$$\begin{aligned} v_n < e(x\eta') \le e(x) = i < 3i + k < e(y\eta') \le e(y) = j \\ < 3j < e(z\eta) < 3\ell + k < e(w\eta) \le e(w) = m\,. \end{aligned}$$

Since $p^{3m}G \neq 0$, it is possible to choose $v_{n+1} > 3m$ such that $B_{v_{n+1}} \neq 0$. Let b_{n+1} be a canonical generator of $B_{v_{n+1}}$. Then $e(b_{n+1}) = v_{n+1}$. Let π_{n+1} denote the canonical projection from G onto $\langle b_{n+1}\rangle$. Let $r'_{n+1} , r_{n+1} , m'_{n+1} , m_{n+1}$ be integers such that

$$b_{n+1}\sigma'\pi_{n+1} = p^{r'_{n+1}}m'_{n+1}b_{n+1} \quad \text{and} \quad b_{n+1}\sigma\pi_{n+1} = p^{r_{n+1}}m_{n+1}b_{n+1},$$

where m'_{n+1} , m_{n+1} are not divisible by p . If $r'_{n+1} \notin [i - 2u'_n - k , i - 2u'_n - 1]$, let $a'_{n+1} = x$. By construction, if $r'_{n+1} \in [i - 2u'_n - k , i - 2u'_n - 1]$, then $r'_{n+1} \notin [j - 2u'_n - k, j - 2u'_n - 1]$. In this case, let $a'_{n+1} = y$. Similarly, r_{n+1} cannot belong to both the intervals $[\ell - 2u_n - k , \ell - 2u_n - 1]$ and $[m - 2u_n - k , m - 2u_n - 1]$. Choose a_{n+1} to be either z or w depending on which is the case. One verifies that the augmented sets of integers and elements in G satisfy the requirements of the lemma. ☐

We shall define two endomorphisms ε and ε' as follows: for each i , define $b_i\varepsilon_i = a_i$ and let $\varepsilon_i = \pi_i\varepsilon_i$. Since $G_{v_i}\pi_i = 0$, each ε_i is an endomorphism of G . Let $\varepsilon = \sum_{i\in\mathbb{N}} p^{u_{i-1}}\varepsilon_i$. By [13, 6.3], $\varepsilon \in \mathcal{E}$. Similarly, define $b_i\varepsilon'_i = a'_i$, $\varepsilon'_i = \pi_i\varepsilon'_i$, and let $\varepsilon' = \sum_{i\in\mathbb{N}} p^{u'_{i-1}}\varepsilon'_i \in \mathcal{E}$.

Lemma 3.7. *Assume the hypotheses of 3.6. Then, for every integer $i \ge 0$, $G_{v_i}[p^{u_{i+1}}]\varepsilon = 0 = G_{v_i}[p^{u_{i+1}}]\varepsilon'$* (Reminder: $v_0 = 0$ and $G_0 = G$).

Proof. Let $i \ge 0$ be an integer and let $x \in G_{v_i}[p^{u_{i+1}}]$. Then $x\pi_j = 0$ for $j \le i$. Let $j \ge i + 1$. Then $x\pi_j = p^{v_j - u_{i+1}}n_jb_j$ for some integer n_j . Thus, $x\pi_j\varepsilon = p^{v_j - u_{i+1} + u_{j-1}}n_ja_j$ which is zero since $v_j - u_{i+1} > 3u_j - u_{i+1} \ge 2u_j$. Thus, $x\varepsilon = \sum_{j\in\mathbb{N}} p^{u_{j-1}}x\pi_j\varepsilon_j = 0$. A similar argument holds for ε' . ☐

Corollary 3.8. *For every $\phi \in \mathcal{E}$, $\varepsilon\phi\varepsilon = \varepsilon'\phi\varepsilon' = 0$. In particular, $\varepsilon^2 = 0 = (\varepsilon')^2$.*

Proof. Since G is reduced, it suffices to show the maps annihilate B , which will be the case if they annihilate every b_i . Let $\phi \in \mathcal{E}$. Note that $b_i\varepsilon\phi = p^{u_{i-1}}a_i\phi \in p^{u_{i-1}}B^{(v_{i-1})} \oplus G_{v_{i-1}}[p^{u_i}]$. The definition of ε together with Lemma 3.7 implies $b_i\varepsilon\phi\varepsilon = 0$. The identical argument shows that $b_i\varepsilon'\phi\varepsilon' = 0$. ☐

We are ready for the

Proof of Proposition 3.1. Assume the situation and notations above. Also, assume by way of contradiction that the conclusion of 3.1 is false. Then η has infinite additive order, and when $p = 2$, so does η'. It follows that G is unbounded. Hence, no matter what prime p was given, both η and η' have infinite order, which means the previous auxiliary results are available.

Using Corollary 3.8, the maps $\gamma = 1 + \varepsilon$ and $\gamma' = 1 + \varepsilon'$ are automorphisms of G. Define $\delta = \gamma^{-1}\alpha^{-1}\gamma\alpha$ and $\delta' = (\gamma')^{-1}(\alpha')^{-1}\gamma'\alpha'$. Then $\delta \in \Delta$ and, if $p = 2$, so is δ'. An easy calculation using (3.4) and 3.8 shows that

$$\delta = 1 + \psi \quad \text{with} \quad \psi = \varepsilon\eta + \sigma\varepsilon + \sigma\varepsilon\eta \quad \text{and} \quad \psi^2 = 0\,,$$

and similarly,

$$\delta' = 1 + \psi' \quad \text{with} \quad \psi' = \varepsilon'\eta' + \sigma'\varepsilon' + \sigma'\varepsilon'\eta' \quad \text{and} \quad (\psi')^2 = 0\,.$$

Thus, for every $n \in \mathbb{N}$, $\delta^n = 1 + n\psi$. Since $\delta \in \Delta$, $\delta^{p^\ell} = 1$ and hence $p^\ell\psi = 0$ for some $\ell \in N$. Choosing ℓ sufficiently large, we also have $p^\ell\psi' = 0$ if $p = 2$. Fix i such that both $u_{i-1} > \ell$ and $u'_{i-1} > \ell$. Then $p^{u_{i-1}}\psi = 0$ and, provided $p = 2$, $p^{u'_{i-1}}\psi' = 0$. Hence

$$0 = p^{u_{i-1}}b_i\psi = p^{u_{i-1}}b_i\varepsilon\eta + p^{u_{i-1}}b_i\sigma\varepsilon + p^{u_{i-1}}b_i\sigma\varepsilon\eta\,. \tag{3.9}$$

Since $b_i\sigma \in B^{(v_i)} \oplus G_{v_i}[p^{v_i}]$, Lemma 3.7 implies that $b_i\sigma = \sum_{j=1}^{i} k_jb_j + x$, where the k_j are integers and $x\varepsilon = 0$. From (3.3) we conclude that p divides k_i and, by 3.6(4),

$$k_i = p^{r_i}m_i \quad \text{with} \quad r_i \geq 1\,, \quad (p, m_i) = 1\,. \tag{3.10}$$

It follows that $p^{u_{i-1}}b_i\sigma\varepsilon = p^{2u_{i-1}}k_ia_i$ and $p^{u_{i-1}}b_i\sigma\varepsilon\eta = p^{2u_{i-1}}k_ia_i\eta$. From (3.9) and $b_i\varepsilon\eta = p^{u_{i-1}}a_i\eta$ we deduce that $(1 + k_i)p^{2u_{i-1}}a_i\eta = -k_ip^{2u_{i-1}}a_i$. Let n be an integer such that $n(1 + k_i) \equiv -m_i (\mathrm{mod}\ p^{u_i})$. By (3.10), p does not divide n and $(p^{2u_{i-1}}a_i)\eta = p^{r_i}n \cdot p^{2u_{i-1}}a_i$, which by construction is nonzero. Hence, $r_i < u_i - 2u_{i-1}$. Also, for every positive integer j, $(p^{2u_{i-1}}a_i)\eta^j = (p^{r_i}n)^j \cdot p^{2u_{i-1}}a_i$. It follows from (3.2) that

$$p^{2u_{i-1}}\left[\sum_{j=1}^{p^k}\binom{p^k}{j}(p^{r_i}n)^j\right]a_i = p^{2u_{i-1}}M(p,k,r_i,n)a_i = 0\,. \tag{3.11}$$

Suppose either that $p \neq 2$, or that $p = 2$ and $r_i \geq 2$. Then, by Lemma 2.2, the highest p–power dividing $M(p,k,r_i,n)$ is p^{k+r_i}. Thus, 3.11 implies that $k + r_i \geq u_i - 2u_{i-1}$; above we saw that $r_i < u_i - 2u_{i-1}$. It follows that

$$r_i \in [u_i - 2u_{i-1} - k\,, u_i - 2u_{i-1} - 1],$$

contrary to our delicate construction 3.6(4). Consequently, we must have that $p = 2$ and $r_i = 1$. In this situation, the primed elements and maps have the identical properties. We have $(\delta')^{2^\ell} = 1$, $(1 + \psi')^{2^\ell} = 1 + 2^\ell\psi' = 1$, and the choice of i was such that

$$0 = 2^{u'_{i-1}}b_i\psi' = 2^{u'_{i-1}}b_i\varepsilon'\eta' + 2^{u'_{i-1}}b_i\sigma'\varepsilon' + 2^{u'_{i-1}}b_i\sigma'\varepsilon'\eta'\,.$$

Let the k'_j be integers such that $b_i\sigma' = \sum_{j=1}^{i} k'_jb_j + x'$ with $x'\varepsilon' = 0$. As before, letting n' be an integer such that $n'(1 + k'_i) \equiv -m'_i (\mathrm{mod}\ 2^{u'_i})$, we have that n' is odd and, for every positive integer j, $2^{2u'_{i-1}}a'_i(\eta')^j = (2^{r'_i}n')^j 2^{2u'_{i-1}}a'_i$. By construction, $r_i' < u_i' - 2u_{i-1}'$. As before, it follows that $2^{2u_{i-1}'}M(2,k,r_i',n')a_i' = 0$. Observing (3.5) and the fact that $r_i = 1$, we conclude that

$$2^{r_i'} m_i' b_i = b_i\sigma'\pi_i = -b_i(2+\sigma)\pi_i = -(2+2^{r_i}m_i)b_i = -2(1+m_i)b_i\,.$$

But m_i is odd, hence $r_i' \geq 2$. It follows from Lemma 2.2 that $k + r_i' \geq u_i' - 2u_{i-1}'$. Thus, r_i' belongs to the interval $[u_i' - 2u_{i-1}' - k\,,\; u_i' - 2u_{i-1}' - 1]$, contrary to 3.6(4). This final contradiction concludes the proof. $\square$

Proposition 3.1 yields the most difficult part of our theorem:

Corollary 3.12. *If G is a reduced p–group, then $\Delta \leq (1+\mathbf{t})\zeta$.*

§4. PROOF OF THE THEOREM

As before, we let $G = H \oplus D$, where H is reduced and D is divisible. By Corollary 2.7, it suffices to show $\Delta \leq (1+\mathbf{t})\zeta$. By 3.12, this is the case when G is reduced. Thus, we may assume that $D \neq 0$. Let $\delta = 1 + \eta \in \Delta$. Since Δ induces a normal p–subgroup of $\operatorname{Aut}(G/D)$, it follows from 3.12 that there exists a natural number m such that either $p^m G\eta \leq D$, or $p = 2$ and $2^m G(2+\eta) \leq D$. If the latter is the case, replace δ by $-\delta = 1 - (2+\eta)$. Thus, we may assume without loss of generality that $p^m G\eta \leq D$. By Corollary 2.4, $\eta \in \mathbf{P}$. If $D\eta = 0$, then $\eta \in \Phi$, and $\delta \in 1 + \mathbf{t}$, by Proposition 2.6. Suppose $D\eta \neq 0$. It follows from Corollary 2.4 that $p = 2$ and $\delta|_D = -1$, the multiplication by -1. Choose any $\theta \in \operatorname{Hom}(H, D)$ and extend it to an endomorphism of G by defining $D\theta = 0$. Then $\theta^2 = 0$ and $\gamma = 1 + 2^m\theta \in \operatorname{Aut} G$. Let $\alpha = \delta\gamma\delta^{-1}\gamma^{-1}$. Then $\alpha \in \Delta$ and $\alpha|_D = 1$. As before, let $\delta^{-1} = 1 + \sigma$. Then $\eta + \sigma + \eta\sigma = 0$. Let $x \in G$. Since $G\eta$ and $G\sigma$ both are contained in $G[2^m] + D$, on which γ acts as the identity, we have

$$x\alpha = x\delta\gamma\delta^{-1}\gamma^{-1} = x + 2^m x\theta\sigma + x\sigma + x\eta + x\eta\sigma,$$

which implies $x(\alpha - 1) = -2^{m+1}x\theta$. It follows that $\alpha - 1 \in \Phi$, and Proposition 2.6 implies that $\theta \in \mathbf{t}$. We have shown that $\operatorname{Hom}(H, D)$ is a torsion group, which, since $D \neq 0$, implies $2^n H = 0$ for some positive integer n. But then $2 + \eta \in \Phi$ and $-\delta = 1 - (2+\eta) \in 1 + \mathbf{t}$, completing the proof.

REFERENCES

1. R. P. Abraham, *Normal p–subgroups of the Automorphism Group of an Abelian p–group*, Journal of Algebra (to appear).
2. H. Freedman, *The automorphisms group of countable primary reduced abelian groups*, Proc. London Math.soc. (3) **12** (1962), 77–99. MR **24:**A3215
3. L. Fuchs, *Infinite Abelian Groups*, Vol. 2, Academic Press, New York, 1973. MR **50:**2362
4. J. Hausen, *Near central automorphisms of abelian torsion groups*, Trans. Amer. Math. Soc. **174** (1972), 199–215. MR **46:**9193
5. J. Hausen, *On the normal structure of automorphism groups of abelian p–groups*, J. London Math. Soc. (2), **5** (1972), 409–413. MR **48:**2275
6. J. Hausen, *How automorphism groups reveal Ulm inveriants*, J. Algebra **44** (1977), 9–28. MR **56:**499
7. J. Hausen and J. A. Johnson, *Characterization of the primary abelian groups, bounded modulo the divisible subgroup, by the radical of their endomorphism rings*, Archiv d. Math. **29** (1977), 566–570. MR **57:**6231
8. J. Hausen, C. E. Praeger and P. Schultz, *Most Abelian p–groups are determined by the Jacobson radical of their endomorphism rings*, Math. Z. **216** (1994), 431–436. MR **95d:**20094
9. P. Hill, *The automorphism groups of primary abelian groups*, Proc. London Math. Soc. (2), **22** (1971), 24–38. MR **43:**7508

10. H. Leptin, *Abelsche p–Gruppen und ihre Automorphismengruppen*, Math. Z., **73** (1960), 235–253. MR **22:**730
11. H. Leptin, *Einige Bemerkungen über die Automorphismen abelscher Gruppen*, in Proc. Colloq. Abelian Groups (Tihany, 1963), Budapest, 1964, pp. 99–104. MR **29:**5929
12. W. Liebert, *Isomorphic automorphism groups of primary Abelian groups*, Abelian group theory: Proceedings of the 1985 Oberwolfach Conference, Eds. R Göbel and E A Walker, Gordon and Breach, New York, 1987, pp. 9–31. MR **90g:**20085
13. R. S. Pierce, *Homomorphisms of primary abelian groups*, in Topics in Abelian Groups (J. M. Irwin and E. A. Walker, eds.), Scott, Foresman and Co., 1963, pp. 215–310. MR **31:**1299
14. C. E. Praeger and P. Schultz, *The Loewy length of the Jacobson radical of a bounded endomorphism ring*, in Abelian Groups and Non-commutative Rings, Amer. Math. Soc., Contemporary Mathematics 130, 1992, pp. 349–360. MR **93h:**16059
15. D. J. S. Robinson, *A Course in the Theory of Groups*, Springer–Verlag, New York, 1982. MR **84k:**20001
16. J. P. Serre, *A Course in Arithmetic*, Springer–Verlag, New York, 1973. MR **49:**8956
17. K. Shoda, *Über die Automorphismen einer endlichen abelschen Gruppe*, Math. Ann. **100** (1928), 674–686.

Department of Mathematics, University of Houston, Houston, Texas 77204-3476
E-mail address: `hausen@uh.edu`

Department of Mathematics, University of Western Australia, Nedlands 6009, Australia
E-mail address: `schultz@maths.uwa.edu.au`