www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650 , ISSN (on-line): 2251-7669
Vol. 01 No.2 (2012), pp. 59-71.

www.ui.ac.ir

THE AUTOMORPHISM GROUP FOR p-CENTRAL p-GROUPS

ANITHA THILLAISUNDARAM

Communicated by Alireza Abdollahi

Abstract. A p-group G is p-central if $G^p \leq Z(G)$, and G is p^2-abelian if $(xy)^{p^2} = x^{p^2}y^{p^2}$ for all $x, y \in G$. We prove that for G a finite p^2-abelian p-central p-group, excluding certain cases, the order of G divides the order of $\mathrm{Aut}(G)$.

1. Introduction

The following conjecture has been the subject of much debate over the past forty years or so.

For G a group, we denote the group of automorphisms of G by $\mathrm{Aut}(G)$. Here $|G|$ denotes the order of the group G.

Well-known Conjecture. *For G a non-cyclic p-group of order p^n with $n \geq 3$, $|G|$ divides $|Aut(G)|$.*

Results in favour of the conjecture have been made by Buckley [1]; Davitt [2, 3, 4, 5]; Exarchakos [6]; Faudree [7]; Fouladi, Jamali & Orfi [8]; Gaschütz [9]; Gavioli [10]; Hummel [12]; Otto [4, 5, 14]; and Yadav [18]. See Result A below for further details. I apologise if I have unknowingly omitted other references.

Notice that each non-central element g of G induces a non-trivial automorphism of G via conjugation. This defines an *inner automorphism* of G. $\mathrm{Inn}(G)$ denotes the subgroup of inner automorphisms of G, which is normal in $\mathrm{Aut}(G)$. The non-inner automorphisms are called *outer automorphisms.* They

MSC(2010): Primary: 20D15; Secondary: 20D45.
Keywords: automorphism group, p-central, p^2-abelian.
Received: 09 December 2011, Accepted: 15 March 2012.

are elements in $\frac{\mathrm{Aut}(G)}{\mathrm{Inn}(G)}$ and so are defined modulo $\mathrm{Inn}(G)$. We denote the group of outer automorphisms of G by $\mathrm{Out}(G)$.

Certainly as $\mathrm{Inn}(G) \cong \frac{G}{Z(G)}$, we can rephrase the question to whether or not $|Z(G)|$ divides $|\mathrm{Out}(G)|$.

The conjecture has been established to be true for several classes of p-groups, as listed below in Result A. We note that a group G is the *central product* of two subgroups H and K if (a) $[H, K] = 1$, (b) $G = HK$, and (c) $H \cap K = Z(G)$; and a group is *modular* if each subgroup commutes with every other subgroup, i.e. for $H, K \leq G$, we have $HK = KH$.

Result A. The conjecture holds for the following finite p-groups:

- p-abelian p-groups [2];
- p-groups of class 2 [7];
- p-groups of maximal class (or coclass 1) [14];
- p-groups of coclass 2 [8];
- p-groups with centre of order p [9];
- p-groups of order at most p^7 [3, 6, 10];
- modular p-groups [4];
- p-groups with $\frac{G}{Z(G)}$ metacyclic [5];
- p-groups with $|\frac{G}{Z(G)}| \leq p^4$ [3];
- $G = A \times B$ where A is abelian and $|B|$ divides $|\mathrm{Aut}(B)|$ [14];
- G a central product of non-trivial subgroups H and A, where A is abelian and $|H|$ divides $|\mathrm{Aut}(H)|$ [12];
- G with a non-trivial normal subgroup N such that $N \cap [G, G] = 1$, and $|\frac{G}{N}|$ divides $|\mathrm{Aut}(\frac{G}{N})|$ [1];
- G such that $xZ(G) \subseteq x^G$ for all $x \in G \backslash Z(G)$, where x^G denotes the conjugacy class of x in G [18].

For $n \in \mathbb{N}$, we have $G^{\{n\}} = \{x^n | x \in G\}$ and $G^n = \langle G^{\{n\}} \rangle$.

We define the *centre* of G as $Z(G) = \big\{x \in G | x^{-1}gx = g \text{ for all } g \in G\big\}$.

We say that a p-group G is *p-central* if $G^p \leq Z(G)$. We define G to be *p^2-abelian* if for all $x, y \in G$, we have $(xy)^{p^2} = x^{p^2}y^{p^2}$.

In this paper, we prove the conjecture for p^2-abelian p-central p-groups.

Theorem 1.1. *For p an odd prime, let G be a non-abelian p^2-abelian p-central p-group, with $|G| \geq p^3$. Suppose that the centre $Z(G)$ of G is of the form*

$$Z(G) \cong \frac{\mathbb{Z}}{p^{e_1}\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{p^{e_n}\mathbb{Z}}$$

where $3 \leq e_1 \leq \ldots \leq e_n$ and $n \geq 3$. Then $|G|$ divides $|Aut(G)|$.

As p-abelian groups are p^2-abelian, Theorem 1.1 partially generalizes the fact that p-abelian p-groups satisfy the conjecture. An example of a p^2-abelian p-central p-group, that is not itself p-abelian, is the

wreath product $W = C_p \wr C_p$, which is of exponent p^2. From ([13], Examples 3.1.5(iii)), we know that W is of order p^{p+1} with maximal class p and is not regular. A result from [17] says that p-groups of maximal class with order p^n, where $4 \leq n \leq p+1$, are p-central. Also, we have an equivalence from [17] that a p-group is p-abelian if and only if it is p-central and regular. Using these two facts, we confirm that W is p^2-abelian p-central and not p-abelian.

In the following, we prove Theorem 1.1, using results on extending automorphisms of subgroups (by Passi, Singh & Yadav [15]) and on counting automorphisms of abelian p-groups (by Hillar & Rhea [11]).

This paper is an extract from my PhD thesis under the supervision of Rachel Camina.

2. **Proof of Theorem 1.1**

Let G be a p^2-abelian p-central p-group and denote $Z(G)$ by simply Z. Let $|\mathrm{Out}(G)|_p$ denote the largest power of p that divides $|\mathrm{Out}(G)|$. This corresponds to the order of a Sylow p-subgroup of $\mathrm{Out}(G)$.

To prove the theorem, as $|\mathrm{Inn}(G)| = |\frac{G}{Z}|$, it suffices to show that

$$|\mathrm{Out}(G)|_p \geq |Z|.$$

Let

$$E : 1 \to N \to G \to Q \to 1$$

be an extension of the group N by the group Q .

Note: if $N \leq Z$, then E is termed a *central* extension.

Here $\mathrm{Aut}^{\frac{G}{Z}}(G)$ is the subgroup of automorphisms of G that induce the identity on $\frac{G}{Z}$. For N normal in G, we define $\mathrm{Aut}_N(G)$ to be the subgroup of automorphisms of G that normalize N.

Our plan is to compute a lower bound for the size of a Sylow p-subgroup of $\mathrm{Out}(G)$. To do this, we choose to consider elements of $\mathrm{Aut}(Z)$ that extend to elements of $\mathrm{Aut}^{\frac{G}{Z}}(G)$. Naturally any such extension of a non-identity automorphism of Z is non-inner.

Such extendable elements of $\mathrm{Aut}(Z)$ are determined by the following result. In the following, $t : Q \to G$ is a left transversal, and $\mu : Q \times Q \to N$ is defined by

$$t(xy)\mu(x, y) = t(x)t(y).$$

Also, N^Q denotes the group of all maps ψ from Q to N such that $\psi(1) = 1$.

Lemma 2.1. [15] *Let $1 \to N \to G \to Q \to 1$ be a central extension. Using the notation above, if $\gamma \in Aut_N(G)$, then there exists a triplet $(\theta, \phi, \chi) \in Aut(N) \times Aut(Q) \times N^Q$ such that for all $x, y \in Q$ and $n \in N$ the following conditions are satisfied:*

(1) $\gamma(t(x)n) = t(\phi(x))\chi(x)\theta(n)$,

(2) $\mu(\phi(x),\phi(y))\theta(\mu(x,y)^{-1}) = \chi(x)^{-1}\chi(y)^{-1}\chi(xy)$.

Conversely, if $(\theta,\phi,\chi) \in Aut(N) \times Aut(Q) \times N^Q$ *is a triplet satisfying equation (2), then* γ *defined by (1) is an automorphism of* G *normalizing* N.

We take $N = Z$, $Q = \frac{G}{Z}$ in the lemma above. It is clear from equation (1) of Lemma 2.1 that when $\phi = 1$, the automorphism γ induces the identity on $\frac{G}{Z}$. So we set $\phi = 1$. Given a suitable $\theta \in \mathrm{Aut}(Z)$, we construct the required χ to satisfy:

$$\mu(x,y)\theta(\mu(x,y)^{-1}) = \chi(x)^{-1}\chi(y)^{-1}\chi(xy). \tag{2.1}$$

In [11], Hillar and Rhea give a useful description of the automorphism group of an arbitrary abelian p-group, and they compute the size of this automorphism group. We sketch their results here. The first complete characterization of the automorphism group of an abelian group was, however, given by Ranum [16].

We will use Hillar and Rhea's account to characterize $\mathrm{Aut}(Z)$. First, we set up the relevant notation and results leading to our desired description.

We begin with an arbitrary abelian p-group H_p, where

$$H_p \cong \frac{\mathbb{Z}}{p^{e_1}\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{p^{e_n}\mathbb{Z}}$$

and $1 \leq e_1 \leq \ldots \leq e_n$ are positive integers.

Hillar and Rhea first describe $\mathrm{End}(H_p)$, the endomorphism ring of H_p, as a quotient of a matrix subring of $\mathbb{Z}^{n\times n}$. Then, as we will see below, the units $\mathrm{Aut}(H_p) \subseteq \mathrm{End}(H_p)$ are characterized from this description.

An element of H_p is represented by a column vector $(\alpha_1,\ldots,\alpha_n)^T$ where $\alpha_i \in \frac{\mathbb{Z}}{p^{e_i}\mathbb{Z}}$.

Definition 2.2. *(*[11]*, Definition 3.1)*

$$R_p = \{(a_{ij}) \in \mathbb{Z}^{n\times n} : p^{e_i - e_j} | a_{ij} \text{ for all } i \text{ and } j \text{ satisfying } 1 \leq j \leq i \leq n\}.$$

From [11], we have that R_p forms a ring.

Let $\pi_i : \mathbb{Z} \longrightarrow \frac{\mathbb{Z}}{p^{e_i}\mathbb{Z}}$ be defined by $x \mapsto x \bmod p^{e_i}$. Let $\pi : \mathbb{Z}^n \longrightarrow H_p$ be the homomorphism given by

$$\pi(x_1,\ldots,x_n)^T = (\pi_1(x_1),\ldots,\pi_n(x_n))^T.$$

Here is the description of $\mathrm{End}(H_p)$ as a quotient of the matrix ring R_p.

Theorem 2.3. [11] *The map* $\psi : R_p \longrightarrow End(H_p)$ *given by*

$$\psi(A)(\alpha_1,\ldots,\alpha_n)^T = \pi(A(\alpha_1,\ldots,\alpha_n)^T)$$

is a surjective ring homomorphism.

Let K be the set of matrices $A = (a_{ij}) \in R_p$ such that $p^{e_i} | a_{ij}$ for all i, j. This forms an ideal.

Lemma 2.4. [11] *The ideal K, as defined above, is the kernel of ψ.*

Theorem 2.3 and Lemma 2.4 give that $\mathrm{End}(H_p)$ is isomorphic to $\frac{R_p}{K}$. For more details, the reader is referred to [11].

The following is a complete description of $\mathrm{Aut}(H_p)$.

Theorem 2.5. *(*[11]*, Theorem 3.6) An endomorphism $M = \psi(A)$ is an automorphism if and only if $A(mod\ p) \in GL_n(\mathbb{F}_p)$.*

Hillar and Rhea illustrate how to calculate $|\mathrm{Aut}(H_p)|$, which is presented in the theorem below. First, the following numbers are defined:

$$d_k = \max\{m : e_m = e_k\},\ c_k = \min\{m : e_m = e_k\}.$$

Since $e_m = e_k$ for $m = k$, we have the two inequalities $d_k \geq k$ and $c_k \leq k$.

Note that

$$c_1 = c_2 = \ldots = c_{d_1},$$

and

$$c_{d_1+1} = \ldots = c_{d_{d_1+1}},$$

etc. So we have

$$c_1 = \ldots = c_{d_1} < c_{d_1+1} = \ldots = c_{d_{d_1+1}} < c_{d_{d_1+1}+1} = \ldots.$$

We introduce the numbers e'_i, C_i, D_i as follows. Define the set of distinct numbers $\{e'_i\}$ such that

$$\{e'_i\} = \{e_j\} \text{ and } e'_1 < e'_2 < \ldots.$$

Let $l \in \mathbb{N}$ be the size of $\{e'_i\}$. So $e'_1 = e_1$, $e'_2 = e_{d_1+1}$, $\ldots$, $e'_l = e_n$.

Now define

$$D_i = \max\{m : e_m = e'_i\} \text{ for } 1 \leq i \leq l$$

and

$$C_i = \min\{m : e_m = e'_i\} \text{ for } 1 \leq i \leq l.$$

Note that $C_1 = 1$ and $D_l = n$. For convenience, we also define $C_{l+1} = n + 1$.

Theorem 2.6. *(*[11]*, Theorem 4.1) The abelian group $H_p = \mathbb{Z}/p^{e_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{e_n}\mathbb{Z}$ has*

$$|Aut(H_p)| = \prod_{k=1}^{n}(p^{d_k} - p^{k-1}) \prod_{j=1}^{n}(p^{e_j})^{n-d_j} \prod_{i=1}^{n}(p^{e_i-1})^{n-c_i+1}.$$

Proof. Their calculation involves finding all elements of R_p that are invertible modulo p, and computing the distinct ways of extending such elements to automorphisms of the group.

So, we need to count all matrices $M \in R_p$ that are invertible modulo p. These M are "upper block triangular" matrices which may be expressed in the following three forms.

$$M = \begin{bmatrix} m_{11} & & & & & & & & & * \\ \vdots & & & & & & & & & \\ m_{D_1 1} & \cdots & m_{D_1 D_1} & & & & & & & \\ & & & m_{C_2 C_2} & & & & & & \\ & & & \vdots & & & & & & \\ & & & m_{D_2 C_2} & \cdots & m_{D_2 D_2} & & & & \\ & & & & & & \ddots & & & \\ & & & & & & & m_{C_l C_l} & & \\ & & & & & & & \vdots & & \\ 0 & & & & & & & m_{D_l C_l} & \cdots & m_{D_l D_l} \end{bmatrix}$$

or

$$M = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1n} \\ \vdots & & & \\ m_{d_1 1} & & & \\ & m_{d_2 2} & & \\ & & \ddots & \\ 0 & & & m_{d_n n} \end{bmatrix} = \begin{bmatrix} m_{1c_1} & & & & * \\ & m_{2c_2} & & & \\ & & \ddots & & \\ 0 & & & m_{nc_n} & \cdots & m_{nn} \end{bmatrix}.$$

The number of such M is

$$\prod_{k=1}^{n} (p^{d_k} - p^{k-1}),$$

since we require linearly independent columns.

So the first step to calculating $|\mathrm{Aut}(H_p)|$ is done. The second half of the computation is to count the number of extensions of M to $\mathrm{Aut}(H_p)$. To extend each entry m_{ij} from $m_{ij} \in \frac{\mathbb{Z}}{p\mathbb{Z}}$ to $a_{ij} \in \frac{p^{e_i - e_j}\mathbb{Z}}{p^{e_i}\mathbb{Z}}$ (if $e_i > e_j$), or $a_{ij} \in \frac{\mathbb{Z}}{p^{e_i}\mathbb{Z}}$ (if $e_i \leq e_j$), such that

$$a_{ij} \equiv m_{ij} \pmod{p},$$

we have p^{e_j} ways to do so for the necessary zeros (that is, when $e_i > e_j$), as any element of $\frac{p^{e_i - e_j}\mathbb{Z}}{p^{e_i}\mathbb{Z}}$ works. Similarly, there are $p^{e_i - 1}$ ways for the not necessarily zero entries (that is, when $e_i \leq e_j$), as any element of $\frac{p\mathbb{Z}}{p^{e_i}\mathbb{Z}}$ will do. □

We apply Hillar and Rhea's method to $M = I_{n \times n}$. We consider all extensions of $I_{n \times n}$ to $\mathrm{Aut}(Z)$. Using Lemma 2.1, we identify which of these elements of $\mathrm{Aut}(Z)$ can be extended to $\mathrm{Aut}^{\frac{G}{Z}}(G)$.

To this end, we prove the following.

Proposition 2.7. *Let G be a finite non-abelian p^2-abelian p-central p-group. Suppose $Z = Z(G) \cong \frac{\mathbb{Z}}{p^{e_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{e_2}\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{p^{e_n}\mathbb{Z}}$ where $2 \leq e_1 \leq e_2 \leq \ldots \leq e_n$ and $n \in \mathbb{N}$. Let $\theta \in Aut(Z)$ be such that:*

(a) θ is represented as a matrix $A \in R_p$;
(b) $A(mod\ p) \equiv I_{n\times n}$;
(c) $a_{ij} \equiv 0\ mod\ p^{e_i-e_j+2}$ for $i \neq j$ with $e_i \geq e_j$, and $a_{ii} \equiv 1\ mod\ p^2$.
Then θ can be extended to $\widetilde{\theta} \in Aut^{\frac{G}{Z}}(G)$.

Proof. By Lemma 2.1, we know that $\theta \in \mathrm{Aut}(Z)$ can be extended to $\mathrm{Aut}(G)$ if there exist ϕ and χ such that condition (2) of the lemma holds. Our strategy is to take $\phi = 1$ and to construct a suitable χ.

Recall equation (2.1):

$$\mu(x,y)\theta(\mu(x,y)^{-1}) = \chi(x)^{-1}\chi(y)^{-1}\chi(xy).$$

We aim to construct χ such that equation (2.1) is satisfied.

We express Z as

$$\langle z_1\rangle \times \langle z_2\rangle \times \ldots \times \langle z_n\rangle \cong \frac{\mathbb{Z}}{p^{e_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{e_2}\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{p^{e_n}\mathbb{Z}}$$

where $\{z_1, \ldots, z_n\}$ generates Z.

Before we prove that a general $\theta \in \mathrm{Aut}(Z)$ which satisfies (a) to (c) can be extended to $\widetilde{\theta}$ in $\mathrm{Aut}(G)$, we illustrate our method by considering the following automorphism θ_0 (in its matrix representation):

$$\varphi(\theta_0) = A_0 = \begin{pmatrix} 1+p^2 & & & 0 \\ & 1+p^2 & & \\ & & \ddots & \\ 0 & & & 1+p^2 \end{pmatrix}.$$

The automorphism θ_0 clearly satisfies our conditions (a) to (c).

Writing $\mu(x,y) \in Z$ as $z_1^{\alpha_1}z_2^{\alpha_2}\ldots z_n^{\alpha_n}$ for $\alpha_i \in \frac{\mathbb{Z}}{p^{e_i}\mathbb{Z}}$, we have that $\theta_0(\mu(x,y))$ is given by

$$A_0 \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 1+p^2 & & & 0 \\ & 1+p^2 & & \\ & & \ddots & \\ 0 & & & 1+p^2 \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

$$= \begin{pmatrix} (1+p^2)\alpha_1 \\ (1+p^2)\alpha_2 \\ \vdots \\ (1+p^2)\alpha_n \end{pmatrix},$$

which translates to

$$z_1^{(1+p^2)\alpha_1}\ldots z_n^{(1+p^2)\alpha_n}.$$

The left-hand side of (2.1) is then

$$(z_1^{-\alpha_1}z_2^{-\alpha_2}\ldots z_n^{-\alpha_n})^{p^2} = (\mu(x,y)^{-1})^{p^2}.$$

As $\mu(x,y) = t(xy)^{-1}t(x)t(y)$, we see that by the p^2-abelian and the p-central properties,

$$\mu(x,y)^{p^2} = t(x)^{p^2}t(y)^{p^2}t(xy)^{-p^2}. \tag{2.2}$$

So setting $\chi_0(x) = t(x)^{p^2}$ (and $\theta_0(z) = z^{1+p^2}$) works as (2.1) is fulfilled. Note that χ_0 is defined on Q as required. Thus θ_0 can be extended to $\widetilde{\theta_0} \in \mathrm{Aut}^{\frac{G}{Z}}(G)$.

We now consider a general element θ satisfying conditions (a) to (c). We may express θ as the matrix A below:

$$A = \begin{pmatrix} 1+s_1p^{r_1} & a_{12} & \dots & a_{1n} \\ a_{21} & 1+s_2p^{r_2} & & \vdots \\ \vdots & & \ddots & a_{n-1,n} \\ a_{n1} & \dots & a_{n,n-1} & 1+s_np^{r_n} \end{pmatrix},$$

where $r_i \geq 2$ and $s_i \in \frac{\mathbb{Z}}{p^{e_i-r_i}\mathbb{Z}}$, and for $i \neq j$,

$$a_{ij} \equiv \begin{cases} 0 & \mod p & \text{if } e_i < e_j \\ 0 & \mod p^{e_i-e_j+2} & \text{if } e_i \geq e_j \end{cases}.$$

Recall that $\mu(x,y) = z_1^{\alpha_1}z_2^{\alpha_2}\dots z_n^{\alpha_n}$, and the left-hand side of (2.1) is $\mu(x,y)\theta(\mu(x,y)^{-1})$.

The left-hand side of (2.1) is now

$$(z_1^{-\alpha_1 s_1 p^{r_1}} \dots z_n^{-\alpha_n s_n p^{r_n}}) \times \left[z_1^{-(a_{12}\alpha_2+\dots+a_{1n}\alpha_n)}\right] \dots \left[z_n^{-(a_{n1}\alpha_1+\dots+a_{n,n-1}\alpha_{n-1})}\right].$$

Now we set up the preliminaries for constructing χ. We note that $t(x)^p \in Z$, as G is p-central. So we may write

$$t(x)^p = z_1^{\beta_1} \dots z_n^{\beta_n}$$

for some $\beta_i \in \frac{\mathbb{Z}}{p^{e_i}\mathbb{Z}}$. Similarly we have

$$t(y)^p = z_1^{\gamma_1} \dots z_n^{\gamma_n}$$

for some $\gamma_i \in \frac{\mathbb{Z}}{p^{e_i}\mathbb{Z}}$, and

$$t(xy)^{-p} = z_1^{\delta_1} \dots z_n^{\delta_n}$$

for some $\delta_i \in \frac{\mathbb{Z}}{p^{e_i}\mathbb{Z}}$.

Again we consider equation (2.2). In terms of $z_1, \dots, z_n$, we have

$$\begin{aligned} z_1^{\alpha_1 p^2} \dots z_n^{\alpha_n p^2} &= (z_1^{\beta_1 p} \dots z_n^{\beta_n p})(z_1^{\gamma_1 p} \dots z_n^{\gamma_n p})(z_1^{\delta_1 p} \dots z_n^{\delta_n p}) \\ &= z_1^{(\beta_1+\gamma_1+\delta_1)p} \dots z_n^{(\beta_n+\gamma_n+\delta_n)p}. \end{aligned}$$

We note that for each $i = 1, \dots, n$,

$$\alpha_i p^2 = (\beta_i + \gamma_i + \delta_i)p + k_i p^{e_i} \tag{2.3}$$

for some $k_i \in \mathbb{Z}$.

We construct χ, which is dependent on $\beta_i, \gamma_i, \delta_i$, as the composition of the two maps below:

$$x \longmapsto t(x)^p = z_1^{\beta_1} \dots z_n^{\beta_n},$$

and

$$z_1^{\beta_1} \dots z_n^{\beta_n} \longmapsto$$

$$(z_1^{\beta_1 s_1 p^{r_1-1}} \dots z_n^{\beta_n s_n p^{r_n-1}}) \times \left[z_1^{(\frac{a_{12}}{p}\beta_2+\dots+\frac{a_{1n}}{p}\beta_n)}\right] \dots \left[z_n^{(\frac{a_{n1}}{p}\beta_1+\dots+\frac{a_{n,n-1}}{p}\beta_{n-1})}\right].$$

Note again that χ is defined on Q.

Using (2.3), we check that the right-hand side of (2.1) matches the previously computed left-hand side.

The right-hand side of (2.1) is

$$\chi(x)^{-1}\chi(y)^{-1}\chi(xy)$$

$$= (z_1^{-\beta_1 s_1 p^{r_1-1}} \dots z_n^{-\beta_n s_n p^{r_n-1}}) \times [z_1^{-(\frac{a_{12}}{p}\beta_2+\dots+\frac{a_{1n}}{p}\beta_n)}] \dots [z_n^{-(\frac{a_{n1}}{p}\beta_1+\dots+\frac{a_{n,n-1}}{p}\beta_{n-1})}] \times$$

$$(z_1^{-\gamma_1 s_1 p^{r_1-1}} \dots z_n^{-\gamma_n s_n p^{r_n-1}}) \times [z_1^{-(\frac{a_{12}}{p}\gamma_2+\dots+\frac{a_{1n}}{p}\gamma_n)}] \dots [z_n^{-(\frac{a_{n1}}{p}\gamma_1+\dots+\frac{a_{n,n-1}}{p}\gamma_{n-1})}] \times$$

$$(z_1^{-\delta_1 s_1 p^{r_1-1}} \dots z_n^{-\delta_n s_n p^{r_n-1}}) \times [z_1^{-(\frac{a_{12}}{p}\delta_2+\dots+\frac{a_{1n}}{p}\delta_n)}] \dots [z_n^{-(\frac{a_{n1}}{p}\delta_1+\dots+\frac{a_{n,n-1}}{p}\delta_{n-1})}]$$

$$= (z_1^{-(\beta_1+\gamma_1+\delta_1)s_1 p^{r_1-1}} \dots z_n^{-(\beta_n+\gamma_n+\delta_n)s_n p^{r_n-1}}) \times$$

$$[z_1^{-(\frac{a_{12}}{p}(\beta_2+\gamma_2+\delta_2)+\dots+\frac{a_{1n}}{p}(\beta_n+\gamma_n+\delta_n)}] \dots [z_n^{-(\frac{a_{n1}}{p}(\beta_1+\gamma_1+\delta_1)+\dots+\frac{a_{n,n-1}}{p}(\beta_{n-1}+\gamma_{n-1}+\delta_{n-1})}].$$

Substituting (2.3) $\beta_i + \gamma_i + \delta_i = \alpha_i p - k_i p^{e_i-1}$ into the above gives the following.

$$(z_1^{-(\alpha_1 p - k_1 p^{e_1-1})s_1 p^{r_1-1}} \dots z_n^{-(\alpha_n p - k_n p^{e_n-1})s_n p^{r_n-1}}) \times$$

$$[z_1^{-\frac{a_{12}}{p}(\alpha_2 p - k_2 p^{e_2-1})+\dots+\frac{a_{1n}}{p}(\alpha_n p - k_n p^{e_n-1})}] \dots [z_n^{-\frac{a_{n1}}{p}(\alpha_1 p - k_1 p^{e_1-1})+\dots+\frac{a_{n,n-1}}{p}(\alpha_{n-1} p - k_{n-1} p^{e_{n-1}-1})}].$$

We simplify the above using the following facts:

(i) $o(z_i) = p^{e_i}$ and $r_i \geq 2$;

(ii) $a_{ij} p^{e_j-2} \equiv 0 \bmod p^{e_i}$ for $i \neq j$.

So the right-hand side of (2.1) is now

$$(z_1^{-\alpha_1 s_1 p^{r_1}} \dots z_n^{-\alpha_n s_n p^{r_n}}) \times \left[z_1^{-(a_{12}\alpha_2+\dots+a_{1n}\alpha_n)}\right] \dots \left[z_n^{-(a_{n1}\alpha_1+\dots+a_{n,n-1}\alpha_{n-1})}\right]$$

and this matches the left-hand side of (2.1), as required. □

Now, we calculate all such matrices in R_p satisfying conditions (a) to (c) in Proposition 2.7, as these extend to distinct elements in $\mathrm{Aut}^{\frac{G}{Z}}(G)$.

We recall the general form of a matrix in R_p. Note the l vertical and l horizontal blocks in the matrix, corresponding to the set $\{e_i' : 1 \leq i \leq l\}$.

$$\begin{bmatrix}
m_{11} & & & & & & & & & * \\
\vdots & & & & & & & & & \\
m_{D_1 1} & \cdots & m_{D_1 D_1} & & & & & & & \\
 & & & m_{C_2 C_2} & & & & & & \\
 & & & \vdots & & & & & & \\
 & & & m_{D_2 C_2} & \cdots & m_{D_2 D_2} & & & & \\
 & & & & & & \ddots & & & \\
 & & & & & & & m_{C_l C_l} & & \\
 & & & & & & & \vdots & & \\
0 & & & & & & & m_{D_l C_l} & \cdots & m_{D_l D_l}
\end{bmatrix}$$

For the diagonal entries we have $|\frac{p^2\mathbb{Z}}{p^{e_1}\mathbb{Z}}| \times \ldots \times |\frac{p^2\mathbb{Z}}{p^{e_n}\mathbb{Z}}| = \frac{|Z|}{p^{2n}}$ choices.

When $e_i < e_j$, we have $p^{e_i - 1}$ choices as any element of $\frac{p\mathbb{Z}}{p^{e_i}\mathbb{Z}}$ works. When $e_i = e_j$ and $i \neq j$, we have $p^{e_i - 2}$ choices as any element of $\frac{p^2\mathbb{Z}}{p^{e_i}\mathbb{Z}}$ works. For each row i, we have $n - C_i$ off-diagonal entries which correspond to $e_i \leq e_j$. Of these $C_{i+1} - C_i - 1$ correspond to $e_i = e_j$ and $n - C_{i+1} + 1$ correspond to $e_i < e_j$. So the number of choices (grouped according to the l blocks) for these entries is

$$\prod_{i=1}^{l} (p^{e_i' - 1})^{(n - C_{i+1} + 1)(C_{i+1} - C_i)} \prod_{i=1}^{l} (p^{e_i' - 2})^{(C_{i+1} - C_i - 1)(C_{i+1} - C_i)}.$$

When $e_i > e_j$, there are $p^{e_j - 2}$ choices as any element of $\frac{p^{e_i - e_j + 2}\mathbb{Z}}{p^{e_i}\mathbb{Z}}$ works. For each column j, there are $n - D_j$ entries corresponding to $e_i > e_j$. So the number of choices for these entries is

$$\prod_{j=1}^{l} (p^{e_j' - 2})^{(n - D_j)(C_{j+1} - C_j)} = \prod_{j=1}^{l} (p^{e_j' - 2})^{(n - C_{j+1} + 1)(C_{j+1} - C_j)}.$$

This enables us to prove the following lemma.

Lemma 2.8. Using the notation from before, for $e_1 \geq 2$,

$$|\mathrm{Aut}^{\frac{G}{Z}}(G)|_p \geq \frac{|Z|}{p^{2n}} \prod_{i=1}^{l} (p^{e_i' - 1})^{(n - C_{i+1} + 1)(C_{i+1} - C_i)} \prod_{i=1}^{l} (p^{e_i' - 2})^{(n - C_i)(C_{i+1} - C_i)}.$$

Furthermore, the non-trivial automorphisms calculated above are all non-inner *automorphisms.*

Proof. The number of extensions $\widetilde{\theta} \in \mathrm{Aut}^{\frac{G}{Z}}(G)$ from Proposition 2.7 is

$$\frac{|Z|}{p^{2n}} \prod_{i=1}^{l} (p^{e_i'-1})^{(n-C_{i+1}+1)(C_{i+1}-C_i)} \prod_{i=1}^{l} (p^{e_i'-2})^{(C_{i+1}-C_i-1)(C_{i+1}-C_i)} \prod_{i=1}^{l} (p^{e_i'-2})^{(n-C_{i+1}+1)(C_{i+1}-C_i)},$$

which simplifies to

$$\frac{|Z|}{p^{2n}} \prod_{i=1}^{l} (p^{e_i'-1})^{(n-C_{i+1}+1)(C_{i+1}-C_i)} \prod_{i=1}^{l} (p^{e_i'-2})^{(n-C_i)(C_{i+1}-C_i)}.$$

Therefore

$$|\mathrm{Aut}^{\frac{G}{Z}}(G)| \geq \frac{|Z|}{p^{2n}} \prod_{i=1}^{l} (p^{e_i'-1})^{(n-C_{i+1}+1)(C_{i+1}-C_i)} \prod_{i=1}^{l} (p^{e_i'-2})^{(n-C_i)(C_{i+1}-C_i)}.$$

It is clear that all the automorphisms $\widetilde{\theta}$ as in Proposition 2.7 are non-inner, since $\widetilde{\theta}$ acts non-trivially on Z.

It remains to show that these non-inner automorphisms have order a power of p. Denote by P this finite set of non-inner automorphisms; more precisely,

$$P = \{\widetilde{\theta} \in \mathrm{Aut}^{\frac{G}{Z}}(G) \mid \theta := \widetilde{\theta}|_Z \text{ satisfies (a) to (c) of Proposition 2.7}\}.$$

It is sufficient to show that P is a subgroup, as then it follows that every element of P has p^{th} power order since P is a p-group.

To prove that we have a subgroup, we need to show that P is multiplicatively closed. That is, for $\widetilde{\theta}_1, \widetilde{\theta}_2 \in P$, the composite $\widetilde{\theta}_1 \cdot \widetilde{\theta}_2 \in P$.

It is enough to consider the restriction to $\mathrm{Aut}(Z)$ since P is characterized by conditions (a) to (c) on $\mathrm{Aut}(Z)$. We have $\theta_1, \theta_2 \in \mathrm{Aut}(Z)$ such that $\widetilde{\theta}_1|_Z = \theta_1$ and $\widetilde{\theta}_2|_Z = \theta_2$. Working with the matrix representations, we note that θ_1, θ_2 satisfy conditions (a) to (c) of Proposition 2.7. Let $\varphi(\theta_1) = (a_{ij})$ and $\varphi(\theta_2) = (b_{ij})$. Then $\varphi(\theta_1 \cdot \theta_2) = \varphi(\theta_1)\varphi(\theta_2) = (c_{ij})$ where $c_{ij} = \sum_k a_{ik}b_{kj}$. It is immediate that $\varphi(\theta_1) \cdot \varphi(\theta_2) \in R_p$ since R_p is a ring. So (a) is satisfied for $\theta_1 \cdot \theta_2$. Using the expression for c_{ij}, it is clear that (b) is satisfied for $\theta_1 \cdot \theta_2$.

For (c), we consider c_{ij} for three cases: (1) $i < j$, (2) $i = j$ and (3) $i > j$.
Case (1). We have $i < j$ and so $e_i \leq e_j$. We write

$$c_{ij} = \sum_{k \leq i} a_{ik}b_{kj} + \sum_{i<k<j} a_{ik}b_{kj} + \sum_{k \geq j} a_{ik}b_{kj}.$$

If $e_i < e_j$, we need to show that $c_{ij} \equiv 0 \bmod p$. As $p|a_{ij}$ and $p|b_{ij}$ for $i \neq j$, it is straightforward that $c_{ij} \equiv 0 \bmod p$.

If $e_i = e_j$, we need to show that $c_{ij} \equiv 0 \bmod p^2$. Again as $p|a_{ij}$ and $p|b_{ij}$ for $i \neq j$, we have that

$$c_{ij} \equiv a_{ii}b_{ij} + a_{ij}b_{jj} \bmod p^2.$$

We further have that $p^2|a_{ij}$ and $p^2|b_{ij}$ since $e_i = e_j$. So $c_{ij} \equiv 0 \bmod p^2$, as required.

Case (2). We have $i = j$, and so

$$c_{ii} = \sum_{k<i} a_{ik}b_{ki} + a_{ii}b_{ii} + \sum_{k>i} a_{ik}b_{ki}.$$

We need to show that $c_{ii} \equiv 1 \bmod p^2$. As before, $c_{ii} \equiv a_{ii}b_{ii} \bmod p^2$. Since $a_{ii} \equiv 1 \bmod p^2$ and $b_{ii} \equiv 1 \bmod p^2$, we have that $c_{ii} \equiv 1 \bmod p^2$, as required.

Case (3). Here $i > j$ and hence $e_i \geq e_j$.We write

$$c_{ij} = \sum_{k<j} a_{ik}b_{kj} + a_{ij}b_{jj} + \sum_{j<k<i} a_{ik}b_{kj} + a_{ii}b_{ij} + \sum_{k>i} a_{ik}b_{kj}.$$

For $k < j$, we have $p^{e_i-e_j+2}$ divides $p^{e_i-e_k+2}$, which in turn divides a_{ik}. Similarly for $k > i$, we have $p^{e_i-e_j+2}$ divides $p^{e_k-e_j+2}$, which divides b_{kj}. For $k = j$, we have $p^{e_i-e_j+2}$ divides a_{ij}. Similarly for $k = i$, we have $p^{e_i-e_j+2}$ divides b_{ij}. For $j < k < i$, we have $p^{e_i-e_k+2}$ divides a_{ik} and $p^{e_k-e_j+2}$ divides b_{kj}. So $p^{e_i-e_j+4}$ divides $a_{ik}b_{kj}$. Therefore $c_{ij} \equiv 0 \bmod p^{e_i-e_j+2}$ as required.

So (c) is satisfied for $\theta_1 \cdot \theta_2$. Thus $\widetilde{\theta}_1 \cdot \widetilde{\theta}_2 \in P$.

Therefore, P is a subgroup as required. □

PROOF OF THEOREM 1.1.

We recall that we need $|\mathrm{Out}(G)|_p \geq |Z|$ to prove the theorem, we now analyse our lower bound for $|\mathrm{Out}(G)|_p$, as given in Lemma 2.8. As $e_1 > 2$, we have

$$\begin{aligned}
|\mathrm{Out}(G)|_p &\geq \frac{|Z|}{p^{2n}} \prod_{i=1}^{l} (p^2)^{(n-C_{i+1}+1)(C_{i+1}-C_i)} \prod_{i=1}^{l} p^{(n-C_i)(C_{i+1}-C_i)} \\
&= \frac{|Z|}{p^{2n}} \prod_{i=1}^{l} p^{(n-C_{i+1}+1)(C_{i+1}-C_i)} \prod_{i=1}^{l} p^{(n-C_{i+1}+1)(C_{i+1}-C_i)} \prod_{i=1}^{l} p^{(n-C_i)(C_{i+1}-C_i)} \\
&= \frac{|Z|}{p^{2n}} \prod_{i=1}^{l} p^{(n-C_{i+1}+1)(C_{i+1}-C_i)} \prod_{i=1}^{l} p^{(C_{i+1}-C_i)[2n+1-(C_{i+1}+C_i)]} \\
&\geq \frac{|Z|}{p^{2n}} \prod_{i=1}^{l} p^{(C_{i+1}-C_i)(2n+1)-(C_{i+1}^2-C_i^2)} \\
&= \frac{|Z|}{p^{2n}} p^{(2n+1)(C_{l+1}-C_1)-(C_{l+1}^2-C_1^2)} \\
&= |Z|p^{n^2-3n}.
\end{aligned}$$

As $n \geq 3$, we have that $|\mathrm{Out}(G)|_p \geq |Z|$ as required. □

Acknowledgments

I am very grateful to Rachel Camina for her time and helpful comments. Also thank you to Chris Brookes and to Gavin Armstrong for a thorough reading of this work.

This research has been made possible through the generous support from the Cambridge Commonwealth Trust, the Cambridge Overseas Research Scholarship, and the Leslie Wilson Scholarship (from Magdalene College, Cambridge).

References

[1] J. Buckley, Automorphism groups of isoclinic p-groups, J. London Math. Soc. (2) 12 (1975), 37-44.

[2] R. M. Davitt, The automorphism group of finite p-abelian p-groups, Illinois J. Math. 16 (1972), 76-85.

[3] R. M. Davitt, On the automorphism group of a finite p-group with a small central quotient, Canad. J. Math. 32 (1980), 1168-1176.

[4] R. M. Davitt & A. D. Otto, On the automorphism group of a finite modular p-group, Proc. Amer. Math. Soc., vol. 35, no. 2 (1972), 399-404.

[5] R. M. Davitt & A. D. Otto, On the automorphism group of a finite p-group with the central quotient metacyclic, Proc. Amer. Math. Soc., vol. 30, no. 3 (1971), 467-472.

[6] T. Exarchakos, On p-groups of small order, Publ. Inst. Math. (Beograd) (N. S.) 45 (59) (1989), 73-76.

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

[8] S. Fouladi, A. R. Jamali & R. Orfi, Automorphism groups of finite p-groups of coclass 2, J. Group Theory 10, no. 4 (2007), 437-440.

[9] W. Gaschütz, Nichtabelsche p-Gruppen besitzen äussere p-Automorphismen (German), J. Algebra 4 (1966), 1-2.

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

[11] C. J. Hillar & D. L. Rhea, Automorphisms of finite abelian groups, Amer. Math. Monthly 114, no. 10 (2007), 917-923.

[12] K. G. Hummel, The order of the automorphism group of a central product, Proc. Amer. Math. Soc., vol. 47, no. 1 (1975), 37-40.

[13] C. R. Leedham-Green & S. McKay, The Structure of Groups of Prime Power Order, London Mathematical Society Monographs New Series 27, Oxford Science Publications (2002).

[14] A. D. Otto, Central automorphisms of a finite p-group, Trans. Amer. Math. Soc. 125 (1966), 280-287.

[15] I. B. S. Passi, M. Singh & M. K. Yadav, Automorphisms of abelian group extensions, J. Algebra 324 (4) (2010), 820-830.

[16] A. Ranum, The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group, Trans. Amer. Math. Soc. 8 (1907) 71-91.

[17] A. Thillaisundaram, PhD Thesis, University of Cambridge, UK (2011).

[18] M. K. Yadav, On automorphisms of finite p-groups, J. Group Theory, Vol. 10, Issue 6 (2007), 859-866.

Anitha Thillaisundaram

Magdalene College, Cambridge, CB3 0AG UK

Email: anitha.t@cantab.net