Finite $p$-Groups of Exponent $p^2$ in Which Each Element Commutes with Its Endomorphic Images

A. CARANTI*

Dipartimento di Matematica, Università di Trento, I-38050 Povo (Trento), Italy

Communicated by Guido Zappa

Received April 25, 1983

1

Various authors have studied the groups $G$ in which each element commutes with all of its images under endomorphisms of $G$. Such groups are called $E$-groups. They can be defined equivalently as the groups $G$ such that the near-ring generated by the endomorphisms of $G$ in the near-ring of maps on $G$ is actually a ring (see [7, Sect. 3; 3, Theorem 4.4.3]; see also the remark following Lemma 3.1 below).

Abelian groups are obviously $E$-groups, and since in an $E$-group each element commutes with all of its conjugates, every $E$-group is nilpotent of class at most 3 (see [5, III.6.4 and III.6.5]). Various examples of finite non-abelian $E$-groups have already appeared in the literature [2, 8, 1]. All the groups $G$ appearing in these papers are finite $p$-groups of exponent $p^2$ and class 2, and satisfy the following conditions:

(i) $G^p \leq G' = \phi(G) = \Omega_1(G) \leq Z(G)$;

(ii) if $\phi$ is an endomorphism of $G$ which is not an automorphism, then $\phi$ maps $G$ into $Z(G)$;

(iii) each automorphism of $G$ is central.

If $G$ is a finite $p$-group satisfying (i), (ii), (iii), then $G$ is clearly an $E$-group (and for this reason the groups of [1], though constructed for a different purpose, are $E$-groups, as claimed above). Malone studied in [7] the question whether every finite $E$-group of exponent $p^2$ must satisfy (i), (ii), (iii). In this paper we settle this problem, for odd $p$, as follows.

Malone proved that (i) is necessary in a finite $E$-group $G$ of exponent $p^2$ with no nontrivial abelian direct factors. He stated that there is an example $G$ due to Meldrum, in which $\Omega_1(G) < Z(G)$. In Section 2 we provide

* Partially supported by funds of MPI-Italy.
another example. Malone also claimed that the first inequality in (i) can be strengthened to \( G^p = G' \). We show in Section 2 that the examples given in [1] are counterexamples to this assertion.

Malone proved that every finite \( E \)-group of exponent \( p^2 \) having no nonabelian proper \( E \)-subgroup satisfies (ii). In Section 4 we prove that in fact a finite \( E \)-group of class at most 2 satisfies (ii) if and only if it cannot be expressed as the direct product of two nonabelian groups. We also give a necessary and sufficient condition for a direct product of \( E \)-groups to be an \( E \)-group, and determine the endomorphisms of a finite \( E \)-group of class at most 2 in terms of the automorphisms of the indecomposable ones. To obtain these results, we need to study the structure of the \( E \)-groups in more detail. This we do in Section 3.

As to (iii), we construct in Section 5 two examples of finite \( E \)-groups of exponent \( p^2 \) which do not satisfy this condition. In the first example the factor group \( \text{Aut}(G)/\text{Aut}_c(G) \), where \( \text{Aut}_c(G) \) is the subgroup of \( \text{Aut}(G) \) consisting of the central automorphisms, is cyclic of order 3, with \( \equiv 1 \pmod{3} \); in the second example \( \text{Aut}(G)/\text{Aut}_c(G) \) is cyclic of order \( p \). In general, in a finite \( E \)-group of exponent \( p^2 \) the factor group \( \text{Aut}(G)/\text{Aut}_c(G) \) has to be abelian of odd order, as shown in Theorem 3.6. (Recall that \( \text{Aut}_c(G) = \{ g \in \text{Aut}(G) \mid g^{-1}g \in Z(G), \text{ for each } g \in G \} \).)

In this paper all groups considered are finite, and \( p \) is always an odd prime. Notation is as in [5, 3], except that if \( G \) is a group, and \( n \) a natural number, we write \( G^n = \langle g^n \mid g \in G \rangle \). An endomorphism of a group is called strict if it is not an automorphism. A \( pE \)-group is a \( p \)-group which is an \( E \)-group. The standard commutator identities in nilpotent groups of class 2 are freely used (see [5, III.1.2 and III.1.3]).

2

Let \( p \) be an odd prime, \( s \geq 2 \) an integer. In [1] it is shown that the groups

\[
G_s = \langle x_i, 1 \leq i \leq 2s + 1/ [x_i, x_j, x_k] = 1, \\
1 \leq i, j, k \leq 2s + 1; [x_i, x_{i+s}] = 1, 1 \leq i \leq s; \\
x_i^p = [x_i, x_{i+1}], 1 \leq i \leq 2s + 1 \rangle,
\]

where \( x_{2s+2} = x_1 \), satisfy (i), (ii), (iii) of Section 1, and actually \( G_s^p \leq G^s = Z(G_s) \). In fact, in the proof of Theorem 2 of [7] Malone appears to misquote from [4] and obtains the incorrect conclusion that \( G^p = G' \) must always hold in a finite nonabelian \( pE \)-group of exponent \( p^2 \).
Now take $s \geq 5$, let $\langle z \rangle$ be a cyclic group of order $p^2$, and consider the central product $H_s = G_s \langle z \rangle$, where $z^p = [x_1, x_2][x_3, x_5]$. $H_s$ satisfies (i), and

$$\Omega_1(H_s) = \Omega_1(G_s) < Z(H_s) = \Omega_1(G_s) \langle z \rangle.$$ 

We claim that $H_s$ is an $E$-group. To prove this, let $u, v \in H_s$, $[u, v] = u^p \neq 1$. Write $u = u'z'$, with $u' \in G_s$, and $v = v'z'$, with $v' \in G_s$. Then $z^p = (u')^{-p}[u', v']$. Now it is not difficult to see that no power of $[x_1, x_2][x_3, x_5]$ different from 1 is of the form $(u')^{-p}[u', v']$, for $u', v' \in G_s$. This forces $z^p = 1$. The Lemma of [1] can now be applied to show that $H_s$ satisfies (ii) and (iii), and is thus an $E$-group.

3

If $G$ is an $E$-group, denote by $E = E(G)$ the ring generated by the endomorphisms of $G$ in the near-ring of maps on $G$, and by $C = C(G)$ the subset of $E$ consisting of the endomorphisms mapping $G$ into $Z(G)$. Note that $E(G)$ consists of the finite sums of endomorphisms of $G$.

As in the whole paper, we bound ourselves to odd primes $p$ and to $pE$-groups of class 2. However, for $p \neq 3$ all $pE$-groups have class at most 2 [5, III.6.5]; and the $pE$-groups of exponent $p^2$ are also of class at most 2 by Theorem 2 of [7].

3.1. Lemma. For a $p$-group $G$ of class 2, $p > 2$, the following are equivalent:

(i) $[a, a^\varphi] = 1$ for each $a \in G$, and each endomorphism $\varphi$ of $G$, i.e., $G$ is an $E$-group;

(ii) $[a^\varphi, b] = [a, b^\varphi]$ for each $a, b \in G$, and each endomorphism $\varphi$ of $G$;

(iii) $[a^\varphi, b^\psi] = [a^\psi, b^\varphi]$ for each $a, b \in G$, and all endomorphisms $\varphi, \psi$ of $G$.

Proof. (i) $\Rightarrow$ (ii) For each $a, b \in G$, and each endomorphism $\varphi$ of $G$, one has

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

(ii) $\Rightarrow$ (iii) For each $a, b \in G$, and all endomorphisms $\varphi, \psi$ of $G$, one has

$$[a^\varphi, b^\psi] = [a, b^\psi \varphi] = [a^\varphi \psi, b] = [a^\psi, b^\varphi].$$
(iii) $\Rightarrow$ (i) Let $a = b$, $\psi = 1$ in (iii) to get

$$[a^\phi, a] = [a, a^\phi] = [a^\phi, a]^{-1}.$$ 

Since $p > 2$, it follows $[a^\phi, a] = 1$.

We remark that for $a = b$, (iii) of Lemma 3.1 gives

$$[a^\phi, a^\psi] = [a^\psi, a^\phi] = [a^\phi, a^\psi]^{-1}.$$ 

For $p$ odd, this is equivalent with $[a^\phi, a^\psi] = 1$, or $a^\phi + \psi = a^\psi + \phi$, and this is Theorem 6 of [7] for $p > 2$.

3.2. PROPOSITION. Let $G$ be a $pE$-group of class 2, $p > 2$, and let $\phi$ be an endomorphism of $G$. If some power of $\phi$ maps $G$ into $Z(G)$, then $\phi$ itself maps $G$ into $Z(G)$.

Proof. Let $i$ be the smallest nonnegative integer such that $\phi^{2^i}$ maps $G$ into $Z(G)$. Assume, by way of contradiction, that $i > 0$. Thus, using Lemma 3.1, we have

$$[a, b]^{\phi^{2^{i-1}}} = [a^{\phi^{2^{i-1}}}, b^{\phi^{2^{i-1}}}] = [a, b^{\phi^{2^i}}] = 1.$$ 

It follows that $G^{i} \subseteq \ker(\phi^{2^{i-1}})$. By Theorem 1 of [7], $G^{\phi^{2^{i-1}}} \subseteq Z(G)$, contradicting the definition of $i$.

In Proposition 3.2, the condition that $\phi$ is an endomorphism, and not merely an element of $E$, is necessary, as can be seen in the second example of Section 5.

3.3. LEMMA. Let $G$ be a $pE$-group of class 2, $p > 2$. Let $\phi_1, \phi_2, \ldots, \phi_k$ be endomorphisms of $G$. Then: $\sum_{i=1}^k \phi_i \in E$ is an endomorphism of $G$ if and only if $\sum_{1 \leq i < j \leq k} \phi_i \phi_j \in E$ maps $G$ into $Z(G)$.

Proof. Let $a, b \in G$, $\phi = \sum_{i=1}^k \phi_i$. Then

$$(ab)^\phi = \prod_{i=1}^k (ab)^{\phi_i} = \prod_{i=1}^k a^{\phi_i} b^{\phi_i},$$

$$a^\phi b^\phi = \prod_{i=1}^k a^{\phi_i} \prod_{j=1}^k b^{\phi_j}.$$ 

Moving successively $b^{\phi_1}, b^{\phi_2}, \ldots$ to the right in the first product, we get

$$(ab)^\phi = a^{\phi_1} b^{\phi_i} \prod_{i=1}^{k-1} \prod_{j=i+1}^k [b^{\phi_i}, a^{\phi_j}].$$
Thus $\varphi$ is an endomorphism of $G$ if and only if, for each $a, b \in G$,

\[
1 = \prod_{i=1}^{k-1} \prod_{j=i+1}^{k} [b^{\varphi_i}, a^{\varphi_j}]
\]

\[
= \prod_{1 \leq i < j \leq k} [b^{\varphi_i \varphi_j}, a] = [b^{\sum_{1 \leq i < j \leq k} \varphi_i \varphi_j}, a]
\]

(using Lemma 3.1), i.e., $\sum_{1 \leq i < j \leq k} \varphi_i \varphi_j \in E$ maps $G$ into $Z(G)$.

3.4. **Lemma.** Let $G$ be a $pE$-group of class 2, $p > 2$. Let $\varphi, \psi$ be endomorphisms of $G$. Then: $\varphi - \psi \in E$ is an endomorphism of $G$ if and only if $\psi(\varphi - \psi) \in E$ maps $G$ into $Z(G)$.

**Proof.** It is easy to give a direct proof of this, as for Lemma 3.3. Otherwise, one remarks that if $G$ has exponent $p^e$, then $-\psi = \psi + \cdots + \psi$ ($p^e - 1$ summands), and applies Lemma 3.3 to $-\psi + \varphi$.

The next two theorems are the main results on $E$-groups of this section.

3.5. **Theorem.** Let $G$ be a $pE$-group of class 2, $p > 2$. Then $C = C(G)$ is a two-sided ideal of $E = E(G)$, and $E/C$ is a finite commutative ring.

3.6. **Theorem.** Let $G$ be a $pE$-group of exponent $p^2$, $p > 2$. Then $\text{Aut}(G)/\text{Aut}_c(G)$ is an abelian group of odd order.

**Proof of 3.5.** $C$ is clearly closed under addition. If now $\varphi \in C$, $\psi \in E$, write $\psi = \psi_1 + \cdots + \psi_k$, with the $\psi_i$'s endomorphisms of $G$. Then $\psi \varphi - \psi_1 \varphi + \cdots + \psi_k \varphi$, and clearly all $\psi_i \varphi$'s are in $C$. We have also $\varphi \psi = \psi_1 \varphi + \cdots + \psi_k \varphi$: if we show that $Z(G)$ is fully invariant, then all $\varphi \psi$'s are in $C$, and $C$ is a two-sided ideal of $E$. In fact, if $z \in Z(G)$, $g \in G$, and $\sigma$ is an endomorphism of $G$, Lemma 3.1 gives $[z^\sigma, g] = [z, g^\sigma] = 1$, and thus $z^\sigma \in Z(G)$.

It remains to show that if $\varphi, \psi$ are endomorphisms of $G$, then $\varphi \psi - \psi \varphi \in C$. Now it is clear from Lemma 3.1 (and actually already contained in its proof) that for each $a, b \in G$,

\[
[a, b^{\psi \varphi \psi^\varphi}] = [a, b^{\psi \varphi}][a, b^{\varphi \psi}]^{-1} = [a^\psi, b^\varphi][a^\varphi, b^\psi]^{-1} = 1.
\]

We have thus only to show that $\varphi \psi - \psi \varphi \in E$ is an endomorphism of $G$. By Lemma 3.4, this is the case if and only if $\psi \varphi(\varphi \psi - \psi \varphi) \in E$ maps $G$ into $Z(G)$. But this is clear, since already $\varphi \psi - \psi \varphi$ maps $G$ into $Z(G)$.

**Proof of 3.6.** $\text{Aut}(G)/\text{Aut}_c(G)$ is isomorphic, as a multiplicative group, to the image of $\text{Aut}(G)$ under the canonical endomorphism $E \to E/C$, and then is abelian by Theorem 3.5.
Let now \( \varphi \in \text{Aut}(G) \) satisfy \( \varphi^2 = 1 \). For each \( a, b \in G \) one has, using Lemma 3.1,

\[
[a, b]^{\varphi} = [a^\varphi, b^\varphi] = [a, b^{\varphi^2}] = [a, b].
\]

This forces \( \varphi = 1 \), for instance, by Theorem 5 of [7] (compare also with the Proposition of [1]).

4

In this section we determine the endomorphisms of a \( p \mathbb{E} \)-group of class at most 2, \( p > 2 \), in terms of the automorphisms of the indecomposable ones.

Our first result refines Corollary 4.2 of [7].

4.1. THEOREM. Let \( G \) be a \( p \mathbb{E} \)-group of class at most 2, \( p > 2 \). Assume that there is a strict endomorphism \( \varphi \) of \( G \), which does not map \( G \) into \( Z(G) \). Then \( G \) is decomposable into a nontrivial product of two \( p \mathbb{E} \)-groups.

Proof. The first part of the proof is an easy analogue of Fitting's lemma [6, p. 113] for finite groups.

Let then \( G \) be any finite group, \( \varphi \) an endomorphism of \( G \). Choose an integer \( n \) such that \( G^\varphi = G^{\varphi^{i+1}} \) for all \( i \geq 0 \). Set \( \psi = \varphi^n \), \( H = G^\psi \), \( K = \ker \psi \). We claim that \( G \) is the semidirect product of \( H \) and \( K \).

In fact, \( K = \ker \psi \) is normal in \( G \). For each \( g \in G \), \( g^\psi \in H = G^\psi = G^{\psi^2} \). Thus there is \( g_1 \in G \) such that \( g^\psi = g_1^\psi \). Then

\[
(g_1^{-\psi}g)^\psi = g_1^{-\psi^2}g^\psi = 1
\]

that is, \( g_1^{-\psi}g \in K \), \( g \in HK \), and so \( G = HK \). Finally, \( \psi \) restricted to \( H \) is clearly an automorphism of \( H \), and thus \( K \cap H = 1 \).

Now assume that \( G, \varphi \) are as in the assumptions of the Theorem, and take \( \psi \) as in the first part of the proof. We claim that the decomposition \( G = HK \) is nontrivial and direct.

In fact, \( K = \ker \psi \supseteq \ker \varphi > 1 \) because \( \varphi \) is not an automorphism of \( G \). If \( H = 1 \), \( \psi = \varphi^n \) is the trivial endomorphism mapping \( G \) onto 1 and \( \varphi^n \) maps in particular \( G \) into \( Z(G) \). By Proposition 3.2, \( \varphi \) itself maps \( G \) into \( Z(G) \), which contradicts the assumptions. Thus both \( H, K \) are nontrivial.

Now take \( k \in K, h \in H \). Thus there exists \( g \in G \) such that \( h = g^\psi \). Using Lemma 3.1 we get

\[
[h, k] = [g^\psi, k] = [g, k^\psi] = 1,
\]

as \( k \in K = \ker \psi \). This shows that \( [H, K] = 1 \) and thus that \( G = H \times K \).
Of course, a direct factor of an $E$-group is an $E$-group by Theorem 4 of [7].

4.2. Theorem. Let $H_1$, $H_2$ be $pE$-groups of class at most 2, $p > 2$, and set $G = H_1 \times H_2$. Then: $G$ is an $E$-group if and only if

for $\{i, j\} = \{1, 2\}$, every homomorphic image

of $H_i$ into $H_j$ lies in $Z(H_j)$ \((*)\)

Proof. If \((*)\) is not satisfied, let, for instance, $\psi: H_1 \to H_2$ be a homomorphism, and $h \in H_1$, $k \in H_2$ be elements such that $[k, h^\psi] \neq 1$. Consider the endomorphism of $G$ given by

$$(h_1, h_2) \mapsto (1, h_1^\psi).$$

We have

$$[(h, k), (1, h_1^\psi)] = (1, [k, h_1^\psi]) \neq 1$$

and thus $G$ is not an $E$-group.

Suppose vice versa that \((*)\) holds. If $\varphi$ is an endomorphism of $G$, define maps $\varphi_{ij}$ by

$$(h_1, 1)^\varphi = (h_1^{\varphi_{11}}, h_1^{\varphi_{12}}), \quad (1, h_2)^\varphi = (h_2^{\varphi_{21}}, h_2^{\varphi_{22}}).$$

Clearly every $\varphi_{ij}: H_i \to H_j$ is a homomorphism. It follows from \((*)\) that for $i \neq j$, $h_1^{\varphi_{ij}} \in Z(H_j)$, so that

$$[(h_1, h_2), (h_1, h_2)^\varphi] = [(h_1, h_2), (h_1^{\varphi_{11}}, h_2^{\varphi_{22}})]$$

$$= ([h_1, h_1^{\varphi_{11}}], [h_2, h_2^{\varphi_{22}}]) = 1,$$

and thus $G$ is an $E$-group.

To illustrate Theorem 4.2, let $G_s$ be as in Section 2. An easy adaptation of the Lemma of [1] shows that, for $s \neq t$, $H_1 = G_s$ and $H_2 = G_t$ satisfy \((*)\). Thus, for $s \neq t$, $G_s \times G_t$ is an $E$-group. On the other hand, if $G$ is any nonabelian $E$-group, it is clear that $G \times G$ is not an $E$-group.

It is now easy to determine the endomorphisms of a $pE$-group of class at most 2, $p > 2$, in terms of the automorphisms of its indecomposable factors. In the next theorem, given a direct product $H \times K$, we extend an automorphism $\alpha$ of, say, $H$ to an endomorphism of $G$ via the definition

$$(h, k)^\alpha = (h^2, 1).$$

4.3. Theorem. Let $G$ be a $pE$-group of class at most 2, $p > 2$.

If $G$ is indecomposable, then the set of endomorphisms of $G$ is $C(G) \cup \text{Aut}(G)$. 

If $G = H_1 \times \cdots \times H_k$, each $H_i$ indecomposable, then

(i) the $H_i$'s are $pE$-groups;

(ii) the endomorphisms of $G$ are of the form

$$\alpha_1 + \cdots + \alpha_k + \xi$$

where $\alpha_i \in \text{Aut}(H_i) \cup \{0\}$, $\xi \in C(G)$;

(iii) the ring $E(G)/C(G)$ is isomorphic to the direct sum of the rings $E(H_i)/C(H_i)$.

**Proof.** If $G$ is indecomposable, one applies Theorem 4.1. If $G$ is written as the direct product of the indecomposable factors $H_i$, (i) is clear, (ii) follows from Theorem 4.2 and the argument used in the second part of its proof, and now (iii) follows from (ii) and the description of $E(G)$ remarked at the beginning of Section 3.

In this section we construct the two examples of $pE$-groups of exponent $p^2$ which do not satisfy (iii) of Section 1, as announced there.

The first example is the following:

$$G = \langle x_i, y_i, 1 \leq i \leq 4 | [a, b, c] = 1, \quad [x_i, y_j] = 1, \quad 1 \leq i, j \leq 4; \quad x_i^p = [y_1, y_2], \quad x_j^p = [y_2, y_3], \quad x_k^p = [y_3, y_4], \quad x_l^p = [y_4, y_1];$$

$$y_i^p = [x_3, x_4], \quad y_j^p = [x_1, x_2], \quad y_k^p = [x_4, x_1], \quad y_l^p = [x_2, x_3] \rangle,$$

with $p \equiv 1 \pmod{3}$.

We have $|G| = p^{20}$, $|G^p| = |G/\phi(G)| = p^8$, and $G' = \phi(G) = \Omega_1(G) = Z(G)$ has order $p^{12}$. It is easy to check that $G$ admits the automorphism $\omega$ of order 3 defined by

$$x_i \mapsto x_i^\lambda,$$

$$y_i \mapsto y_i^{\omega^2},$$

where $\lambda$ is a primitive third root of 1 (mod $p$), and that $[g^\omega, g^\omega] = 1$ for each $g \in G$. We claim that if $\varphi$ is an endomorphism of $G$ that does not map $G$ into $Z(G)$, then $\varphi$ is an automorphism of $G$, and $\varphi = \omega^i (\text{mod Aut}_c(G))$, for some $i$. It will then be clear that $G$ is an $E$-group with $\text{Aut}(G) = \langle \omega \rangle \text{Aut}_c(G)$ and $E/C \cong GF(p) \oplus GF(p)$.

Here and in the next example, we consider $V = G/\phi(G)$ and $\phi(G)$ as
OF CERTAIN $p$-GROUPS OF EXPONENT $p^2$

$GF(p)$-vector spaces, using for them the additive notation. A bar denotes the canonical homomorphism $G \to V$, and if $\phi$ is an endomorphism of $G$, $\bar{\phi}$ denotes the endomorphism that $\phi$ induces on $V$. Note that the $p$th power is well defined as a map $V \to \phi(G)$, since $(gh)^p = g^p$ for every $g \in G$ and $h \in \phi(G) = Z(G) = \Omega_1(G)$; and the commutator form is well defined as a map $V \times V \to \phi(G)$, since $[g_1, h_1, g_2, h_2] = [g_1, g_2]$ for all $g_1, g_2 \in G$ and $h_1, h_2 \in \phi(G) = Z(G)$.

Let thus $\phi$ be an endomorphism of $G$ such that $\bar{\phi} \neq 0$. Then $x_i^\phi \neq 0$ or $y_i^\phi \neq 0$ for some $i$. If, for instance, $x_i^\phi \neq 0$, one gets by the relation $x_i^\phi = [y_1, y_2]$ of (1) $1 \neq (x_i^\phi)^p = [y_1^p, y_2^p]$. If $\dim \langle \bar{y}_1, \bar{y}_2 \rangle^\phi < 2$, clearly $1 = [\bar{y}_1^p, \bar{y}_2^p] = [y_1^p, y_2^p]$, a contradiction. Thus $\langle \bar{y}_1^p, \bar{y}_2^p \rangle$ is 2-dimensional, so that in particular $\bar{y}_1^p \neq 0$, $\bar{y}_2^p \neq 0$. It is easy to exploit this argument, using the defining relations (1), to obtain that $\bar{\phi}$ preserves the dimension of every subspace $\langle \bar{x}_i, \bar{x}_{i+1} \rangle$, $\langle \bar{y}_i, \bar{y}_{i+1} \rangle$, $1 \leq i \leq 4$ (indices being taken modulo 4). Now let

$$U = \langle \bar{x}_i/1 \leq i \leq 4 \rangle, \quad W = \langle \bar{y}_i/1 \leq i \leq 4 \rangle,$$

and note that

$$U^\phi = [\langle \bar{y}_1, \bar{y}_3 \rangle, \langle \bar{y}_2, \bar{y}_4 \rangle], \quad W^\phi = [\langle \bar{x}_1, \bar{x}_3 \rangle, \langle \bar{x}_2, \bar{x}_4 \rangle].$$

If, say $\langle \bar{y}_1, \bar{y}_3 \rangle^\phi$ has dimension 1, then the first formula of (2) implies that $U^\phi$ has dimension at most 2, and the second formula yields that $W^\phi$ is at most 1-dimensional, a contradiction. Thus also the 2-dimensional subspaces

$$\langle \bar{x}_1, \bar{x}_3 \rangle, \langle \bar{x}_2, \bar{x}_4 \rangle, \langle \bar{y}_1, \bar{y}_3 \rangle, \langle \bar{y}_2, \bar{y}_4 \rangle$$

of $V$ retain their dimension under $\bar{\phi}$. Using (1), it is not difficult to see that

$$U \cup W = \{v \in V/\dim([v, V]) \leq 3\}$$

and that

$$\{v \in U \cup W/\dim([v, V] \cap G^p) \leq 2\} = \langle \bar{x}_1, \bar{x}_2 \rangle \cup \langle \bar{x}_2, \bar{x}_4 \rangle \cup \langle \bar{y}_1, \bar{y}_3 \rangle \cup \langle \bar{y}_2, \bar{y}_4 \rangle.$$

Thus $\bar{\phi}$ maps the set-theoretic union of the subspaces (3) into itself. This implies that $\bar{\phi}$ is an automorphism of $V = G/\phi(G)$, and thus that $\phi$ is an automorphism of $G$.

Now $\langle \bar{y}_1, \bar{y}_3 \rangle^p$ and $\langle \bar{y}_2, \bar{y}_4 \rangle^p$ consist of commutators, since

$$\langle \bar{y}_1, \bar{y}_3 \rangle^p = [\bar{x}_3, \langle \bar{x}_1, \bar{x}_4 \rangle], \quad \langle \bar{y}_2, \bar{y}_4 \rangle^p = [\bar{x}_2, \langle \bar{x}_1, \bar{x}_3 \rangle].$$
Since not all elements of $\langle \bar{x}_1, \bar{x}_3 \rangle^p$ and $\langle \bar{x}_2, \bar{x}_4 \rangle^p$ are commutators (compare with the remarks at the end of Section 1 of [9]), it follows that $U$ and $W$ are left invariant by $\bar{\phi}$. In fact, each subspace of (3) is left invariant by $\bar{\phi}$. Assume, for instance, that $\bar{\phi}$ interchanges $\langle x_1, x_3 \rangle$ and $\langle x_2, x_4 \rangle$; (4) implies that $\bar{\phi}$ interchanges $\langle y_1, y_3 \rangle$ and $\langle y_2, y_4 \rangle$, so that $\bar{\phi}$ should map $x_i$ into $\langle \bar{x}_2, \bar{x}_4 \rangle \cap \langle \bar{x}_1, \bar{x}_3 \rangle \cap \langle \bar{x}_1, \bar{x}_3 \rangle = \emptyset$, a contradiction.

Now write $\bar{\phi}$ as a matrix in the base
\[
\{ \bar{x}_i, 1 \leq i \leq 4; \; \bar{y}_i, 1 \leq i \leq 4 \}
\]
of $V$, so that $\bar{\phi}$ has the form
\[
\begin{pmatrix}
\alpha & \beta & \gamma & \delta \\
\epsilon & \xi & \eta & \theta \\
\alpha' & \beta' & \gamma' & \delta' \\
\epsilon' & \xi' & \eta' & \theta'
\end{pmatrix}
\]
We apply $\bar{\phi}$ to the defining relations (1) for the $y_i^p$'s: $y_i^p = [x_3, x_4]$ gives
\[
\alpha' y_i^p + \beta' y_i^p
\]
and so $\alpha' = \delta \theta, \; \beta' = -\gamma \theta, \; \gamma \eta = \delta \eta = 0$, which yields $\eta = 0$. From $y_i^p = [x_1, x_2]$ one obtains $\xi = 0$ and $\epsilon' = \alpha \xi, \; \xi' = -\beta \epsilon$; from $y_i^p = [x_4, x_1]$ one gets $\gamma' = \beta \theta$ and $\delta' = \alpha \theta$; from $y_i^p = [x_2, x_3]$, finally, $\eta' = -\gamma \epsilon$ and $\delta' = \epsilon \theta$. Now using similarly the defining relations for the $x_i^p$'s, one obtains in sequence: $\alpha = \alpha \delta \theta \epsilon, \; \beta = 0$, so that $\gamma' = \xi' = 0; \; \epsilon = \alpha ^2 \epsilon \theta, \; \gamma = 0$, so that $\beta' = \eta' = 0; \; \delta = \alpha \theta e \delta, \; \theta = \delta ^2 \theta e$. This yields easily $\alpha = \epsilon = \delta = \theta, \; \alpha ^3 = 1$, as required.

The second example is
\[
G = \langle x_i, y_i; 1 \leq i \leq 4 | [a, b, c] = 1, \]
\[
\text{for all } a, b, c \in G; \; [x_i, y_i] = 1, 1 \leq i \leq 4; \]
\[
[y_i, y_j] = 1, \; [x_i, y_j] = [y_i, x_j], \; 1 \leq i, j \leq 4; \]
\[
x_i^p = [x_i, x_{i+1}], \; y_i^p = [x_i, y_{i+1}]^2, \; 1 \leq i \leq 3; \]
\[
x_i^p = [x_1, x_3][x_1, y_3], \; y_i^p = [x_1, y_3]^2, \]
\[
\text{with } p > 2. \; \text{Note that } [x_i, y_i] = 1 \text{ is then actually redundant.}
\]
G has order $p^{20}$, $|G^p| = |G/\phi(G)| = p^8$, and $G' = \phi(G) = \Omega_1(G) = Z(G)$ has order $p^{12}$. It is easy to check that $G$ admits the automorphism $\psi$ defined by

$$x_i \mapsto x_i, y_i,$$

$$y_i \mapsto y_i,$$

that $\psi^p \in \text{Aut}_c(G)$, and that $[g, g^\psi] = 1$, for all $g \in G$. Note also that $\psi - 1 \in E$ does not map $G$ into $Z(G)$, while $(\psi - 1)^2 = 0$: compare with the remark after Proposition 3.2. We claim that if $\phi$ is an endomorphism of $G$ that does not map $G$ into $Z(G)$, then $\phi$ is an automorphism of $G$, and $\phi = \psi^i \pmod{\text{Aut}_c(G)}$ for some $i$. It will thus be clear that $G$ is an $E$-group with $\text{Aut}(G) = \langle \psi \rangle \text{Aut}_c(G)$ and $E/C \cong GF(p)[x]/(x^2)$.

Denote by $V_i$, $1 \leq i \leq 4$, the 2-dimensional subspaces $\langle \bar{x}_i, \bar{y}_i \rangle$ of the $GF(p)$-vector space $V = G/\phi(G)$. The relations (5) give

$$V'_1 = [V_1, V_2], \quad V'_2 = [V_2, V_3], \quad V'_3 = [V_3, V_4], \quad V'_4 = [V_1, V_3]. \quad (6)$$

Let $\phi$ be an endomorphism of $G$ that does not map $G$ into $Z(G)$, so that $\phi \neq 0$ on $V$. Equation (6) gives immediately that all $V'_i$'s are nonzero. If every $V_i$ retains its dimension under $\phi$, it is easy to see that $\phi$ must be an automorphism of $G$. In this case $\phi$ leaves each $V_i$ invariant, as follows from the following chain of equalities:

$$V_3 = \{v \in V/\langle v, V \rangle \subseteq G^p\},$$

$$\langle V_3, V_4 \rangle = \{v \in V/\langle v, V_3 \rangle \subseteq V^p_3\},$$

$$\langle V_2, V_3, V_4 \rangle^p = G^p \cap \langle V, \langle V_2, V_3, V_4 \rangle \rangle,$$

$$\langle V_2, V_3 \rangle^p = G^p \cap \langle V_2, V_3, V_4 \rangle,$$

$$V_2 = [V_3, \langle V_2, V_3 \rangle], \quad \langle V_1, V_2 \rangle^p = G^p \cap \langle V, V_2 \rangle,$$

$$V'_1 = \langle V_1, V_2 \rangle, \quad V'_4 = [V_1, V_3].$$

Now let the action of $\phi$ on the $V_i$'s be described by

$$\bar{x}_i^\phi = \alpha_i \bar{x}_i + \beta_i \bar{y}_i,$$

$$\bar{y}_i^\phi = \gamma_i \bar{x}_i + \delta_i \bar{y}_i,$$

for $1 \leq i \leq 4$. If $\alpha_1 = 0$, applying $\phi$ to the relation $y_1^\phi = 2[x_1, y_2]$ and comparing the coefficients of $[x_1, y_2]$ on both sides, we get $\gamma_1 = 2\alpha_1\gamma_2 = 0$, a contradiction. Then $\alpha_1 \neq 0$, and by multiplying $\phi$ by a suitable power of $\psi$ we may assume $\beta_1 = 0$. We want now to prove $\phi = 1$. Using the relations
for $1 \leq i \leq 3$, we readily obtain $\alpha_2 = \alpha_3 = \alpha_4 = 1$ and $\beta_2 = \beta_3 = \beta_4 = 0$. Applying $\varphi$ to the symmetry relations $[x_i, y_i] = [y_i, x_i]$, we get, for all $i, j$,

$$
\alpha_i \gamma_j = \alpha_j \gamma_i,
$$

(7)

Letting $i = 1, j \neq 1$ in the first equation of (7), we get $\alpha_1 \gamma_j = \gamma_1$; in particular $\gamma_1 = \alpha_1 \gamma_2$, and since also $\gamma_1 = 2 \alpha_1 \gamma_2$, as seen above, we get $\gamma_2 = 0$, and then $\gamma_j = 0$ for each $j$. Now the second equation of (7) gives, for suitable choices of $i, j, \delta_2 = \delta_3 = \delta_4, \delta_1 = \alpha_1 \delta_2$. Finally, applying $\varphi$ to $x'_2 = [x_1, x_3] + [x_1, y_3]$ we get $1 = \alpha_4 = \alpha_1 \alpha_3 = \alpha_1$ and $0 = \delta_3 - 1$ so that $\bar{\varphi} = 1$, as required.

We must still deal with the case $\dim(V_i) = 1$ for some $i$. Equation (6) then gives $\dim(V_i) = 1$ for all $i$. We may then choose $0 \neq v_i \in V_i, 1 \leq i \leq 4$, so that $V_i = \langle v_i \rangle$ and

$$
v_i = [v_1, v_2], \quad v_2 = [v_2, v_3], \quad v_3 = [v_3, v_4], \quad v_4 = \lambda [v_1, v_3]
$$

(8)

for some $0 \neq \lambda \in GF(p)$. However, no such $\{v_1, v_2, v_3, v_4\}$ exists. This can be proved in the following way.

We first solve the equation

$$
v^p = [v, w], \quad v, w \in V, v \neq 0.
$$

Calculations yield the following possibilities, up to scalar factors, and setting $U = \langle \bar{y}_i/j \leq 4 \rangle$:

$$
v \equiv \bar{x}_1 \pmod{U}, \quad w \equiv \bar{x}_2 \pmod{U}
$$

$$
v \equiv \bar{x}_2 \pmod{U}, \quad w \equiv \bar{x}_3 \pmod{U}
$$

$$
v \equiv \bar{x}_3 \pmod{U}, \quad w \equiv a \bar{x}_3 + \bar{x}_4 \pmod{U},
$$

(9)

for some $a \in GF(p), or v \subset U, w \notin U$.

Now consider what $v_1$ could be. If $v_1 \in U$, from the last equality in (8) it follows $v_4 \in U$: but this does not fit into (9). Thus we get $v_1 = \bar{x}_4 \pmod{U}$, and more detailed calculations, using the first three equalities of (8), give

$$
v_1 = \bar{x}_1 + b \bar{y}_1, \quad v_2 = \bar{x}_2 + b \bar{y}_2,
$$

$$
v_3 = \bar{x}_3 + b \bar{y}_3,
$$

$$
v_4 = a \bar{x}_3 + \bar{x}_4 + c \bar{y}_3 + b \bar{y}_4,
$$
for certain $a, b, c \in GF(p)$. Inserting these values into the last equality of (8), we get

$$v_4^2 = ax_4^2 + x_4^2 + cy_4^2 + by_4^2$$

$$= a[x_3, x_4] + [x_1, x_3] + 2c[x_3, y_4] + (1 + 2b)[x_1, y_3]$$

$$= \lambda[v_1, v_3] = \lambda[x_1, x_3] + 2\lambda b[x_1, y_3].$$

But then $\lambda = 1$ and $1 + 2b = 2b$, a contradiction.

ACKNOWLEDGMENTS

Part of this paper was written in Würzburg under CNR–NATO Grant 215.13/1. Lemma 3.1 and Proposition 3.2 are joint work with P. Legovini.

REFERENCES