On a question about automorphisms of finite p-groups

GIOVANNI CUTOLO

ABSTRACT. This paper deals with an old problem: are there nontrivial finite p-groups which are isomorphic to their full automorphism group, besides the dihedral group of order 8? The answer (in the negative) is obtained in some special cases, including groups of class 2, powerful groups, groups with centre of prime order or an abelian subgroup of prime index, class-3 groups with cyclic centre, groups with coclass at most 3 and others.

The dihedral group D_8 of order 8 is a well known example of a group which is, up to isomorphisms, the full automorphism group of some group but, at the same time, one of a rather special nature: some of its unusual properties, that even characterise it among automorphism groups of finite groups, were discussed in [2] and [3].

Of course the most relevant peculiarity is that D_8 is (or, at least, appears to be) the only known example of a nontrivial finite group of prime-power order which is isomorphic to its own automorphism group. It is an old problem whether more such examples do exist; this question has rather recently been asked in [7], Question 10, also see [8], Problem 15.29.

The aim of this paper is contributing to shed some light on this question, by investigating the structure of possible new examples. Partial solutions are actually found in a number of special cases. For instance, we obtain that D_8 is, up to isomorphisms, the only nontrivial finite p-group G such that $G \simeq \operatorname{Aut} G$ (for some prime p) among groups of class 2 (see Theorem 2.4; the abelian case is obvious), among groups whose centre has prime order (Theorem 4.2), among groups with an abelian maximal subgroup (Proposition 3.4). Similarly, nontrivial powerful p-groups and groups of class 3 with cyclic centre are excluded from having this property (Corollary 5.2 and Theorem 5.4) as are, apart from D_8, groups of coclass at most 3 (the case of coclass 1, that is of groups of maximal class, also follows from [2]), groups of size dividing p^7 and groups of rank 2, in particular metacyclic groups; this latter is a very special case of various results in Section 5 about the ranks of abelian subgroups in the groups under consideration.

Throughout the paper p will always denote a prime. We will also use the standard notation $d(G)$ and $\operatorname{rk}(G)$ for the minimum number of generators of a (finite) group G and for its (Prüfer) rank. By lack of uniform notation in the literature we shall write $\operatorname{mk}(H)$ and $\operatorname{mk}_G(H)$ for the maximun of the ranks of the abelian (resp. G-invariant abelian) subgroups of H; we are assuming that H is a normal section of G. We will generally write $\sim$ for the natural conjugation epimorphism $G \twoheadrightarrow \operatorname{Inn} G$, thus $\tilde{g}$ will be the inner automorphism of G determined by g, which group is G shall be made clear by the context. $\operatorname{Aut}_c G$ will denote the group $C_{\operatorname{Aut} G}(\operatorname{Inn} G)$ of the central automorphisms of G. We will often make use of the fact (established in [1] as Theorem 1) that for every finite group G with no nontrivial abelian direct factor one has $|\operatorname{Aut}_c G| = |\operatorname{Hom}(G, Z(G))|$. For the sake of compactness we shall write $C_X(Y_1, Y_2, \dots, Y_n)$ to mean $C_X(Y_1) \cap C_X(Y_2) \cap \dots \cap C_X(Y_n)$, whatever X, Y_1, …, Y_n happen to be. Finally, $H \lessdot G$ means that H is a maximal subgroup of G and $\Phi(G)$ denotes the Frattini subgroup of G, while $G[n]$ is the set of all $g \in G$ such that $g^n = 1$ and $\mathcal{C}_n$ is the cyclic group of order n.

1. Some lemmas on derivations

As is well-known, derivations (or 1-cocycles) of groups play an important rôle in the description of homomorphism and automorphisms. Indeed, if K and L are normal subgroups of a group G,

2000 *Mathematics Subject Classification.* 20D15, 20D45, 20E36, 20F28.
Key words and phrases. automorphism groups, finite p-groups .

then there is a bijection from the set of all endomorphisms of G inducing the identity on both K and G/L and the set of all derivations from G/K to $C_L(K)$: the image of an endomorphism ε is the derivation defined by $gK \mapsto [g,\varepsilon]$ for all $g \in G$. If $L \leq K$ then the endomorphisms just referred to are automorphisms and $C_L(K) = L \cap Z(K)$ can be viewed as a (G/K)-module by conjugation; it also follows that the same bijection is an isomorphism between $C_{\mathrm{Aut}\,G}(K, G/L)$ and the derivation group $\mathrm{Der}\big(G/K, C_L(K)\big)$. We will use this fact without further comment throughout the paper, sometimes in the special case when $C_L(K) \leq Z(G)$ and so $\mathrm{Der}\big(G/K, C_L(K)\big) = \mathrm{Hom}\big(G/K, C_L(K)\big)$.

Therefore, it seems convenient to collect here some elementary (and probably known) remarks on derivations that will be useful in the sequel. If $G = \langle g \rangle$ is a finite cyclic group of order n and A is a G-module (and $a \in A$) then the assignment $g \mapsto a$ defines a derivation from G to A if and only if a belongs to the kernel of the trace endomorphism $\tau = 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1}$, where σ is the automorphism induced by g in A; thus $\mathrm{Der}(G, A) \simeq \ker\tau$. A special case is the following. A G-central series is a series whose factors are trivial G-modules.

Lemma 1.1. *Let n, $t \in \mathbb{N}$, let $G = \langle g \rangle$ be a cyclic group of finite order p^t and let A be a $\mathbb{Z}_pG$-module with a G-central series of length n. Suppose that $n < p^t$. Then the mapping $\delta \in \mathrm{Der}(G, A) \mapsto g^\delta \in A$ is an isomorphism.*

Proof. Let σ be the automorphism induced by g in A. Thus $(\sigma - 1)^n = 0$. In the polynomial ring $\mathbb{Z}_p[x]$ it holds $1 + x + \cdots + x^{p^t-1} = (x-1)^{p^t-1}$; therefore $1 + \sigma + \sigma^2 + \cdots + \sigma^{p^t-1} = 0$, and the result follows. □

Of course this lemma can be applied when A is an elementary abelian subgroup contained in the n-th centre of a group X and G is a suitable quotient of X.

Lemma 1.2. *Let $G = U \times V$ be a group, and let A be an G-module. Let α and β be derivations from U and V respectively to A. Then α and β have a common extension to a derivation from G to A if and only if $[u^\alpha, v] = [v^\beta, u]$ for all $u \in U$ and $v \in V$. In particular, if $[U, A] = 1$ then $\mathrm{Der}(G, A) \simeq \mathrm{Hom}\big(U, C_A(G)\big) \times \mathrm{Der}(V, A)$.*

Proof. The first half of the statement is checked directly: if the condition is satisfied then the only possible extension of the given derivations is the mapping $uv \mapsto u^{\alpha v} v^\beta$, with obvious notation. The second half follows: if $[U, A] = 1$ then the condition translates into $[u^\alpha, v] = 1$ for all $u \in U$ and $v \in V$, which is equivalent to $U^\alpha \leq C_A(G)$. □

Lemma 1.3. *Let p be an odd prime, let G be an elementary abelian p-group, and let A be a $\mathbb{Z}_pG$-module of finite $\mathbb{Z}_p$-rank n. Suppose that both $C_A(G)$ and $[A, G]$ have order p. Then $G/C_G(A)$ has rank $n-1$ and $\mathrm{Der}(G, A)$ has rank $\mathrm{rk}(G) + \binom{n}{2}$.*

Proof. The hypothesis implies that $Z := C_A(G)$ and $[A, G]$ coincide. Also, it follows from Lemma 1.2 that we may assume that $C_G(A) = 1$. Then G embeds in $\mathrm{Hom}(A/Z, Z) \simeq A/Z$. On the other hand Z is the intersection of the centralizers in A of the elements of a basis of G. Each of these centralizers has index p; it follows that the above embedding is an isomorphism. Thus $\mathrm{rk}(G) = n - 1$, as required; more precisely, to any ordered basis $(z, a_1, a_2, \ldots, a_{n-1})$ of A, with $z \in Z$, there corresponds a "dual basis" $(x_1, x_2, \ldots, x_{n-1})$ of G such that, for all $i, j \in I := \{1, 2, \ldots, n-1\}$, we have $[a_i, x_j] = 1$ if $i \neq j$ and $[a_i, x_i] = z$. This shows that the module structure of A is determined by the hypotheses. This structure can be realised by making A into a normal subgroups of the extra-special p-group P of exponent p generated by A and elements $y_1, y_2, \ldots, y_{n-1}$ subject to $[a_i, y_j] = 1 = [y_i, y_j]$ if $i \neq j$ and $[a_i, y_i] = z$ for all $i, j \in I$. Now $\mathrm{Der}(G, A) \simeq \mathrm{Der}(P/A, A) \simeq C_{\mathrm{Aut}\,P}(A, P/A) =: \varGamma$. If $\gamma \in \varGamma$ then $a^\gamma = a$ for all $a \in A$ and $y_i^\gamma = y_i z^{\mu_i} \prod_{j \in I} a_j^{\lambda_{ij}}$ for all $i \in I$ and for suitable $\mu : I \to \mathbb{Z}_p$ and matrix $\lambda : I \times I \to \mathbb{Z}_p$. Moreover the relations $[y_i^\gamma, y_j^\gamma] = 1$ for all $i, j \in I$ show that λ is symmetric. Conversely, every such μ and symmetric λ define an element of $\varGamma$. The result follows. □

As so often happens, the corresponding result for the case where $p = 2$ is slightly different, in that the derivation group has smaller rank. So, to construct the number of automorphisms that some of our arguments will require we will need an extended version of the lemma for 2-groups. We make the following remark first.

Lemma 1.4. *Let G be an abelian group of exponent dividing p^2, and let $G^p \leq C \leq G$. Then $G = U \times V$, for suitable subgroups U and V such that $U \leq C$ and $C \cap V = V^p$.*

Proof. Let F be a maximal homocyclic subgroup of exponent p^2 of C, or let $F = 1$ if $\exp C \leq p$. Then $G = F \times E$ for some subgroup E, and $C = F \times K$, where $K = E \cap C$ has exponent p at most. As $G^p \leq C$ we have $E^p \leq K$, thus E^p has a complement L in K and $E = L \times V$ for some subgroup V such that $E^p = V \cap K$. Let $U = FL$. Since $V^p = E^p$ it is clear that all requirements for U and V are satisfied and the lemma is proved. □

Lemma 1.5. *Let G be a finite abelian group of exponent dividing 4, and let A be a $\mathbb{Z}_2G$-module of finite $\mathbb{Z}_2$-rank n. Let $C = C_G(A)$ and suppose that both $C_A(G)$ and $[A, G]$ have order 2. Then $C \geq G^2$, moreover G/C has rank $n-1$ and $\operatorname{Der}(G, A)$ has rank $\operatorname{rk}(G) + \operatorname{rk}(G^2) - \operatorname{rk}(C^2) + \binom{n-1}{2}$.*

Proof. The proof is similar to that of Lemma 1.3. We have that $Z := C_A(G) = [A, G]$ and $G/C \simeq A/Z$, therefore $C \geq G^2$. Let us first consider the case when $C = G^2$. In this case $\operatorname{rk}(G) = \operatorname{rk}(G/C) = n - 1$ and, as in the proof of Lemma 1.3, the structure of the module A is determined and can be realised by making A into a normal subgroup of a central product P defined as follows. Let $(z, a_1, a_2, \dots, a_{n-1})$ be an ordered basis of A, with $z \in Z$, and write G as $\mathrm{Dr}_{i=1}^{n-1} \langle x_i \rangle$, where each x_i has order $\sigma_i \in \{2, 4\}$. Let P be generated by A and pairwise commuting elements $y_1, y_2, \dots, y_{n-1}$ subject to $[y_i, a_i] = z = y_i^{\sigma_i}$ (hence each y_i has order $2\sigma_i$) and $[a_i, y_j] = 1$ if $i \neq j$, for all $i, j \in I := \{1, 2, \dots, n-1\}$. Up to the isomorphism given by $x_i \mapsto Ay_i$ for all i, the structure of (P/A)-module of A is the same as its original G-module structure. Thus $\operatorname{Der}(G, A) \simeq \operatorname{Der}(P/A, A) \simeq \mathit{\Gamma} := C_{\operatorname{Aut} P}(A, P/A)$. The elements γ of $\mathit{\Gamma}$ are determined by the mapping $\mu : I \to \mathbb{Z}_2$ and the matrix $\lambda : I \times I \to \mathbb{Z}_2$ such that $y_i^\gamma = y_i z^{\mu_i} \prod_{j \in I} a_j^{\lambda_{ij}}$ for all $i \in I$. Again, such λ is symmetric, since $[y_i^\gamma, y_j^\gamma] = 1$ for all $i, j \in I$. Moreover, for each i, direct computation yields $z = z^\gamma = (y_i^\gamma)^{\sigma_i} = zz^{\lambda_{ii}\sigma_i/2}$, hence $\lambda_{ii} = 0$ if $\sigma_i = 2$. Conversely, every μ and λ satisfying these conditions define an element of $\mathit{\Gamma}$. The number of $i \in I$ such that $\sigma_i = 4$ is $\operatorname{rk}(G^2)$, therefore $\operatorname{rk}\bigl(\operatorname{Der}(G, A)\bigr) = \operatorname{rk}(\mathit{\Gamma}) = \operatorname{rk}(G) + \operatorname{rk}(G^2) + \binom{n-1}{2}$.

In the general case, by Lemma 1.4 we can decompose G as $U \times V$, for suitable $U \leq C$ and $V \leq G$ such that $C = U \times V^2$. Hence $\operatorname{Der}(G, A) \simeq \operatorname{Hom}(U, Z) \times \operatorname{Der}(V, A)$, by Lemma 1.2. Now $\operatorname{Der}(V, A)$ has rank $\operatorname{rk}(V) + \operatorname{rk}(V^2) + \binom{n-1}{2}$ by the previous case, while $\operatorname{Hom}(U, Z) \simeq U$ has rank $\operatorname{rk}(G) - \operatorname{rk}(V)$; moreover $C^2 = U^2$, as V^2 has exponent 2 at most, so $\operatorname{rk}(G^2) = \operatorname{rk}(C^2) + \operatorname{rk}(V^2)$. The result is now clear. □

The typical situation in which the previous lemmas will apply is when A is an elementary abelian normal subgroup of the finite p-group G contained in $Z_2(G)$, and $|A \cap Z(G)| = p$.

2. Groups of class 2

Noncyclic finite abelian groups have nonabelian automorphism groups, therefore it is straightforward that no nontrivial finite abelian group can be isomorphic to its own automorphism group. As a next step we consider (finite) p-groups of class 2. The proofs in this section are largely independent of the results in the previous one.

Lemma 2.1. *Let G be a finite p-group of class 2 such that $G \simeq \operatorname{Aut} G$. Then $Z(G)$ is cyclic.*

Proof. Let $Z = Z(G)$, and assume that $r := \operatorname{rk}(Z) > 1$. Let $s = \operatorname{rk}(G/Z)$, so that $\operatorname{rk}(G) \leq r + s$, while $\mathit{\Gamma} := C_{\operatorname{Aut} G}(Z, G/Z) \simeq \operatorname{Hom}(G/Z, Z)$ has rank rs. Since $\mathit{\Gamma}$ embeds in $\operatorname{Aut} G \simeq G$ it follows that $rs \leq r + s$. As $r > 1$ and $s > 1$ because G is not abelian, $r = s = 2$. Therefore G/Z is 2-generator, hence G' is cyclic, of order q, say, and it follows that $G/Z \simeq \mathcal{C}_q \times \mathcal{C}_q$. Moreover, $\operatorname{Hom}(G/Z[p], Z[p]) \simeq C_{\operatorname{Aut} G}(Z[p], G/Z[p])$ also embeds in G, hence its rank $2\operatorname{rk}(G/G'Z[p])$ cannot exceed the rank $rs = 4$ of G; thus $\operatorname{rk}(G/G'Z[p]) = 2$. Now recall that G has a subgroup A isomorphic to $\mathit{\Gamma}$. Thus $A \simeq \operatorname{Hom}(\mathcal{C}_q \times \mathcal{C}_q, Z)$; since $\mathcal{C}_q \simeq G' \leq Z$ and $\operatorname{rk}(Z) = 2$ then $A = B \times C$ for some subgroups $B \simeq \mathcal{C}_q \times \mathcal{C}_q$ and C of rank 2. Let x be an element of G such that xZ has order q. Then $C_G(x) = \langle x \rangle Z$ has rank 3 (at most), so $x \notin A$. This shows that $\exp(AZ/Z) < q$. Two consequences of this fact are that $B[p] = Z[p]$ and $q > p$, hence $B[p] < B$. It follows that $A/Z[p]$ has rank 4. This is a contradiction, since $\operatorname{rk}(G/G'Z[p]) = 2$ and G' is cyclic. □

The conclusion of Lemma 2.1 allows us to make use of the following key observation from [3].

Lemma 2.2 (see [3], Lemma 3.2 and context)**.** *Suppose that G is a finite p-group such that both Z and $Z(\operatorname{Aut} G)$ are cyclic. Then G has exactly one maximal subgroup M which is characteristic. Moreover, M contains all proper characteristic subgroups of G. Further, $Z\big(\operatorname{Aut} G\big)[p] = C_{\operatorname{Aut} G}(M) \cap C_{\operatorname{Aut} G}(G/Z[p])$,*

To streamline the proof of the main result of this section we also record this elementary fact.

Lemma 2.3. *Let G be a finite p-group of class 2 with cyclic centre Z, and suppose that G/Z has rank 2. Then there exist elements $a, b \in G$ such that, after setting $B = \langle b \rangle Z$, we have $G = B \langle a \rangle$ and $|B \cap \langle a \rangle| \leq 2$ (in particular, $G = B \rtimes \langle a \rangle$ if $p > 2$).*

Proof. Choose a pair (a, b) of generators of G modulo Z in such a way that a has the least possible order. Clearly $B \cap \langle a \rangle = \langle a^q \rangle = Z \cap \langle a \rangle$, if $B = \langle b \rangle Z$ and $q = \exp(G/Z)$, moreover $\circ(a) \leq \circ(b)$. Since $G^q \leq Z$ and Z is cyclic, there exists $t \in \mathbb{N}$ such that $a^q = b^{qt}$. Let $a_1 = ab^{-t}$. Then $\circ(a) \leq \circ(a_1)$ by the choice of a. Now, if $p \neq 2$ then $a_1^q = 1$, and $a_1^{2q} = 1$ even if $p = 2$. This proves the result. □

Theorem 2.4. *Let G be a nontrivial finite p-group of class 2 such that $G \simeq \operatorname{Aut} G$. Then $G \simeq D_8$.*

Proof. Let $Z = Z(G)$. Then Z is cyclic by Lemma 2.1, hence G is a central product $\prod_{i=1}^{n} G_i$, where each of the subgroups G_i can be written as $\langle a_i, b_i \rangle Z$ for suitable a_i and b_i and $G_i \cap G_j = Z$ if $i \neq j$; by the previous lemma we may also choose the elements a_i and b_i such that $G_i = \langle b_i \rangle Z \langle a_i \rangle$ and $|\langle b_i \rangle Z \cap \langle a_i \rangle| \leq 2$ for each i. Then G has an automorphism φ that fixes all a_i and maps every b_i and all elements of Z to their inverses. This shows that $p = 2$, since either φ or each of the b_i must have order 2. Moreover, since $\operatorname{Aut} G$ has class 2 then $[g, \operatorname{Aut} G, \operatorname{Aut} G] \leq Z$ for every $g \in G$, hence $b_i^4 = [b_i, \varphi, \varphi] \in Z$. Now the order q of G' is the maximum of the orders of the elements $b_i Z$, therefore $q \leq 4$. Also, $|\operatorname{Aut}_c G| = |\operatorname{Hom}(G_{\mathrm{ab}}, Z)|$ by Theorem 1 of [1]. But $\exp G_{\mathrm{ab}} \leq |Z/G'| \exp(G/Z) = |Z/G'| \cdot |G'| = |Z|$, hence $\operatorname{Hom}(G_{\mathrm{ab}}, Z) \simeq G_{\mathrm{ab}}$. As $|\operatorname{Aut} G| = |G|$ it follows that $|\operatorname{Aut} G : \operatorname{Aut}_c G| = q$. Let $\Psi = \langle \varphi \rangle \operatorname{Aut}_c G$. Since $\varphi \notin \operatorname{Aut}_c G$ if (and only if) $q = 4$ then Ψ is maximal in $\operatorname{Aut} G$. Let M be the unique characteristic maximal subgroup of G. One of the elements a_i, b_i does not belong to M, call it x. Then $\langle x \rangle^{\operatorname{Aut} G}$ is a characteristic subgroup of G not contained in M, hence $\langle x \rangle^{\operatorname{Aut} G} = G$. But $\langle x \rangle^{\Psi} \leq \langle x \rangle Z$; it follows that G/Z is two-generator. In other words the number n of factors in the above decomposition of G as a central product is 1. From now on let $a = a_1$, $b = b_1$ and $B = \langle b \rangle Z$. Note that $\operatorname{Aut} G$ contains $\operatorname{Inn} G \simeq \mathcal{C}_q \times \mathcal{C}_q$ as a subgroup, hence it has an element of order q avoiding the centre. The same must be true of G, thus we may suppose that a has been chosen such that $\langle a \rangle \cap B = 1$. Let $\mathit{\Gamma} = C_{\operatorname{Aut} G}(B, G/B[2])$. For every odd integer n let σ_n be the automorphism of G mapping a to itself and every element of B to its n-th power; these automorphisms form a subgroup $\mathit{\Sigma}$ of $\operatorname{Aut} G$ isomorphic to the group of all power automorphisms of B, and $\langle \mathit{\Gamma}, \mathit{\Sigma} \rangle = \mathit{\Gamma} \times \mathit{\Sigma}$. If $q = 4$ then $\mathit{\Gamma} \simeq B[2]$ by Lemma 1.1; since G has rank $1 + \operatorname{rk}(B)$ at most and contains a subgroup isomorphic to $\mathit{\Gamma} \times \mathit{\Sigma}$, then $\mathit{\Sigma}$ is cyclic, which means that $\exp B \leq 4$. Thus $b^4 = 1$, but then $(ba)^4 = b^4 a^4 [a, b]^2 = [a, b]^2 \neq 1$, and after replacing b with ba, as we certainly may, we obtain a contradiction. Hence $q = 2$. Therefore the maximal abelian subgroups of G have order 2 modulo Z, which is cyclic; thus G (that is to say, $\operatorname{Aut} G$) has no abelian subgroups of rank 3. Since $C_{\operatorname{Aut} G}(G_{\mathrm{ab}}, G') \simeq G/G^2$ then $d(G) = 2$ and so $G = \langle a, b \rangle$. As a consequence, $B = \langle b \rangle G'$. As Z is cyclic then either $Z = G'$ or $Z \leq \langle b \rangle$. In the former case, since $|G'| = 2$ it is clear that $|G| = 8$; in the latter case B is cyclic, hence $\operatorname{rk}(G) = 2$ and the embedding $\mathit{\Gamma} \times \mathit{\Sigma} \rightarrowtail G$ shows that $\mathit{\Sigma} \simeq \operatorname{Aut} B$ is cyclic, thus $|B| \leq 4$ and $|G| = 8$ again. Therefore, in either case, $G \simeq D_8$. □

3. Inner and central automorphisms

In this section we consider two subgroups of immediate relevance to our problem and that will have a rôle in several of the upcoming proofs. Let G be a finite p-group and assume that there exists an isomorphism $\alpha : \operatorname{Aut} G \to G$. Let $I := (\operatorname{Inn} G)^{\alpha}$ and $C := C_G(I)$, so that $C = (\operatorname{Aut}_c G)^{\alpha}$. As can be expected the existence of the normal subgroup $I \simeq G/Z(G)$ together with further restrictions that can be established on both I and C and the way in which they are embedded in G strongly influences the structure of G. One of the restrictions is that if G has no nontrivial abelian direct factor (which is necessarily true if $Z(G)$ is cyclic, or also if $p > 2$, for otherwise G would have an automorphism of order 2) then $|C| = |\operatorname{Hom}\big(G, Z(G)\big)|$ by the already quoted result from [1]. Further information is provided by the following lemma—recall the definition of $\operatorname{mk}_G(C)$ given in the introduction.

Lemma 3.1. *Let G be a finite nontrivial p-group, and let I and $C = C_G(I)$ be as just defined. Let $Z = Z(G)$, $r = \operatorname{rk}(Z)$, $d = d(G)$ and $\bar{d} = d(G/Z[p])$. Then:*

(*i*) *$\operatorname{mk}_G(C) \geq \bar{d}r > r$, in particular $Z < C$; also, $d - 1 \leq \bar{d} \leq d$ and $\bar{d} = d$ if $p > 2$, and $\operatorname{mk}_G(C) \geq (d-1)r$;*

(*ii*) *$Z(I) \nleq Z$; in particular $IC < G$ and $|C| < |Z_2(G)|$.*

Proof. Since the statement holds for D_8, in view of Theorem 2.4 we may assume that the nilpotency class of G is greater than 2, that is, that I is not abelian. Thus $\bar{d} > 1$, and the first half of part (*i*) follows from the fact that $\operatorname{Hom}(G/Z[p], Z[p])$, which has rank $\bar{d}r$, is isomorphic to the subgroup $C_{\operatorname{Aut} G}(Z[p], G/Z[p])$ of $\operatorname{Aut}_c G$, which is normal in $\operatorname{Aut} G$. As $\operatorname{Aut} G$ is a p-group, G has no direct factor of odd prime order nor any isomorphic to V_4, the noncyclic group of order 4. Then $|Z[p]\Phi(G)/\Phi(G)| \leq 2$, hence $d \leq \bar{d} + 1$ and (*i*) follows

To prove part (*ii*) let $Z_2 = Z_2(G)$ and $s = \operatorname{rk}(G/Z_2)$—note that $G/Z_2 \simeq I/Z(I)$. Suppose that $Z(I) \leq Z$. Then

$$\operatorname{rk}(I) \leq \operatorname{rk}\big(Z(I)\big) + \operatorname{rk}\big(I/Z(I)\big) = \operatorname{rk}\big(Z(I)\big) + s \leq r + s,$$

on the other hand $I \simeq G/Z \geq IC/Z = (IZ/Z) \times (C/Z)$ and $IZ/Z \simeq I/Z(I)$, so:

$$\operatorname{rk}(I) \geq \operatorname{rk}\big(I/Z(I)\big) + \operatorname{rk}(C/Z) = s + \operatorname{rk}(C/Z) \geq s + \operatorname{rk}(C) - r \geq s + (\bar{d}-1)r \geq r + s.$$

Therefore all these inequalities must hold as equalities. In particular, $\bar{d} = 2$, and $\operatorname{rk}\big(Z(I)\big) = \operatorname{rk}(Z) = r = \operatorname{rk}(C/Z)$; the first equality also shows that $Z[p] \leq Z(I)$; moreover IZ/Z and C/Z are nontrivial normal subgroups of G/Z with trivial intersection, hence $Z(I) \simeq Z_2/Z$ is not cyclic and $r > 1$. Next we shall prove that $Z[p] \leq \Phi(G)$. If $Z[p] \nleq \Phi(G)$ then ($p = 2$ and) $G = U \times V$ for some $U, V \leq G$ such that $|U| = 2$. By what we have just proved $U \leq Z[2] \leq I$ and $I = U \times (V \cap I)$. But since $\bar{d} = 2$ then $d(I) = 2$, hence $V \cap I$ is cyclic and I is abelian, a contradiction. Therefore $Z[p] \leq \Phi(G)$, and hence $d(G) = 2$. Moreover, since $IC/IZ \simeq C/Z$ has rank $r > 1$ and hence G/I is not cyclic, it follows that $I \leq \Phi(G)$. Now let $S/Z = (Z_2/Z)[p]$. Clearly $G/C_G(S)$ is elementary abelian, so $I \leq \Phi(G) \leq C_G(S)$, hence $S \leq C$. This leads to a contradiction again, as $IZ \cap S > Z$. Therefore, $Z(I) \nleq Z$, as we wanted to show. That $IC < G$ is an obvious consequence. Finally, $|C| = |Z(I)| \cdot |C/Z(I)| = |Z_2/Z| \cdot |IC/I| < |Z_2/Z| \cdot |G/I| = |Z_2|$. □

Remark 3.2. This seems to be a good place to make some further comment on the possibility that $Z[p]$ is not contained in $\Phi(G)$, that is, on the value of $\bar{d}$ compared to that of d, in the notation of the previous lemma. As already remarked, either $Z[p] \leq \Phi(G)$ and $\bar{d} = d$ or $Z[p] \nleq \Phi(G)$ and $\bar{d} = d - 1$. In this latter case $p = 2$ and $G = U \times V$ for some $U, V \leq G$ such that $|U| = 2$ and $Z(V)[2] \leq V^2$, since G cannot have the noncyclic group of order 4 as a direct factor. Although this information suffices for our purposes it is worth noticing that it seems rather unlikely that this case can occur at all. In fact, if it does, $\operatorname{Aut} V$ has an obvious embedding in $\operatorname{Aut} G$, and it is easy to deduce that since $|\operatorname{Aut} G| = 2|V|$ then $|\operatorname{Aut} V|$ properly divides $|V|$—more precisely, it can be checked that the index of the image of $\operatorname{Aut} V$ in $\operatorname{Aut} G$ is $2^{(r-1)(d-1)}$, where $r = \operatorname{rk}(Z) > 1$, and $d \geq 3$. Now, to the contrary, it is a famous long-standing conjecture that the order of every finite nonabelian p-group divides that of its automorphism group (see, e.g. [5] and the discussion in [7], p. 363). Thus an example of a finite p-group G such that $G \simeq \operatorname{Aut} G$ and $Z[p] \nleq \Phi(G)$ would also disprove this conjecture. Note that the conjecture has been verified in a number of cases, including that of groups of order at most p^7, a fact that we cite here for further reference.

The inner automorphism $\tilde{g} : x \mapsto x^g$ of a group G lies in the centre of $\operatorname{Inn} G$ if and only if $[g, \operatorname{Aut} G] \leq Z(G)$. Thus, an equivalent way of stating part (*ii*) of Lemma 3.1 is the following.

Corollary 3.3. *Let G be a finite nontrivial p-group such that $G \simeq \operatorname{Aut} G$. Then $\operatorname{Aut} G$ acts non-trivially on $Z_2(G)/Z(G)$.*

A simple consequence of Lemma 3.1 is the following proposition, which characterises D_8 in the same spirit of Theorem 2.4.

Proposition 3.4. *Let G be a finite p-group such that $G \simeq \operatorname{Aut} G$. If G has an abelian subgroup of index p then $G \simeq D_8$.*

Proof. Let A be an abelian subgroup of index p in G, and let I and C be defined as in Lemma 3.1. By Theorem 2.4 it will be enough to show that G has class 2. Assume that this is false, then $I \nleq A$, hence $G = IA$ and so $A \cap C = Z(G)$. It follows that C is abelian, as $|C/Z(G)| \le p$, and $C \le A$, otherwise $G = AC$ and G would have class 2. Therefore $C = Z(G)$, but this is excluded by Lemma 3.1. □

4. Groups with cyclic centre

Our first result in this section settles the case of those groups whose centre has prime order. Its proof uses a lemma which basically reproduces the main inductive step in the proof of Gaschütz-Schmid theorem on the existence of outer automorphisms in finite p-groups, see [9], pp. 74–75.

Lemma 4.1. *Let G be a finite p-group and let M be a maximal subgroup of G. If $Z(G) < C_G(M) < M$ then G has an outer automorphism θ of p-power order such that $M^\theta = M$ and $[Z(M), \theta] = 1$.*

Proof. Let $Q = G/M$ and let $A = Z(M)$. If χ is the coupling of the (canonical) extension $M \rightarrowtail G \twoheadrightarrow Q$ then the Wells sequence gives the exact sequence

$$0 \longrightarrow H^1(Q, A) \longrightarrow N_{\operatorname{Out} G}(M) \xrightarrow{\text{res}} N_{\operatorname{Out} M}(Q^\chi)/Q^\chi \longrightarrow H^2(Q, A).$$

If our statement fails then p does not divide $|H^1(Q, A)|$, hence $H^1(Q, A) = 0$. It follows that $H^2(Q, A) = 0$ and so the mapping labelled by 'res' actually is an isomorphism. Thus every automorphism of M normalizing Q^χ can be extended to an automorphism of G. By Gaschütz-Schmid Theorem p divides $|C_{\operatorname{Out} M}(A)|$; since $C_{\operatorname{Out} M}(A) \lhd \operatorname{Out} M$ it follows that Q^χ centralizes an element $\bar{\theta}_0 = \theta_0 \operatorname{Inn} M$ of order p in $C_{\operatorname{Out} M}(A)$. Now $C_{\operatorname{Out} M}(A) \cap Q^\chi = 1$, because $C_G(A) = M$; thus $\bar{\theta}_0 Q^\chi \neq 1$. Therefore, by the above isomorphism, θ_0 can be extended an outer automorphism θ of G such that $M^\theta = M$. □

We could add, even if this facts will not be needed in this paper, that this construction makes sure that θ induces either the identity or an outer automorphism on M. Also, the lemma remains true if the hypothesis that $Z(G) < C_G(M) < M$ is replaced by $C_G(M) \nleq M$, since in this case G can be decomposed as central product $G = MC_G(M)$.

Theorem 4.2. *Let G be a finite p-group such that $G \simeq \operatorname{Aut} G$. If $|Z(G)| = p$ then $G \simeq D_8$.*

Proof. Suppose that $Z := Z(G)$ has order p. Arguing by contradiction, assume $G \not\simeq D_8$. First we shall show that all maximal subgroups of G with the possible exception of the characteristic one (see Lemma 2.2) have Z as their centre. Indeed, let $M \lessdot G$ and assume that $Z(M) \neq Z$. As $|Z| = p$ it is obvious that $C_G(M) = Z(M)$, moreover M is not abelian by Proposition 3.4, so we can apply Lemma 4.1 to produce an outer automorphism θ of G such that $M^\theta = M$. But $\operatorname{Aut} G = \langle\theta\rangle \operatorname{Inn} G$, because $\operatorname{Inn} G \lessdot \operatorname{Aut} G$ since $|Z| = p$, therefore M is characteristic in G. Thus our claim is established.

Now let I and C be as in Lemma 3.1. Then $I \lessdot G$ and $C \simeq \operatorname{Aut}_c G = C_{\operatorname{Aut} G}(Z, G/Z) \simeq \operatorname{Hom}(G/Z, Z) \simeq G/\Phi(G)$, moreover $C \le I$ (by Lemma 3.1, or because otherwise G would have a direct factor of order p), thus $C = Z(I)$. This shows that $Z(I) \neq Z$, hence I is the only characteristic maximal subgroup of G, by the above part of the proof. On the other hand for every $g \in Z_2 \setminus Z$ we have $1 \neq G/C_G(g) \simeq [G, g] \le Z$, hence $C_G(g) \lessdot G$; as $Z\bigl(C_G(g)\bigr) > Z$ then $C_G(g) = I$. Thus $Z_2 \le C$, but $C = Z(I) \simeq Z_2/Z$, so we have a contradiction. Hence $G \simeq D_8$. □

If G is a p-group with cyclic centre Z and $G \simeq \operatorname{Aut} G$ then the main result of [1] applies, as remarked earlier, thus $\operatorname{Aut}_c G$ is the set of all mappings $g \in G \mapsto gg^\varepsilon \in G$ with ε ranging over $\operatorname{Hom}(G, Z)$. This suggests a description of $Z(\operatorname{Aut} G)$, in a slightly more general setting.

Lemma 4.3. *Let G be a finite p-group such that $Z = Z(G)$ is cyclic and $Z(\operatorname{Aut} G) \simeq Z$. Then there exists an epimorphism $\varepsilon : G \twoheadrightarrow Z$ such that $Z(\operatorname{Aut} G)$ is generated by $\varepsilon^* : g \in G \mapsto gg^\varepsilon \in G$. If $K = \ker \varepsilon$ then K is characteristic in G and G/K is $(\operatorname{Aut} G)$-isomorphic to Z. Moreover:*

(*i*) *either $Z \le K$ or $\exp(G/ZG') = |K \cap Z| < |Z|$;*

(*ii*) *if* $p = 2$ *then* $|K \cap Z| > 2$.

Proof. Let $|Z| = p^\lambda$. We know that $Z(\operatorname{Aut} G)$ (which is contained in $\operatorname{Aut}_c G$) is generated by an automorphism defined as ε^* for some suitable $\varepsilon \in \operatorname{Hom}(G, Z)$. We have to show that $\operatorname{im} \varepsilon = Z$. For every $t \in \mathbb{N}$ we have $(\varepsilon^*)^t = \sum_{i=0}^{t} \binom{t}{i} \varepsilon^i$; let us compute this power for $t = p^{\lambda-1}$—as we know ε^* has order p^λ and so $(\varepsilon^*)^{p^{\lambda-1}} \neq 1$. Let i be an integer such that $1 \leq i \leq p^{\lambda-1}$. If p divides i exactly r times (i.e., $p^r \mid i$ but $p^{r+1} \nmid i$) then p divides $\binom{p^{\lambda-1}}{i}$ exactly $\lambda - 1 - r$ times; moreover, since p^r divides i we have $r < 2^r \leq p^r \leq i$, so $r + 1 \leq i$ and $\lambda - 1 - r \geq \lambda - i$. Let $K = \ker \varepsilon$. Since $K \cap Z \neq 1$ then $Z^\varepsilon < Z$. By an easy induction argument, $\operatorname{im} \varepsilon^i \leq Z^{p^{i-1}}$ (which proves that $\varepsilon^{\lambda+1} = 0$), and $\operatorname{im} \varepsilon^i \leq Z^{p^i}$ if $\operatorname{im} \varepsilon < Z$. In this latter case, then, $p^{\lambda-i} \varepsilon^i = 0$ if $i \leq \lambda$; it follows that $(\varepsilon^*)^{p^{\lambda-1}} = 1 + \sum_{i=1}^{\lambda} \binom{p^{\lambda-1}}{i} \varepsilon^i = 1$, and this is a contradiction. Therefore ε is an epimorphism, as we wanted to show. As a consequence, $G/K \simeq Z$. Also, from the fact that $\varepsilon^* \in Z(\operatorname{Aut} G)$ it follows that K is characteristic in G and G/K is $(\operatorname{Aut} G)$-isomorphic to Z.

We still have to check (*i*) and (*ii*). Let $p^\mu = |K \cap Z|$ and note that $p^\mu = |G/KZ| \leq \exp(G/ZG')$. As an immediate consequence of what has just been proved, $C_{\operatorname{Aut} G}(Z, G/Z)$ also centralizes G/K, hence the image of every homomorphism from G/Z to Z is contained in $K \cap Z$. Thus $G/ZG'G^{p^\lambda}$ has exponent p^μ, and (*i*) follows. To prove (*ii*) we can repeat the above computation for $(\varepsilon^*)^{p^{\lambda-1}}$ by looking at the terms $\binom{p^{\lambda-1}}{i} \varepsilon^i$ again. Earlier arguments show that if i is an integer such that $2 \leq i \leq p^{\lambda-1}$ and p divides i exactly r times then $\binom{p^{\lambda-1}}{i} \varepsilon^i = 0$ unless $\lambda - 1 - r = \lambda - i$ or, equivalently, $r + 1 = 2^r = p^r = i$, which amounts to saying that $r = 1$ and $p = 2 = i$. Thus, if $p = 2$ then $(\varepsilon^*)^{2^{\lambda-1}} = 1 + 2^{\lambda-1} \varepsilon + 2^{\lambda-2}(2^{\lambda-1} - 1)\varepsilon^2$. Now let x be a generator of G modulo K. Then $\langle x^\varepsilon \rangle = Z$, hence $x^{2^{\lambda-1}\varepsilon}$ is the nontrivial element of $Z[2]$. But $Z[2]$ also contains $y = x^{2^{\lambda-2}\varepsilon^2}$, because $\operatorname{im} \varepsilon^2 \leq Z^2$. Since $(\varepsilon^*)^{2^{\lambda-1}} \neq 1$ then $y = 1$. Thus $\operatorname{im} \varepsilon^2 < Z^2$, which means that (*ii*) holds. □

Another piece of information on $Z(\operatorname{Aut} G)$, under more general hypotheses, comes from the next lemma.

Lemma 4.4. *Let G be a finite p-group, and let $\zeta \in \operatorname{Aut} G$. If ζ centralizes all automorphisms of G of order p, then ζ acts like a power automorphism on $G/\Phi(G)$ and on $Z(G)[p]$. In particular, if ζ also has p-power order then it centralizes $G/\Phi(G)$ and $Z(G)[p]$.*

Proof. We may assume that $|G| > p$. Let $M \lessdot G$. Then M contains a minimal normal subgroup N of G, and G has an automorphism α of order p centralizing M and G/N. Then $M^\zeta = \big(C_G(\alpha)\big)^\zeta = C_G(\alpha^\zeta) = C_G(\alpha) = M$. It follows that ζ induces a power automorphism on $G/\Phi(G)$. The proof for the socle $Z(G)[p]$ is similar: if N is a minimal normal subgroup of G, choose any maximal subgroup M of G containing N. Define α as above, then from $N = [G, \alpha]$ and $\alpha^\zeta = \alpha$ it follows that $N^\zeta = N$, and hence the statement. □

Corollary 4.5. *Let G be a finite p-group such that $Z(G)$ is cyclic and $Z(\operatorname{Aut} G) \simeq Z(G)$. Then $Z(G) \leq \Phi(G)$.*

Proof. Lemma 4.3 shows that $Z(G) = [G, Z(\operatorname{Aut} G)]$, Lemma 4.4 that $[G, Z(\operatorname{Aut} G)] \leq \Phi(G)$. □

The hypothesis that $Z(\operatorname{Aut} G)$ and $Z(G)$ have the same order is needed in this corollary. Indeed, there are examples of p-groups G such that $\operatorname{Aut} G$ is a p-group and both $Z(G)$ and $Z(\operatorname{Aut} G)$ are cyclic, yet $Z(G) \nleq \Phi(G)$. The easiest examples are the cyclic groups of order 2 or 4; a more interesting one is the following: let H be the holomorph of $\mathcal{C}_8$, and let G be the central product HZ, where $Z \simeq \mathcal{C}_4$ and $Z^2 = Z(H)$, so $Z = Z(G)$ and $|G| = 2^6$. Then $|\operatorname{Aut} G| = 2^9$ and $|Z(\operatorname{Aut} G)| = 2$, but $Z \nleq \Phi(G)$.

We pause for a further remark on what was discussed in the previous section. Corollary 3.3 makes sure that, even without extra hypotheses on the centre, the second upper central factor of the groups that we are dealing with cannot have order p. A slight improvement is the following.

Lemma 4.6. *Let G be a finite nontrivial p-group such that $G \simeq \operatorname{Aut} G$. If $G \not\simeq D_8$ then $|Z_2(G)/Z(G)| > p^2$.*

Proof. Let G be a counterexample, hence $|Z_2(G)/Z(G)| = p^2$. By Lemma 3.1, in the notation used there, as $Z < C$ and $|C| < |Z_2|$ we have $Z \lessdot C$; since $\mathrm{rk}(C) \geq \bar{d}r$ this implies that Z is cyclic and $\bar{d} = 2$. Hence $Z \leq \Phi := \Phi(G)$ by Corollary 4.5, and so $d(G) = 2$. Also, $I \cap Z < Z(I)$ by Lemma 3.1 and $|Z(I)| = p^2$, so $|G/I\Phi| \leq |G/IZ| = |I \cap Z| = p$; thus $I \nleq \Phi$ and G/I is cyclic, of order $p^\lambda = |Z|$. By [1] we have that $p^{\lambda+1} = |C| = |\operatorname{Hom}(G, Z)|$; as $\lambda > 1$ by Theorem 4.2, then $G_{\mathrm{ab}} \simeq \mathcal{C}_{p^\tau} \times \mathcal{C}_p$ for some integer $\tau \geq \lambda$. Let K be the characteristic subgroup of G such that $G/K \simeq Z$ introduced in Lemma 4.3. Then $K \cap \Phi = G'G^{p^\lambda}$ and so $K \cap Z = K \cap \Phi \cap Z = G'G^{p^\lambda} \cap Z \leq I \cap Z$; thus $|K \cap Z| = p$. Hence by Lemma 4.3 (or also by a direct argument) $\exp(G/ZG') = p$, that is: $ZG' = \Phi$. Therefore $C_{\operatorname{Aut} G}(Z, G/Z) \simeq \operatorname{Hom}(G/\Phi, Z)$ has order p^2. Hence G has a normal subgroup S—corresponding to $C_{\operatorname{Aut} G}(Z)$ in an isomorphism $\operatorname{Aut} G \to G$ mapping $\operatorname{Inn} G$ onto I—such that $|S \cap C| = p^2 = |I \cap C|$ and $I < S$, that the latter inclusion is strict is a consequence of the already quoted Gaschütz-Schmid Theorem, or also of the fact that G/S embeds in $\mathrm{Aut}(Z)$ and so $|G/S| < |G/I|$. Then $S \cap C = I \cap C$, hence $S \cap IC = I(S \cap C) = I$; as G/I is cyclic this proves that $IC = I$, which is a contradiction since $IC \lessdot G$. □

Together with Theorem 4.2 this yields:

Corollary 4.7. *Let G be a finite nontrivial p-group such that $G \simeq \operatorname{Aut} G$. If G has coclass at most 3 then $G \simeq D_8$.*

Consider again the special case of groups with cyclic centre. The next lemma gives strong information on the embedding of $\operatorname{Inn} G$ in $\operatorname{Aut} G$ in this case, showing that $\operatorname{Inn} G$ is cyclic modulo the commutator subgroup of $\operatorname{Aut} G$.

Lemma 4.8. *Let G be a finite p-group such that $G \simeq \operatorname{Aut} G$ and $Z = Z(G)$ is cyclic. Let $I \simeq \operatorname{Inn} G$ be defined as in Lemma 3.1. Then both $G/[G, \operatorname{Aut} G]$ and $I/[I, G]$ are cyclic.*

Proof. That $G/[G, \operatorname{Aut} G]$ is cyclic follows from Lemma 2.2: if M is the subgroup defined there $M/[G, \operatorname{Aut} G]$ is the only maximal subgroup of $G/[G, \operatorname{Aut} G]$. By applying the natural conjugation epimorphism $\sim : G \twoheadrightarrow \operatorname{Inn} G$, since $[G, \operatorname{Aut} G]^\sim = [\operatorname{Inn} G, \operatorname{Aut} G]$ we see that $\operatorname{Inn} G/[\operatorname{Inn} G, \operatorname{Aut} G]$ is cyclic, but this quotient is isomorphic to $I/[I, G]$ because of the isomorphisms from $\operatorname{Aut} G$ to G mapping $\operatorname{Inn} G$ onto I. □

Lemma 4.9. *Let G be a nontrivial finite p-group such that $G \simeq \operatorname{Aut} G$. If $Z(G)$ is cyclic and $G \not\simeq D_8$ then G has exactly one characteristic subgroup V which is elementary abelian of rank 2. Moreover,*

(*i*) *$C_G(V)$ is the only characteristic maximal subgroup of G;*

(*ii*) *G has a characteristic subgroup L such that G/L is cyclic of order p^2, and $V \leq Z(L) \cap \Phi(G)$.*

Proof. We first establish the uniqueness of V. Suppose that V is as required in the first part of the statement. Then $V \nleq Z := Z(G)$ and so $|G/C_G(V)| = p$. Lemma 2.2 shows that G has exactly one characteristic maximal subgroup M; since $C_G(V)$ is characteristic then $M = C_G(V)$ (thus after proving that such a V does exist we will have proved (*i*) as well). If V_1 is a characteristic subgroup of G isomorphic to V then, by the same reason, $M = C_G(V_1)$. Let $A = VV_1$. Since A is characteristic $A \leq Z(M)$, by Lemma 2.2 again. Also, both V and V_1 lie in $Z_2(G)$, but not in Z, hence $1 \neq [G, A] \leq A \cap Z$, and $|A \cap Z| = p$. Thus we are in position to apply Lemmas 1.3 and 1.5 to G/M and A; we obtain that $1 = \mathrm{rk}(G/M) = \mathrm{rk}(A) - 1$, so $\mathrm{rk}(A) = 2$. Therefore $V = V_1$, and uniqueness is proved.

Next we note that $\Phi := \Phi(G)$ is not cyclic. In fact G has an elementary abelian normal subgroup E of rank $d(G)$, as $C_{\operatorname{Aut} G}(\Phi, G/Z[p]) \simeq G/\Phi$. If Φ is cyclic then $|G/E\Phi| = |E \cap \Phi| \leq p$, thus G/E is cyclic; but then $G' \leq E \cap \Phi$, hence G has class 2, which is false by Theorem 2.4. Now we may apply [6], Hilfssatz III.7.5: since Φ is a noncyclic normal subgroup of $G \rtimes \operatorname{Aut} G$ and is contained in the Frattini subgroup of the latter then Φ contains a subgroup V with the required property: it is characteristic in G and isomorphic to $\mathcal{C}_p \times \mathcal{C}_p$.

Finally, it follows from Theorem 4.2 and Lemma 4.3 that G has a characteristic subgroup L such that G/L is cyclic of order p^2, and $L \lessdot M$. If L is cyclic, then $M = VL$ and since $V \leq Z(M)$ then M is abelian, but this is a contradiction by Proposition 3.4. Thus L is not cyclic. As $M = G^p[G, \operatorname{Aut} G]$ by Lemma 4.8, we have $L \leq M \leq \Phi(G \rtimes \operatorname{Aut} G)$, so, by the same Hilfssatz used above, we can find a subgroup of the required type inside L, but then this subgroup is V, by uniqueness. So $V \leq Z(L)$, and the proof is complete. □

5. Ranks of abelian subgroups

The main theme of this section is computing (maximal) ranks of abelian subgroups in normal sections of the group that we are studying. The first relevant information is that G has a normal abelian subgroup of rank greater than $d(G)$.

Proposition 5.1. *Let G be a finite nontrivial p-group such that $G \simeq \operatorname{Aut} G$. If $G \not\simeq D_8$ then $\operatorname{mk}_G(G) > d(G)$.*

Proof. If $Z(G)$ is not cyclic the result follows from Lemma 3.1 in a straightforward way: in the notation used there $\operatorname{mk}_G(G) \geq \operatorname{mk}_G(C) \geq \bar{d}r \geq 2\bar{d}$, and $2\bar{d} > d$ since $1 < \bar{d} \geq d-1$. We may therefore assume that $Z := Z(G)$ is cyclic. We can choose characteristic subgroups L and V in G such as in Lemma 4.9. Then $C_{\operatorname{Aut} G}\big(L \cap \Phi(G), G/V\big) \simeq \operatorname{Der}\big(G/L \cap \Phi(G), V\big)$ is elementary abelian of rank $d+1$ by Lemmas 1.3 and 1.5. The result follows. □

Since $\operatorname{rk}(G) = d(G)$ for every powerful p-group G, we have:

Corollary 5.2. *Let G be a finite nontrivial powerful p-group. Then $G \not\simeq \operatorname{Aut} G$.*

Lemma 4.9 shows that in the groups that we are considering the second centre cannot be cyclic, nor can the Frattini subgroup, if the centre is cyclic. Both these remarks can be improved upon. We start with the first, the second is deferred since the argument for the Frattini subgroup will be made simpler after the proof of Theorem 5.4.

Proposition 5.3. *Let G be a finite nontrivial p-group such that $G \simeq \operatorname{Aut} G$. If $G \not\simeq D_8$ then $\operatorname{mk}_G\big(Z_2(G)\big) \geq 3$.*

Proof. Suppose first that $Z := Z(G)$ is not cyclic. We may obviously assume that Z has rank 2. Proposition 5.1 implies that G has a normal elementary abelian subgroup E of rank 3 containing $Z[p]$. Then $E \leq Z_2(G)$ and the result is proved in this case. Now suppose that Z is cyclic. Let L and V be characteristic subgroups of G such that $V \simeq \mathcal{C}_p \times \mathcal{C}_p$, $G/L \simeq \mathcal{C}_{p^2}$ and $V \leq Z(L) \cap \Phi(G)$ (see Lemma 4.9). Then $\varGamma := C_{\operatorname{Aut} G}(L \cap \Phi(G), G/V)$, which is abelian, contains $\varGamma_1 := \varGamma \cap \operatorname{Aut}_c G = C_{\operatorname{Aut} G}(\Phi(G), G/Z[p]) \simeq G/\Phi(G)$ and $\varGamma_2 := C_{\operatorname{Aut} G}(L, G/V) \simeq V$ (see Lemma 1.1). Thus $\varGamma_1 \cap Z_2(\operatorname{Aut} G)$ has rank at least 2. Moreover $\varGamma_1 \cap \varGamma_2 = C_{\operatorname{Aut} G}(L\Phi(G), G/Z[p])$, and since $L\Phi(G)$ is the characteristic maximal subgroup of G, Lemma 2.2 shows that $\varGamma_1 \cap \varGamma_2$ is in $Z(\operatorname{Aut} G)$ and so has order p. Hence $\varGamma_2 \not\leq \varGamma_1$, thus $\big(\varGamma_1 \cap Z_2(\operatorname{Aut} G)\big)\varGamma_2$ is an elementary abelian subgroup of $Z_2(\operatorname{Aut} G)$ of rank at least 3 and normal in $\operatorname{Aut} G$. Thus the proposition is proved. □

The main result in this section is the following theorem.

Theorem 5.4. *Let G be a finite p-group of class 3 with cyclic centre. Then $G \not\simeq \operatorname{Aut} G$.*

Proof. Let us fix some notation first. Let $Z = Z(G)$, $Z_2 = Z_2(G)$ and $\gamma_3 = \gamma_3(G)$. Throughout the proof A will always denote a (suitably chosen) elementary abelian G-invariant subgroup of Z_2 not contained in Z, and, for any choice of A, we will let $B = C_G(A)$, $n = \operatorname{rk}(A)$ and $t = \operatorname{rk}\big(A\Phi(G)/\Phi(G)\big)$. Then $[G, A] = C_A(G) = Z[p]$ and G/B embeds in $\operatorname{Hom}(A/Z[p], Z[p])$, so $\Phi(G) \leq B$, and we will be in position to apply Lemma 1.3 or Lemma 1.5 to A. Thus $\operatorname{rk}(G/B) = n-1$. We also set $d = d(G)$, $m = \operatorname{mk}(G)$ and $s = \operatorname{rk}(G')$. We argue by contradiction and suppose that $G \simeq \operatorname{Aut} G$. Hence we can choose normal subgroups I and C of G as in Lemma 3.1, so $I \simeq \operatorname{Inn} G$ and $C = C_G(I) \simeq \operatorname{Aut}_c G$. We have:

$$d - t \geq 2, \qquad s \leq 1 + \binom{d}{2}, \qquad d \leq s + 1, \qquad m \leq s + 2. \tag{1}$$

The first two inequalities are obvious, since G has class 3 (hence G/A is not cyclic) and γ_3 is cyclic. The remaining two are consequences of the fact that $I/[I, G]$ is cyclic (see Lemma 4.8). We have $d(I) \leq 1 + \operatorname{rk}([I, G]) \leq 1 + s$, but $d(I) = d$ because $Z \leq \Phi(G)$ by Corollary 4.5. Finally, $I \simeq G/Z$ has an elementary abelian subgroup of rank $m-1$; as $I/[I, G]$ is cyclic then $[I, G]$ has an abelian subgroup of rank $m-2$, hence $s \geq m-2$.

Consider the case when $p \neq 2$. Then, by Lemma 1.3, $\operatorname{Aut} G$ has an abelian subgroup of rank $d-t+\binom{n}{2}$, namely $C_{\operatorname{Aut} G}(A\Phi(G), G/A)$, hence $m \geq d-t+\binom{n}{2}$. By Proposition 5.3 we may choose A such that $n=3$, so that $m \geq d-t+3 \geq 5$. Thus $s \geq m-2 \geq 3$. On the other hand, if we choose $G'[p]$ for A, then $n=s$ and $t=0$. Thus $s+2 \geq m \geq d+\binom{s}{2}$, hence $s \geq \binom{s}{2}$ and so $s=3$, but also $d=2$. This is a contradiction, by (1). Therefore we may assume that p is 2.

The proof in this case relies on Lemma 1.5. Let $W = AG'G^4$ and set $w = \operatorname{rk}(AG^2/W)$ and $b = \operatorname{rk}(B^2W/W)$. By considering $C_{\operatorname{Aut} G}(W, G/A)$, and thanks to Lemma 1.5 we obtain a lower bound for m:

$$m \geq d-t+\binom{n-1}{2}+w-b. \tag{2}$$

It is clear that $w \geq b$. Also, b is the rank of the image of the endomorphism $g \in B/W \mapsto g^2 \in B/W$, whose kernel contains AG^2/W, hence $b \leq \operatorname{rk}(B/AG^2)$. Since $d = \operatorname{rk}(G/G^2) = t + \operatorname{rk}(B/AG^2) + \operatorname{rk}(G/B)$ and the last summand equals $n-1$, it follows that

$$0 \leq b \leq d-t-n+1 \qquad \text{and} \qquad m \geq w+\binom{n}{2}; \tag{3}$$

the second part follows from the first and from (2). Recall that G/G' has a cyclic quotient of size $|Z| > 2$, by Lemma 4.3. Thus, by choosing $G'[p]$ for A we have $w > 0$ and $n = s$, hence $s+2 \geq m \geq 1+\binom{s}{2}$, by employing (1) too. Therefore:

$$s \leq 3 \qquad \text{and} \qquad m \leq 5. \tag{4}$$

As a consequence, $\operatorname{mk}_G(Z_2) = 3$, for we know from Proposition 5.3 that $\operatorname{mk}_G(Z_2) \geq 3$, and if this inequality were strict then we could choose A such that $n=4$, so (3) would give $m \geq w+6$, in contradiction to (4).

From now on we shall assume that A has been chosen such that $n=3$. Note that $G'[2] \leq A$, since $[G', A] = 1$ and $\operatorname{rk}(A) = \operatorname{mk}_G(Z_2)$. We consider the possibility of low values for w. We have:

$$w \leq 1 \implies [G^2, G] \leq \gamma_3 \text{ and } |\gamma_3| = \exp(G'/\gamma_3) = 2. \tag{5}$$

In fact $w = \operatorname{rk}(AG^2/AG')$, hence if $w \leq 1$ then G/AG' is the direct product of a cyclic group by an elementary abelian one. Let $R/\gamma_3 = Z(G/\gamma_3)$. Then $AG' \leq R$ (recall that $[G, A] \leq Z[2] \leq \gamma_3$); since G/R must have a noncyclic homocyclic direct factor of exponent $\exp(G/R)$ (see for instance [3], Lemma 1.6) it follows that $AG^2 \leq R$. Thus $\exp(G'/\gamma_3) = \exp(G/R) = 2$, a fortiori $\exp(G/Z_2) = 2$, so $\exp(\gamma_3) = 2$; since γ_3 is cyclic (5) follows. Our next aim will be showing that $w \neq 0$, that is to say, $W < AG^2$. So, assume that $w = 0$. Then $G^2 \leq W$, hence $G^2 \leq AG'$. By using Lemma 4.3 again we deduce that $\exp(G_{\mathrm{ab}}) = |Z| = 4$, and $Z \leq K$, where K is a characteristic subgroup of G such that G/K is $(\operatorname{Aut} G)$-isomorphic to Z. Then every central automorphism of G acts trivially on G/K and so on Z, hence $\operatorname{Aut}_c G \simeq \operatorname{Hom}(G/Z, Z)$. On the other hand, by [1], $|\operatorname{Aut}_c G| = |\operatorname{Hom}(G, Z)|$. It follows that Z is in the kernel of every homomorphism from G to Z, hence $Z \leq G'$, and $\operatorname{Aut}_c G \simeq G_{\mathrm{ab}}$. From Lemma 3.1 we know that $|C| < |Z_2|$; more precisely the argument there shows that $|Z_2|/|C| = |G/IC| > 1$. Since $|C| = |G_{\mathrm{ab}}|$ then $|G'| > |G/Z_2| \geq 4$. By (5), on the other hand, $|G'| \leq 2^{s+1}$, hence $s \geq 2$. Now $G'[2] = A \cap G'$ and $|AG'/G'| = |A/G'[2]| \leq 2$. But $G' < G^2 \leq AG'$, thus $G^2 = AG'$ and $\big|A/G'[2]\big| = 2$, that is, $s = 2$. Earlier inequalities now give that $|G'| = 8$ and $|G/Z_2| = 4$, and also $|G/IC| = |Z_2|/|G_{\mathrm{ab}}| = 2$. By using (5) we deduce that $|G'/\gamma_3| > 2$ and hence also that $G^2 = AG'$ does not have index 4 in G. Thus $d > 2$. Also, since $Z \leq G'$ then $G' = ZG'[2]$. Therefore $C_G(G')$ is a characteristic subgroup of index 2 in G, hence it is M, the only characteristic maximal subgroup of G (see Lemma 2.2). Clearly $G' \leq I$, as $|G/I| = |Z| = 4$, hence $C = C_G(I) \leq M$, while $I \not\leq M$, since $G' \not\leq Z(I)$ because I/G' is cyclic by Lemma 4.8. In particular, $M \neq IC$. Now, $Z_2 \leq M$, by the uniqueness of M. If $Z_2 \not\leq IC$ then $G = Z_2IC$, because IC is maximal, and so $[I, G] = [I, Z_2]I' \leq Z(I)$. This is a contradiction, by Lemma 4.8 again. Therefore $Z_2 \leq IC$; as $|G/Z_2| = 4$ then $Z_2 = IC \cap M$, and therefore $C \leq Z_2$. Now $C \simeq G_{\mathrm{ab}}$, so $A_1 := C[2]$ is an elementary abelian G-invariant subgroup of Z_2 of rank $d > 2$ (in other words, A_1 is a possible choice for A). Hence $G/C_G(A_1)$ should have rank $d-1$, but A_1 is centralized by IC, which is maximal in G. This contradiction establishes our claim:

$$w > 0. \tag{6}$$

If $t = 0$ (that is, if $A \leq G^2$) then $A \leq Z(G^2)$, and since $\mathrm{rk}(A) = 3 = \mathrm{mk}_G(Z_2)$ then A is the socle of $Z(G^2) \cap Z_2$, hence it is characteristic in G. Then also W is characteristic, so $C_{\mathrm{Aut}\,G}(W, G/A) \lhd \mathrm{Aut}\,G$ and it follows that the lower bounds for m found in (2) and (3) also hold for $m' := \mathrm{mk}_G(G)$ in place of m. Moreover, if $S/W = (G/W)[2]$ then both S and B are characteristic in G, and $S < G$ by (6). Hence, by Lemma 2.2, both S and B are contained in M, as defined above, so that $SB < G$. Since $w = \mathrm{rk}(G/S)$ and $b = \mathrm{rk}(SB/S)$ we can draw the following conclusion:

if $t = 0$ then:

$$w > b, \qquad m \geq m' \geq d + 1 + w - b \geq d + 2, \qquad m' \geq w + 3 \geq 4. \tag{7}$$

The next step in the proof consists in computing d, s and m. If $d > 3$ then $s \geq d - 1 \geq 3$ by (1). Then $A = G'[2]$. Hence $t = 0$ and the middle chain of inequalities in (7) gives $m > 5$, which is impossible by (4). Thus $d \in \{2, 3\}$. Suppose that $d = 2$. Then $s \leq 2$ and $m \leq 4$ by (1). On the other hand $|G/G^2| = 4 = |G/B|$, hence $B = G^2$, so $A \leq G^2$, i.e., $t = 0$, and (7) applies to show that $m' = 4$ and $w = 1$. Thus $G^2 = Z_2$, by (5), so $A = G^2[2]$, and G has an elementary abelian normal subgroup E of rank 4. Since $EG^2 < G$ and $\mathrm{mk}_G(G^2) = 3$ then $E \cap G^2$ has rank 3, hence $E \cap G^2 = A$, but this is a contradiction since $E \not\leq G^2 = C_G(A)$. Therefore $d = 3$. Now the first half of (3) translates into $0 \leq b \leq 1 - t$, hence $t \leq 1$. We shall prove that $m = 5$—we already know that $m \leq 5$, by (4). If $t = 0$ this immediately follows from (7); similarly $m = 5$ if $w \geq 2$, by the second part of (3). So we may assume that $t = 1$ and $w = 1$. Then from (5) it follows that AG^2/γ_3 is a central subgroup of index 4 in G/γ_3, and hence $|G'| = 4$. This is a contradiction, by an argument already used for (1): as $I/[I, G]$ is cyclic, $3 = d = d(I) = \mathrm{rk}(I/I')$ and $I' \neq 1$, we must have $\big|[I, G]\big| > 4$. Therefore $m = 5$. Then $s = 3$ by (1) and (4). As above, this implies that $A = G'[2]$, thus $t = 0$ and $m' = 5$ by (7), that also yields $w - b = 1$. Furthermore $Z_2 \leq G^2$, otherwise $\mathrm{rk}(G/Z_2) = 2$, hence $G'Z/Z$ is cyclic and $s = \mathrm{rk}(G') = 2$. Now let E be an elementary abelian normal subgroup of rank 5 in G. As $\mathrm{rk}(G/Z_2) = 3$ we have that $\mathrm{rk}(E \cap Z_2) \geq 2$. If $A \not\leq E$ then AE cannot be abelian (otherwise it would have rank 6) and E is maximal in AE. Then $AE \cap Z = E \cap Z = Z[2] = [A, E]$. Hence AEZ/Z is elementary abelian of rank 5, and $\mathrm{mk}(I) = 5$. Then, since $I/[I, G]$ is cyclic, $\mathrm{rk}(G') \geq \mathrm{rk}[I, G] \geq 4$, a contradiction. Therefore $A \leq E$. It follows that $E \leq B = C_G(A)$; since $|B/G^2| = 2$ then $\mathrm{rk}(E \cap G^2) > 3$ and so $G^2 \neq Z_2$. Then $w > 1$ by (5), so $w = 2$ by (3). If $E \not\leq G^2$ then $B = EG^2$, so B/W has exponent 2 and $b = 0$. This is impossible, since we showed that $w - b = 1$. Therefore $E \leq G^2$. Now $\mathrm{rk}(G^2/G') = w = 2$ and it follows that EG'/G' is the socle of G^2/G'. Since $G' \leq Z_2 \leq G^2$ and $EG' \cap Z_2 = AG' = G'$, then $Z_2 = G'$. We have: $\exp(G_{\mathrm{ab}}) = \exp(G/Z_2) = \exp(\gamma_3) = |\gamma_3| \leq |Z|$; on the other hand G has a quotient isomorphic to Z, by Lemma 4.3, hence $\exp(G_{\mathrm{ab}}) = |Z|$ and $\gamma_3 = Z$. It also follows that $\exp(Z_2/Z) = \exp(G'/\gamma_3) = |Z|$. Let $|Z| = 2^\lambda$. Then, as $w = 2$ and $G_{\mathrm{ab}} = G/Z_2$ has a noncyclic homocyclic subgroup of exponent 2^λ we have that $G_{\mathrm{ab}} \simeq \mathcal{C}_{2^\lambda} \times \mathcal{C}_{2^\lambda} \times \mathcal{C}_2$. Then $Z_2/Z = G'/\gamma_3$ is a cyclic extension of an elementary abelian group; since it has rank 3 at most $|Z_2/Z| \leq 2^{\lambda+2}$. All central automorphisms act trivially on the commutator subgroup, hence $C \simeq \mathrm{Hom}(G_{\mathrm{ab}}, Z) \simeq G_{\mathrm{ab}}$. As $1 < |G/IC| = |Z_2|/|C|$ we obtain that $|Z_2/Z| = 2^{\lambda+2}$, thus $Z(I) \simeq Z_2/Z \simeq \mathcal{C}_{2^\lambda} \times \mathcal{C}_2 \times \mathcal{C}_2$, and $|G/IC| = 2$. Now $Z(I) = I' \leq G'$, as $Z_2 = G'$. Thus A is the socle of $Z(I)$. Then IC centralizes A, and this is a contradiction, since $|G/B| = 4$. This completes the proof of the theorem. □

Proposition 5.5. *Let G be a finite nontrivial p-group such that $G \simeq \mathrm{Aut}\,G$ and $G \not\simeq D_8$. Let E be an elementary abelian normal subgroup of G of maximal rank. Then $|E \cap \Phi(G)| > p^2$. In particular,* $\mathrm{mk}_G\big(\Phi(G)\big) \geq 3$.

Proof. Let $\Phi = \Phi(G)$ and $d = d(G)$. Suppose that $|E \cap \Phi| \leq p^2$. Since $E\Phi < G$ and so $|E/E \cap \Phi| \leq p^{d-1}$, and since $\mathrm{rk}(E) = \mathrm{mk}_G(G) > d$ by Proposition 5.1, it follows that $\mathrm{mk}_G(G) = d + 1$ and $|E \cap \Phi| = p^2$, thus $|G/E\Phi| = p$, so G/E is cyclic. Therefore $G' \leq E \cap \Phi$ and $G' = E \cap \Phi$ by Theorem 2.4; also, $|G/C_G(G')| = p$, hence $C_G(G') = E\Phi$. Since $\Phi/G' \simeq E\Phi/E$ is cyclic, Φ is abelian. Now G has class 3, therefore $Z := Z(G)$ is not cyclic, by Theorem 5.4. Since $\mathrm{mk}_G(G) = d + 1$ it follows from Lemma 3.1 that Z has rank 2 and $d(G/Z[p]) = d - 1$, so $p = 2$, and also that $d \leq 3$. This also means that G has a direct factor of order 2, since it is not abelian then $d = 3$. Hence $F := Z[2]\Phi$ has index 4 in G. Now G/E is cyclic and E is not maximal in G, because it is abelian (see Proposition 3.4), so there exists a subgroup $L \lhd G$ such that $E \leq L$ and G/L is cyclic of order 4. Let $\Sigma = C_{\mathrm{Aut}\,G}(L \cap F, G/Z[2]G')$; it is abelian since $Z[2]G' \leq L \cap F$.

Then Σ contains $C_{\operatorname{Aut} G}(F, G/Z[2])$, that has rank 4, but also some noncentral automorphisms in $C_{\operatorname{Aut} G}(L, G/G')$, as follows from Lemma 1.1. Hence $\operatorname{rk}(\Sigma) > 4$, so G has an elementary abelian subgroup A of rank 5. As $A\Phi < G$ then $A \cap \Phi$ has rank 3 at least. But $\operatorname{rk}(\Phi) \leq 3$, for $\operatorname{rk}(G') = 2$ and Φ/G' is cyclic. Then $A = \Phi[2] \geq G'$, so $A \lhd G$. On the other hand $\operatorname{mk}_G(G) = d + 1 = 4$, hence we have reached a contradiction. Thus the proof is complete. □

As an application of our results we can show that 'small' p-groups cannot provide new examples of groups isomorphic to their automorphism groups.

Proposition 5.6. *Let G be a finite nontrivial p-group. If $G \simeq \operatorname{Aut} G$ and $|G| \leq p^7$ then $G \simeq D_8$.*

Proof. Suppose that G is not isomorphic to D_8. As $|Z| > p$ and $|Z_2/Z| > p^2$ (see Theorem 4.2 and Lemma 4.6; we are still writing Z and Z_2 for $Z(G)$ and $Z_2(G)$), and by Theorems 2.4 and 5.4, we immediately have that G has order p^7 and class 3, its upper central factors are elementary abelian, $|Z| = |G/Z_2| = p^2$ and $|Z_2/Z| = p^3$. If $Z \nleq \Phi(G)$ then $G \simeq \mathcal{C}_p \times H$ for a suitable group H, and it easily follows that $p = 2$ and $|\operatorname{Aut} H| < |H|$; this is impossible because $|H| = p^6$ (see Remark 3.2). Let I and $C = C_G(I)$ be defined as in Lemma 3.1 and look at the embedding $\operatorname{Hom}\big(G/Z, Z\big) \rightarrowtail C$ already considered there. Since $|C| < |Z_2| = p^5$ (by the same lemma) and $Z \leq \Phi(G)$ then C is elementary abelian of rank 4 and $d(G) = 2$, so that $\Phi(G) = Z_2$; moreover the embedding actually is an isomorphism, and this means that $\operatorname{Aut}_c G$ acts trivially on Z_2. Now $C \nleq I$, because $Z(I) \simeq Z_2/Z$ has rank 3, hence $I \lessdot IC \lessdot G$ by Lemma 3.1. Also, since $C = Z(IC)$ then IC/C is not cyclic; therefore $C \leq \Phi(G) = Z_2$, actually $C \lessdot Z_2$ and so Z_2 is abelian. If $p > 2$ then $\operatorname{Der}(G/Z_2, C)$ has rank 6; this follows from Lemmas 1.1 and 1.2 as $[I, C] = 1$; hence G has an abelian maximal subgroup. This is impossible by Proposition 3.4, so $p = 2$. Moreover, as $IC \lessdot G$ and $C \leq \Phi(G)$ then $I \nleq \Phi(G)$ and G/I is cyclic. Let x be an element of G such that $G = \langle x \rangle\, I$, and let u be any element of $C \smallsetminus I$. It is not hard to check that the assignments $x^\theta = xu$ and $y^\theta = y$ for all $y \in I$ define an automorphism θ of G. Since $x^2u \in I$ then $x^2u = (x^2u)^\theta = (xu)^2u^\theta$, and so $u^\theta = u^{xu} = u^x$; hence $x^{\theta^2} = xuu^x = xu^xu = x^u$. Therefore θ^2 is the inner automorphism determined by u. As $\operatorname{Aut} G/\operatorname{Inn} G \simeq G/I$ is cyclic this shows that $\theta \in (\operatorname{Inn} G)(\operatorname{Aut}_c G)$. Thus $\theta = \alpha\tilde{g}$, for some $\alpha \in \operatorname{Aut}_c G$ and $g \in G$, here $\tilde{g}$ denotes the inner automorphism of G determined by g. Since $[I, \theta] = [Z_2, \alpha] = 1$ then g centralizes $D = I \cap Z_2$. Now $C_G(D)$ contains Z_2, which is abelian, and $C_I(D) = D$, because I is not abelian and $D \lessdot I$. Then $C_G(D)/D$ is cyclic, since G has no abelian maximal subgroups it follows that $C_G(D) = Z_2$. Therefore $g \in Z_2$ and so $\tilde{g} \in \operatorname{Aut}_c G$. This is a contradiction, because $\theta \notin \operatorname{Aut}_c G$. □

Remark 5.7. In the previous proof the fact that θ is an automorphism can be also seen as a special case of Lemma 1.1 and the following, whose proof we do not reproduce here: *Let G be a finite p-group, let A be an elementary abelian normal subgroup of G, and let N be a normal subgroup of G such that $[A, N] = 1$, $[A, G] \leq N$ and $A \leq N\Phi(G)$. Then to every derivation δ from G/N to A we can associate an automorphism $\delta^* : g \in G \mapsto g(gN)^\delta \in G$, and the mapping $\delta \in \operatorname{Der}(G/N, A) \mapsto \delta^* \in C_{\operatorname{Aut} G}(N, G/A)$ is bijective.*

A further remark is that, in the case when $p = 2$, Proposition 5.6 can also be proved by a computer-aided direct inspection, which is easy to carry out with a system like GAP (see [4]). The same procedure can be used to show that *no group of order 2^8 is isomorphic to its own automorphism group*, thus extending the scope of our proposition.

As a matter of fact, Eamon O'Brian has also obtained Proposition 5.6 (for arbitrary primes) as a side result of a much more sophisticated computer calculation. The author thanks the referee for pointing out this unpublished work.

References

[1] J.E. Adney and T. Yen, *Automorphisms of a p-group*, Illinois J. Math. **9** (1965), 137–143.

[2] G. Cutolo, H. Smith, and J. Wiegold, *p-groups of maximal class as automorphism groups*, Illinois J. Math. **47** (2003), no. 1-2, 141–156.

[3] ———, *Wreath products of cyclic p-groups as automorphism groups*, J. Algebra **282** (2004), no. 2, 610–625.

[4] The GAP Group, *Gap–Groups, Algorithms, and Programming, Vers. 4.4*, 2004, (`http://www.gap-system.org`).

[5] N. Gavioli, *The number of automorphisms of groups of order p^7*, Proc. Roy. Irish Acad. Sect. A **93** (1993), no. 2, 177–184.

[6] B. Huppert, *Endliche Gruppen. I*, Springer-Verlag, Berlin, 1967.
[7] A. Mann, *Some questions about p-groups*, J. Austral. Math. Soc. Ser. A **67** (1999), no. 3, 356–379.
[8] V.D. Mazurov and E.I. Khukhro (eds.), *The Kourovka notebook*, augmented ed., Rossiĭskaya Akademiya Nauk Sibirskoe Otdelenie Institut Matematiki, Novosibirsk, 2002, Unsolved problems in group theory.
[9] D.J.S. Robinson, *Applications of cohomology to the theory of groups*, Groups—St. Andrews 1981 (St. Andrews, 1981), London Math. Soc. Lecture Note Ser., vol. 71, Cambridge Univ. Press, Cambridge, 1982, pp. 46–80.

Università degli Studi di Napoli "Federico II", Dipartimento di Matematica e Applicazioni "R. Caccioppoli", Via Cintia — Monte S. Angelo, I-80126 Napoli, Italy
E-mail address: cutolo@unina.it
URL: http://www.dma.unina.it/~cutolo/