RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

PETER V. HEGARTY

Minimal abelian automorphism groups of finite groups

Rendiconti del Seminario Matematico della Università di Padova, tome 94 (1995), p. 121-135

<http://www.numdam.org/item?id=RSMUP_1995__94__121_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 94 (1995)

Minimal Abelian Automorphism Groups of Finite Groups.

PETER V. HEGARTY (*)

ABSTRACT - We determine the smallest odd-order Abelian group which occurs as the automorphism group of a finite group.

1. Introduction.

Finite (non-cyclic) groups whose automorphism group is Abelian were first studied extensively by G. A. Miller, who wrote down in [8] a group of order 64 whose automorphism group is Abelian of order 128. Following the author of [3], I term a finite group G «miller» if $\operatorname{Aut} G$ is Abelian. Since $\operatorname{Inn} G$ is a normal subgroup of $\operatorname{Aut} G$ and $\operatorname{Inn} G \cong G/Z(G)$, a miller group is nilpotent of class at most 2. Hence, in any attempt to characterize miller groups one can confine one's attention to p-groups. By a well-known result (see [2]), the only Abelian miller groups are the cyclic groups. In the non-Abelian case, the smallest miller 2-group is well-known to be the example constructed in [8]. In the odd prime case, the question of the smallest miller p-group took much longer to resolve. It was tackled by Earnley [3] and finally settled recently by Morigi [9]. She constructed a group of order p^7 whose automorphism group is Abelian of order p^{12}, where p is any odd prime, and showed that no smaller miller p-groups existed.

In this paper I propose to answer the natural question running alongside the issue of minimal miller groups-namely, «What is the or-

(*) Indirizzo degli AA.: Department of Mathematics, University College, Cork, Ireland.

der of a smallest Abelian group which occurs as the automorphism group of a finite, non-cyclic, p-group?». For $p = 2$, the answer is G. A. Miller's group [8] of order 128. This is borne out by the classification, in [5], of all the groups whose orders divide 128, and which can occur as the automorphism group of a finite group. For p odd, it is natural to conjecture that the smallest Abelian group with the desired property is the one of order p^{12} in Morigi's paper. I shall prove that this is indeed the case.

2. Notation and terminology.

Most of the notation used is standard. All groups considered are finite.

Cent G will denote the group of central automorphisms of a group G.

A purely non-Abelian group (PN-group) is one with no Abelian direct factor.

$d(G)$ will denote the number of elements in a minimal generating system for G.

$G_n = \langle x \in G \mid x^n = 1 \rangle$ where $n \in N$.

Similarly, $G^n = \langle x^n \mid x \in G \rangle$.

$\boldsymbol{Z}_p$ denotes the field of integers mod p. An elementery Abelian p-group G of rank n will be considered as a vector space of dimension n over $\boldsymbol{Z}_p$. For a fixed basis $\{x_1, \ldots, x_n\}$ of such a group, we shall associate to each $\alpha \in$ Aut G a matrix $A = (a_{ij})$ with entries in $\boldsymbol{Z}_p$ such that $(x_i)\alpha = \sum_{j=1}^{n} a_{ij} x_j$.

The following piece of terminology is non-standard: I shall call two groups G and H *hypomorphic* if and only if

$$G' \cong H'; \quad Z(G) \cong Z(H); \quad G/G' \cong H/H'; \quad G/Z(G) \cong H/Z(H).$$

The set of all groups hypomorphic with G I shall term a *hypomorphism class*.

3. Statement of theorem and preliminary analysis.

It is our purpose to prove the following

MAIN THEOREM 3.1. *Let G be a finite non-cyclic p-group, p odd, for which* Aut G *is Abelian. Then p^{12} divides* $|\text{Aut}\, G|$.

Henceforth, then, p denotes an odd prime, G a finite p-group.

If Aut G is Abelian then Aut G = Cent G (see [3], 2.2), and G is a PN-group ([3], 2.3). Consequently, Aut G is a p-group ([3], 2.4). Thus, if G is to contradict the theorem, Aut G must have order p^n for some $n \leqslant \leqslant 11$. By Morigi's result, $|G| \geqslant p^7$. On the other hand $|G|$ divides $|\mathrm{Aut}\, G|$ when G is miller. Thus $p^7 \leqslant |G| \leqslant p^{11}$.

Our first result allows us to eliminate $|G| = p^{11}$, and may be of independent interest. One may observe that the result is just a slight improvement upon a special case of that of Faudree [4], that the order of every finite p-group of class 2 divides that of its automorphism group. It is not surprising, therefore, that the proof follows precisely the approach of Faudree. The notation for the proof is taken entirely from [4], and henceforth I will assume the familiarity of the reader with that paper.

LEMMA 3.2. *Let G be a miller p-group, p odd. Then* $|G|$ *properly divides* $|\mathrm{Aut}\, G|$ (1).

PROOF. Let G be a counterexample. Aut G is a p-group. Following [4], Aut G has a subgroup T whose order is given by

$$(1) \qquad |T| = \prod_{\mu=a}^{f} \left([\![k_\mu / m_1]\!] \times \prod_{j=1}^{n} \min\{k_\mu, m_j\} \right).$$

Since $k_a \geqslant k_b \geqslant m_1$, it follows that

$$(2) \qquad |T| = |G/G'| \left(\prod_{j=2}^{n} m_j \right)^2 \prod_{\mu=c}^{f} \prod_{j=2}^{f} \min\{k_\mu, m_j\}.$$

Then Faudree constructs a subgroup U of Aut G and shows that $(UT:T) \geqslant m_1/m_2$, in all cases. Thus, $|\mathrm{Aut}\, G|_p \geqslant |G|$ unless $n \leqslant 2$. But if $n = 2$, we still get $|UT| > |G|$ unless $d(G) = 2$, which implies that G' is cyclic i.e.: that $n = 1$.

Hence we can assume that G' is cyclic, and $|T| = |G/G'|$ in this case. We consider the same automorphisms $\sigma_1, \sigma_2, \tau_1$ and τ_2 as did Faudree, and distinguish 3 possible relationships between the quantities t_a and t_b, namely

$$(3) \qquad \text{I)}\ t_b = rt_a (r \geqslant 1), \qquad \text{II)}\ t_a = rt_b (r \geqslant l), \qquad \text{III)}\ t_a = rt_b (1 < r < l).$$

(1) The author has been able to prove this result also for $p = 2$. The proof is omitted, as it would be irrelevant to the purpose of this paper.

Suppose I) holds. Replace b by $a^{-lr}b$ to get $t_b = m_1$. Thus τ_1 has order $[\![m_1^2/k_b]\!]$ mod Cent G, so Aut G Abelian $\Rightarrow k_b \geqslant m_1^2$. But then σ_1 has order k_b/m_1 mod T, so $|\text{Aut } G|_p \geqslant |G|$, with equality possible if and only if $k_b = m_1^2$. A similar analysis shows that we must have σ_1 having order m_1 mod T, and $k_a = k_b$, $t_a = 1$. Consequently, $\langle \sigma_1, \sigma_2, T\rangle$ is a p-group of order $m_1|G|$—a contradiction!

Suppose II) holds. Replace a by $b^{-r/l}a$ to get $t_a = m_1$. Then τ_2 must lie in Cent G so $k_a \geqslant m_1^2$. Then $|\langle \sigma, \sigma_2, T\rangle|$ will be strictly divisible by $|G|$ unless $k_b = m_1$, in which case $\sigma_1 \in T$ and $|\langle \sigma_2, T\rangle| = |G|$. Since $t_a = m_1$, it is clear that Cent G properly contains $\langle \sigma_2, T\rangle$ unless $d(G) = 2$. In this case, a non-central autmorphism fixing $\langle G', b\rangle$ elementwise is easily constructed, using Lemma 3.7 below.

Finally, suppose III) applies. $\tau_1 \in$ Cent G so $k_b \geqslant m_1^2$. Then, as with I), we easily deduce that $|\langle \sigma_1, \sigma_2, T\rangle|$ is strictly divisible by $|G|$.

This completes the proof of the lemma.

Hence, we can assume that if G contradicts the theorem, then $p^7 \leqslant |G| \leqslant p^{10}$. My approach will be to eliminate all possible hypomorphism classes of groups one-by-one. For most of these, straightforward applications of well-known results suffice, and no complete proofs will be given. Some individual classes cause greater difficulty and will be dealt with in more detail. I will require a long sequence of results from the literature. First, I note an immediate corollary of equation (1) above.

LEMMA 3.3. *Let G be a counterexample to the main theorem. Then $d(G') \leqslant 3$.*

This follows straight from equation (1). Lemmas 3.4-3.8 are all well-known results:

LEMMA 3.4 [10]. *Let G be a PN-group, for any prime p. Then*

$$|\text{Cent}\, G| = \prod_{i=1}^{k} |Z_{p^i}|^{r_i} \tag{4}$$

where p^k is the exponent of G/G' and, in a cyclic decomposition of G/G', there occur r_i factors of order p^i.

Recall that in a finite Abelian p-group A, the *height* of an element x is given by

$$\text{height}_A(x) = n \text{ if } x \text{ lies in } A^{p^n} \text{ but not in } A^{p^{n+1}}. \tag{5}$$

We now have

LEMMA 3.5 [1]. *Let G be a class 2 p-group with $G/G' = \prod_{i=1}^{n} \langle G' x_i \rangle$. Define*

$$K(G) = \langle x \in G \,|\, \mathrm{height}_{G/G'}(G'x) \geq b \rangle \tag{6}$$

where p^b is the exponent of G'. Also define

$$R(G) = \langle z \in Z(G) \,|\, |z| \leq p^d \rangle \tag{7}$$

where $p^d = \min(\exp Z, \exp G/G')$. Then Cent G *is Abelian if and only if $R(G) = K(G)$ and either*

(i) *$d = b$ or*

(ii) *$d > b$ and $R/G' = \langle G' x_1^{p^b} \rangle$ where x_1 is chosen from among $x_1, \dots, x_n$ such that $|x_1^{p^b}| = p^d$. In particular, R/G' is cyclic.*

LEMMA 3.6. *Let G be a finite p-group. Then* Aut G *is not Abelian if any of the following holds:*

(i) *$Z(G)$ is cyclic* [3], 2.6,

(ii) *$d(G/Z) = 2$* [3], 4.1,

(iii) exp $G = p$ [3], 3.3,

(iv) *$d(G) = 3$ and either G is special or $|G'| = p$.* [3], 4.4.

LEMMA 3.7 [6]. *Let N be a normal subgroup of a finite group G such that G/N is cyclic of order n. Write $G/N = \langle Ng \rangle$. Let $x \in Z(N)$ such that $g^n = (gx)^n$. Then the map $\alpha: G \to G$ given by*

$$n\alpha = n \ \ \forall n \in N, \qquad g\alpha = gx \tag{8}$$

can be extended to an automorphism of G.

LEMMA 3.8 [7]. *Suppose the finite group G splits over an Abelian normal subgroup A. Then G has an automorphism of order 2 which inverts A elementwise.*

4. Proof of main theorem.

Let G be a counterexample. We already know that $p^7 \leq |G| \leq p^{10}$. Now most of the hypomorphism classes of groups of these orders can be eliminated by using Lemmas 3.2-3.8 above. Obviously, the number of classes involved is far too large for detailed proofs to be given here. Details may be obtained from the author if required.

The analysis revealed a small number of classes, or collections of similar classes, which were not amenable to such straightforward treatment. I now give a list of these:

Class I. $G' \cong C_p \times C_p$; $Z(G) \cong C_{p^n} \times C_p$ for some $n \geq 2$; $G/G' \cong$ $\cong C_{p^n} \times C_p \times C_p \times C_p$; $G/Z \cong C_p \times C_p \times C_p \times C_p$.

Class II. $G' \cong C_p \times C_p$; $Z(G) \cong C_{p^n} \times C_p \times C_p$ for some $n \geq 2$; $G/G' \cong C_{p^{n+1}} \times C_p \times C_p$; $G/Z \cong C_p \times C_p \times C_p$..

Class III. $G' \cong C_p \times C_p \times C_p$; $Z(G) \cong C_{p^n} \times C_p \times C_p$ for some $n \geq 2$, $G/G' \cong C_{p^n} \times C_p \times C_p$; $G/Z \cong C_p \times C_p \times C_p$.

Class IV. $G' \cong C_p \times C_p$; $Z(G) \cong C_{p^n} \times C_p$ for some $n \geq 1$; $G/G' \cong$ $\cong C_{p^n} \times C_p \times C_p \times C_p \times C_p$; $G/Z \cong C_p \times C_p \times C_p \times C_p \times C_p$.

I shall eliminate the classes individually in a series of four lemmas. Each of the groups listed will be shown to have a non-central automorphism. My principal tool will be the following powerful criterion, due to Earnley [3], 3.2, for groups with homocyclic central quotient - a property possessed by all the groups above—to possess a non-central automorphism.

LEMMA 4.1. *Consider the extension* $1 \to Z \to G \to G/Z \to 1$ *where* G *is a* p*-group and* G/Z *is a direct product of* $n (n \geq 2)$ *copies of* C_{p^t} *for some fixed* t. *Let* $T : G/Z \to Z/Z^{p^t}$ *be the homomorphism given by* $(Zx)T = Z^{p^t} x^{p^t}$. *Also let* $[,] : G/Z \times G/Z \to Z$ *be given by* $(Zx, Zy)[,] =$ $= [x, y]$. *Now let* α *be in* Aut (G/Z) *and* β *be in* Aut Z.

Then G *has an automorphism inducing* α *on* G/Z *and* β *on* Z *if and only if the following two diagrams commute*:

$$\begin{array}{ccc} G/Z \times G/Z & \xrightarrow{[,]} & Z \\ \alpha \times \alpha \big\downarrow & & \big\downarrow \beta \\ G/Z \times G/Z & \xrightarrow{[,]} & Z \end{array} \qquad\qquad \begin{array}{ccc} G/Z & \xrightarrow{T} & Z/Z^{p^t} \\ \alpha \big\downarrow & & \big\downarrow \overline{\beta} \\ G/Z & \xrightarrow{T} & Z/Z^{p^t} \end{array}$$

where $(Z^{p^t} z)\overline{\beta} = Z^{p^t}(z\beta)$.

We now begin the process of elimination.

LEMMA 4.2. *Let* G *be a member of* Class I. *Then* G *has a non-central automorphism.*

PROOF. Let G be a counterexample. Write

$$G/G' = \langle G'a\rangle \times \langle G'b\rangle \times \langle G'c\rangle \times \langle G'd\rangle \tag{9}$$

where a^{p^n}, b^p, c^p and d^p are all in G'. Cent G is Abelian so, by Lemma 3.5, a can be chosen to have order p^{n+1} and so that $Z(G) = \langle a^p, G'\rangle$. Clearly, $|G_pZ/Z| \geqslant p^2$. First suppose that a may also be chosen so that $C_G(a)\backslash Z$ meets G_p. Then $[a, b] = b^p = 1$ WLOG. We claim that c and d can be chosen to commute. Choose both arbitrarily to begin with. $[c, d] \neq 1$ by assumption. But $C_G(b) \cap \langle c, d\rangle \subseteq Z = \phi$ as otherwise $C_G(b)$ would be a maximal subgroup of G and a non-central automorphism of G could be constructed by Lemma 3.7. Thus $G' = \langle [b, d], [c, d]\rangle$ and our claim follows easily. Indeed, we can also assume that $c^p = 1$ WLOG. But if we could also choose d of order p, then G would split over the normal Abelian subgroup $\langle Z, a, b\rangle$ and have a (non-central) automorphism of order 2, by Lemma 3.8. So we can take it that $G' = \langle a^{p^n}\rangle \times \langle d^p\rangle$. Set $a^{p^n} = z_1$ and $d^p = z_2$ for convenience. There exist i, j, k, l, m, n in $\boldsymbol{Z}_p$ such that

$$[a, c] = z_1^i z_2^j, \qquad [b, c] = z_1^k z_2^l, \qquad [b, d] = z_1^m z_2^n. \tag{10}$$

Consider the matrices

$$M = \begin{bmatrix} 1 & 0 & \gamma & \delta \\ 0 & 1 & \varepsilon & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad N = \begin{pmatrix} 1 & 0 \\ \delta & 1 \end{pmatrix}, \tag{11}$$

with entries in $\boldsymbol{Z}_p$. Let α and β be the automorphisms of G/Z and Z associated with M and N, and with respect to the bases $\{Za, Zb, Zc, Zd\}$ and $\{z_1, z_2\}$ of G/Z and G' respectively. Then one may verify that, by Lemma 4.1, there exists an automorphism of G inducing α and β provided that

$$\begin{pmatrix} k & m \\ l & n \end{pmatrix}\begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} i\varepsilon \\ j\varepsilon \end{pmatrix}. \tag{12}$$

But $(i, j) \neq (0, 0)$ as otherwise $C_G(c)$ would be maximal in G and a non-central automorphism of G could be constructed using Lemma 3.7. Similarly, $C_G(b)$ is not maximal in G, so $\det \begin{pmatrix} k & m \\ l & n \end{pmatrix} \neq 0$. So choose $\varepsilon \neq 0$ and a (unique) solution (γ, δ) to equation (12), and hence a non-central automorphism of G, is guaranteed to exist.

We may therefore assume that a cannot be chosen so that $C_G(a)\backslash Z$ meets G_p. Thus we may choose a and b so that $[a, b] = 1$ and $G' = \langle a^{p^n} \rangle \times \langle b^p \rangle$. Consequently, we can choose c and d both to have order p. It follows that $C_G(c)$ and $C_G(d)$ must both be contained in $N = \langle Z, b, c, d \rangle$. From this we easily deduce that either $[c, d] = 1$ or $Z(N)$ properly contains $Z(G)$. In the former case, G splits over the Abelian normal subgroup $\langle Z, a, b \rangle$ and has an automorphism of order 2. In the latter case, a non-central automorphism is easily constructed using 3.7.

This completes the proof of Lemma 4.2.

We continue immediately to

LEMMA 4.3. *Let G be a member of* Class II. *Then G has a non-central automorphism.*

PROOF. Let G be a counterexample. Write

$$G/G' = \langle G' a \rangle \times \langle G' b \rangle \times \langle G' c \rangle \tag{13}$$

where $a^{p^{n+1}}$, b^p and c^p are all in G'. Cent G is Abelian so, by 3.5, we must have $|a| = p^{n+1}$ and $Z(G) = G' \times \langle a^p \rangle$. If b and c could be chosen to commute, then $A = \langle G', b, c \rangle$ would be Abelian with $G/A \cong C_{p^{n+1}}$, and so G would have a non-central automorphism by 3.7. It follows that $[a, b] = 1$ WLOG. If b could be chosen to have order p, then a non-central automorphism fixing $B = \langle Z, a, b \rangle$ elementwise could be constructed using 3.7. If c could be chosen of order p, then G would split over B and have an automorphism of order 2, by 3.8. Thus we can take it that $G' = \langle b^p \rangle \times \langle c^p \rangle$. Set $z_1 = b^p$, $z_2 = c^p$ and $z_3 = a^p$. There exist i, j, k, l in $\boldsymbol{Z}_p$ such that

$$[a, c] = z_1^i z_2^j, \qquad [b, c] = z_1^k z_2^l. \tag{14}$$

Let α be the map on G/Z associated with the matrix

$$\begin{bmatrix} \gamma & \delta & 0 \\ 0 & 1 & 0 \\ 0 & \varepsilon & \phi \end{bmatrix}$$

relative to the basis $\{Za, Zb, Zc\}$. Let $\beta : Z \to Z$ be the map defined by

$$z_1\beta = z_1, \qquad z_2\beta = z_1^{\varepsilon} z_2^{\phi}, \qquad z_3\beta = z_1^{\delta} z_3^{\gamma}. \tag{15}$$

One may verify that the conditions of Lemma 4.1 are satisfied provided the following equations hold:

$$(16)\qquad \begin{pmatrix} i & k \\ j & l \end{pmatrix}\begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{bmatrix} \dfrac{i}{\phi} + j\dfrac{\varepsilon}{\phi} \\ j \end{bmatrix},$$

$$(17)\qquad k\phi = k + l\varepsilon .$$

Since $\det \begin{pmatrix} i & k \\ j & l \end{pmatrix} \neq 0$, one can readily check that a solution $(\gamma, \delta, \varepsilon, \phi) \neq$ $\neq (1, 0, 0, 1)$ to these equations exists in all cases. Furthermore we can choose our solution to satisfy $\gamma \neq 0$ and $\phi \neq 0$, thus guaranteeing that α and β define (non-trivial) automorphisms of G/Z and Z respectively, and hence the existence of a non-central automorphism of G.

This completes the proof of Lemma 4.3.

Next we have

LEMMA 4.4. *Let G be a member of* Class III. *Then G has a non-central automorphism.*

PROOF. Let G be a counterexample. Write

$$(18)\qquad G/G' = \langle G'a\rangle \times \langle G'b\rangle \times \langle G'c\rangle$$

where a^{p^n}, b^p and c^p are all in G'. Cent G is Abelian so we must, by 3.5, have $|a| = p^{n+1}$ WLOG. Let $Z = \langle z_1, z_2, z_3\rangle$ with $z_3 = a^p$ and $G' =$ $= \langle z_1, z_2, z_3^{p^{n-1}}\rangle$. WLOG, there exist i, j, k, l in $\boldsymbol{Z}_p$ such that

$$(19)\qquad b^p = z_1^i z_2^j, \qquad c^p = z_1^k z_2^l .$$

I distinguish two cases, according to whether $[a, G] \cap \langle z_3\rangle$ is trivial or not.

So first suppose that $[a, G] \cap \langle z_3\rangle = \{1\}$. Then there is no loss of generality in assuming that $[a, b] = z_1$, $[a, c] = z_2$ and $[b, c] = z_3^{p^{n-1}}$. Let α be the automorphism of G/Z associated with the matrix

$$\begin{bmatrix} 1 & \gamma & \delta \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

relative to the basis $\{Za, Zb, Zc\}$. Let β be the automorphism of Z defined by

$$(20)\qquad z_1\beta = z_1 z_3^{-\delta p^{n-1}}, \qquad z_2\beta = z_2 z_3^{\gamma p^{n-1}}, \qquad z_3\beta = z_1^{\varepsilon} z_2^{\phi} z_3 .$$

One verifies easily that the conditions imposed by Lemma 4.1 reduce to the matrix equation

$$\begin{pmatrix} i & k \\ j & l \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \varepsilon \\ \phi \end{pmatrix}. \tag{21}$$

But β is an automorphism of Z for any choice of ε and ϕ. Hence a solution $(\gamma, \delta, \varepsilon, \phi) \neq (0, 0, 0, 0)$ to equation (21) is guaranteed, and G has a non-central automorphism.

Now secondly suppose that $[a, G] \cap \langle z_3 \rangle$ is non-trivial. In this case, there is no loss of generality in assuming that $[a, b] = z_3^{p^{n-1}}$, $[a, c] = z_2$ and $[b, c] = z_1$. Let α be the automorphism of G/Z associated with the matrix

$$\begin{bmatrix} \alpha & \beta & 0 \\ 0 & 1 & 0 \\ 0 & \gamma & \alpha^{-1} \end{bmatrix}, \qquad \alpha \neq 0$$

relative to the basis $\{Za, Zb, Zc\}$. Let β be the automorphism of Z defined by

$$z_1\beta = z_1^{\alpha^{-1}}; \qquad z_2\beta = z_1^{\beta\alpha^{-1}} z_2\, z_3^{\alpha\gamma p^{n-1}}; \qquad z_3\beta = z_1^{i\beta} z_2^{j\beta} z_3^{\alpha}.$$

One easily verifies that the conditions imposed by Lemma 4.1 reduce to the following 3 equations in the 3 unknowns α, β, γ

$$i\alpha^{-1} + j\beta\alpha^{-1} = i; \qquad l\beta\alpha^{-1} = i\gamma; \qquad l = j\gamma + l\alpha^{-1}.$$

Notice that the first two imply the third when $\beta \neq 0$. But there obviously exists a solution (α, β, γ) to the first two equation for which $\alpha \neq 0$, $\beta \neq 0$. Hence G has a non-central automorphism.

This completes the proof of Lemma 4.4.

I now turn to the final and most complicated case.

LEMMA 4.5. *Let G be a member of* Class IV. *Then G has a non-central automorphism.*

PROOF. Clearly, $(G : G_pZ) \leqslant p^2$, and $(G : C_G(x)) \leqslant p^2$ for all $x \in G$. The case in which $(G : G_pZ) = (G : C_G(x)) = p^2$ for all $x \in G$ is that which causes the most dificulty, and we assume this to be the case in what follows, until otherwise indicated. Write

$$G/Z = \langle Za \rangle \times \langle Zb \rangle \times \langle Zc \rangle \times \langle Zd \rangle \times \langle Ze \rangle \tag{22}$$

where $G_p = \langle G', b, c, d\rangle$. Cent G is Abelian so, by 3.5, a can be chosen so that $|a| = p^{n+1}$ and $Z = \langle a^p, G'\rangle$. We must have $Z/Z^p = \langle Z^p a^p\rangle \times \times \langle Z^p e^p\rangle$, but will find it necessary not to assume that $e^p \in G'$. The following two assertions are easily verified:

(i) G has no Abelian subgroup of index p^2.

(ii) Let $x_1 \in G\backslash Z$. Let $x_2 \in C_G(x_1)\backslash\langle Z, x_1\rangle$. Let $x_3 \in C_G(x_2)\backslash C_G(x_1)$. Then $C_G(x_3) \not\subset \langle C_G(x_1), x_3\rangle$—otherwise stated, $\langle C_G(x_1), C_G(x_2), C_G(x_3)\rangle = G$.

We divide the analysis into 2 parts, according to whether $Z(G_p)\backslash Z$ is empty or not (the non-central automorphism we finally construct will be slightly different in the two cases).

So first suppose that $Z(G_p) \subset Z$. It is easy to see that for some g not in G_pZ, $|(C_G(g)\,G_p)/G'| = p^2$. We claim that a has this property WLOG. Suppose not. Then if g has the property we must have $g^p \in G'$. Let $[g, b] = [g, c] = 1$. Then $[b, c] \neq 1$ by assertion (i) so $[b, d] = 1$ WLOG. By assertion (ii), a can be chosen so that $[c, a] = 1$. Let $x \in \in C_G(d)\backslash Z\langle a, c, g\rangle$. Clearly x exists. But x cannot be chosen to lie in $\langle c, g\rangle$ by assertion (ii). Therefore, we can replace a by x and we have $[a, c] = = [a, d] = 1$, thus proving our claim. By similar reasoning it is easy to deduce that, for an appropriate choice of a, b, c, d and e, the following commutation relations hold:

$$[a, b] = [a, c] = [b, d] = [c, e] = [d, e] = 1\,. \tag{23}$$

Let $G' = \langle z_1\rangle \times \langle z_2\rangle$ where $z_1 = a^{p^n}$. Now there exist $i, j, k, l, m, n, q, r, s, t$ in $\boldsymbol{Z}_p$ such that

$$\begin{cases} [a, d] = z_1^i z_2^j\,, & [a, e] = z_1^k z_2^l\,, \quad [b, c] = z_1^m z_2^n\,, \\ [b, e] = z_1^q z_2^r\,, & [c, d] = z_1^s z_2^t\,. \end{cases} \tag{24}$$

Let $\alpha : G/Z \to G/Z$ be the mapping associated with the matrix

$$\begin{bmatrix} \gamma & \delta & 0 & \varepsilon & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & \phi & \gamma & \lambda & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & \mu & 0 & \nu & \gamma \end{bmatrix}$$

relative to the basis $\{Za, Zb, Zc, Zd, Ze\}$. Let $\beta : Z \to Z$ be the mapping defined by

$$a^p\beta = a^{\gamma p}\,, \qquad z_2\beta = z_2^\gamma \tag{25}$$

α and β define automorphisms of their respective groups provided $\gamma \neq 0$. The conditions imposed by Lemma 4.1 reduce, as may be verified by the reader, to the following set of equations:

$$\begin{pmatrix} i & -s \\ j & -t \end{pmatrix}\begin{pmatrix} \lambda \\ \varepsilon \end{pmatrix} = -\delta\begin{pmatrix} m \\ n \end{pmatrix}, \tag{26}$$

$$\begin{pmatrix} q & -m \\ r & -n \end{pmatrix}\begin{pmatrix} \phi \\ \mu \end{pmatrix} = -\nu\begin{pmatrix} s \\ t \end{pmatrix}, \tag{27}$$

$$\begin{pmatrix} i & q \\ j & r \end{pmatrix}\begin{pmatrix} \nu \\ \delta \end{pmatrix} = (1-\alpha)\begin{pmatrix} k \\ l \end{pmatrix}, \tag{28}$$

for the seven variables $\gamma, \dots, \nu$. If $\det\begin{pmatrix} i & q \\ j & r \end{pmatrix} = 0$ set $\gamma = 1$. Otherwise, set $\gamma = 2$, say. In either case, a solution $(\nu, \delta) \neq (0, 0)$ to (28) is guaranteed. Now $C_G(d)$ is not maximal in G, so $\det\begin{pmatrix} i & -s \\ j & -t \end{pmatrix} \neq 0$. Thus when we substitute δ into (26), the existence of a solution (λ, ε) is guaranteed. Similarly, $C_G(b)$ is not maximal in G, so $\det\begin{pmatrix} q & -m \\ r & -n \end{pmatrix} \neq 0$, and when we substitute ν into (29) the existence of a solution (ϕ, μ) is guaranteed.

Hence (26)-(28) have a solution according to which α is a non-trivial automorphism of G/Z, and we conclude that G has a non-central automorphism in this case.

Secondly, suppose that $Z(G_p) \nsubseteq Z$. G_p is not Abelian, by assertion (i), so $Z(G_p) = \langle G', b\rangle$ WLOG. A series of routine calculations lead us to conclude that a, c, d and e may be chosen so that the following commutation relations hold:

$$[a, c] = [a, e] = [b, c] = [b, d] = [d, e] = 1\,. \tag{29}$$

Let z_1 and z_2 be defined as before. Then there exist $i, j, k, l, m, n, q, r, s, t$ in $\mathbf{Z}_p$ such that

$$\begin{cases} [a, d] = z_1^i z_2^j\,, \quad [a, b] = z_1^k z_2^l\,, \quad [c, e] = z_1^m z_2^n\,, \\ [b, e] = z_1^q z_2^r\,, \quad [c, d] = z_1^s z_2^t\,. \end{cases} \tag{30}$$

Let α and β represent exactly the same mappings of G/Z and Z respectively as before. Once again α and β define automorphisms of their respective groups provided $\gamma \neq 0$. This time, the conditions imposed by Lemma 4.1 reduce to the following, slightly different, set of equations:

$$\begin{pmatrix} i & -s \\ j & -t \end{pmatrix}\begin{pmatrix} \lambda \\ \varepsilon \end{pmatrix} = -\delta \begin{pmatrix} k \\ l \end{pmatrix}, \tag{31}$$

$$\begin{pmatrix} k & q \\ l & r \end{pmatrix}\begin{pmatrix} \mu \\ \delta \end{pmatrix} = -\nu \begin{pmatrix} i \\ j \end{pmatrix}, \tag{32}$$

$$\begin{pmatrix} q & s \\ r & t \end{pmatrix}\begin{pmatrix} \phi \\ \nu \end{pmatrix} = (1 - \gamma) \begin{pmatrix} m \\ n \end{pmatrix}. \tag{33}$$

Now one reasons in precisely the same manner as before, to conclude that G possesses a non-central automorphism.

We have now dealt entirely with the case in which $(G : G_p) = (G : C_G(x)) = p^2$ for all $x \notin Z(G)$. Next, we continue to assume that $(G : G_p Z) = p^2$, but also that there exists x such that $(G : C_G(x)) = p$. If x could be chosen to lie in G_p, then we could easily construct a non-central automorphism using 3.7. Keeping the same notation for G/G' as in equation (24), I claim that for an appropriate choice of a, b, c, d and e, $e^p \in G'$, $(G : C_G(a)) = p$ and the following commutation relations hold:

$$[a, b] = [a, c] = [b, c] = [d, e] = [a, e] = 1\,. \tag{34}$$

In what follows I am assuming that $e^p \in G'$. I prove the claim in a number of stages.

Step 1. $Z(G_p) \subset Z(G)$. Suppose the contrary. G_p is clearly non-Abelian, by 3.7, so let $Z(G_p) = \langle G', b\rangle$. x (as defined above) lies outside G_p. Then we can choose c and d so that $C_G(x) = \langle Z, c, d, x, y\rangle$ for some $y \notin G_p Z$. Then $C_G(g)$ is maximal in G for some $g \in \langle c, d\rangle \backslash G'$, and G has a non-central automorphism by 3.7—contradiction!

Step 2. Suppose $C_G(x) \supset G_p$ i.e.: that x can be chosen so that $[x, b] = [x, c] = [x, d] = 1$. If $x^p \in G'$ then $G/\langle G_p, x\rangle \cong C_{p^n}$, so G has a non-central automorphism, by 3.7, unless $n = 1$, in which case a and e are interchangeable. This means we can choose x for a. Now $[b, c] = 1$ WLOG, whence $\langle a, b, c\rangle$ is Abelian. There is some g in $C_G(e)\backslash Z\langle a, b, c\rangle$, but g cannot lie in $\langle b, c\rangle$ by 3.7. Thus, we replace a by g to obtain $[a, b] =$

$= [a, c] = [b, c] = [a, e] = 1$. But now it is clear that d can also be chosen to commute with e, and the claim is established in this case.

Step 3. We must have $C_G(x) \supset G_p$ for some choice of x. Suppose not. For a given x we can still choose b and c so that $[x, b] = [x, c] = 1$. If $[b, c] = 1$, proceed as in *Step 2*. Thus $[b, d] = 1$ WLOG. Let $y \in C_G(x) \backslash \langle G_p Z, x \rangle$. Routine calculations show that y and c can be chosen to commute, whence $A = \langle Z, x, c, y \rangle$ is a normal, Abelian, complemented subgroup of G and G has an automorphism of order 2 by 3.8—contradiction! Our claim regarding equation (36) is now established in full.

Now write $G' = \langle z_1 \rangle \times \langle z_2 \rangle$ with $z_1 = a^{p^n}$ and $z_2 = e^p$. There exist i, j, k, l in $\boldsymbol{Z}_p$ such that

$$[b, e] = z_1^i z_2^j, \qquad [c, e] = z_1^k z_2^l. \tag{35}$$

Let α be the automorphism of G/Z associated with the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & \gamma & \delta & 1 & 0 \\ 0 & \varepsilon & \phi & 0 & 1 \end{bmatrix}$$

relative to the basis $\{Za, Zb, Zc, Zd, Ze\}$. Let β be the identity map on Z. The conditions imposed by Lemma 4.1 are readily checked to reduce to the matrix equation

$$\begin{pmatrix} i & k \\ j & l \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \varepsilon \\ \phi \end{pmatrix} \tag{36}$$

for the four unknowns $\gamma, \delta, \varepsilon, \phi$. The above system is underdetermined, thus guaranteeing the existence of a non-trivial solution $(\gamma, \delta, \varepsilon, \phi) \neq (0, 0, 0, 0)$ and consequently of a non-central automorphism of G.

We have now shown that Lemma 4.5 is true when $(G : G_p Z) = p^2$. One proceeds in exactly the same way as above when one assumes that $(G : G_p Z) = p$ or that $G = G_p Z$. In fact, the argument simplifies in places but, in any event, I do not think it necessary to go into any further detail. Hence, the proof of Lemma 4.5, and consequently that of the main theorem, is complete.

REFERENCES

[1] J. E. ADNEY - T. YEN, *Automorphisms of a p-group*, Illinois J. Math., **9** (1965), pp. 137-143.

[2] J. DIXON, *Problems in Group Theory*, Blaisdell, New York (1976).

[3] B. E. EARNLEY, *On finite groups whose group of automorphisms is Abelian*, Ph. D. thesis, Wayne State University, 1975, Dissertation Abstracts, V. 36, p. 2269 B.

[4] R. FAUDREE, *A note on the automorphism group of a p-group*, Proc. Amer. Math. Soc., **19** (1968), pp. 1379-1382.

[5] J. FLYNN - D. MACHALE - E. A. O'BRIEN - R. SHEEHY, *Finite groups whose automorphism groups are 2-groups*, Proc. R. Ir. Acad., **94A**, No. 2 (1994), pp. 137-145.

[6] O. J. HUVAL, *A note on the outer automorphisms of finite nilpotent groups*, Amer. Math. Monthly (1966), pp. 174-175.

[7] D. MACHALE - R. SHEEHY, *Finite groups with odd order automorphism groups*, Proc. R. Ir. Acad., to appear.

[8] G. A. MILLER, *A non-Abelian group whose group of automorphisms is Abelian*, Messenger Math., **43** (1913), pp. 124-125.

[9] M. MORIGI, *On p-groups with Abelian automorphism group*, Rend. Sem. Mat. Univ. Padova, **92** (1994).

[10] P. R. SANDERS, *The central automorphisms of a finite group*, J. London Math. Soc., **44** (1969), pp. 225-228.

Manoscritto pervenuto in redazione il 18 aprile 1994.