Arch. Math. *Online First*

DOI 10.1007/s00013-008-2807-5

**Archiv der Mathematik**

# On automorphisms of A-groups

Martin R. Pettet

**Abstract.** Let $G$ be an $A$-group (i.e. a group in which $xx^\alpha = x^\alpha x$ for all $x \in G$, $\alpha \in \mathrm{Aut}(G)$) and let $A_{\mathcal{C}}(G)$ denote the subgroup of $\mathrm{Aut}(G)$ consisting of all automorphisms that leave invariant the centralizer of each element of $G$. The quotient $\mathrm{Aut}(G)/A_{\mathcal{C}}(G)$ is an elementary abelian 2-group and natural analogies exist to suggest that it might always be trivial. It is shown that, in fact, for any odd prime $p$ and any positive integer $r$, there exist infinitely many finite $pA$-groups $G$ for which $\mathrm{Aut}(G)/A_{\mathcal{C}}(G)$ has rank $r$.

**Mathematics Subject Classification (2000).** Primary 20D45; Secondary 20D15, 16Y30.

**Keywords.** $A$-group, graph, automorphism.

**1. Introduction.** For an (additively written) group $G$, let $M_0(G)$ be the near-ring of all identity-preserving maps from $G$ to itself (under pointwise addition and composition) and let $S$ be a semigroup (under composition) of endomorphisms of $G$. A problem that has attracted some interest among near-ring theorists is to characterize those $G$ for which the subnear-ring of $M_0(G)$ generated by $S$ is actually a ring. This is the case precisely when $x^\eta$ commutes with $x$ for all $x \in G$, $\eta \in S$ and so, despite its near-ring theoretic motivation, the question is essentially a group theoretic one.

If this commuting hypothesis holds for $S = \mathrm{Inn}(G)$, the group of inner automorphisms of $G$, then $G$ is a 2-Engel group. As follows from [4, 12.3.6], such groups are precisely those in which the centralizer of every element is invariant under $S$ (i.e. normal in $G$). If it holds for $S = \mathrm{End}(G)$, the semigroup of all endomorphisms of $G$, $G$ is said to be an $E$-group. Recently, it was shown [3, Theorem III.5] that finite $E$-groups are, again, precisely those in which each centralizer is invariant under $S$ (i.e. fully invariant in $G$). In view of these facts, the question was posed in [3] whether finite groups satisfying the commuting hypothesis with $S = \mathrm{Aut}(G)$

(i.e. $A$-groups) are precisely those in which all centralizers are characteristic. The purpose of this note is to provide a negative answer to this question.

Let $A_{\mathcal{C}}(G)$ denote the subgroup of $\mathrm{Aut}(G)$ consisting of those automorphisms of $G$ that leave invariant the centralizer $C_G(x)$ of each element $x$ of $G$. If $\mathrm{Aut}_c(G)$ denotes the group $C_{\mathrm{Aut}(G)}(G/Z(G))$ of *central* automorphisms of $G$, then

$$\mathrm{Aut}_c(G) \leq A_{\mathcal{C}}(G) = \bigcap_{x \in G} N_{\mathrm{Aut}(G)}(C_G(x)) \trianglelefteq \mathrm{Aut}(G).$$

For $G$ to be an $A$-group, it is clearly sufficient that $\mathrm{Aut}(G)/A_{\mathcal{C}}(G) = 1$. The question alluded to in the preceding paragraph is whether this condition is necessary.

If $G$ is an $A$-group and $\alpha \in \mathrm{Aut}(G)$, the equations $[x, x^\alpha] = [y, y^\alpha] = 1 = [xy, (xy)^\alpha]$ yield that $[x^\alpha, y] = [x, y^\alpha]$ for all $x, y \in G$. (See, for example, [1, Lemma 2.1] or [3, Lemma III.1].) It follows that if $y \in C_G(x)$ then $[x, y^{\alpha^2}] = [x^\alpha, y^\alpha] = [x, y]^\alpha = 1$ and so $y^{\alpha^2} \in C_G(x)$. Therefore, $\alpha^2 \in A_{\mathcal{C}}(G)$ for all $\alpha \in \mathrm{Aut}(G)$ and so the quotient $\mathrm{Aut}(G)/A_{\mathcal{C}}(G)$ is an elementary abelian 2-group. (See also [1, Lemma 2.4].) This represents the limit of what can be said in general about this quotient for, not only can $\mathrm{Aut}(G)/A_{\mathcal{C}}(G)$ be non-trivial, it can be of arbitrary rank.

**Theorem 1.1.** *Let $r$ be a positive integer and $p$ be an odd prime. Then there exist infinitely many finite $p$-groups $G$ such that $G$ is an $A$-group, $A_{\mathcal{C}}(G) = \mathrm{Aut}_c(G)$ and the elementary abelian 2-group $\mathrm{Aut}(G)/A_{\mathcal{C}}(G)$ has rank $r$.*

As mentioned above, if $G$ is an $E$-group, all centralizers are fully invariant and so $\mathrm{Aut}(G)/A_{\mathcal{C}}(G) = 1$. Thus, the theorem provides infinitely many examples of $A$-groups that are not $E$-groups, extending [3, Theorem III.6]. As in the earlier result, the argument is a variation of the graph theoretic approach developed by Heineken and Liebeck [2] and hinges on a determination of the centralizers in a $p$-group $G_{\hat{\Gamma}}$ whose presentation is encoded by a graph $\hat{\Gamma}$ (Proposition 3.2). In certain circumstances, $G_{\hat{\Gamma}}$ is an $A$-group with $|\mathrm{Aut}(G_{\hat{\Gamma}})/A_{\mathcal{C}}(G_{\hat{\Gamma}})| = 2$ and direct products of such groups furnish the examples that establish the theorem.

Except as motivation, near-ring theory plays no role in this note and so we shall write all groups multiplicatively.

**2. The prismoidal extension of a graph.** Let $\Gamma$ be a finite (undirected) graph with vertex set $V\Gamma$ and edge set $E\Gamma$. By the *prismoidal extension* $\hat{\Gamma}$ of $\Gamma$, we shall mean the graph obtained by taking an isomorphic copy $\Gamma^\alpha$ of $\Gamma$ (with graph isomorphism $\alpha : \Gamma \to \Gamma^\alpha$) and setting $V\hat{\Gamma} = V\Gamma \cup V\Gamma^\alpha$ and $E\hat{\Gamma} = E\Gamma \cup E\Gamma^\alpha \cup E^*$, where $E^* = \{\{x, x^\alpha\} : x \in V\Gamma\}$. (Alternatively, $\hat{\Gamma}$ may be described as the graph Cartesian product of $\Gamma$ with the Cayley graph of a cyclic group of order 2.)

We shall refer to the involutary automorphism of $\hat{\Gamma}$ induced by $\alpha$ (also denoted by $\alpha$) as the *prismoidal automorphism*. Extending the action of $\mathrm{Aut}(\Gamma)$ to $\hat{\Gamma}$ by defining $(x^\alpha)^\gamma = x^{\gamma\alpha}$ for all $x \in V\Gamma$ and $\gamma \in \mathrm{Aut}(\Gamma)$ allows the direct product $\mathrm{Aut}(\Gamma) \times \langle\alpha\rangle$ to be identified as a subgroup of $\mathrm{Aut}(\hat{\Gamma})$.

If $x \in V\Gamma$, denote by $N_\Gamma[x]$ (the *neighborhood* of $x$) the subset of $V\Gamma$ consisting of $x$ and all vertices adjacent to it (i.e. $N_\Gamma[x] = \{x\} \cup \{y \in V\Gamma : \{x,y\} \in E\Gamma\}$). Recall that the *girth* of $\Gamma$ is the length of the shortest irreducible cycle in $\Gamma$.

**Proposition 2.1.** *Let $\Gamma$ be a connected graph of girth at least 5 in which every vertex has valence at least 2. Then* $\mathrm{Aut}(\hat{\Gamma}) = \mathrm{Aut}(\Gamma) \times \langle\alpha\rangle$.

*Proof.* Note that under the hypotheses, $\hat{\Gamma}$ is connected with girth 4, any quadrilateral (ie. cycle of length 4) in $\hat{\Gamma}$ has one pair of opposite edges in $E^*$, and no two edges in $E^*$ share a common vertex.

Let $\beta \in \mathrm{Aut}(\hat{\Gamma})$ and let $x \in V\Gamma$. Let $y$ and $z$ be distinct vertices in $N_\Gamma[x]\backslash\{x\}$. Then the six vertices $\{y, x, z, z^\alpha, x^\alpha, y^\alpha\}$ define two quadrilaterals with a unique common edge $\{x, x^\alpha\} \in E^*$ and of course, the six images of these vertices under $\beta$ form a similar configuration. In the quadrilateral $\{y^\beta, x^\beta, x^{\alpha\beta}, y^{\alpha\beta}\}$, the pair of opposite edges $\{x^\beta, y^\beta\}$ and $\{x^{\alpha\beta}, y^{\alpha\beta}\}$ cannot lie in $E^*$ for if so, neither of the edges $\{x^\beta, z^\beta\}$ nor $\{x^\beta, x^{\alpha\beta}\}$ could (by virtue of sharing the vertex $x^\beta$ with $\{x^\beta, y^\beta\}$ ) lie in $E^*$ and so the quadrilateral $\{x^\beta, z^\beta, z^{\alpha\beta}, x^{\alpha\beta}\}$ would have no edges in $E^*$. It follows that the edge $\{x, x^\alpha\}^\beta = \{x^\beta, x^{\alpha\beta}\}$ lies in $E^*$ and so $x^{\alpha\beta} = x^{\beta\alpha}$. Since $x$ and $\beta$ were arbitrary, this proves that $E^*$ is invariant under $\mathrm{Aut}(\hat{\Gamma})$ and $\alpha \in Z(\mathrm{Aut}(\hat{\Gamma}))$.

Because $\Gamma$ is connected and $E^*$ is invariant under $\mathrm{Aut}(\hat{\Gamma})$, it follows that each element of $\mathrm{Aut}(\hat{\Gamma})$ either leaves the subgraphs $\Gamma$ and $\Gamma^\alpha$ invariant or it interchanges them. Therefore, $|\mathrm{Aut}(\hat{\Gamma}) : \mathrm{Aut}(\Gamma)| = 2$ and so $\mathrm{Aut}(\hat{\Gamma}) = \mathrm{Aut}(\Gamma) \times \langle\alpha\rangle$. □

**3. Groups defined by prismoidal extensions.** We continue to assume in this section that $\Gamma$ is a finite graph of girth at least 5 having no vertices of valence less than 2 (although connectedness is no longer needed). Let $V\Gamma = \{x_i : 1 \le i \le v\}$ and let $\hat{\Gamma}$ and $\alpha$ be, respectively, the prismoidal extension of $\Gamma$ and the prismoidal automorphism, as defined in Section 2. The symbols $i^\alpha$, $1 \le i \le v$, will be used as subscripts for the vertices of $\Gamma^\alpha$ so that $x_{i^\alpha} = x_i^\alpha$ and $x_{i^\alpha}^\alpha = x_i$. However, when there is no chance of ambiguity, we will occasionally use $x_i$ (with the range of $i$ unspecified) to denote any vertex of $\hat{\Gamma}$.

Let $F = F(V\hat{\Gamma})$ be the free group on $V\hat{\Gamma}$ so $\alpha$ induces an automorphism of order 2 (still to be denoted by $\alpha$) of $F$. For each $x_i \in V\Gamma$, let $\omega_i$ be an element of $F'$ (to be defined more explicitly later) and let $\omega_{i^\alpha} = \omega_i^\alpha$.

For an odd prime $p$ and a particular choice of the $\omega_i$'s, define the group $G_{\hat{\Gamma}} = \langle V\hat{\Gamma} : R\rangle = F/R^F$ where $R \subseteq F$ consists of the following relators:

$$(3.1) \quad \begin{cases} \text{(i) } [[x_i, x_j], x_k] \text{ for all } x_i, x_j, x_k \in V\hat{\Gamma} \\ \text{(ii) } \omega_i^{-1} x_i^p \text{ and } \omega_{i^\alpha}^{-1} x_{i^\alpha}^p \text{ for } 1 \le i \le v \\ \text{(iii) } [x_i, x_j] \text{ and } [x_{i^\alpha}, x_{j^\alpha}] \text{ if } 1 \le i < j \le v \text{ and } \{x_i, x_j\} \in E\Gamma \\ \text{(iv) } [x_i, x_j]^{-1}[x_{i^\alpha}, x_{j^\alpha}] \text{ and } [x_i, x_{j^\alpha}]^{-1}[x_{i^\alpha}, x_j] \text{ for } 1 \le i < j \le v \end{cases}$$

Let $G = G_{\hat{\Gamma}}$. We may identify $V\hat{\Gamma}$ with the set of generators $\{x_i R^F : x_i \in V\hat{\Gamma}\}$ of $G$, and in fact, when it is clear that we are referring to elements of $G$, we shall denote the generator $x_i R^F$ by $x_i$ and $\omega_i R^F$ by $\omega_i$.

By (i) and (ii) of (3.1), $G^p \leq G' \leq Z(G)$ and so both the power map $x \mapsto x^p$ and (for fixed $g \in G$) the maps $x \mapsto [x, g]$ and $x \mapsto [g, x]$ are endomorphisms of $G$. Both $G'$ and $G/G'$ are elementary abelian $p$-groups and so, may be regarded as (multiplicatively-written) vector spaces over the finite field $GF(p)$.

Let $H_\Gamma = \langle x_i : \ x_i \in V\Gamma\rangle$ (so $G = \langle H_\Gamma, (H_\Gamma)^\alpha\rangle$ and $H_\Gamma \cap (H_\Gamma)^\alpha = 1$). Let $B_\Gamma = \{[x_i, x_j] : 1 \leq i < j \leq v,\ \{x_i, x_j\} \notin E\Gamma\}$ and $B_0 = \{[x_i, x_{j^\alpha}] : 1 \leq i < j \leq v\}$ so $B_\Gamma$ is a basis for $H'_\Gamma$ and $B_\Gamma \cup B_0$ is a basis for $G'_{\hat{\Gamma}} = G'$. Because $R \cup R^{-1}$ is $\alpha$-invariant, $\alpha$ induces an automorphism of order 2 (again denoted by $\alpha$) of $G$ with $G' \leq C_G(\alpha)$ (by (3.1(iv)). Also, $[x, y^\alpha] = [x, y^\alpha]^\alpha = [x^\alpha, y^{\alpha^2}] = [x^\alpha, y]$ for all $x, y \in G$ and so $[x, x^\alpha] = [x^\alpha, x] = [x, x^\alpha]^{-1}$. Since $p > 2$, $[x, x^\alpha] = 1$ for all $x \in G$.

**Definition 3.1.** If $x \in G = G_{\hat{\Gamma}}$ and $x \equiv \prod_{i=1}^v x_i^{e_i} \prod_{i=1}^v x_{i^\alpha}^{e_{i^\alpha}} \mod G'$ where $e_i, e_{i^\alpha} \in GF(p)$, then *supp*$(x)$ (the *support* of $x$) denotes the set

$$\{x_i \in V\Gamma : e_i \neq 0\} \cup \{x_{i^\alpha} \in V\Gamma^\alpha : e_{i^\alpha} \neq 0\}.$$

The key to Theorem 1.1 is the following technical proposition that severely restricts the possibilities for the order of the centralizer of an element of $G_{\hat{\Gamma}}$:

**Proposition 3.2.** *Assume that $\Gamma$ is a graph of girth at least 5 such that every vertex of $\Gamma$ has valence at least 2. Let $V\Gamma = \{x_i : 1 \leq i \leq v\}$ and for $1 \leq i \leq v$, let $\delta_i$ be the valence of $x_i$ in $\Gamma$. Let $G = G_{\hat{\Gamma}}$ and $\bar{G} = G/G'$ and suppose that $\bar{1} \neq \bar{a} \in \bar{G}$.*

(a) *If $\bar{a} \in [\bar{G}, \alpha] \cup C_{\bar{G}}(\alpha)$ then $|C_G(a) : G'| = p^{v+1}$.*
(b) *If $\bar{a} \notin [\bar{G}, \alpha] \cup C_{\bar{G}}(\alpha)$ then $|C_G(a) : G'| \leq p^3$ unless $\bar{a} \in \langle \bar{x}_i, \bar{x}_i^\alpha\rangle$ for some $x_i \in V\Gamma$, in which case $|C_G(a) : G'| = p^{\delta_i+2}$.*
(c) $3 < \delta_i + 2 < v + 1$ *for all $i$, $1 \leq i \leq v$.*

*Proof.* Let $\bar{1} \neq \bar{a} \in \bar{G}$ so $a \equiv u_a v_a \not\equiv 1 \mod G'$, where $u_a = \prod_{k=1}^v x_k^{a_k} \in H_\Gamma$ and $v_a = \prod_{k=1}^v x_{k^\alpha}^{a_{k^\alpha}} \in H_\Gamma^\alpha$ with $a_k, a_{k^\alpha} \in GF(p)$ for $1 \leq k \leq v$. Replacing $a$ by $a^\alpha$ if necessary, we may assume that $u_a \not\equiv 1 \mod G'$ (i.e. *supp*$(a) \cap V\Gamma \neq \emptyset$).

Let $z \in C_G(a)$ so $z \equiv u_z v_z \mod G'$, where $u_z = \prod_{k=1}^v x_k^{z_k} \in H_\Gamma$ and $v_z = \prod_{k=1}^v x_{k^\alpha}^{z_{k^\alpha}} \in H_\Gamma^\alpha$ with $z_k, z_{k^\alpha} \in GF(p)$ for $1 \leq k \leq v$.

For any $x_i, x_j \in V\hat{\Gamma}$, $[x_i, x_j] = [x_{i^\alpha}, x_{j^\alpha}] = [x_j, x_i]^{-1} = [x_{j^\alpha}, x_{i^\alpha}]^{-1}$ and if $\{x_i . x_j\} \notin E\hat{\Gamma}$ (i.e. $[x_i, x_j] \neq 1$), then one of these four elements lies in the basis $B_\Gamma \cup B_0$ of $G'$. Because $1 = [a, z] = \prod_{x_i, x_j \in V\hat{\Gamma}} [x_i, x_j]^{a_i z_j}$, expressing this product in terms of $B_\Gamma \cup B_0$ yields that if $\{x_i, x_j\} \notin E\hat{\Gamma}$, then $a_i z_j + a_{i^\alpha} z_{j^\alpha} - a_j z_i - a_{j^\alpha} z_{i^\alpha} = 0$. This equation holds vacuously if $\{x_i, x_j\} \in E^*$ (i.e. if $j = i^\alpha$) and so

$$a_i z_j + a_{i^\alpha} z_{j^\alpha} = a_j z_i + a_{j^\alpha} z_{i^\alpha} \text{ if } \{x_i, x_j\} \notin E\Gamma \cup E\Gamma^\alpha. \tag{3.2}$$

**Case 1:** $\bar{a} \notin \langle \bar{u}_a, \bar{u}_a^{\alpha} \rangle$

Let $x_i \in supp(a) \cap V\Gamma$ (so $a_i \neq 0$) and let $m = a_{i^\alpha}/a_i$. Then $a_{j^\alpha}/a_j \neq m$ for some $j$ such that $1 \leq j \leq v$ (for otherwise, $\bar{a} = \bar{u}_a \bar{u}_a^{m\alpha} \in \langle \bar{u_a}, \bar{u_a}^{\alpha} \rangle$) and so, if $d_{i,j} = \det \begin{pmatrix} a_i & a_{i^\alpha} \\ a_j & a_{j^\alpha} \end{pmatrix}$, then $d_{i,j} \neq 0$.

If $1 \leq k \leq v$ then certainly none of the pairs $\{x_i, x_{k^\alpha}\}, \{x_j, x_{k^\alpha}\}$ or $\{x_i, x_{j^\alpha}\}$ lies in $E\Gamma \cup E\Gamma^\alpha$ and so by (3.2),

(a) $a_i z_{k^\alpha} + a_{i^\alpha} z_k = a_{k^\alpha} z_i + a_k z_{i^\alpha}$
(b) $a_j z_{k^\alpha} + a_{j^\alpha} z_k = a_{k^\alpha} z_j + a_k z_{j^\alpha}$ and
(c) $a_i z_{j^\alpha} + a_{i^\alpha} z_j = a_{j^\alpha} z_i + a_j z_{i^\alpha}$.

From (a) and (b), $\begin{pmatrix} a_i & a_{i^\alpha} \\ a_j & a_{j^\alpha} \end{pmatrix} \begin{pmatrix} z_{k^\alpha} \\ z_k \end{pmatrix} = \begin{pmatrix} z_i & z_{i^\alpha} \\ z_j & z_{j^\alpha} \end{pmatrix} \begin{pmatrix} a_{k^\alpha} \\ a_k \end{pmatrix}$ and so

$$\begin{pmatrix} z_{k^\alpha} \\ z_k \end{pmatrix} = \begin{pmatrix} a_i & a_{i^\alpha} \\ a_j & a_{j^\alpha} \end{pmatrix}^{-1} \begin{pmatrix} z_i & z_{i^\alpha} \\ z_j & z_{j^\alpha} \end{pmatrix} \begin{pmatrix} a_{k^\alpha} \\ a_k \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} a_{k^\alpha} \\ a_k \end{pmatrix},$$

where $A = (1/d_{i,j})(a_{j^\alpha} z_i - a_{i^\alpha} z_j)$ and $D = (1/d_{i,j})(-a_j z_{i^\alpha} + a_i z_{j^\alpha})$ But by (c), $A = D$ and so $z_{k^\alpha} = A a_{k^\alpha} + B a_k$ and $z_k = C a_{k^\alpha} + A a_k$. Thus, if $1 \leq k \leq v$, then $x_k^{z_k} = x_k^{C a_{k^\alpha} + A a_k} \equiv (x_k^{a_k})^A (x_{k^\alpha}^{a_{k^\alpha}})^{\alpha C} \mod G'$ and $x_{k^\alpha}^{z_{k^\alpha}} = x_{k^\alpha}^{A a_{k^\alpha} + B a_k} \equiv (x_k^{a_k})^{\alpha B} (x_{k^\alpha}^{a_{k^\alpha}})^A \mod G'$. Therefore, $z \equiv u_a^A v_a^{\alpha C} u_a^{\alpha B} v_a^A \equiv a^A u_a^{\alpha B} v_a^{\alpha C} \mod G'$ and so $z \in \langle a, u_a^\alpha, v_a^\alpha \rangle G'$. Since $z$ was chosen arbitrarily in $C_G(a)$, it follows that $C_G(a) \leq \langle a, u_a^\alpha, v_a^\alpha \rangle G'$ and so $|C_G(a) : G'| \leq p^3$. (Indeed, if $\{x_i, x_j\} \notin E\Gamma \cup E\Gamma^\alpha$, then additionally, $B = C$ and so $C_G(a) \leq \langle a, a^\alpha \rangle G'$ and $|C_G(a) : G'| \leq p^2$.)

**Case 2:** $\bar{a} \in \langle \bar{u}_a, \bar{u}_a^{\alpha} \rangle$

In this case, $\bar{a} = \bar{u}_a^l \bar{u}_a^{m\alpha}$ for some $l, m \in GF(p)$. Because we assumed that $supp(a) \cap V\Gamma \neq \emptyset$, $l \neq 0$ and so if $r = l^{-1} \in GF(p)$, $\bar{a}^r = \bar{u}_a \bar{u}_a^{mr\alpha}$. Since $|C_G(a)| = |C_G(a^r)|$, we may assume that $l = 1$, whence $\bar{a} = \bar{u}_a \bar{u}_a{}^{m\alpha}$.

Before proceeding with this case, we note the following:

**Lemma 3.3.** *Let $u, z \in G$.*

(a) $[uu^{m\alpha}, z] = [u, zz^{m\alpha}]$ *and in particular, $z \in C_G(uu^{m\alpha})$ if and only if $zz^{m\alpha} \in C_G(u)$.*
(b) $[z^{-1} z^{m\alpha}, uu^{m\alpha}] = [z, u]^{m^2 - 1}$ *and in particular, if $m \neq \pm 1$ then $z \in C_G(u)$ if and only if $z^{-1} z^{m\alpha} \in C_G(uu^{m\alpha})$.*
(c) *If $m \neq \pm 1$, the maps $C_G(uu^{m\alpha}) \to C_G(u)$ and $C_G(u) \to C_G(uu^{m\alpha})$ defined by $x \mapsto xx^{m\alpha}$ and $x \mapsto x^{-1} x^{m\alpha}$, respectively, are each bijective and so $|C_G(uu^{m\alpha})| = |C_G(u)|$.*

*Proof.* Using the fact that for any $g \in G$, the maps $x \mapsto [x, g]$ and $x \mapsto [g, x]$ are endomorphisms, statement (a) follows from the computation

$$[uu^{m\alpha}, z] = [u, z][u^\alpha, z]^m = [u, z][u, z^\alpha]^m = [u, zz^{m\alpha}]$$

and (b) follows from

$$[z^{-1}z^{m\alpha}, uu^{m\alpha}] = [z,u]^{-1}[z,u^{\alpha}]^{-m}[z^{\alpha},u]^{m}[z^{\alpha},u^{\alpha}]^{m^2} = [z,u]^{m^2-1}.$$

Because $xx^{\alpha} = x^{\alpha}x$ for all $x \in G$, the set $\{a + b\alpha : \ a, b \in GF(p)\} \subseteq M_0(G)$ is a ring in which $(1+m\alpha)(1-m\alpha) = 1-m^2 = (1-m\alpha)(1+m\alpha)$. Since $1-m^2 \neq 0$, the power map $x \mapsto x^{1-m^2}$ is bijective and so the maps $1 - m\alpha$ and $1 + m\alpha$ are also bijective. This proves (c). $\square$

Observe that by statement (c) of the lemma, if $m \neq \pm 1$ then $|C_G(a)| = |C_G(u_a u_a^{m\alpha})| = |C_G(u_a)|$ and so in this case, we may assume that $a = u_a$ (i.e. $m = 0$ and $\emptyset \neq supp(a) \subseteq V\Gamma$). Thus, Case 2 splits into two subcases.

**Case 2a:** $m = 0$

In this case, if $1 \leq i, j \leq v$ then, because $a_{i^{\alpha}} = 0 = a_{j^{\alpha}}$ and $\{x_i, x_{j^{\alpha}}\} \notin E\Gamma \cup E\Gamma^{\alpha}$, (3.2) yields that $a_i z_{j^{\alpha}} = a_j z_{i^{\alpha}}$. Moreover, if $\{x_i, x_j\} \notin E\Gamma$ then $a_i z_j = a_j z_i$.

Let $x_i \in supp(a)$. Then if $s = z_{i^{\alpha}}/a_i \in GF(p)$, $z_{j^{\alpha}} = sa_j$ for all $j$, $1 \leq j \leq v$, whence, $v_z = \prod_{i=1}^{v} x_{i^{\alpha}}^{sa_i} \equiv (u_a^{\alpha})^s \equiv (a^{\alpha})^s \mod G'$. Next we consider the possibilities for $u_z$.

Suppose first that $|supp(a)| \geq 2$ and let $V_a = \langle \bigcap_{x_j \in supp(a)} N_{\Gamma}[x_j] \rangle$ (so $V_a \subseteq C_G(a)$). Because $|supp(a)| \geq 2$, the non-existence of quadrilaterals in $\Gamma$ implies that $|V_a| \leq p$. We claim now that there is a constant $r$ such that for every $x_k \in supp(z)$, either $z_k = ra_k$ or $x_k \in V_a$. It will follow then that $u_z \in a^r V_a$.

Note that if $x_k \in supp(z) \backslash supp(a)$ (so $a_k = 0$) then $x_k \in V_a$, for otherwise $\{x_j, x_k\} \notin E\Gamma$ for some $x_j \in supp(a)$ and so $a_j z_k = a_k z_j = 0$, contradicting $a_j \neq 0 \neq z_k$. Thus, it suffices to prove the claim for $x_k \in supp(z) \cap supp(a)$.

Let $\Delta$ be the graph complement in $\Gamma$ of the subgraph spanned by $supp(a)$ (so $V\Delta = supp(a)$ and if $x_i, x_j \in V\Delta$, $\{x_i, x_j\} \in E\Delta$ if and only if $\{x_i, x_j\} \notin E\Gamma$).

If $\{x_i, x_j\} \in E\Delta$, then $\{x_i, x_j\} \notin E\Gamma$ and so $a_i z_j = a_j z_i$, whence, $z_i/a_i = z_j/a_j$. If $\Delta$ is connected, then for some $r \in GF(p)$, $z_k = ra_k$ for all $x_k \in supp(a)$ and the claim is proved. Suppose that $\Delta$ is not connected. Because $\Gamma$ contains no triangles, $\Delta$ has two connected components. Moreover, because $\Gamma$ contains no quadrilaterals, one component consists of a single vertex, say $x_i$. Because $supp(a) \backslash \{x_i\}$ is contained in a connected component of $\Delta$, there is an $r \in GF(p)$ such that for any $x_k \in supp(a) \backslash \{x_i\}$, $z_k = ra_k$. Also $\{x_i, x_j\} \in E\Gamma$ for any $x_j \in supp(a) \backslash \{x_i\}$ (since $\{x_i, x_j\} \notin E\Delta$) and so $x_i \in V_a$. This proves the claim.

Therefore, if $|supp(a)| \geq 2$ then $u_z \in a^r V_a$ and so $z \equiv u_z v_z \equiv a^r (a^{\alpha})^s \mod V_a G'$. Hence, $C_G(a) \leq \langle a, a^{\alpha}, V_a \rangle G'$ and $|C_G(a) : G'| \leq p^3$.

Next, suppose that $|supp(a)| = 1$ so $supp(a) = \{x_i\}$ for some $i$, $1 \leq i \leq n$. For purposes of computing $|C_G(a) : G'|$, we may assume that $a_i = 1$ and so $\bar{a} = \bar{x_i}$. In this case, if $1 \leq j \leq v$ with $j \neq i$, $\{x_i, x_{j^{\alpha}}\} \notin E\hat{\Gamma}$ and so $z_{j^{\alpha}} = a_i z_{j^{\alpha}} = a_j z_{i^{\alpha}} = 0$.

Therefore, $supp(z) \cap V\Gamma^{\alpha} \subseteq \{x_{i^{\alpha}}\} \subseteq N_{\hat{\Gamma}}[x_i]$. Moreover, if $x_j \notin N_{\hat{\Gamma}}[x_i]$ (so $\{x_i, x_j\} \notin E\Gamma$) then because $a_j = 0$, $z_j = a_i z_j = a_j z_i = 0$. Hence, $supp(z) \cap V\Gamma \subseteq N_{\hat{\Gamma}}[x_i]$. Therefore, $supp(z) \subseteq N_{\hat{\Gamma}}[x_i]$ and so $C_G(a) = C_G(x_i) = \langle N_{\hat{\Gamma}}[x_i]\rangle G'$. In particular, if $x_i$ has valence $\delta_i$ in $\Gamma$ (so $|N_{\hat{\Gamma}}[x_i]| = \delta_i + 2$), then $|C_G(x_i) : G'| = p^{\delta_i+2}$.

**Case 2b:** $m = \pm 1$

This is the case precisely when $\bar{a} \in [\bar{G}, \alpha] \cup C_{\bar{G}}(\alpha)$ or equivalently, when $\langle \bar{a} \rangle$ is $\alpha$-invariant. Let $G_m = \langle x_i x_i^{m\alpha} : 1 \leq i \leq v\rangle G'$ where $m = \pm 1$. Then $G_{-1}/G' = [\bar{G}, \alpha]$ and $G_1/G' = C_{\bar{G}}(\alpha)$ and so (since $p > 2$), $G = G_{-1}G_1$ and $G_{-1} \cap G_1 = G'$. Also, the map $x \mapsto xx^{m\alpha}$ induces an isomorphism from $H_\Gamma G'/G'$ to $G_m/G'$ and so $|G_{-1} : G'| = |G_1 : G'| = |H_\Gamma G'/G'| = p^v$.

Since $m^2 = 1$, Lemma 3.3 (b) implies that $[G_{-1}, G_1] = 1$ and so, since $\bar{a} \in \bar{G}_m$, $G_{-m} \leq C_G(a)$. Therefore, $C_G(a) = G_{-m}G_m \cap C_G(a) = G_{-m}(G_m \cap C_G(a))$.

If $g \in G_m$, $g^{\alpha} \equiv g^m \mod G'$, whence, $g \equiv g^{m\alpha} \mod G'$and so $[a, g] = [u_a, g]$ $[u_a^{m\alpha}, g^{m\alpha}] = [u_a, g]^2$. Since $p > 2$, it follows that $G_m \cap C_G(a) = G_m \cap C_G(u_a)$ and so $C_G(a) = G_{-m}(G_m \cap C_G(u_a))$. We claim now that $G_m \cap C_G(u_a) = G'\langle a\rangle$.

By Case 2a, if $|supp(u_a)| \geq 2$ then $C_G(u_a) = \langle u_a, u_a^{\alpha}, V_a\rangle G' = \langle a, u_a, V_a\rangle G' = \langle u_a, V_a\rangle G'\langle a\rangle \leq H_\Gamma G'\langle a\rangle$ whereas, if $supp(u_a) = \{x_i\} \subseteq V\Gamma$, then $C_G(u_a) = C_G(x_i) = \langle N_{\hat{\Gamma}}[x_i]\rangle G' = \langle x_i x_i^{m\alpha}, N_\Gamma[x_i]\rangle G' = \langle N_\Gamma[x_i]\rangle G'\langle a\rangle \leq H_\Gamma G'\langle a\rangle$. In either case, since $G_m \cap H_\Gamma = 1$, $G_m \cap C_G(u_a) \leq G_m \cap H_\Gamma G'\langle a\rangle = G'\langle a\rangle \leq G_m \cap C_G(u_a)$, as claimed.

It follows that $C_G(a) = G_{-m}G'\langle a\rangle$ so $|C_G(a) : G'| = p|G_{-m} : G'| = p^{v+1}$. This completes the proof of statements (a) and (b) of the proposition.

Finally, statement (c) of the proposition follows easily from the hypotheses that $\delta_i \geq 2$ for all $i$, $1 \leq i \leq v$, and that $\Gamma$ has girth at least 5. □

For our purposes, it is unfortunate that (by Lemma 3.3 (c)) the *order* of its centralizer is not sufficient to distinguish a canonical generator $x_i \in V\hat{\Gamma}$ of $G$ from an element of the form $x_i x_i^{m\alpha}$, $m \neq \pm 1$. However, by a more judicious choice of the elements $\omega_i$ introduced in the presentation of $G_{\hat{\Gamma}}$, we can at least ensure that these two types of elements have non-isomorphic centralizers.

**Corollary 3.4.** *Assume the hypotheses of Proposition 3.2. Assume additionally that for each $k$, $1 \leq k \leq v$, the element $\omega_k \in F(V\hat{\Gamma})$ in the presentation (3.1) is a commutator $[x_r, x_s]$, where $x_r$ and $x_s$ are distinct elements of $N_\Gamma[x_k]\backslash\{x_k\}$, and that $\omega_{k^{\alpha}} = \omega_k^{\alpha}$. If $a \in G$ such that $C_G(a) \cong C_G(x_j)$ for some $x_j \in V\hat{\Gamma}$ then there exists a unique $x_i \in V\hat{\Gamma}$ such that $\langle aG'\rangle = \langle x_i G'\rangle$.*

*Proof.* The uniqueness statement is clear. So assume that $C_G(a) \cong C_G(x_j)$ for some $x_j \in V\hat{\Gamma}$. It follows from Proposition 3.2 that $\langle aG'\rangle = \langle x_i^l x_i^{m\alpha} G'\rangle$ for some $x_i \in V\hat{\Gamma}$ and $l, m \in GF(p)$, $l \neq \pm m$. If $l = 0$, $\langle aG'\rangle = \langle x_{i^{\alpha}} G'\rangle$ and we are done. If $l \neq 0$, we may assume that $l = 1$ (so $m \neq \pm 1$) and it remains to prove that $m = 0$.

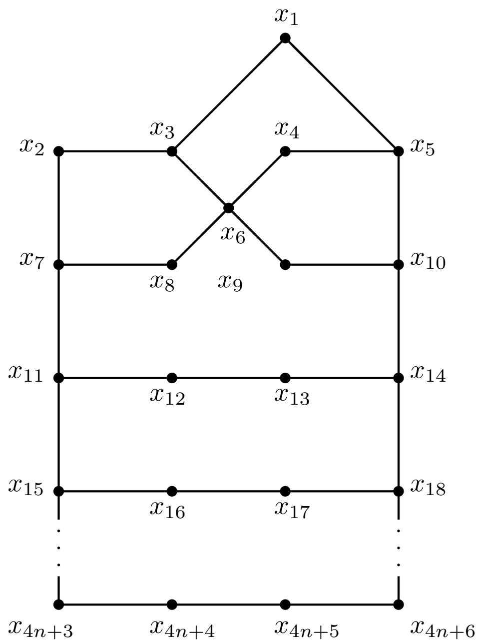


Figure 1. The graph $\Gamma_n$

Let $C_j = C_G(x_j)$ and $D_i = C_G(x_i x_i^{m\alpha})$ so $C_j \cong C_G(a) \cong D_i$. Regarding $\omega_j$ as an element of $G$, $1 \neq \omega_j = x_j^p \in C_j' \cap C_j^p$ and so $D_i' \cap D_i^p \neq 1$.

By Lemma 3.3(c), the map $C_i \to D_i$, $x \mapsto x^{-1}x^{m\alpha}$ is bijective and so it induces an isomorphism $C_i/G' \to D_i/G'$. Hence, $D_i = \langle x_l^{-1}x_l^{m\alpha} : x_l \in N_{\hat{\Gamma}}[x_i]\rangle G'$. It follows that $D_i' = \langle u_{r,s} : x_r, x_s \in N_{\hat{\Gamma}}[x_i]\rangle$ where $u_{r,s} = [x_r^{-1}x_r^{m\alpha}, x_s^{-1}x_s^{m\alpha}] = [x_r, x_s]^{1+m^2}[x_r, x_s^{\alpha}]^{-2m}$. Since $D_i' \cap D_i^p \neq 1$, some non-trivial product $\Pi_{r,s}\, u_{t,s}^{n_{r,s}}$ lies in $D_i^p$. But then $\Pi_{r,s}[x_r, x_s^{\alpha}]^{-2m})^{n_{r,s}} \in \langle B_\Gamma\rangle$, whence, because $B_\Gamma \cup B_0$ is linearly independent over $GF(p)$, each $mn_{r,s} = 0$ and so $m = 0$. □

**4. Proof of Theorem 1.1.** We consider the nested family of graphs $\Gamma_n$, $n \geq 1$, indicated in Figure 1. (The first of these, $\Gamma_1$, was used in the proof of [3, Theorem III.6].) Each $\Gamma_n$ has girth 5 and all vertices have valence 2, 3 or 4. In addition, each $\Gamma_n$ has trivial automorphism group. (As the unique vertex of valence 4, $x_6$ is fixed by every element of $\mathrm{Aut}(\Gamma_n)$, from which it is easily seen that $\mathrm{Aut}(\Gamma_1) = 1$. As the subgraph spanned by the vertices of $\Gamma_n$ that lie at most two edges away from $x_6$, $\Gamma_1$ is invariant under (and hence, fixed by) $\mathrm{Aut}(\Gamma_n)$ and the triviality of $\mathrm{Aut}(\Gamma_n)$ follows by induction on $n$.) Note that $|V\Gamma_n| = 4n + 6$.

Fix an odd prime $p$ and an integer $n \geq 1$ and let $\Gamma = \Gamma_n$. Let $\hat{\Gamma}$ and $\alpha$ be, respectively, the corresponding prismoidal extension of $\Gamma$ and the prismoidal automorphism, as defined in Section 2. We begin by defining explicitly the elements $\omega_i$ in the presentation (3.1) of the corresponding group $G_{\hat{\Gamma}}$, making use of a decomposition of $\Gamma$ into oriented paths and cycles.

Observe that $\Gamma$ may be expressed as $\bigcup_{i=1}^{k+2} \Lambda_i$ where $\Lambda_1$ is the oriented cycle $(x_6, x_3, x_2, x_7, x_8)$ of length 5, $\Lambda_2$ is the oriented cycle $(x_6, x_9, x_{10}, x_5, x_4)$ of length 5, $\Lambda_3$ is the oriented path $(x_3, x_1, x_5)$ of length 2 and for $i \geq 4$, $\Lambda_i$ is the oriented path $(x_{4i-9}, x_{4i-5}, x_{4i-4}, x_{4i-3}, x_{4i-2}, x_{4i-6})$ of length 5.

If $x \in V\Gamma$, let $m$ be minimal such that $x \in V\Lambda_m$. Then $x$ is not one of the ends of $\Lambda_m$ (since, if $\Lambda_m$ is not a cycle, its end vertices lie in $\Lambda_{m-1}$) and so we may define $x^\sigma$ and $x^\tau$ to be, respectively, the vertices immediately preceding and succeeding $x$ in $\Lambda_m$. (So, for example, $x_1^\sigma = x_3$, $x_1^\tau = x_5$, $x_2^\sigma = x_3$, $x_2^\tau = x_7$ etc.) The functions $\sigma$ and $\tau$ extend to $\hat{\Gamma}$ via $(x^\alpha)^\sigma = (x^\sigma)^\alpha$ and $(x^\alpha)^\tau = (x^\tau)^\alpha$. For each $x_i \in V\hat{\Gamma}$, we now define $\omega_i = [x_i^\sigma, x_i^\tau]$ (whence, $\omega_{i^\alpha} = \omega_i^\alpha$). (Of course, this explicit definition of the $\omega_i$'s is consistent with the hypotheses of Corollary 3.4.)

Finally, we construct the groups postulated by Theorem 1.1.

Let $p$ be an odd prime and let $r$ be a positive integer. Let $c$ be an integer such that $c > 5r+4$ and $c \equiv 1 \mod 4$. For $1 \leq k \leq r$, let $v_k = c^k+1$ (so $v_k \equiv 2 \mod 4$) and let $n_k = (v_k - 6)/4 \in \mathbb{Z}$. (Thus, $|V\Gamma_{n_k}| = 4n_k + 6 = v_k$.) Let $G_k = G_{\hat{\Gamma}_{n_k}}$ be the corresponding $p$-group (as defined by (3.1) with the $\omega_i$'s as specified above) and let $G = G_1 \times G_2 \times \ldots \times G_r$.

**Lemma 4.1.** *For each $k$, $1 \leq k \leq r$, $G'G_k$ is a characteristic subgroup of $G$.*

*Proof.* Let $1 \leq k \leq r$ and let $x \in V\Gamma_{n_k}$. By Proposition 3.2, $|C_{G_k}(x) : G_k'| = p^{\delta_x+2}$ and so $|x^G| = |G_k : G_k'|/|C_{G_k}(x) : G_k'| = p^{2v_k-\delta_x-2} = p^{2c^k-\delta_x}$, where $\delta_x$ is the valence of $x$ in $\Gamma_{n_k}$ (so $2 \leq \delta_x \leq 4$). Because $G_k = \langle V\hat{\Gamma}_{n_k}\rangle$, it suffices to show that the elements of $G$ with precisely $p^{2c^k-\delta_x}$ conjugates all lie in $G'G_k$.

Suppose that $y = (y_1, \ldots, y_r) \in G$ (with each $y_i \in G_i$) such that $|x^G| = |y^G|$. Proposition 3.2 implies that $|y_j^G| = |y_j^{G_j}| = |G_j : G_j'|/|C_{G_j}(y_j) : G_j'| = p^{\eta_j v_j-\epsilon_j}$, where either $1 \leq \eta_j \leq 2$ and $1 \leq \epsilon_j \leq 6$ or (if $y_j \in G_j'$) $\eta_j = \epsilon_j = 0$. Since $|y^G| = |y_1^G| \ldots |y_r^G|$, $\log_p |y^G| = \sum_{j=1}^r(\eta_j v_j - \epsilon_j) = \sum_{j=1}^r \eta_j c^j + \sum_{j=1}^r(\eta_j - \epsilon_j)$. Equating this with $\log_p |x^G|$ yields that $\delta_x+\sum_{j=1}^r(\eta_j-\epsilon_j) = 2c^k-\sum_{j=1}^r \eta_j c^j$ and so $c$ divides $\delta_x+\sum_{j=1}^r(\eta_j-\epsilon_j)$. However, $|\delta_x+\sum_{j=1}^r(\eta_j-\epsilon_j)| \leq |\delta_x|+\sum_{j=1}^r |\eta_j-\epsilon_j| \leq 4+5r < c$ and so $2c^k - \sum_{j=1}^r \eta_j c^j = 0$. Since $0 \leq \eta_j \leq 2 < c$ for all $j$, it follows that $\eta_k = 2$ and $\eta_j = 0$ for all $j \neq k$. Therefore, $y_j \in G'$ for all $j \neq k$ and so $y \in G'G_k$. $\square$

For $1 \leq k \leq r$, let $\alpha_k$ denote the prismoidal automorphism of $\hat{\Gamma}_{n_k}$ and also the corresponding involutory automorphisms of $G_k$ and of $G$. By Proposition 1, $\mathrm{Aut}(\hat{\Gamma}_{n_k}) = \langle\alpha_k\rangle$. Let $E = \langle\alpha_1, \alpha_2, \ldots, \alpha_r\rangle \leq \mathrm{Aut}(G)$, so $E$ is an elementary abelian 2-subgroup of rank $r$. We shall prove that $G$ is an $A$-group, that $A_{\mathcal{C}}(G) = \mathrm{Aut}_c(G)$ and that $\mathrm{Aut}(G)$ is a semidirect product of $E$ with $A_{\mathcal{C}}(G)$.

Suppose that $\beta \in \mathrm{Aut}(G)$ and let $1 \leq k \leq r$. By Lemma 4.1, if $a \in G_k$, $a^\beta \in bG'$ for some $b \in G_k$. If $H_k = \prod_{j \neq k} G'_j$, then $G' = H_k \times G'_k$ and so $H_k \times C_{G_k}(a) = C_{G'G_k}(a) \cong C_{G'G_k}(a^\beta) = C_{G'G_k}(b) = H_k \times C_{G_k}(b)$. Therefore, $C_{G_k}(a) \cong C_{G_k}(b)$.

It follows from Corollary 3.4 that there is a permutation $\theta_k$ of $V\hat{\Gamma}_{n_k}$ such that for any $x \in V\hat{\Gamma}_{n_k}$, $\langle x^\beta G'_k \rangle = \langle x^{\theta_k} G'_k \rangle$ and so, for each such $x$ there is a $c_x \in GF(p) \backslash \{0\}$ such that $x^\beta \equiv (x^{\theta_k})^{c_x} \mod G'_k$. In fact, $\theta_k \in \mathrm{Aut}(\hat{\Gamma}_{n_k}) = \langle \alpha_k \rangle \leq E$ because if $\{x, y\} \in E\hat{\Gamma}_k$, then $[x, y] = 1$ and so $[x^{\theta_k}, y^{\theta_k}]^{c_x c_y} = [x, y]^\beta = 1$, whence $[x^{\theta_k}, y^{\theta_k}] = 1$ and $\{x^{\theta_k}, y^{\theta_k}\} \in E\hat{\Gamma}_{n_k}$.

If $x \in V\Gamma_{n_k}$ then $G_k^p \leq G'_k \leq C_{G_k}(E)$ and so $(x^p)^\beta = (x^p)^{\theta_k c_x} = (x^p)^{c_x} = [x^\sigma, x^\tau]^{c_x}$. But also, $(x^p)^\beta = [x^\sigma, x^\tau]^\beta = [(x^\sigma)^\beta, (x^\tau)^\beta] = [(x^\sigma)^{\theta_k c_{x^\sigma}}, (x^\tau)^{\theta_k c_{x^\tau}}] = [x^\sigma, x^\tau]^{c_{x^\sigma} c_{x^\tau}}$. Therefore, $c_x = c_{x^\sigma} c_{x^\tau}$ for all $x \in V\Gamma_{n_k}$

We claim that $c_x = 1$ for all $x \in V\hat{\Gamma}_{n_k}$. This is a consequence of the following general observation: Assume that in a graph, $\Lambda$ is an oriented path of length $l$ with vertices (in sequence) $v_0, v_1, v_2, \ldots, v_l$. Suppose that $K$ is a field and $f$ is a function from $V\Lambda$ to $K \backslash \{0\}$ such that if $f_i = f(v_i)$, then $f_i = f_{i-1} f_{i+1}$ for $1 \leq i \leq l-1$ (and also, $f_0 = f_l = f_{l-1} f_1$ if $\Lambda$ is a cycle with $v_0 = v_l$). Then for any non-negative integer $j$, $f_{6j} = f_0$, $f_{6j+1} = f_1$, $f_{6j+2} = f_1 f_0^{-1}$, $f_{6j+3} = f_0^{-1}$, $f_{6j+4} = f_1^{-1}$ and $f_{6j+5} = f_0 f_1^{-1}$. If $\Lambda$ is a cycle with $l \equiv \pm 1 \mod 6$, it follows that $f_i = 1$ for all $i$. Also, if $\Lambda$ is a path (cycle or not) with $l \equiv \pm 1 \mod 3$ and such that $f_0 = 1 = f_l$ then, again, $f_i = 1$ for all $i$.

Because $c_x = c_{x^\sigma} c_{x^\tau}$ for all $x \in V\Gamma_{n_k}$, applying these considerations successively to the paths $\Lambda_1, \Lambda_2, \ldots, \Lambda_{n_k+2}$ in the decomposition $\Gamma_{n_k} = \bigcup_{i=1}^{n_k+2} \Lambda_i$ described earlier, we conclude that $c_x = 1$ for all $x \in V\Gamma_{n_k}$. Similarly, $c_x = 1$ for all $x \in V\Gamma_{n_k}^\alpha$.

Therefore, for any $x \in V\hat{\Gamma}_{n_k}$ (and hence, for any $x \in G_k$), $x^\beta \equiv x^{\theta_k} \mod G'_k$. It follows that if $\theta = (\theta_1, \ldots, \theta_r) \in E$ then $g^\beta \equiv g^\theta \mod G'$ for all $g \in G$ and so $\beta \in C_{\mathrm{Aut}(G)}(G/G')E \leq \mathrm{Aut}_c(G)E$. Also, because $[x, x^{\alpha_k}] = 1$ for all $x \in G_k$, $[x, x^{\theta_k}] = 1$ for all $x \in G_k$ and so $[g, g^\beta] = 1$ for all $g \in G$. Therefore, $G$ is an $A$-group and $\mathrm{Aut}(G) = C_{\mathrm{Aut}(G)}(G/G')E = \mathrm{Aut}_c(G)E$.

If $\gamma \in E$ and $\gamma \neq 1$, then $\gamma$ maps some $\Gamma_{n_k}$ to $\Gamma_{n_k}^{\alpha_k}$. If $\{x, y\} \in E\Gamma_{n_k}$ then since $\{x^{\alpha_k}, y\} \notin E\hat{\Gamma}_{n_k}$, $y \in C_{G_k}(x) \backslash C_{G_k}(x^{\alpha_k})$. We conclude that $\gamma \notin A_{\mathcal{C}}(G)$ and so $E \cap A_{\mathcal{C}}(G) = 1$, whence, $A_{\mathcal{C}}(G) = \mathrm{Aut}_c(G)$. Therefore, $\mathrm{Aut}(G)/A_{\mathcal{C}}(G) \cong E \cong (\mathbb{Z}_2)^r$. Since $r$ was chosen arbitrarily, the proof of Theorem 1.1 is complete. □

## References

[1] M. Deaconescu, G. Silberberg, and G. L. Walls, On commuting automorphisms of groups, Arch. Math. **79**, 423–429 (2002).

[2] H. Heineken and H. Liebeck, The occurrence of finite groups in the automorphism groups of nilpotent groups of class 2, Arch. Math. **25** (1974), 8–16.

[3] C. J. Maxson and M. R. Pettet, Maximal subrings and $E$-groups, Arch. Math. **88**, 392–402 (2007).

[4] D. J. S. Robinson, A Course in the Theory of Groups, Springer-Verlag, Berlin-Heidelberg-New York, 1982.

Martin R. Pettet, Department of Mathematics, The University of Toledo, Toledo, Ohio 43606, U.S.A.
e-mail: mpettet@math.utoledo.edu

Received: 23 March 2008

Revised: 20 May 2008